



ユーザーマニュアル EWS シリーズコントローラ

バージョン 3.90.0004

著作権について

Edgecore Networks Corporation

©著作権 2023 Edgecore Networks Corporation.

ここに記載されている情報は、予告なく変更されることがあります。本書は情報提供のみを目的としており、Edgecore Networks Corporationが提供する機器、機器機能、またはサービスに関する明示または黙示を問わず、いかなる保証も記載していません。Edgecore Networks Corporationは、ここに含まれる技術的または編集上の誤りまたは記載漏れについて責任を負いません。

著作権

本書の内容は、Edgecore, INC.の書面による許可がなく、いかなる部分または全体として複製、保管、情報検索システムへの転写、言語への翻訳、または機械的、磁氣的、電子的、光学的、コピー、マニュアル、その他あらゆる形態や手段で送信することはできません。

免責事項

Edgecore, INC.は、本書に記載されている製品またはソフトウェアのアプリケーションまたは使用から生じる一切の責任を負いません。また、当社の特許権や他の特許権のもとでライセンスを供与することもあります。Edgecoreはさらに、ここに記載されている製品に予告なく変更を加える権利を留保します。この出版物は、予告なく変更されることがあります。

商標

Edgecoreは、Edgecore, INC.の登録商標です。本書に記載されているその他の商標は、識別目的でのみ使用され、それぞれの所有者の所有物である場合があります。

目次

第1章	はじめに	1
1.1	EWS 無線 LAN ゲートウェイコントローラシリーズ	1
1.2	EWS コントローラモデル	3
1.3	Edgecore ソリューションの概要	3
1.4	主な用語と概念	5
1.5	推奨される構成順序	8
1.5.1	共通設定	8
1.5.2	詳細設定とアプリケーション	8
第2章	WMI とセットアップウィザード	10
2.1.	Web 管理インターフェース	10
2.2	ウィザードの実行	12
第3章	基本ネットワーク設定	16
3.1.	ネットワーク計画	16
3.2.	アップリンク (WAN 側) の構成	18
3.2.1	WAN 設定.....	18
3.2.2.	デュアルアップリンク	19
3.2.3.	デュアル WAN1/WAN2 モデル用の WAN ポート選択	21
3.2.4.	WAN トラフィック制御	22
3.2.5.	アップリンク検出とフェイルオーバー	23
3.3.	ダウンリンク (LAN 側) VLAN オプション	26
3.3.1.	ポートベースのサービスゾーン	26
3.3.2.	タグベースのサービスゾーン	27
第4章	ユーザー認証データベース	28
4.1.	認証データベースの構成	28
4.2.	組み込み認証データベース	30
4.2.1.	ローカルユーザーデータベース	30
4.2.2.	オンデマンドユーザーデータベース	33
4.2.3.	ゲスト認証オプション	38
4.2.4.	ワンタイムパスワード	42
4.3.	外部認証オプション	44
4.3.1.	RADIUS	44
4.3.2.	POP3	47
4.3.3.	LDAP	47
4.3.4.	NT ドメイン	48
4.3.5.	SIP	49
4.3.6.	ソーシャルメディア	51
第5章	グループ属性とポリシールール	54
5.1	コンセプトの概要	54
5.2	グループとポリシーの実用的な設定	56
第6章	基本的なサービスゾーン設定	63
5.3	サービスゾーンの概念	63
5.4	サービスゾーンの設定	63
6.2.1.	タグベースまたはポートベースのサービスゾーン	63
6.2.2.	NAT モードまたはルータモード	65
6.2.3.	サービスゾーンネットワークインターフェース	66
6.2.4.	DHCP サーバーオプション	67
6.2.5.	認証オプション	68
6.2.6.	キャプティブポータルのカスタマイズ	71
第7章	基本的な AP 管理	74
7.1.	はじめに	74

7.2 ローカルエリア AP 管理 (EWS101、EWS5203、EWS5204、EWS5207)	76
7.2.1 AP リスト	77
7.2.2 AP の追加と設定の適用	78
7.2.3 テンプレートの設定	81
7.2.4 AP ファームウェア管理	83
7.2.5 WDS リンク	84
7.2.6 不正 AP スキャン	86
7.2.7 AP ロードバランシング機能	87
7.3 ワイドエリア AP 管理	89
7.3.1 アクセスポイントの追加	90
7.3.2 AP 検出による複数のアクセスポイントの検出	90
7.3.3 テンプレートを使用する AP 設定	91
7.3.4 CAPWAP を使用した AP の自動検出と設定	93
7.3.5 トンネリングされた VAP ロケーションマッピングの設定	99
7.3.6 Google マップでのアクセスポイントの監視	101
7.3.7 AP のグループ化	106
7.3.8 不正 AP スキャン	108
7.3.9 AP ロードバランシング機能	109
第 8 章 ネットワーク環境の詳細設定	112
8.1 IPv4/IPv6 デュアルスタックネットワーク	112
8.2 ユーザーアクセス制御	116
8.3 認定	119
8.3.1 システム証明書	119
8.3.2 内部ルート CA	121
8.3.3 内部発行証明書	122
8.3.4 信頼できる証明書発行者	122
8.4 管理アクセス	123
第 9 章 コントローラ管理用ユーティリティ	124
9.1 EWS コントローラ管理	124
9.2 設定のバックアップと復元	126
9.3 ファームウェアのアップグレード	128
9.4 再始動	129
第 10 章 監視用のレポートとログ	130
10.1 システム関連のステータス	130
10.1.1 ダッシュボード	130
10.1.2 システムの概要	131
10.1.3 ネットワークインターフェース	133
10.1.4 ルーティング	134
10.1.5 DHCP サーバー	135
10.2 クライアント関連のステータス	136
10.2.1 オンラインユーザー	136
10.2.2 関連付けられた非ログインユーザー	137
10.2.3 クロスゲートウェイローミングユーザー	138
10.2.4 オンデマンドローミングアウトユーザー	138
10.2.5 MAC ログインデバイス	139
10.2.6 認証されたユーザー	139
10.2.7 スマートログインユーザー	140
10.2.8 セッションリスト	141
10.3 ログとレポート	142
10.3.1 システム関連	142
10.3.2 ユーザーイベント	143

10.4	レポートと通知	144
第11章	ホットスポットアプリケーション.....	147
11.1	オンデマンド請求プラン	147
11.2	オンデマンド請求プランのタイプ.....	148
11.2.1	使用時間（有効期限あり）	148
11.2.2	使用時間（有効期限なし）	150
11.2.3	ホテルカットオフ時間	152
11.2.4	ボリューム	153
11.2.5	経過時間を含む継続時間	155
11.2.6	カットオフ時間付き継続時間.....	157
11.2.7	開始時間と終了時間を含む継続時間	158
11.3	POS プリンタのセットアップ.....	159
11.4	POS チケットのカスタマイズ.....	163
11.5	アカウントの作成	167
11.6	ユーザーセルフサービス	169
第12章	PMS 統合.....	174
12.1	ホテルの部屋ロケーションマッピング	174
12.2	PMS 設定	176
第13章	アカウントローミング.....	179
13.1	ローミング関連	179
13.2	ISP ローミング用の WiSpr	179
13.3	クロスゲートウェイローミング	181
13.4	ローカル/オンデマンドアカウントのローミングアウト	182
第14章	VPN	185
14.1	サイト間	185
14.2	リモートクライアント.....	187
第15章	スイッチ管理.....	189
15.1	スイッチリスト	189
15.2	PoE スケジュールテンプレート.....	190
15.3	バックアップ設定	191
第16章	プラットフォームに依存する機能.....	192
16.1	高可用性（HA）（EWS5203、EWS5204、EWS5207）	192
16.2	WiFi モニター（EWS5203、EWS5204、EWS5207）	195
16.2.1	フロアプランを追加する	196
16.2.2	シミュレーション AP	198
16.2.3	フロアプランの AP 監視.....	200
付録 A	EWS モデルと設置.....	202
付録 B	外部ページ.....	214
付録 C	便利な管理および評価ツール.....	227
付録 D	オンデマンドアカウントタイプ.....	229
付録 E	UI リファレンスインデックス.....	236
	I. Dashboard.....	236
	II. Setup Wizard	237
	A. System.....	238
	1) General.....	238
	2) WAN	241
	3) IPv6	243
	4) LAN ポート	243
	5) MGMT Port	244
	6) High Availability	244

7) Service Zones	246
8) Port Location Mapping	252
9) PMS Interface	255
B.Users	257
1) Groups	257
2) Internal Authentication	259
a) Local Authentication	259
b) On-Demand Authentication	260
c) Guest Authentication	267
d) One Time Password	268
3) External Authentication.....	269
a) Social Media Authentication	270
4) On-Demand Accounts	270
5) Schedule.....	271
6) Policies	272
7) Blacklists	274
8) Privilege Lists	274
9) Additional Control	275
C.Devices	278
1) Local Area AP Management	278
a) 概要	278
b) List	278
c) Adding	279
d) Discovery	280
e) Templates	281
f) Firmware	289
g) Upgrade.....	290
h) WDS Management.....	290
i) Rogue AP Detection.....	291
j) AP Load Balancing.....	293
2) Wide Area AP Management.....	294
a) AP List	294
b) AP Grouping	297
c) Map	305
d) Discovery	306
e) Adding	307
f) Template	308
g) WDS List.....	315
h) Backup Config	315
i) Firmware	315
j) CAPWAP	316
k) Rogue AP Detection	317
l) AP Load Balancing.....	317
m) Third Party AP Management.....	319
3) Switches	320
a) Switch List	320
b) PoE Schedule Template	320
c) Backup Configuration.....	322
E.Network.....	323
1) NAT	323
2) Monitor IP	325
3) Walled Garden and Walled Garden Ad	325

4) VPN	327
5) Proxy Server	328
6) Local DNS Record.....	330
7) Dynamic Routing.....	330
8) DDNS	334
9) Client Mobility.....	335
F.Utilities	337
1) Administrator Account	337
2) Backup & Restore.....	340
3) Certificates.....	342
4) Network Utilities	345
5) Restart	346
6) System Upgrade	346
G.Status.....	347
1) System Summary	347
2) Interface.....	349
3) Monitor Users	351
4) WiFi Monitor	352
6) Process Monitor	354
7) Logs & Reports	354
8) Reporting	356
9) Session List.....	363
10) DHCP Lease.....	364
11) Routing Table.....	365
AP キャパビリティ	367

付録F

第1章 はじめに

1.1 EWS 無線 LAN ゲートウェイコントローラシリーズ

Edgecore EWS 無線 LAN ゲートウェイコントローラは、ネットワークサービスのプロビジョニング、認証、セキュリティ、および管理用に設計された機能豊富なネットワークエッジデバイスです。配置の規模に応じて、Edgecore EWS 無線 LAN ゲートウェイコントローラモデルを選択し、さまざまな容量におけるネットワークの需要を満たすことができます。

Edgecore EWS コントローラは、認証、認可、アカウントिंगを表すトリプル A (AAA) など、あらゆるネットワーク環境の基本的なニーズに対応するように設計されています。

Edgecore EWS コントローラを使用すると、ユーザーの役割に基づいてさまざまなユーザーが認証され、そこからユーザーのアクセス可能なネットワークセグメント、ユーザーのネットワークポートフォリオ（アクセス可能な時間、QoS、ルーティングルール、ファイアウォールルール、使用条件、権限を含む）が定義され、総称して「認可」と呼ばれます。最後に、クライアントがネットワークを使用している間に Edgecore EWS コントローラによって定期的にアカウントिंगが実行されます。配置に応じて、このクライアントのアカウントिंग情報が内部ユーザーデータベースまたは外部ユーザーデータベースに更新されます。

複数の AP を配置する規模になる場合、ワイヤレスネットワークのプロビジョニングは簡単な作業ではありません。Edgecore EWS コントローラは、ローカルエリアネットワーク (LAN) の下でローカルに配置された 4ipent の AP デバイスだけでなく、Edgecore EWS コントローラの位置を基準に、ワイドエリアネットワーク (WAN) にリモートに配置された Edgecore AP デバイスもカバーする包括的な AP 管理機能を備えています。さらに、サードパーティの AP 管理インターフェースにより、Edgecore EWS コントローラは、関連するオンラインユーザー監視、GUI インターフェースへのショートカット、非 Edgecore AP の位置計画など、一般的な AP 管理機能を実行できます。

ネットワークの安全性とトラフィック制御もまた、ネットワーク所有者、ホテル経営者にとって懸念される大きな分野であり、ネットワーク環境全体の品質と安定性を決定する主要な要因です。Edgecore EWS コントローラは、最適なパス選択のための静的および動的ルーティング

機能、個々のユーザーに帯域幅制御を適用するための QoS マッピング、システムのアップリンク帯域幅制御、カスタマイズされたファイアウォールプロトコルとルールにより、これらのニーズに対応します。

一般的なネットワーク機能は、Edgecore EWS コントローラに十分に詰め込まれています。3 種類の NAT 機能、無料のウェブサイト閲覧できるウォールド・ガーデン、ネットワークデバイス監視ツール、静的 DNS 変換、プロキシサーバー、VPN を提供します。Edgecore EWS コントローラは、複数のネットワーク機能を 1 つのデバイスに組み込んで、外部 NAT サーバー、プロキシサーバー、VPN ゲートウェイなどをセットアップする必要がなくなり、配置の複雑さを軽減します。

ネットワークメンテナンスとネットワーク監視タスクは、システムトラフィック、CPU 使用率やメモリ消費量などのシステムリソース使用率、オンラインユーザー記録、DHCP リース記録などの組み込みディスプレイで簡単に行うことができます。イベントログを外部サーバーに送信して、長期的な記録保持や詳細な分析を行うことができます。

1.2 EWS コントローラモデル

Edgecore EWS コントローラの製品ラインには、さまざまな規模のネットワーク配置を対象とする以下のモデルが用意されています。

SMB およびエンタープライズ無線 LAN ゲートウェイコントローラ
EWS100、EWS5203、VEWS5203、VEWS5204

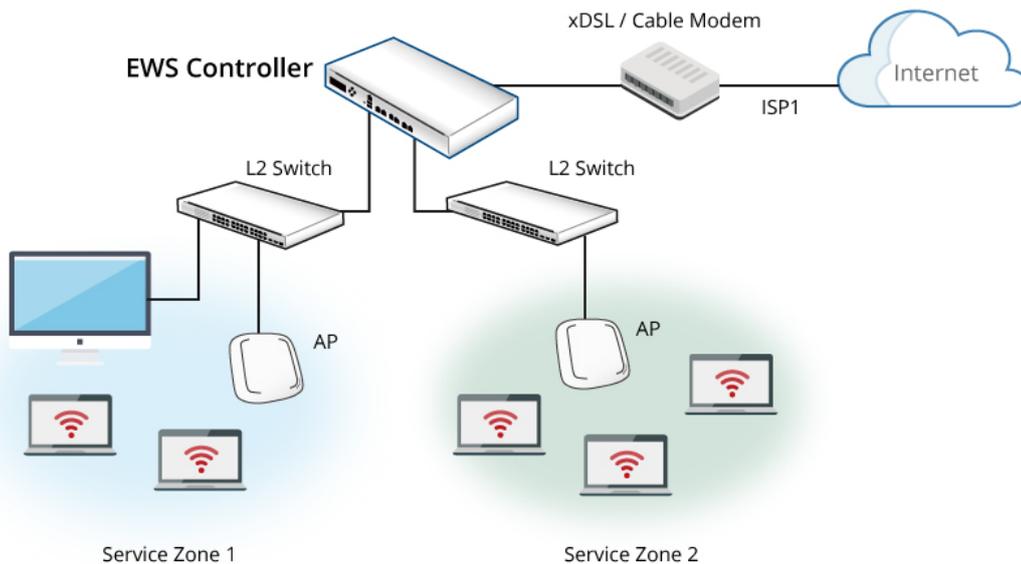
大規模エンタープライズおよびキャリアグレードコントローラ
EWS5204、EWS5207、VEWS5207、VEWS1000

注：Edgecore は引き続き新しいプラットフォームを導入する場合があります、古いプラットフォームを廃止する場合があります。最新の製品ラインについては、当社のウェブサイト <http://www.Edgecore.com> を参照してください。各モデルのハードウェアおよび設置方法の詳細なリストについては、**付録 A** を参照してください。

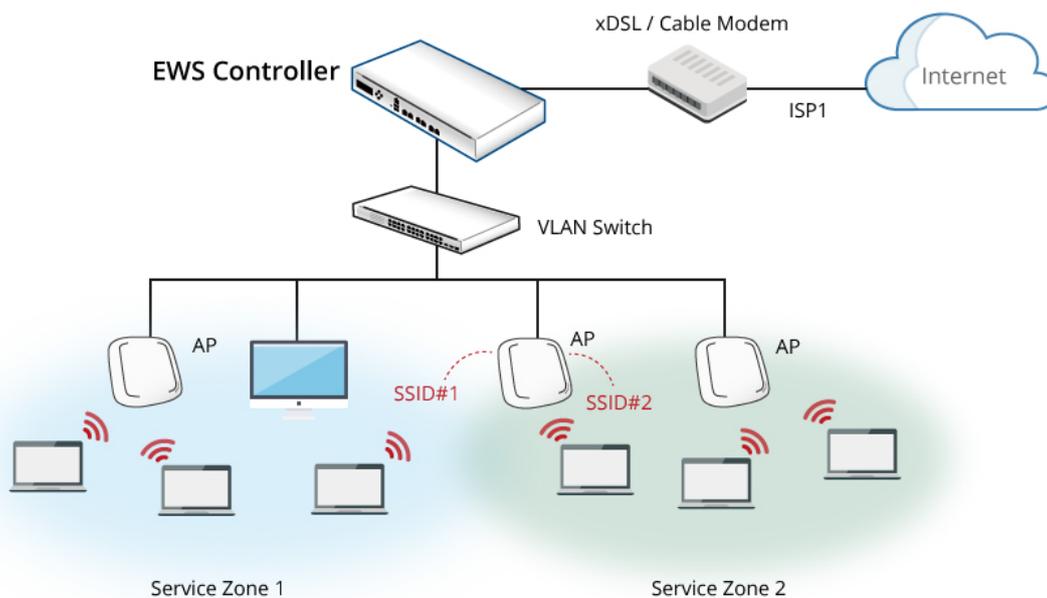
1.3 Edgecore ソリューションの概要

Edgecore EWS コントローラは、現在のほとんどすべてのネットワークアーキテクチャ、レイヤ2（データリンク層）およびレイヤ3（ネットワーク層）のネットワーク管理用に設計されています。

レイヤ2 ネットワークは、Edgecore EWS コントローラの LAN ポートで物理的に広がる相対的な単純なネットワーク配置トポロジです。次の2つの配置シナリオを示します。

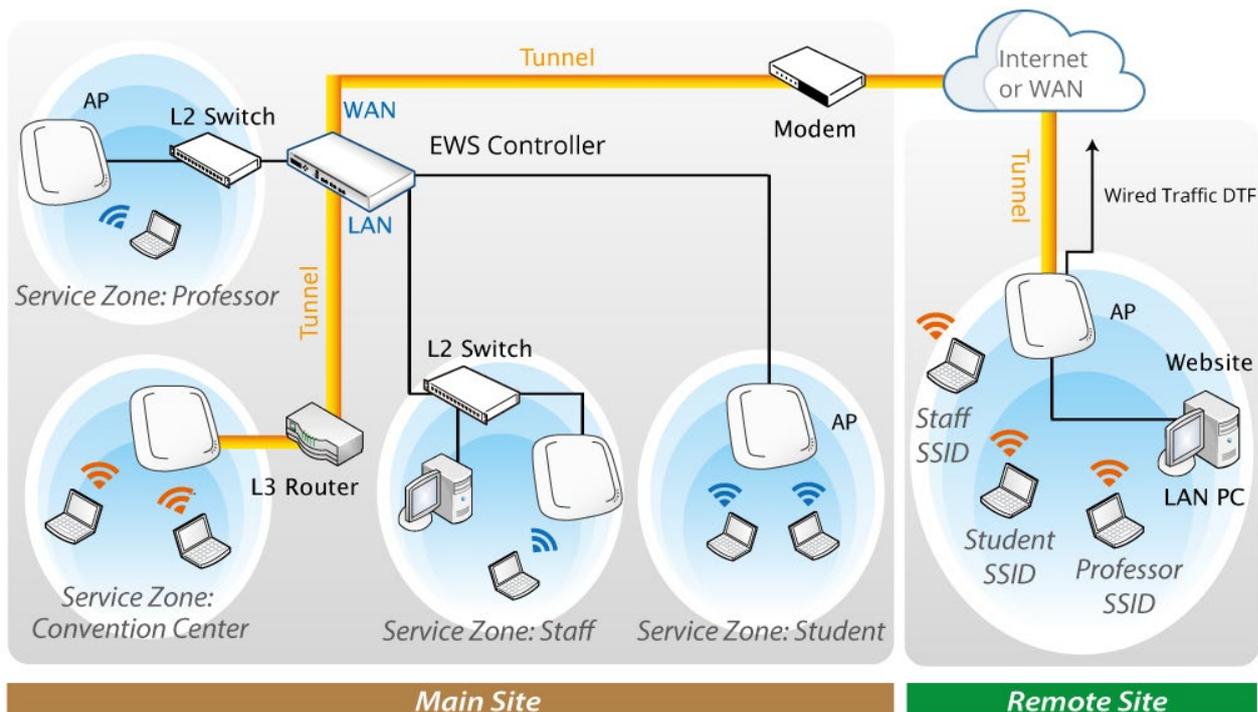


【ポートベースモードのレイヤ2 ネットワーク】



【タグベースモードのレイヤ2 ネットワーク】

レイヤ 3 ネットワークは、Edgecore EWS コントローラの LAN ポートで物理的に広がるだけでなく、トンネル経由でルーティング可能な IP アドレスを持つリモートサイトを管理するために、異なる IP ネットワーク経由で到達することもできます。



【トンネルを持つレイヤ3ネットワーク】

1.4 主な用語と概念

ゲートウェイは、小さなネットワークがより大きなネットワークに接続するエッジデバイスまたはネットワークノードです。Edgecore EWS コントローラは、本質的にネットワーク環境のゲートウェイです。通常、大きなネットワークとはWAN側またはアップストリームネットワーク（物理的にWANポート経由で接続されている）を指しており、小さなネットワークとはLAN側を指しています。

ローカルユーザーは、アカウント資格情報が Edgecore EWS コントローラの「ローカル」という組み込みデータベースに格納されているユーザーのタイプです。Edgecore EWS コントローラの「ローカル」データベース容量は、モデルによって異なります。一度作成されたローカルユーザーアカウントには有効期限がありません。管理者がローカルアカウントを削除する場合は、Web管理インターフェースから手動で削除する必要があります。また、Edgecore EWS コントローラのLocalデータベースは、アカウントローミング用の別の Edgecore EWS コントローラの外部RADIUSデータベースとして構成できます。

オンデマンドユーザーは、アカウント資格情報が Edgecore EWS コントローラの「オンデマンド」という組み込みデータベースに格納されているユーザーのタイプです。Edgecore EWS

コントローラの「オンデマンド」データベース容量は、モデルによって異なります。オンデマンドユーザーは、短期的な使用目的のために設計され、時間または容量の制約と有効期限があります。オンデマンドアカウントの記録は、15日以上経過していた場合、または管理者/マネージャによって手動で削除された場合、新しいオンデマンドアカウントを作成するためにリサイクルされます。また、Edgecore EWS コントローラのオンデマンドデータベースは、アカウントローミング用の別の Edgecore EWS コントローラの外部 RADIUS データベースとして構成できます。

外部認証データベースは、Edgecore EWS コントローラに組み込まれていないユーザーアカウントデータベースです。Edgecore EWS コントローラは、ローカルデータベースとオンデマンドデータベースの他に、RADIUS、POP3、LDAP（Active Directory を含む）、NTDomain（Win2K の NTDS）の 4 種類の外部認証データベースをサポートしています。外部認証データベースは、アカウントローミングの実装と集中管理の両方に役立ちます。

サービスゾーンは、Edgecore EWS コントローラの LAN の論理パーティションです。サービスゾーンは、独自のゲートウェイプロパティ（LAN IP アドレス、DHCP サーバー設定、認証オプションなど）やカスタマイズ可能なログインポータルページを持つ仮想ゲートウェイです。最大 9 つの独立したサービスゾーンプロファイルを備えた Edgecore EWS コントローラは、単一のデバイスで複数のホットスポットフランチャイズに対応できます。

LAN ポートマッピングは、サービスゾーンと Edgecore EWS コントローラ上の物理 LAN ポートなどの論理ネットワークパーティションの対応関係です。マッピングには、「ポートベース」と「タグベース」の 2 つのモードがあります。ポートベースモードでは、サービスゾーンを物理 LAN ポートの下流のクライアントに静的にマッピングします。このモードでは、物理 LAN ポートの数に応じた最大数のサービスゾーンのみサービスを提供します。タグベースモードでは、トラフィックパケットにタグ付けされた VLAN ID に基づいて、クライアントをサービスゾーンに動的にマッピングします。

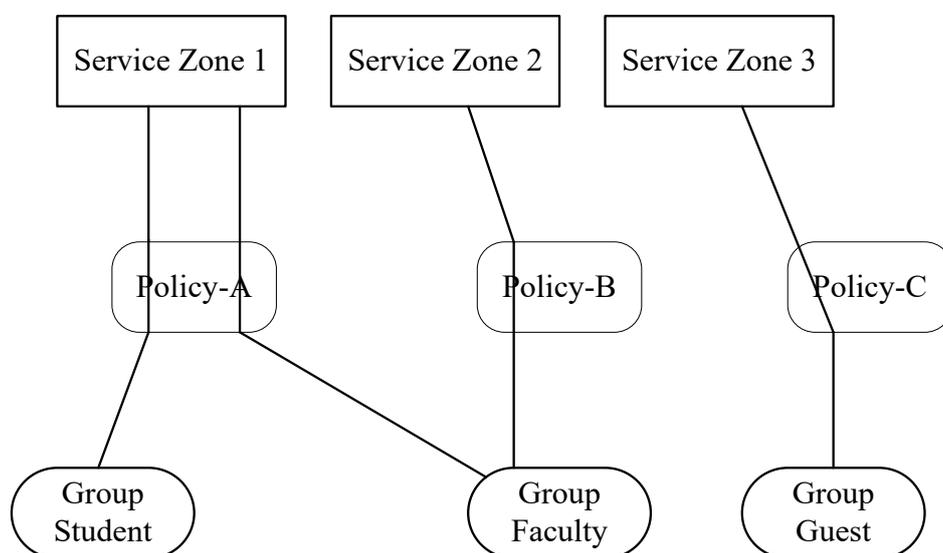
グループは、異なるサービスゾーンへのユーザーのアクセス性を定義するユーザーの役割プロファイルであり、アクセスが許可されたときの QoS プロパティとネットワークポリシーを定義します。接続している各ユーザーは、認証に使用されるユーザーアカウントのタイプによって決定されるグループに属します。管理者が新しいアカウントを特定のグループに割り当てない

場合、または認証が不要なユーザーに割り当てない場合、デフォルトでは「無し」という名前のキャッチオールグループに属します。

ポリシーは、ユーザーのグループプロファイルが決定された後のユーザー制御の第2階層です。ポリシーは、特定のグループのユーザーに適用されるファイアウォールルール、権限、ログインスケジュール、ルーティングルール、およびセッション制限を定義します。ユーザーは1つのグループにのみ属することができますが、異なるサービスゾーンにアクセスしている間、異なるポリシーによって管理することができます。

「無し」グループに属するユーザー、またはネットワークポリシーを明示的に割り当てられていないユーザーについては、「グローバルポリシー」というデフォルトのキャッチオールポリシーによって管理されます。グローバルポリシーは基本ポリシーであり、別のポリシーが適用されない場合はすべてのユーザーに適用されます。

次の図は、サービスゾーン、グループ、およびポリシーの関係を示す例です。この例では、サービスゾーン1にログインした学生および学部は、ポリシーAによって管理されます。お客様は、サービスゾーン3のみにアクセスでき、ポリシーCによって制限されます。学部は、2つの異なるポリシーの下でサービスゾーン1とサービスゾーン2の両方にアクセスできます。



【サービスゾーン、グループ、ポリシーの関係】

1.5 推奨される構成順序

- システムのタイムゾーン、NTP サーバー、DNS サーバー、WAN1 アドレスを設定する
- 少なくとも 1 つのサービスゾーンの LAN アドレス範囲を構成し、その認証を有効にする。
- 有効なサービスゾーンで、有線回線を介してログインページをテストするためのユーザーアカウントを作成する。
- オンデマンドユーザーを生成し、アカウントをテストする。
- サービスゾーンのワイヤレス設定を構成し、AP を追加する。
- アプリケーションに応じて必要なサービスゾーンを構成する。
- グループとポリシー（ファイアウォールルールとセッション制限を含む）を設定する。
- ポータルログインページをカスタマイズし、必要に応じてワールド・ガーデンの広告リンクを追加する。
- 必要に応じて、オンデマンドアカウントに対してエンドユーザーのクレジットカードによる自己支払を許可するように支払いゲートウェイを設定する。
- 操作前に Web サーバーの SSL 証明書をロードする。
- 生成されたステータスページとレポートを監視する。
- 他の特定のアプリケーションに対してその他の詳細設定を行う。

1.5.1 共通設定

標準ネットワークで最も一般的に配置されるシナリオについては、第 3 章～7 章を参照してください。

第 3 章～7 章には、一般的なネットワーク環境で最も一般的に使用される機能を含む構成トピックが含まれています。ユーザーは、第 3 章から始め、第 7 章まで進めることが推奨されます。

1.5.2 詳細設定とアプリケーション

第 8 章～10 章では、セキュリティ、システムメンテナンス、および監視について説明します。これらの内容は、必要な機能を正常に構成し、ネットワークが起動して実行された後の操作に役立ちます。

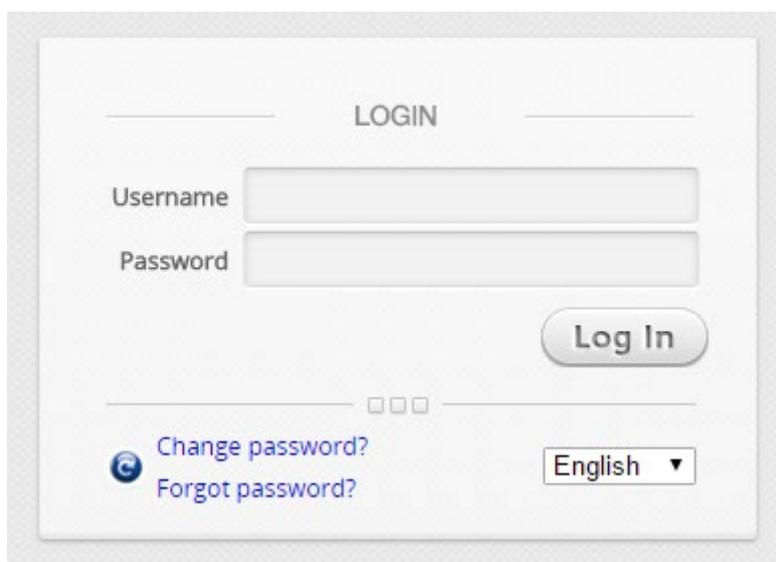
特定のアプリケーション、サードパーティのデバイスとの統合、カスタマイズなどのニ

ーズがあるお客様は、高度な機能の設定については、**第 11 章以降**を参照してください。

第2章 WMI とセットアップウィザード

2.1. Web 管理インターフェース

EWS コントローラの Web 管理インターフェース（WMI）は、デフォルトの IP アドレスである **192.168.1.254** で LAN インターフェースに接続された任意の PC の Web ブラウザ（Firefox、Chrome、Safari 推奨）を介してアクセスすることができます。

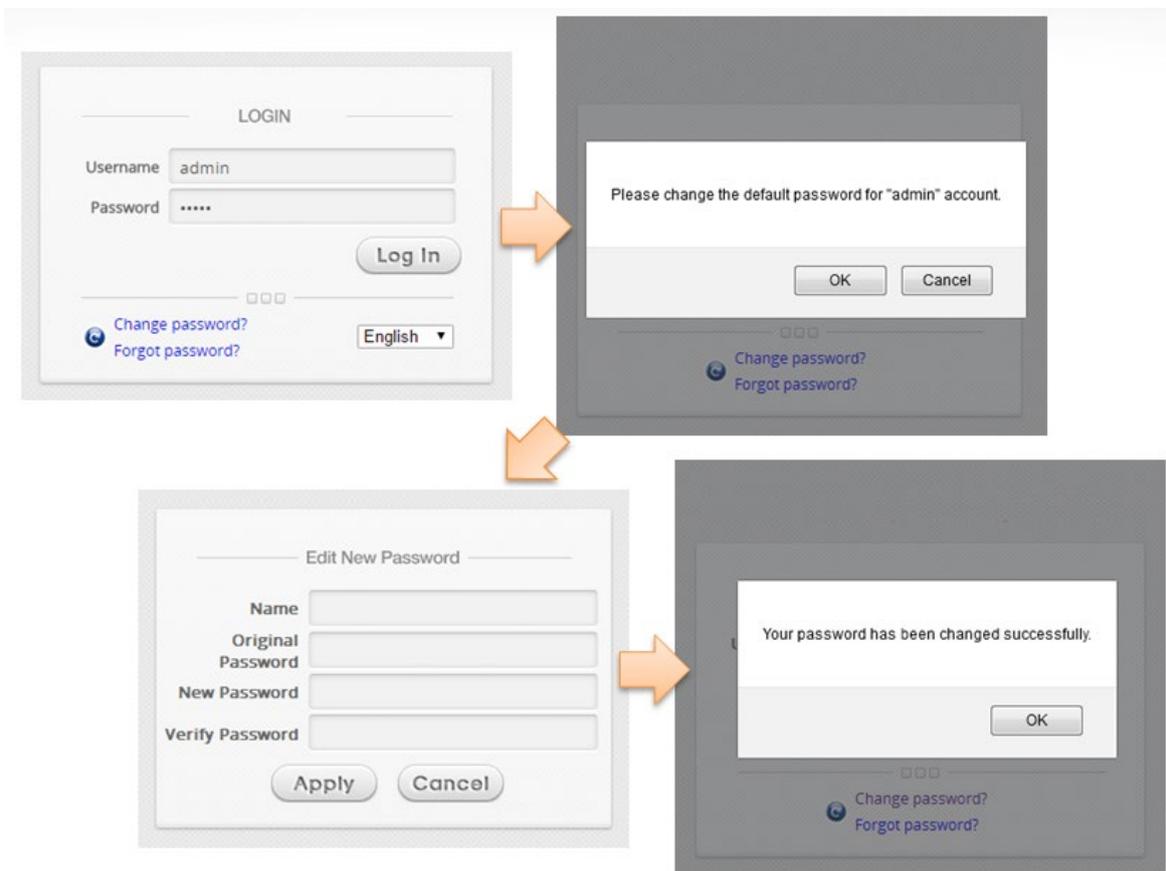


デフォルトの管理者アカウントとパスワードは次のとおりです。

- ユーザー名 : 「admin」
- パスワード : 「admin」

最初のログイン時に、システムセキュリティを強化するためにパスワードを変更するよう管理者に要求します。パスワードは 6 文字以上で、アルファベットと数字を少なくとも 1 つ含める必要があります。

管理者アカウントの設定の詳細については、付録 F のパート E を参照してください。



ダッシュボードページは、管理者ログインに成功すると以下ようになります。



メモ

1. ログアウトするには、インターフェースの右上隅にある **Logout** アイコンをクリックしてログイン画面に戻ります。

2.2 ウィザードの実行

セットアップウィザードには、最小限の構成でネットワークのセットアップと運用に不可欠な一連の構成手順が用意されています。

セットアップウィザードを使用して EWS をすばやく構成するには、WMI ホームページの右上隅にある **Setup Wizard** ボタンをクリックして、構成プロセスを開始してください。

ステップ1 一般設定

- ▶ **Time Zone** のドロップダウンリストから適切なタイムゾーンを選択する。
- ▶ **Next** をクリックして続行する。

The screenshot shows the 'General' configuration screen of the Setup Wizard. At the top, a progress bar indicates four steps: 1. FIRST STEP (Set Time Zone), 2. SECOND STEP (Configure WAN1), 3. THIRD STEP (Create A Local User), and 4. YOU'RE DONE (Restart the System). The current step is Step 1. On the left, a message states: 'It is recommended to select an appropriate time zone for the system.' The main area is titled 'General' and contains a 'Time Zone' dropdown menu with '(GMT+08:00)Taipei' selected. At the bottom right, there are 'Exit' and 'Next' buttons.

ステップ2 WAN1 ポートの接続タイプを選択

- ▶ 次の3種類のWAN接続から選択：**静的IPアドレス**、**動的IPアドレス**、および**PPPoEクライアント**。適切なインターネット接続タイプを選択する。以下は、動的IP接続の使用例を示す。
- ▶ **Next** をクリックして続行する。
- ▶ **静的IPアドレス**または**PPPoEクライアント**の場合は、画面の指示に従う。

1 FIRST STEP Set Time Zone

2 SECOND STEP Configure WAN1

3 THIRD STEP Create A Local User

4 YOU'RE DONE Restart the System

Please select connection type of the WAN1 interface and configure the settings.

WAN1 Interface

- Static (Use the following IP settings)
- Dynamic (IP settings assigned automatically)
- PPPoE

Exit Back Next

ステップ3 ローカルユーザーアカウントの追加（オプション）

- ▶ 新しいユーザーをローカルユーザーデータベースに追加できる。ここにユーザーを追加するには、**ユーザー名**（例：testuser）、**パスワード**（例：testuser）を入力し、**適用されたグループ**をこの特定のユーザーに割り当てる（またはデフォルトの**グループ1**を使用する）。
- ▶ **Next** をクリックして続行する。

1 FIRST STEP Set Time Zone

2 SECOND STEP Configure WAN1

3 THIRD STEP Create A Local User

4 YOU'RE DONE Restart the System

You can choose to add local user accounts for a quick configuration.

Local User Account (Optional)

Username:

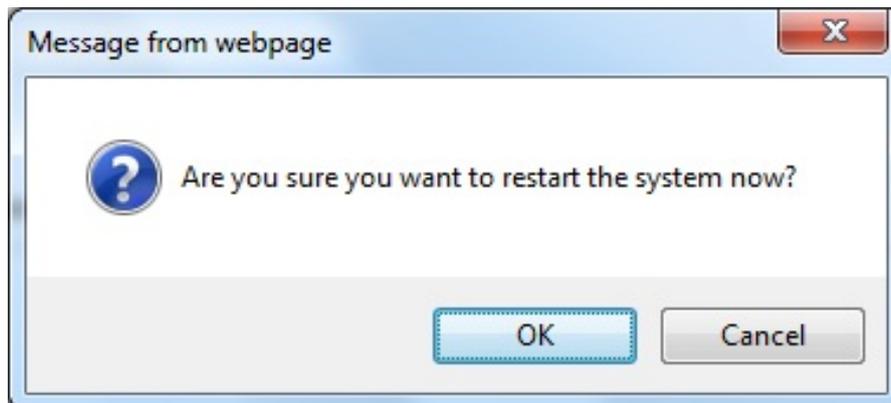
Password:

Group:

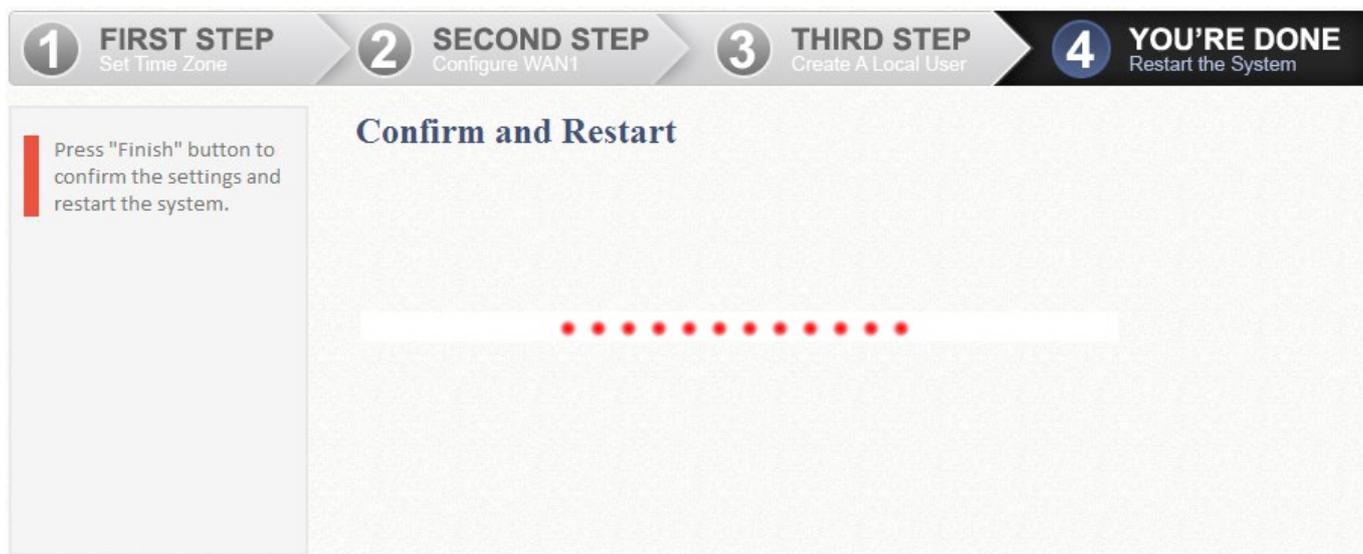
Exit Back Skip Next

ステップ 4EWS の確認と再始動

- **Finish** をクリックして現在の設定を保存し、システムを再始動する。
- 確認のダイアログボックスが表示される。**OK** をクリックして続行する。

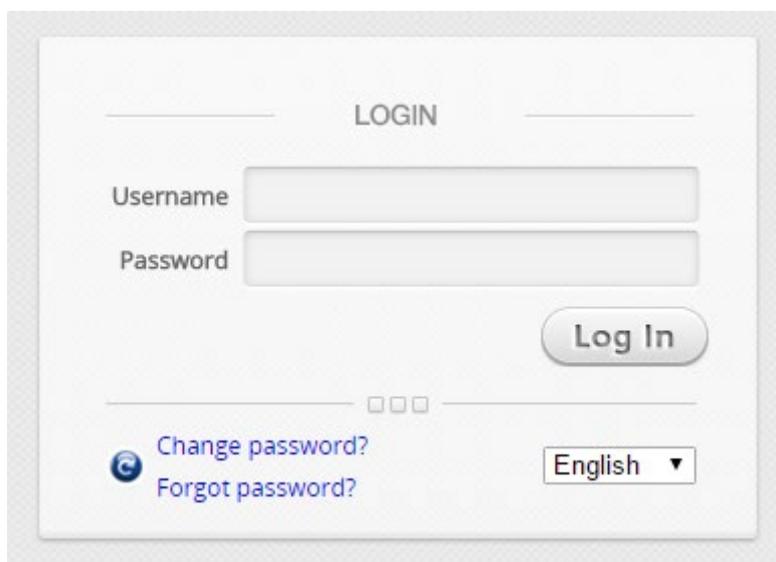


- 再起動プロセス中に、**確認と再始動**のメッセージが画面に表示される。管理者ログインページが表示されるまで、システムを中断しないでください。



再起動プロセスが完了したことを示す管理者ログインページが再び表示されるまで、EWSの再起動プロセスを中断しないでください。

再起動プロセスが完了しました。



第3章 基本ネットワーク設定

3.1. ネットワーク計画

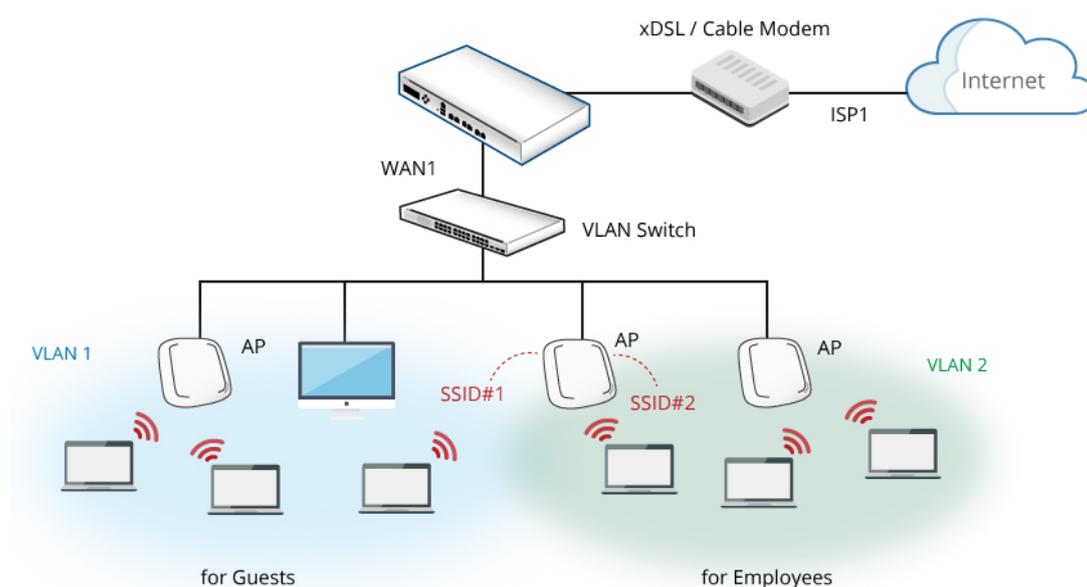
Edgecore EWS コントローラを設置する前に、ネットワークリソースを最も効率的に利用してネットワークのニーズを満たすために、慎重なネットワーク計画が必要です。組織の IT スタッフは、利用可能なネットワークリソースを評価し、回復力、容量、生存性を念頭に置いて、適切なネットワークトポロジを設計する必要があります。

通常、今日の組織ネットワークは、管理可能な有線 LAN と無線 LAN（場合によってはリモート LAN）を組み合わせたものです。ほとんどの配置ニーズを満たすように設計されており、Edgecore EWS コントローラがサポートしているネットワークトポロジは、主に次の 2 つのカテゴリに分かれています。

- 1) レイヤ 2 トポロジ
- 2) レイヤ 3 トポロジ

レイヤ 2 トポロジ

このネットワークトポロジは、オフィスビル、ホテル、学校施設などの限られた物理的エリアにネットワークサービスを提供するために、有線および無線機能で構成されたマネージドローカルエリアネットワーク（LAN）を構築することを目的としています。



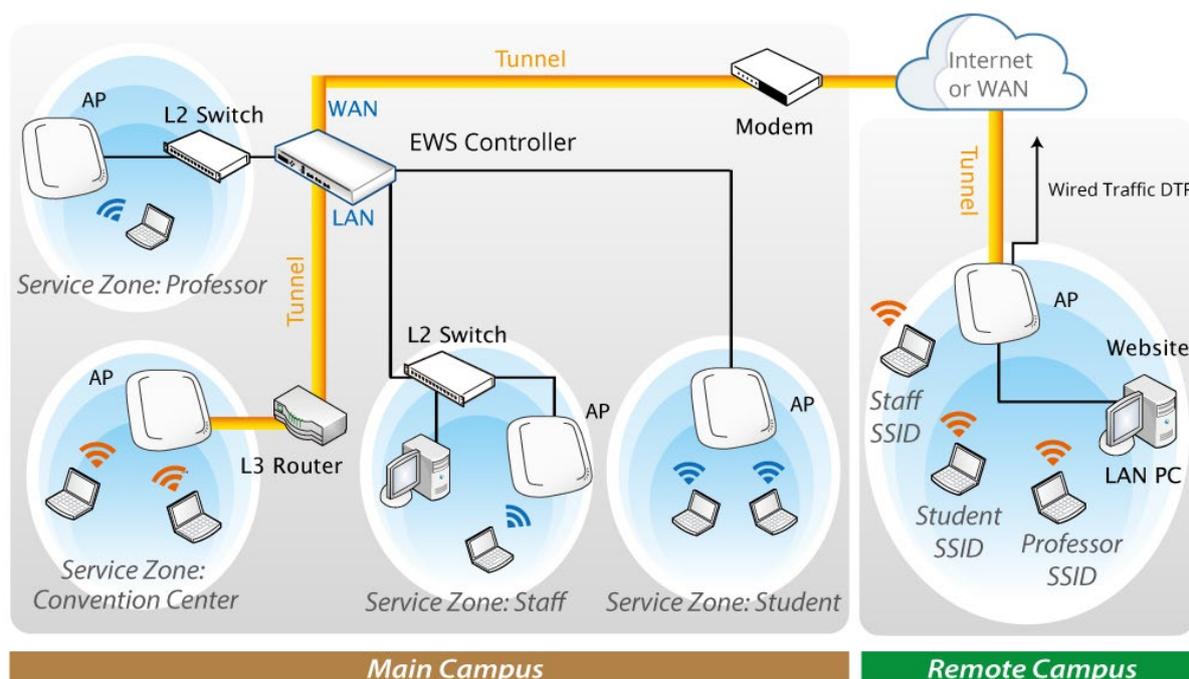
【レイヤ 2 トポロジのグラフィック図】

レイヤ2 ネットワーク設計ガイドライン

- 常に階層的に接続する。建物内に複数のスイッチがある場合は、集約スイッチを使用する。
- 集約スイッチをネットワークコア（メインフレームハウジングなど）の近くに配置する
- エッジスイッチをユーザーの近くに配置する（例：フロアごとに1つ）

レイヤ3 トポロジ

このネットワークトポロジは、企業ビル、ホテルチェーン、大学キャンパスなどのローカルおよびリモートの物理エリアにネットワークサービスを提供するために、有線および無線機能で構成されたマネージドローカルエリアネットワーク（LAN）を構築することを目的としています。



【レイヤ3 トポロジのグラフィック図】

レイヤ3 ネットワーク設計のガイドライン

- ローカル LAN でもリモート LAN でも、常に階層的に接続する。建物内に複数のスイッチがある場合は、集約スイッチを使用する。
- 集約スイッチをネットワークコア（メインフレームハウジングなど）の近くに配置する
- エッジスイッチをユーザーの近くに配置する（例：フロアごとに1つ）
- リモートサイトのデバイス（Edgecore AP または Edgecore EWS コントローラ）のアップリンクは、メイン EWS コントローラの WAN IP アドレスと同じサブネット内にパブリック IP アドレスまたは IP アドレスを持つ必要がある。

3.2. アップリンク（WAN 側）の構成

3.2.1 WAN 設定

設定パス : [Main Menu >> System >> WAN](#)

WAN ポートは、Static、Dynamic、PPPoE および PPTP の 4 つの接続構成をサポートしています。これらの接続タイプは、ほとんどの ISP をサポートするのに十分です。**Physical Mode** ドロップダウンリストでは、管理者は WAN 接続の速度と二重を選択できます。自動ネゴシエーションがオンの場合、システムはインターフェースに接続されたシステムとデバイスの両方がサポートする最高性能の伝送モード（速度/二重/フロー制御）を選択します。

The screenshot shows the 'WAN1 Configuration' page. Under 'Physical Mode', a dropdown menu is set to 'Auto'. Under 'Interface Type', the 'Static (Use the following IP settings)' option is selected. The static IP settings are: IP Address: 10.29.42.101, Subnet Mask: 255.255.0.0, Default Gateway: 10.29.0.1, Preferred DNS Server: 168.95.1.1, and Alternate DNS Server: (empty). Other options like Dynamic, PPPoE, and PPTP are unselected.

WAN ポートが接続している ISP のインターフェースデバイスに応じて、適切な接続タイプを選択する必要があります。例えば、ISP が動的アドレスを発行するケーブルモデムである場合は、**Dynamic** 接続を選択します。

Static : WAN ポートの IP アドレスを手動で指定します。赤いアスタリスクの付いたフィールドは、入力する必要があります。

Dynamic : DHCP サーバーがアップストリームネットワークで利用可能なネットワーク環境にのみ適用されます。IP アドレスを自動的に取得するには、**Renew** ボタンをクリックしてください。

PPPoE : ISP が PPPoE ダイアルアップ接続を提供している場合、ISP はパスワード付きのアカウントを発行します。ISP にダイアルアップするには、WAN 構成ページでアカウント資格情報を入力する必要があります。

PPTP : 一般的な方法ではありませんが、ダイアルアップ接続用の PPTP プロトコルは、いくつかの ISP（ヨーロッパ諸国）で採用されています。PPTP ISP は、パスワードと PPTP サーバーのアドレスを持つアカウントを発行します。

メモ

1. 不明な場合は、契約しているアップリンクサービスの詳細について ISP プロバイダにお問い合わせください。

3.2.2. デュアルアップリンク

EWS コントローラは、ロードバランシングとフェイルオーバーをサポートするために 2 つの WAN ポートを備えています。WAN1 接続が確立されると、サービスに対して WAN2 を有効にすることができます。

2 つ目のインターネットフィードを使用する場合は、WAN2 ポートに適用可能な 3 つの接続タイプのいずれかを選択してください。つまり、**Static**、**Dynamic**、**PPPoE** から選択してください。WAN2 ポートの物理モードを選択できます。

The screenshot shows the 'WAN2 Configuration' section of a web interface. It contains two main settings:

- Physical Mode**: A dropdown menu currently set to 'Auto'.
- Interface Type**: A list of radio button options:
 - None
 - Static (Use the following IP settings)
 - Dynamic (IP settings assigned automatically)
 - PPPoE

Static : WAN ポートの IP アドレスを手動で指定します。赤いアスタリスクの付いたフィールドは、入力する必要があります。

Dynamic : DHCP サーバーがアップストリームネットワークで利用可能なネットワーク環境にのみ適用されます。IP アドレスを自動的に取得するには、**Renew** ボタンをクリックしてください。

PPPoE : ISP が PPPoE ダイアルアップ接続を提供している場合、ISP はパスワード付きのアカウントを発行します。ISP にダイアルアップするには、WAN 構成ページでアカウント資格情報を入力する必要があります。

メモ

1. 不明な場合は、契約しているアップリンクサービスの詳細について ISP プロバイダにお問い合わせください。
 2. WAN ロードバランシングおよび WAN フェールオーバー機能は、WAN2 を構成した場合にのみ使用できます。
-

3.2.3. デュアル WAN1/WAN2 モデル用の WAN ポート選択

EWS コントローラモデル EWS5204 以上は、WAN1 と WAN2 にそれぞれ SFP ポートとイーサネットポートを搭載したキャリアグレードモデルです。管理者は、どの物理ポートを WAN1 または WAN2、イーサネットポート、SFP ポート、イーサネットと SFP ポート、または集約されたスループットでボンディングされるポートとして配置するかをさらに決定できます。

設定パス : [Main Menu >> System >> WAN](#)

The screenshot displays the WAN1 Configuration interface. It is divided into three main sections: Physical Mode, Interface Type, and Transmission Option. The Physical Mode is set to 'Auto'. Under Interface Type, 'Dynamic (IP settings assigned automatically)' is selected, with a 'Renew' button. A checkbox for 'Obtain DNS server address automatically' is checked, and the Preferred DNS Server is set to '168.95.1.1'. Under Transmission Option, 'Fiber Port and Ether Port' is selected.

Section	Setting
Physical Mode	Auto
Interface Type	Dynamic (IP settings assigned automatically)
Obtain DNS server address automatically	Checked
Preferred DNS Server	168.95.1.1
Alternate DNS Server	
Transmission Option	Fiber Port and Ether Port

WAN2 Configuration

Physical Mode	<input type="text" value="Auto"/>
Interface Type	<input type="radio"/> Static (Use the following IP settings)
	<input checked="" type="radio"/> Dynamic (IP settings assigned automatically) <input type="button" value="Renew"/>
	<input checked="" type="checkbox"/> Obtain DNS server address automatically.
Preferred DNS Server:	<input type="text" value="168.95.1.1"/> *
Alternate DNS Server:	<input type="text"/>
	<input type="radio"/> PPPoE
	<input type="radio"/> PPTP
Transmission Option	<input type="radio"/> Ether Port
	<input type="radio"/> Fiber Port
	<input checked="" type="radio"/> Fiber Port and Ether Port
	<input type="radio"/> Bonding

配置オプションは次のとおりです。

- **Ether Port** : サービス用に銅線イーサネット WAN ポートを配置します。
- **Fiber Port** : サービス用の SFP ポートを配置します。
- **Fiber Port and Ether Port** : ファイバポートとイーサネットポートの橋渡しをします。物理的には、SFP ポートまたはイーサポート経由で 1 つのアップリンクだけを接続します。
- **Bonding** : サービス用に SFP ポートと銅線イーサネットポートの両方を配置します。このオプションは、2 つの接続を集約し、集約されたスループットが高くなります。

3.2.4. WAN トラフィック制御

WAN Traffic Settings

Bandwidth Limitation	<input checked="" type="checkbox"/> Enable Bandwidth limitation on WAN
Max Uplink Bandwidth	<input type="text" value="2000000"/> Kbps
Max Downlink Bandwidth	<input type="text" value="2000000"/> Kbps

ここで構成するアップリンク帯域幅とダウンリンク帯域幅は、WAN1 および WAN2 を含む WAN インターフェースの合計帯域幅です。ただし、実際の帯域幅は、ISP オペレータのネットワーク速度によって制限されることに注意してください。例えば、ISP のネットワーク速度が 1 Gbps に制限されている場合、コントローラで 2 Gbps を設定しても、このような制約の下でのスループットの合計は 1 Gbps を超えることはできません。

3.2.5. アップリンク検出とフェイルオーバー

アップリンク検出

WAN インターフェースが有効なアップリンク接続で構成されている場合、管理者はアップリンクサービスが活着しているかダウンしているかを検証するために、検出対象として最大 3 つのアウトバウンドサイトを指定できます。コントローラは定期的にアップリンクのステータスをチェックします。

警告メッセージテキストのフィールドは、管理者がカスタマイズできます。このフィールドは、3 つの検出対象がすべて応答しなかった場合にユーザーの Web ブラウザに表示されます。

WAN Traffic Settings

Bandwidth Limitation

Enable Bandwidth limitation on WAN

Max Uplink Bandwidth Kbps

Max Downlink Bandwidth Kbps

Address for Detecting Internet Connection

Warning of Internet Disconnection

When the addresses for detecting internet connection are unreachable, this message will be shown on the browser.

ロードバランシング

管理者は、セッション、バイト、またはパケットを使用して計算された負荷の割合に基づいて、システムトラフィックを WAN1 および WAN2 ポートに分散させることができます。

WAN Traffic Settings

Bandwidth Limitation

Enable Bandwidth limitation on WAN

Max Uplink Bandwidth Kbps

Max Downlink Bandwidth Kbps

Function of WAN2

Disable(None)

Load Balancing
The "Load Balancing" function when Enabled also acts as the "Failover" function when one of the WAN interfaces is down.

Basis WAN1 Load Allocation: %

Wan Failover

WAN フェールオーバー

有効にすると、WAN1 がダウンするたびに、WAN2 は WAN1 によって処理されたトラフィックを処理します。ネストされたオプションが選択されている場合、WAN1 リンクが再び立ち上がると、サービスは WAN1 リンクに戻されます。この機能は、ロードバランシングと同時に使用することはできません。

WAN Traffic Settings

Bandwidth Limitation	<input checked="" type="checkbox"/> Enable Bandwidth limitation on WAN
	Max Uplink Bandwidth <input type="text" value="2000000"/> Kbps
	Max Downlink Bandwidth <input type="text" value="2000000"/> Kbps
Function of WAN2	<input type="radio"/> Disable(None)
	<input type="radio"/> Load Balancing The "Load Balancing" function when Enabled also acts as the "Failover" function when one of the WAN interfaces is down.
	<input checked="" type="radio"/> Wan Failover
	<input checked="" type="checkbox"/> Fall back when WAN1 connection is restored

メモ

1. WAN フェールオーバー機能は、ロードバランシング機能と同時に有効にすることはできません。

3.3. ダウンリンク（LAN 側）VLAN オプション

EWS コントローラのダウンリンクは、基本的にサービス用に配置された管理対象ネットワークです。EWS コントローラの LAN ポートに接続されたネットワークには、次の 2 種類の配置モードがあります。ポートベースモードとタグベースモードです。

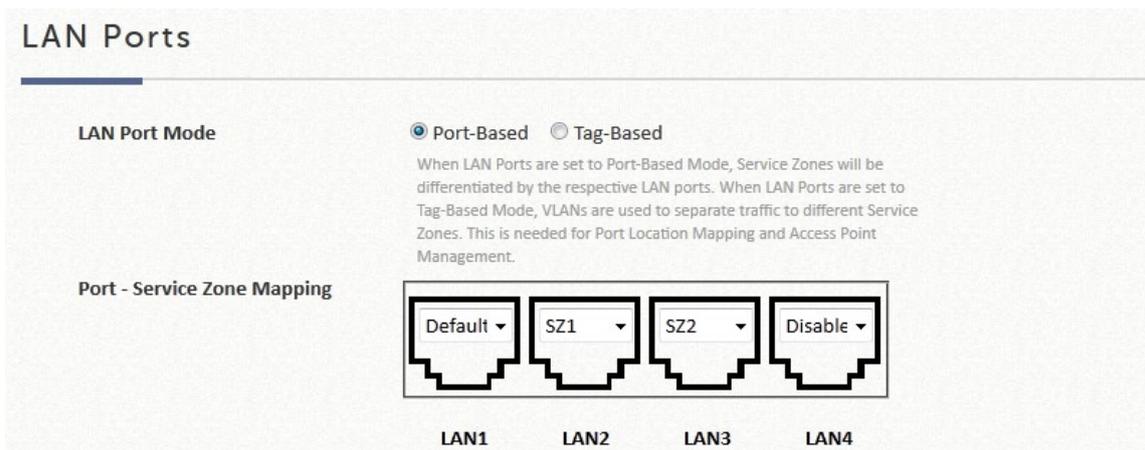
メモ

1. HA 機能が有効になっている場合、LAN1 は専用の HA ポートに変換され、どのサービスゾーンにもサービスを提供できなくなります。
2. VEWS-Series コントローラーは、Tag-Based Service Zone のみサポートしています。

設定パス : [Main Menu >> System >> LAN Ports](#)

3.3.1. ポートベースのサービスゾーン

ポートベースモードは、各物理 LAN ポートを有効なサービスゾーンにマッピングするか、サービスの提供を無効にするという原則で動作します。したがって、ポートベースモードでの動作は、実際にサービスを提供するために利用可能なサービスゾーンの最大量は、コントローラ上の LAN ポートの数によって決まります。



3.3.2. タグベースのサービスゾーン

タグベースの動作モードは、異なるサービスゾーンが VLAN ID によって識別されるという原則の下で動作します。つまり、タグベースの動作により、各物理 LAN ポートは、有効なサービスゾーンのトラフィックを受け入れることができます。トラフィック処理は、パケットが伝送する VLAN ID トラフィックに応じて内部的に処理されます。

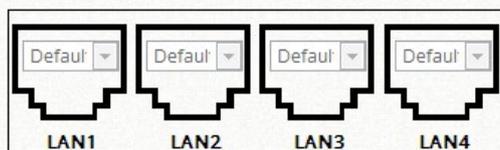
LAN Ports

LAN Port Mode

Port-Based Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping



第4章 ユーザー認証データベース

4.1. 認証データベースの構成

認証データベースは、ユーザーの資格情報の有効性を照会できるストレージデバイスです。サービスゾーンで有効な認証にユーザーが関連付けられている場合、Edgecore EWS コントローラは、ユーザーがネットワークアクセスを取得するために送信されたユーザーID とパスワードの組み合わせが存在するかどうかについて、データベースをチェックします。Edgecore EWS コントローラは、組み込みおよび外部認証データベースをサポートしています。

すべての認証オプションは以下のとおりです。

組み込み認証オプション

ローカル：組み込みのローカルデータベースにユーザーの資格情報が格納されています。

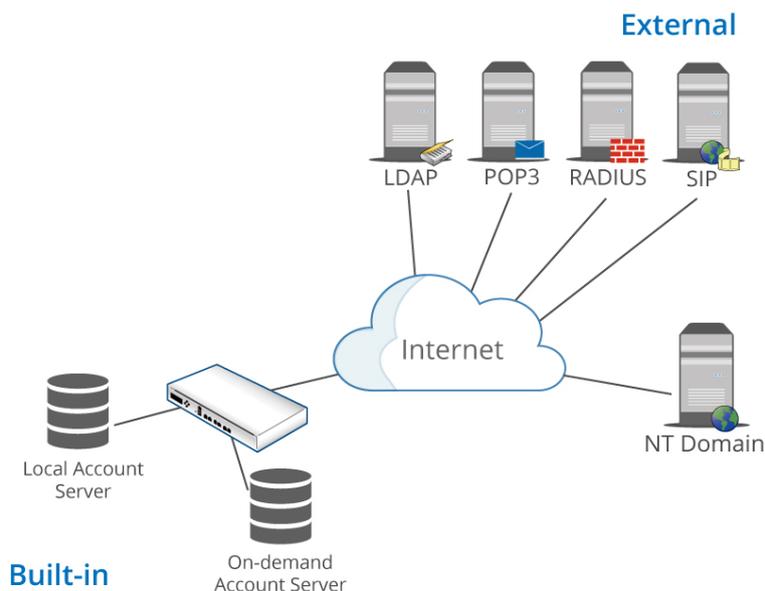
オンデマンド：組み込みのオンデマンドデータベースにユーザーの資格情報が格納されています。

ゲスト：ユーザーがログインページ上の任意の指定の ID トークンを使用してネットワークにアクセスできるようにするアクセスオプションです。

ワンタイムパスワード：SMS によって送信されたパスワードでユーザーがネットワークにアクセスできるようにするアクセスオプションです。このパスワードは、1つのログインセッションでのみ有効です。

外部認証オプション

これらのオプションは、外部サーバーを使用して認証プロセスを実装します。Edgecore EWS コントローラは、最も一般的な外部認証オプションをサポートしています。それは、**RADIUS、LDAP、NT ドメイン、POP3、SIP、ソーシャルメディア**です。



【EWS コントローラに関連する認証データベースの図】

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>

内部認証と外部認証の認証オプションの設定は別々に行われます。5つの外部認証サーバー（RADIUS、POP3、LDAP、NTドメイン、SIP）はカスタマイズ可能で、同時に有効にできます。

メモ

1. 認証オプションは、各サービスゾーンプロファイルでユーザーを認証するために選択的に有効または無効にすることができます。

4.2.組み込み認証データベース

設定パス : [Main Menu >> Users >> Internal Authentication](#)

4.2.1.ローカルユーザーデータベース

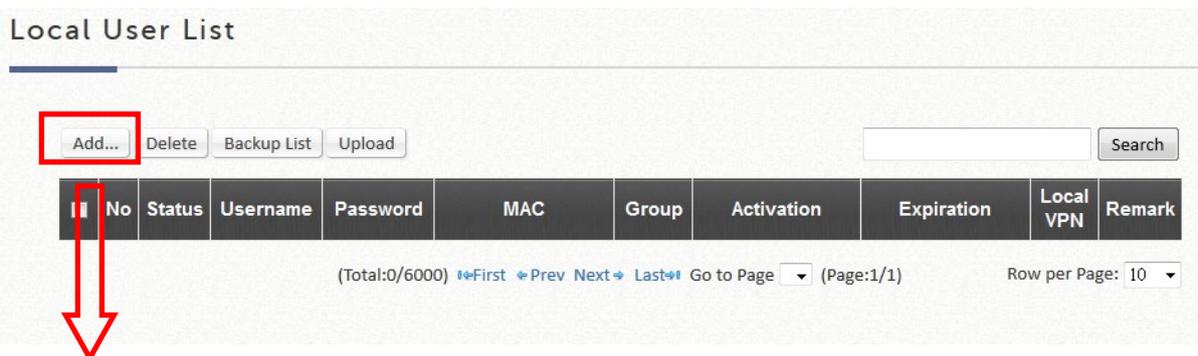
このタイプの認証方法は、ユーザー、多くの場合、スタッフと資格情報を内部的に格納するローカルデータベースをチェックします。ローカルユーザーデータベースは、管理者が手動で実行しない限り、削除されない静的アカウントを保存するように設計されています。

設定パス : [Main Menu >> Users >> Internal Authentication >> Local >> Local User List](#)

アカウント生成

Add User をクリックして、1つまたは複数のアカウントを作成してください。

Local User List



Buttons: Add... Delete Backup List Upload Search

No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
----	--------	----------	----------	-----	-------	------------	------------	-----------	--------

(Total:0/6000) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

Username	Password	MAC Address	Group	Local VPN	Account Span	Remark
example	●●●●●●		Group 1	<input type="checkbox"/>	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	<input type="checkbox"/>	
			Group 1	<input type="checkbox"/>	<input type="checkbox"/>	

メモ

1. 赤いアスタリスクの付いたフィールドは必須フィールドであり、その他のフィールドはオプションです。
 2. **MAC Address** フィールドが設定されると、指定されたデバイスを使用してのみアクセスを許可できるという条件の下で、この特定のアカウントがバインドされます。
 3. **Group** フィールドでは、作成するアカウントのグループプロファイルを指定します。
 4. **Remark**（備考）は、管理者が強調したい追加のメモのためのものです。これは、ユーザーリストに表示されます。
 5. **Enable Local VPN** チェックボックスをチェックして、アカウントとコントローラを使用してデバイス間に安全な VPN トンネルを構築できます。
 6. **Expiration**（有効期限）は、**the Account Span** オプションがチェックされている場合に、このアカウントに強制されるオプションの時間制約です。これは、**複数のログイン**を補完して使用する場合に便利な属性です。例えば、セミナーのイベント中など、特定の時間だけグループのユーザーにネットワークアクセスを提供するのに理想的です。
 7. Username や Password の長さは 1~64 文字になります。使える文字は、「0~9」、「A~Z」、「a-z」、「.」、「-」、「_」だけになります。
-

アカウントのインポートとエクスポート

ローカルユーザーデータベースでは、アップロード機能とダウンロード機能を使用して、ユーザー資格情報をインポートおよびエクスポートできます。ダウンロードファイルは、新しいブラウザウィンドウに表示される csv 形式のテキストファイルになり、管理者は「名前を付けて保存」を実行して、将来の使用のために PC ストレージ内のユーザーアカウントをバックアップすることができます。アップロード操作は、バックアップされた txt ファイルを参照して行い、アカウントをローカルユーザーデータベースにインポートして戻します。

Local User List

No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
(Total:0/6000)	First	Prev	Next	Last	Go to Page	(Page:1/1)	Row per Page: 10		

メモ

1. 生成された txt ファイルは、すべてのモデルで定義された csv 形式が一貫しているため、すべての EWS コントローラシリーズで相互に使用することができます。
2. アカウントが重複すると、アップロードに失敗し、警告メッセージが表示されます。

アカウント資格情報の変更

既存のユーザーアカウントの場合、ページ上のユーザー名のハイパーリンクをクリックするだけで、アカウント属性を再設定し、さらに変更を加えることができます。

Local User List

No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
1	Valid	example	example		Group 1			Disable	

Editing Existing User Data

Username	<input type="text" value="example"/>
Password	<input type="text" value="example"/>
MAC Address	<input type="text"/>
Applied Group	<input type="text" value="Group 1"/>
Enable Local VPN	<input type="checkbox"/>
Remark	<input type="text"/>
Enable Expire Time	<input type="checkbox"/>
Begin Date	<input type="text"/> <input type="button" value="Select Date"/>
End Date	<input type="text"/> <input type="button" value="Select Date"/>

アカウントの削除

ローカルユーザーデータベースのアカウントは、個別に削除でき、または「すべて選択」チェックボックスを選択することで、全部に削除することもできます。アクションを実行することを確認するポップアップウィンドウが表示されます。

Local User List

<input type="checkbox"/>	No	Status	Username	Password	MAC	Group	Activation	Expiration	Local VPN	Remark
<input checked="" type="checkbox"/>	1	Valid	example	example		Group 1			Disable	

4.2.2. オンデマンドユーザーデータベース

オンデマンドユーザーデータベースは、時間またはトラフィック量の制約があるゲストユーザーアカウントのプロビジョニング用に設計されています。ホテル、ホットスポット会場、企業の訪問者受付などの配置ニーズに最適です。オンデマンド認証オプションは、カスタマイズのための多くのオプションを提供します。POS チケットはビジネスニーズに合わせてカスタマイズできます。また、EWS コントローラでは複数の支払いオプションを利用できます。

設定パス : [Main Menu >> Users >> Internal Authentication >> On-Demand](#)

On-Demand Authentication

User Postfix	<input type="text" value="ondemand"/>
Billing Plans	<input type="button" value="Configure"/>
Currency	<input type="radio"/> None <input type="radio"/> \$ USD <input type="radio"/> € EUR <input type="radio"/> £ GBP <input type="text"/>
	<small>This is used when the currency is not defined in the Paypal account. Or input another desired monetary unit (max. 3 letters) in the blank field.</small>
Expired Account Cache	<input type="text" value="30"/> day(s)
Out-of-quota Account Cache	<input type="text" value="30"/> day(s)
Set Ticket's Serial Number	<input type="text" value="000001"/> <input type="button" value="Set"/>
Web Printout	<input type="button" value="Configure"/>
	<small>This will be applied to the regular printer printout when creating a single On-Demand account.</small>
POS Tickets	<input type="button" value="Configure"/>
	Number of Tickets <input checked="" type="radio"/> 1 <input type="radio"/> 2
	<small>This will be applied to printouts from the POS ticket printer. Templates can be edited for customization.</small>
Terminal Server	<input type="button" value="Configure"/>
	<small>Terminal Servers are add-on devices such as the SDS100 or SDS200W.</small>
Payment Gateway	<input type="button" value="Configure"/>
SMS Gateway	<input type="button" value="Configure"/>
Account Roaming Out	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

オンデマンドアカウント設定

1. オンデマンドアカウントデータベースの一般設定は、このページで設定できます。一般設定には、POS/Web チケットのカスタマイズ、支払いゲートウェイオプションなどが含まれます。チケットプリンター（EC-PP200 など）がアカウント生成用に配置されている場合は、ターミナルサーバー構成で IP とポートを構成することを忘れないでください。EWS コントローラは、Clickatell SMS サーバーと連携して、オンデマンドアカウントの資格情報を SMS メッセージでユーザーに送信することができます。

SMS Gateway

Selection

Disable Clickatell

Send SMS for

Account purchases via Payment Gateway Free Account Registration Both

Clickatell Configuration

API ID *

User Name *

Password *

API URL *

Registration before Accounts Expired Allow Block

Query Balance

Billing Plans for Clickatell

Plan	Activation	Quota	Price	Remark
1	<input type="checkbox"/>			<input type="text"/>
2	<input type="checkbox"/>			<input type="text"/>
3	<input type="checkbox"/>			<input type="text"/>
4	<input type="checkbox"/>			<input type="text"/>
5	<input type="checkbox"/>			<input type="text"/>
6	<input type="checkbox"/>			<input type="text"/>
7	<input type="checkbox"/>			<input type="text"/>
8	<input type="checkbox"/>			<input type="text"/>
9	<input type="checkbox"/>			<input type="text"/>
0	<input type="checkbox"/>			<input type="text"/>

Account Registration Control

Disable Black List White List

Web Page Customization

Clickatell アカウントのユーザー名/パスワードのセットを使用すると、オンデマンドアカウントの作成時に SMS メッセージを送信するように SMS ゲートウェイを構成できます。SMS サービスは、無料アクセス、支払いゲートウェイ統合による有料アクセス、またはその両方に使用できます。API ID を定義し、必要な請求プランをアクティブにしてください。必要に応じて、複数の請求プランをアクティブにするこ

とができます。アカウント生成のための SMS クエリによって SMS ゲートウェイがフラッディングされないようにするには、アカウント登録制御オプションを使用できます。さらに、管理者は、アカウントの有効期限が切れる前にユーザーが新しいアカウントを登録することを許可または禁止するオプションがあります。有効なアカウントが新しいアカウントを要求することをブロックするには、オプションを「有効」に設定してください。

SMS ゲートウェイを有効にすると、請求プラン選択ページが次のように表示されます。

Plan (s)	Price (円)	Remark
<input checked="" type="radio"/> 1 min(s) of connection time quota with expiration	11	

Information

Cell Phone Number *

Note

(A) Please enter the cell phone number with country code
(B) After clicking on "Register" button, account information will be sent to the cell phone the one you fill above.

[Back](#) [Register](#)

請求プラン選択ページは、必要に応じてカスタマイズできます。

2. **請求プラン**でアカウント使用条件を定義してください。管理者は、最大 10 の請求プランプロファイルを使用し、適切なアカウントタイプを選択して使用条件をカスタマイズできます。各請求プランのユーザーグループプロファイルもここで割り当てられます。

Billing Plans

No	Plan Type	Quota	Price	Active	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	2	<input checked="" type="checkbox"/>	Group 1	Reset
2	Volume	500 Mbyte(s) of traffic volume quota	5	<input checked="" type="checkbox"/>	Group 2	Reset
3	Hotel Cut-off-time	Valid until 12:00 the following day	10	<input checked="" type="checkbox"/>	Group 3	Reset
4	Duration-time	Valid for 4 hour(s) elapsed time	3.99	<input checked="" type="checkbox"/>	Group 4	Reset
5	N/A			<input type="checkbox"/>	Group 1	Reset
6	N/A			<input type="checkbox"/>	Group 1	Reset
7	N/A			<input type="checkbox"/>	Group 1	Reset
8	N/A			<input type="checkbox"/>	Group 1	Reset
9	N/A			<input type="checkbox"/>	Group 1	Reset
0	N/A			<input type="checkbox"/>	Group 1	Reset

メモ

1. 4つの主要なアカウントタイプの詳細については、**付録 D** を参照してください。
2. チケットのカスタマイズの詳細については、オンラインヘルプまたはチケットのカスタマイズに関する Edgecore アプリケーションノートを参照してください。

オンデマンドアカウント

設定パス : [Main Menu >> Users >> On-Demand Accounts](#)

選択した請求プランを有効にすると、**On-Demand Account Creation**（オンデマンドアカウントの作成）でオンデマンドアカウントの生成が可能になります。オンデマンドアカウントは、個別に作成することも、一括で作成することもできます。

On-Demand Accounts List（オンデマンドアカウントリスト）には、既存のオンデマンドアカウントがすべて表示されます。各アカウントのステータス、クォータなどが表示されます。オンデマンドアカウントのインポート、エクスポート、削除、管理者の引き換えもこのページで実行されます。

オンデマンドアカウントのステータスは、有効、クォータ切れ、および期限切れとして定義されます。

有効 = オンデマンドアカウントがアクティブであるか、またはクォータが残って

いる

合計 = 有効 + クォータ切れ + 期限切れ

また、そのような有効なオンデマンドアカウントおよび総数は、このリストの最後に記載されています。

Main > Users > On-Demand Accounts > Account List

On-Demand Account List

Delete Restore List Backup List Delete Expired Delete Out of Quota Search

<input type="checkbox"/>	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
<input type="checkbox"/>	4ykg	0 sec(s)	Out of Quota	Group 8			Redeem
<input type="checkbox"/>	7g5z	500 M Byte(s)	Normal	Group 4			Redeem
<input type="checkbox"/>	a4gf	Until 2016/08/24-23:30	Normal	Group 7			
<input type="checkbox"/>	znvf	5 hr(s) 10 min(s)	Normal	Group 8			

(Valid:3/7000) (Total:4/10000) **First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 10

4.2.3.ゲスト認証オプション

ゲスト認証オプションは技術的にはユーザーデータベースではなく、ユーザーがユーザーアカウントやパスワードなしでネットワークにアクセスして閲覧できるように特別に設計されたオプションです。

この機能により、ユーザーは特定のサービスゾーンに関連付けて、管理者が定義した社会保障番号や電子メールなどのテキスト文字列を入力し、実際の認証なしでネットワークを使用することができます。

使用条件と使用制約は、ゲスト認証オプションプロファイルで設定できます。

設定パス : [Main Menu >> Users >> Internal Authentication >> Guest](#)

ステップ 1 : ゲスト認証プロファイルの設定

Guest Authentication

Group	Group 1 ▾
Guest Information	View
Guest Questionnaire	Configure
Guest Access Time	<input type="radio"/> Unlimited <input checked="" type="radio"/> 1 Day Access <input type="radio"/> Multi-Day Access
Quota	0 hour(s) 30 minute(s) 0 MByte(s) *(Range:0~1000000, 0:Unlimited)
Reactivation	After 0 hour(s) 1 minute(s)
Access Limit	30 per day *(0:Unlimited)
Email Verification	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Guest Quota List	View
E-mail Denial List	<input checked="" type="radio"/> Disable <input type="radio"/> Enable Configure

E-mail Denial List（電子メール拒否リスト）は、迷惑メールボックスの防止が必要な場合、電子メールアドレスにログイン許可を確認します。**Guest Questionnaire**（ゲストアンケート）は、管理者がゲストログイン用のログインページで追加の質問をカスタマイズできるオプションに提供します。ゲストユーザーからのアクセス情報が収集され、**Guest Information**（ゲスト情報）リストに表示されます。**Guest Access Time**（ゲストアクセス時間）を「制限付き」に設定すると、MAC アドレスに基づいて使用時間の制約が強制されます。**Quota** を 30 分に設定した場合、各デバイスの使用は 30 分しか許可されず、**Reactivation**（再アクティブ化）時間が経過した場合にのみ新しいセッションが可能になります。管理者は、**Access Limit**（アクセス制限）を設定することで、デバイスが 1 日に無料アカウントを要求できる回数を決定することもできます。次に、ゲストユーザーは、ポリシーアプリケーション用に選択されたユーザーグループにマッピングされます。**Guest Quota List** を使用すると、管理者は、アクセスを制限されたゲストアカウントの残りの許容回数を MAC アドレスと電子メールアドレスで確認できます。（毎日午前 0 時に自動的に更新され、最大クォータである 12000 に達すると、最も古いエントリは削除されます。）

Main - Users - Internal Authentication - Guest Authentication - Guest Questionnaire

Guest Questionnaire

No.	Active	Question
1	<input checked="" type="checkbox"/>	Age
2	<input checked="" type="checkbox"/>	Cell Phone
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
5	<input type="checkbox"/>	

Guest Information

Download Delete All

Email Address / Unique ID	Custom 1 (Age)	Custom 2 (Cell Phone)	Last Login	MAC of Last Login
example@edgecore.com	35	01234556789	2019-06-14 16:13:11	00-AA-BB-CC-DD-EE
testvia@edgecore.com	21	0987654321	2019-06-14 17:46:56	00:22:44:66:88:00

(Total:0/12000) **First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

Email verification (Eメールの検証)により、入力された電子メールが有効な電子メールアドレスであることが確認されます。このオプションを有効にすると、アクティベーション時間がクライアントに割り当てられます。その後、クライアントはメールサーバーから送信されたメール内のリンクをクリックすることで、アクティベーション時間内にこのアカウントをアクティブにして、使用時間を延長する必要があります。アクティベーションは単なるタイマーであり、アカウントのクォータには追加されないことに注意してください。送信者名、電子メールの件名、電子メールの内容（最大 2000 文字）は、SMTPサーバーの準備が整うとすぐにカスタマイズできます。SMTPサーバーの設定は、「Assign SMTP Server」（SMTPサーバーを割り当てる）ボタンをクリックして行います。

Email Verification Disable Enable

Email activation time hour(s) minute(s)

Sender name

Activation email subject

Activation email content

Activation link

Guest Account List

SMTP server is not ready

アカウントの一部の情報は、管理者のさらなる分析やマーケティングを目的として、**Guest Information**（ゲスト情報）リストに収集できます。電子メールアドレス、デバイスの MAC アドレス、最終ログイン時刻、およびゲストアンケートの回答が含まれます。

Guest Information

Download Delete All

Email Address / Unique ID	Custom 1 (Age)	Custom 2 (Phone No.)	Last Login	MAC of Last Login
example@edgecore.com	35	01234556789	2019-06-14 16:13:11	00:AA:BB:CC:DD:EE
testvia@edgecore.com	21	0987654321	2019-06-14 17:46:56	00:22:44:66:88:00

(Total:0/12000) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

管理者は、「Download」ボタンをクリックして収集したゲスト情報をダウンロードできます。また、「Delete All」ボタンは、保存されたデータをすべて削除できます。管理者は、エクスポート後にすべてのエントリを削除して、リストを最新の状態に保つことができます。

メモ

- **Guest Questionnaire**（ゲストアンケート）が有効な場合、コントローラはクライアントから情報を収集します。クレームとリマインダーを含めるには、免責事項またはカスタマイズされたログインページを有効にしてください。

ステップ 2：特定のサービスゾーンとログインページへの実装

ゲスト認証オプションを適用するサービスゾーンを選択してください。Main Menu > System > Service Zone > Configure の順に選択してください。ページを下にスクロールして、**Authentication Options**（認証オプション）が表示されます。次の図に示すように、ゲスト認証オプションを有効にする場合はチェックを入れてください。

Authentication Options				
Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
Guest	FREE	N/A	<input type="radio"/>	<input checked="" type="checkbox"/>

その結果、ステップ 1 とステップ 2 の設定を行った後、エンドユーザーは、ゲストアクセスの追加セクションがサービスゾーンのログインページに表示されることが見えます。

電子メールアドレスを入力して login をクリックし、公衆 Wi-Fi の無料アクセス条件を承認することで、ゲストユーザーはゲスト認証オプションプロファイルとグループプロファイルで指定された制約でネットワークにアクセスできるようになります。無料アクセスの悪意のある使用を避けるために、MAC アドレスがチェックされます。

The screenshot shows a web interface for login. It has a decorative header with red and blue wavy lines. Below the header, there are two distinct login sections. The first section is titled 'LOGIN' and contains two input fields: 'Username' and 'Password'. To the right of the 'Password' field is a red 'Login' button. The second section is titled 'FREE LOGIN' and contains one input field: 'Email'. Below the 'Email' field is the text 'Enter your Email account to login for free.' and a red 'Login' button.

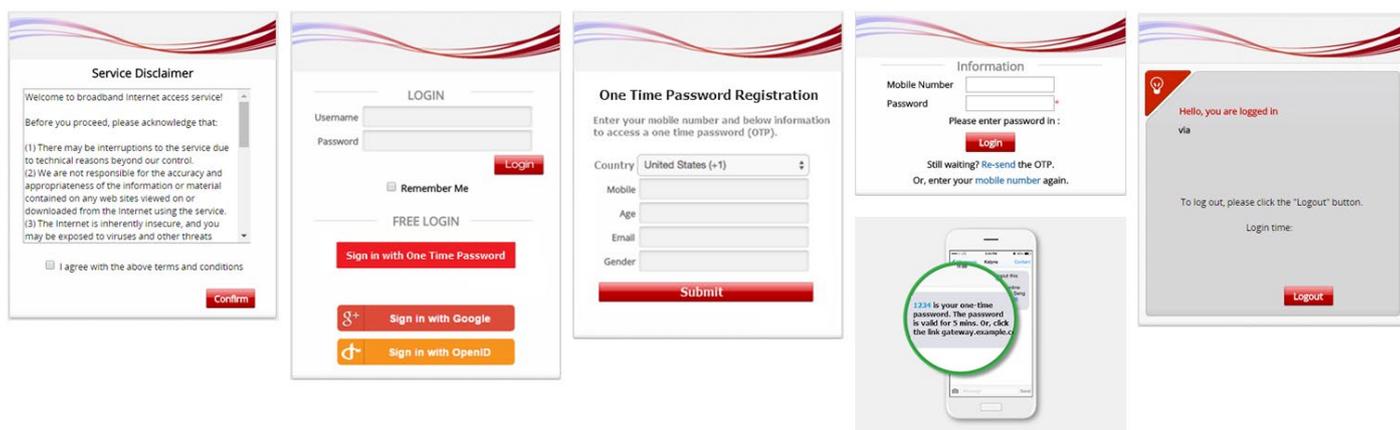
4.2.4.ワンタイムパスワード

ワンタイムパスワード (OTP) 認証オプションの場合、クライアントは自分の携帯電話番

号を入力し、認証ページに入力するために必要なワンタイムパスワードを含む SMS メッセージを受信することで、インターネットにアクセスできます。その後、クライアントはインターネット閲覧を始めることができます。

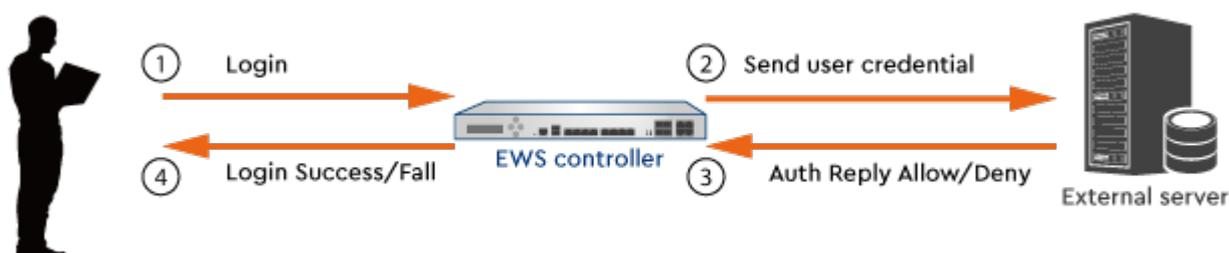
通常、ユーザーログインフローには、次の手順とページが含まれます。

- A. サービス免責事項：（有効になっている場合）ログインプロセスを続行するための利用規約とサービスに同意すること
- B. 一般ログインページ：sign in with one time password ボタンをクリックすること
- C. OTP 登録ページ：携帯電話番号を入力し、有効になっている場合は他のアンケートを入力すること
- D. OTP で SMS を受信：クライアントの携帯電話にパスコード付きのテキストが受信されること
- E. OTP 認証ページ：検証および認証を行う OTP を入力すること
- F. ログイン成功ページ：インターネット閲覧ができること



4.3.外部認証オプション

ほとんどの組織では、一元化されたユーザーアカウントサーバーがすでに構築されています。そのため、Edgecore EWS コントローラは、アカウントローミングをサポートし、既存のネットワークに適応するために、さまざまな外部認証オプションを備えています。外部認証を使用する簡単な例を以下に示します。



メモ

1. 組み込みデータベースと外部データベースのどちらを使用するかに関係なく、認証オプションを設定した場合は、有効な各サービスゾーンで個別に有効にする必要があります。

4.3.1.RADIUS

リモート認証ダイヤルインユーザーサービス (RADIUS) は、コンピュータがネットワークサービスに接続して使用するために、認証、認可、アカウントिंग (AAA) の一元管理を提供するネットワークプロトコルです。また、現在使用されている外部認証メカニズムの中で最も一般的に使用されているものです。

設定パス : [Main Menu >> Users >> External Authentication](#)

Server No. 2: Server 2

External RADIUS Server Settings

Group	Group 1
Local VPN	<input type="checkbox"/> Enable Local VPN
802.1X Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Username Format	<input checked="" type="radio"/> Leave Unmodified <input type="radio"/> Complete (e.g. user1@postfix) <input type="radio"/> Only ID (e.g. user1)
NAS Identifier	<input type="text"/>
NAS Port Type	<input type="text" value="19"/> *(Default 19, Range: 0~35)
Accounting Delay Time	<input type="text" value="0"/> *(Default: 0)
Service Type	<input type="text" value="1"/> *(Default: 1, Range: 1~11)
Class	<input type="text"/>
Class-Group Mapping	<input type="button" value="Configure"/>

サーバー2 は、デフォルトで RADIUS 認証を使用するように構成されています。

Edgecore EWS コントローラは、RADIUS 認証、RADIUS クラスマッピング、および 802.1X を使用した RADIUS 透過ログインをサポートします。

以下に、RADIUS 設定の詳細設定ページを示します。**Primary RADIUS Server** と **Secondary RADIUS Server** の属性は、サービスの配置に応じて設定できます。

External RADIUS Server Related Settings

802.1X Authentication Enable Disable

Username Format Leave Unmodified Complete (e.g. user1@postfix) Only ID (e.g. user1)

NAS Identifier

NAS Port Type *(Default 19, Range: 0~35)

Accounting Delay Time *(Default: 0)

Service Type *(Default: 1, Range: 1~11)

Class

Class-Group Mapping

This shows the mapping of RADIUS class attributes to the different Groups.

DM & CoA Settings

Send Acct Interim when users' IP changes Enable Disable

Failover between RADIUS Servers Enable Disable

Attributes Priority

Standard RADIUS Attributes

Session Timeout Minutes *(Range: 5-1440 mins)

Idle Timeout Minutes *(Range: 1-120 mins)

Acct Interim Interval Minutes *(Range: 1~120 mins, 0 is disable)

WISPr Vendor Specific Attributes

Redirection URL

Billing Class Of Service

Session Terminate on Billing Time Enable Disable

Session Terminate Time Never

Bandwidth Setting Group 1

Retransmission Settings

Number of Retries *(Default: 3)

Timeout *(Default: 6)

Primary RADIUS Server

Authentication Server *(Domain Name/IP Address)

Authentication Port *(Default: 1812)

Authentication Secret Key *

Authentication Protocol

Accounting Service Enable Disable

Accounting Server *(Domain Name/IP Address)

Accounting Port *(Default: 1813)

Accounting Secret Key *

Secondary RADIUS Server

Authentication Server (Domain Name/IP Address)

Authentication Port

Authentication Secret Key

Authentication Protocol

Accounting Service Enable Disable

Accounting Server (Domain Name/IP Address)

Accounting Port

Accounting Secret Key

もう 1 つの重要な設定フィールドは、このページの **Class-Group Mapping** です。これは、RADIUS クラスを Edgecore EWS コントローラ上の異なるグループにマッピングする変換設定で、異なる RADIUS アカウントを異なるグループに組み込むことができます。

4.3.2.POP3

POP3 は、電子メールが特定のインターネットサーバーによって保持される一般的なメールサービスプロトコルです。Edgecore EWS コントローラは、管理者に POP3 サーバーに格納されている電子メールアドレスとパスワードを入力して、インターネットサービスを許可する認証方法を提供します。

設定パス : [Main Menu >> Users >> External Authentication](#)

サーバー5 は、デフォルトで POP3 認証を使用するように構成されています。**Server Name** をクリックすると、詳細な設定ページが表示され、POP3 サーバーアドレス、セカンダリ POP3 サーバーの仕様など、必要な設定を確認できます。

Server No. 5: Server 5

POP3 Server Settings

Group: Group 1

Local VPN: Enable Local VPN

Username Format: Complete Only ID
Example of a Only ID username: user1.

Primary POP3 Server Settings

Server: *(Domain Name/IP Address)

Port: *(Default: 110)

SSL Connection: Enable

Secondary POP3 Server Settings

Server:

Port:

SSL Connection: Enable

4.3.3.LDAP

ライトウェイトディレクトリアクセスプロトコル (LDAP) は、IP ネットワーク経由で分散ディレクトリ情報サービスにアクセスして維持するためのアプリケーションプロト

コルです。

ユーザー認証用に LDAP サーバーを配置する場合は、完全なセットアップに進んでください。

設定パス : [Main Menu >> Users >> External Authentication](#)

サーバー4 は、デフォルトで LDAP データベースを使用してユーザーの資格情報をチェックするように選択されています。

Server Name をクリックして、LDAP の詳細設定ページに入ります（セカンダリ LDAP サーバーをバックアップサーバーとして指定することができます）。さらに、LDAP 設定ページには、LDAP 属性を Edgecore EWS コントローラ上の異なるグループにマッピングする **Attribute-Group Mapping**（属性-グループマッピング）ページがあり、異なるアカウントを異なるグループに組み込むことができます。

The screenshot displays the LDAP configuration interface. At the top, there is a 'Group' dropdown menu set to 'Group 1'. Below this is the 'Local VPN' section with an 'Enable Local VPN' checkbox. The 'Primary LDAP Server Settings' section includes fields for 'Server' (with a placeholder note: *(Domain Name/IP Address)), 'Port' (with a placeholder note: *(e.g. 389 for LDAP, 636 for LDAPS)), 'Service Protocol' (radio buttons for LDAP, LDAPS, and LDAP+StartTLS), 'Base DN' (with a placeholder note: *(e.g. cn=users,dc=domain,dc=com)), 'Binding Type' (dropdown menu set to 'User Account'), and 'Account Attribute' (radio buttons for UID and CN). The 'Secondary LDAP Server Settings' section has identical fields. At the bottom, the 'Group Mapping' section includes an 'Attribute-Group Mapping' dropdown menu and a 'Configure' button.

4.3.4.NT ドメイン

NT ドメインオプションは、Windows ドメインデータベースをサポートし、ユーザーの資格情報認証を実行します。

設定パス : [Main Menu >> Users >> External Authentication](#)

Server No. 3: Server 3

NT Domain Server Settings

Group: Group 1

Local VPN: Enable Local VPN

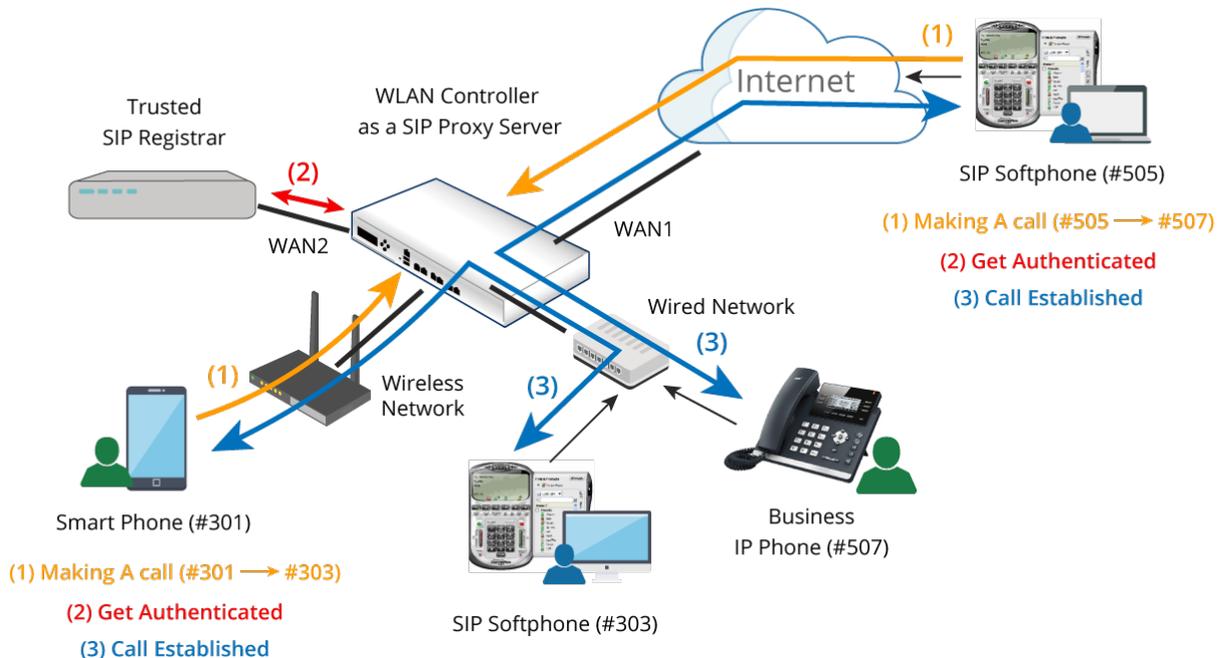
NTDomain Server Settings: Server: *

Transparent Login: Enable Disable (Windows 2000, 2003 or above)

サーバー3 はデフォルトで NT ドメインを使用するように選択されています。管理者は、ユーザーの資格情報が格納されているドメインコントローラの IP アドレスを入力するだけです。さらに、Windows Active Directory がデバイスアクセスの ID チェックとして配置されている場合、**Transparent Login**（透過ログイン）機能を有効にして、単一のログインアクションでデバイスとネットワークへのアクセスを許可できます。

4.3.5.SIP

SIP（セッション開始プロトコル）は、VoIP（Voice over Internet Protocol）およびその他のマルチメディアセッション用に定義された IETF プロトコルです。Edgecore EWS コントローラは、SIP 認証と SIP 電話の使用をサポートします。Edgecore EWS コントローラに加えて、管理者は SIP 電話を成功させるために、他のデバイスを設定する必要があります。これには以下が含まれます。有効な SIP レジストラ、SIP 電話です。



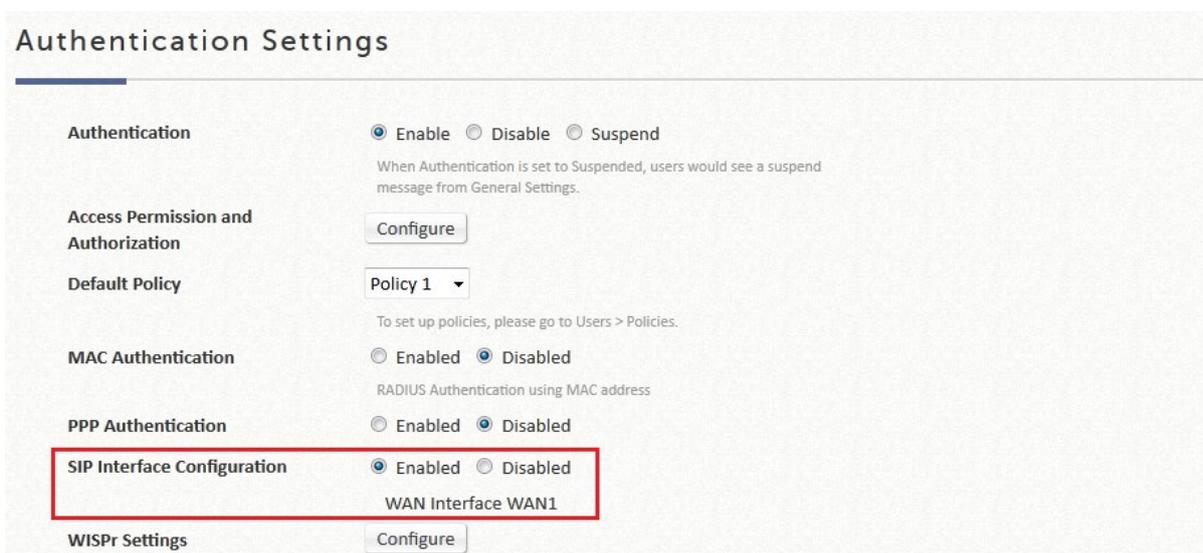
- (1) ユーザーがSIPベースの電話（例：#301 → #303）を介してコールを発信しています。
- (2) ユーザーがSIPレジストラに登録されている場合、ユーザーは透過的に認証されます。
- (3) コールが正常に確立されました。

設定パス：[Main Menu >> Users >> External Authentication](#)

デフォルトでは、認証オプションのデータベースとして SIP が選択されていません。それぞれのサービスゾーンで認証設定から SIP を有効にしてください。管理者は、コールサービスを提供するために、少なくとも 1 つの有効な SIP レジストラをコールセンターとして入力する必要があります。最大 4 つを指定できます。対応するグループプロファイルには、音声アプリケーションをサポートするように適切に設定されている QoS 設定が必要です。

Authentication Server - SIP	
Trusted Registrar	
IP Address	Remark
<input type="text"/>	<input type="text"/>

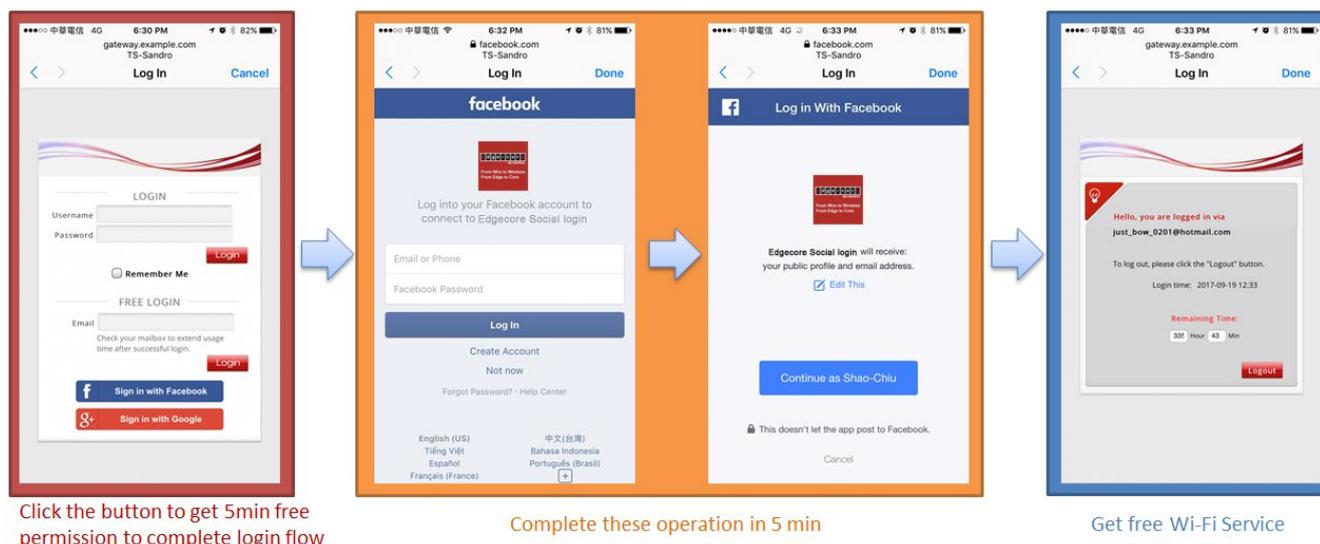
また、正しく機能するために、対応するサービスゾーンの SIP Interface Configuration (SIP インターフェース設定) で「Enable」(有効)になっていることを確認してください。



4.3.6. ソーシャルメディア

ソーシャルメディアログインを使用すると、Wi-Fiユーザーは面倒なアカウント登録プロセスを経ずにインターネットにアクセスできます。Edgecore EWS シリーズコントローラは、LINE、Facebook、Twitter、Weibo、VK、dAccount、およびオープンIDなどのソーシャルメディアアカウントをサポートしています。すべての管理者は、対応するIDとシークレットを適用する必要があります。

ユーザーがソーシャルメディアアカウントでサインインするためにボタンをクリックすると、ログインと許可を与えるためのソーシャルメディアサイトにリダイレクトされます。ウォールド・ガーデンのジレンマに悩まされる必要はありません。接続されたクライアントは、ソーシャルログインボタンのいずれかをクリックしている限り、5分間の無料許可を取得します。その後、5分間に必要なソーシャルアカウント情報を使用してログインプロセスを完了する必要があります。その後、それは下の図のようにインターネット閲覧を開始する時間です。



この設定ページでは、コントローラがソーシャルメディアサイトに接続するように設定できます。

- LINE : LINE Developers サイト (<https://developers.line.me/console/>) にアクセスし、「LINE ログイン」アプリを申請して、アプリタイプでウェブを選択してチャンネル ID とチャンネルシークレットを取得してください。
- Facebook : Facebook 開発者サイト (<https://developers.facebook.com/>) にアクセスし、「Facebook ログイン」アプリを申請してアプリ ID とアプリのシークレットを取得してください。
- Twitter : Twitter developers サイト (<https://developer.twitter.com/>) にアクセスし、「Twitter API」を申請して API キーと API シークレットを取得してください。
- Weibo : Weibo 開発者サイト (<http://open.weibo.com/liveapi/index.php>) にアクセスし、「LINE ログイン」アプリを申請して、アプリタイプでウェブを選択してチャンネル ID とチャンネルシークレットを取得してください。
- VK : VK 開発者サイト (<https://vk.com/dev>) にアクセスし、「LINE ログイン」アプリを申請して、アプリタイプでウェブを選択してチャンネル ID とチャンネルシークレットを取得してください。
- dAccount : dAccount・コネクトサイト (https://id.smt.docomo.ne.jp/src/index_business.html?btn01) にアクセスし、クライアント ID とクライアントシークレットの取得を申請してください。
- オープン ID : ログインパスを通過し、OpenID Walled Garden に追加する必要があります。リダイレクト先は OpenID プロバイダに依存します。

Social API Credentials

Line Login	<input type="checkbox"/>
Line App ID	<input type="text"/>
Line App Secret	<input type="text"/>
Facebook Login	<input type="checkbox"/>
Facebook App ID	<input type="text"/>
Facebook App Secret	<input type="text"/>
Twitter Login	<input type="checkbox"/>
Twitter API Key	<input type="text"/>
Twitter API Secret	<input type="text"/>
Weibo Login	<input type="checkbox"/>
Weibo App ID	<input type="text"/>
Weibo App Secret	<input type="text"/>
VK Login	<input type="checkbox"/>
VK App ID	<input type="text"/>
VK App Secret	<input type="text"/>
dAccount Login	<input type="checkbox"/>
dAccount Client ID	<input type="text"/>
dAccount Client Secret	<input type="text"/>
OpenID Login	<input type="checkbox"/>

Please use a valid and trusted HTTPS certificate when enabling dAccount login.

Apply

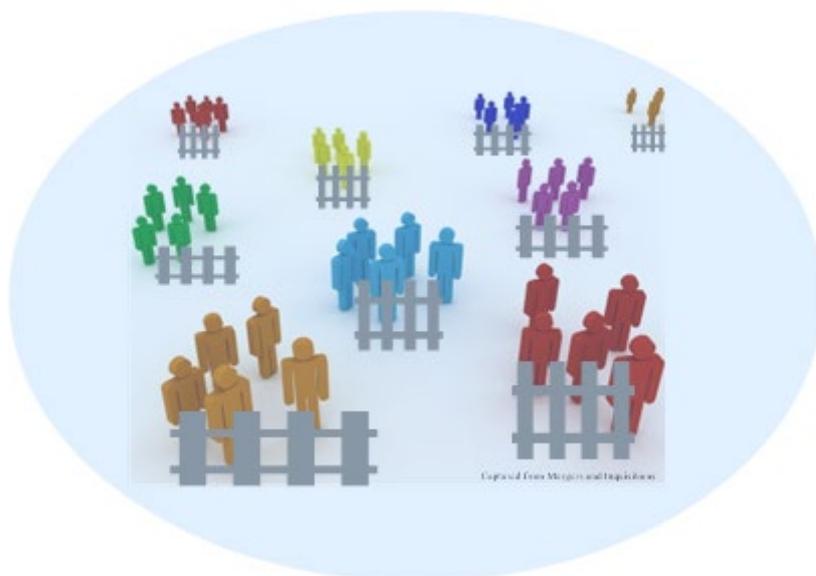
Cancel

第5章 グループ属性とポリシールール

すべての Edgecore EWS コントローラモデルでは、「グループ」と「ポリシー」を使用して、ユーザーのアクセス性とネットワーク権限を定義し、ユーザーの動作に制約を設定します。グループ化、ポリシー設定、およびサービスゾーンは互いに絡み合っているため、このセクションでは、グループ化、ポリシー、およびサービスゾーンとの関係の概念、および、これら3つの属性に関する実用的な設定プロセスについて説明します。

5.1 コンセプトの概要

- グループ



グループは、役割ベースなどのある程度類似した特性を共有していると管理者にみなされる一連のユーザーです。例えば、大学では、一般的に学生、教職員、ゲストがいます。したがって、IT スタッフは、これら3つのカテゴリのインターネットサービスユーザーを区別する3つのグループを設定して、これらのグループに異なるインターネットアクセス性の許可を与えることができます。Edgecore EWS モデルには、モデルの容量に応じて、8~24 個のグループプロファイルがあります。

オンデマンドユーザーとローカルユーザーは、アカウントごとに異なるグループに割り当てることができます。外部サーバーによって認証されるユーザーについては、Edgecore EWS コントローラは、クラスグループマッピングと属性グループマッピングを使用して、RADIUS オプションと LDAP オプションに対するアカウントごとのグループ割り当ても提供します。

各グループプロファイルには、管理者が定義できる属性がいくつかあります。

1. サービス品質 (QoS) :

音声、ビデオ、ベストエフォート、およびバックグラウンドのトラフィッククラスを選択です。

すべてのグループのメンバーが共有するアップリンクとダウンリンクの合計レート
個々の最大ダウンリンクおよびアップリンクレート

2. 権限プロファイル :

オンデマンドアカウント権限は、特定のグループの認証されたユーザーが、コントローラのデフォルト/テンプレートログイン成功ページでオンデマンドアカウントを生成できるようにします。

パスワード変更権限は、コントローラのデフォルト/テンプレートログイン成功ページで、ログインに成功した後で、ユーザーが自分のパスワードを変更できるようにします。

最大同時セッション数は、ユーザーごとに許可される同時ログインの数を決定します。

3. サービスゾーンへのアクセス性 :

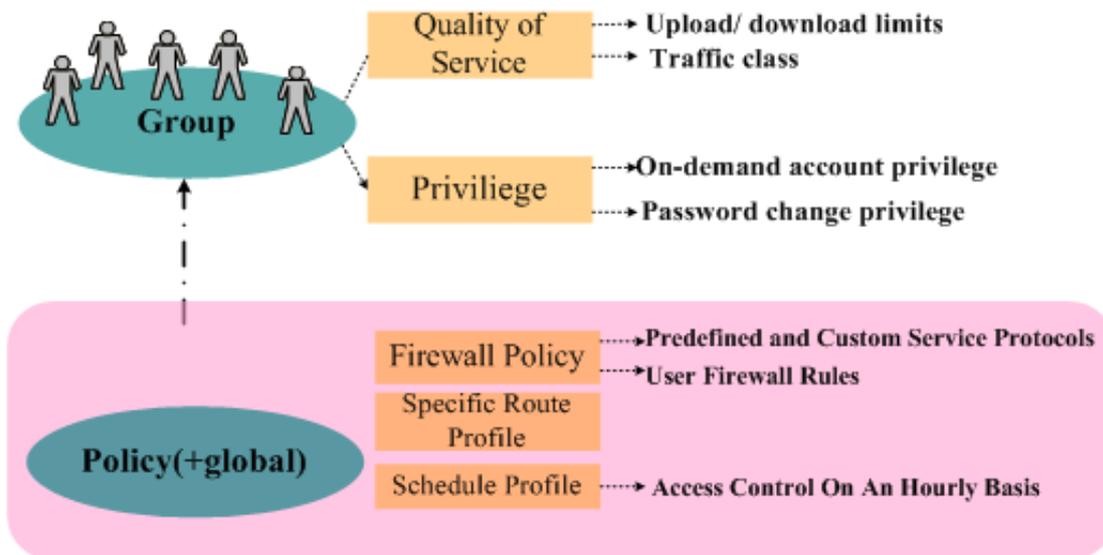
特定のサービスゾーンへのアクセス許可またはアクセス拒否と、バンドルされたポリシーを設定できます。

● ポリシー

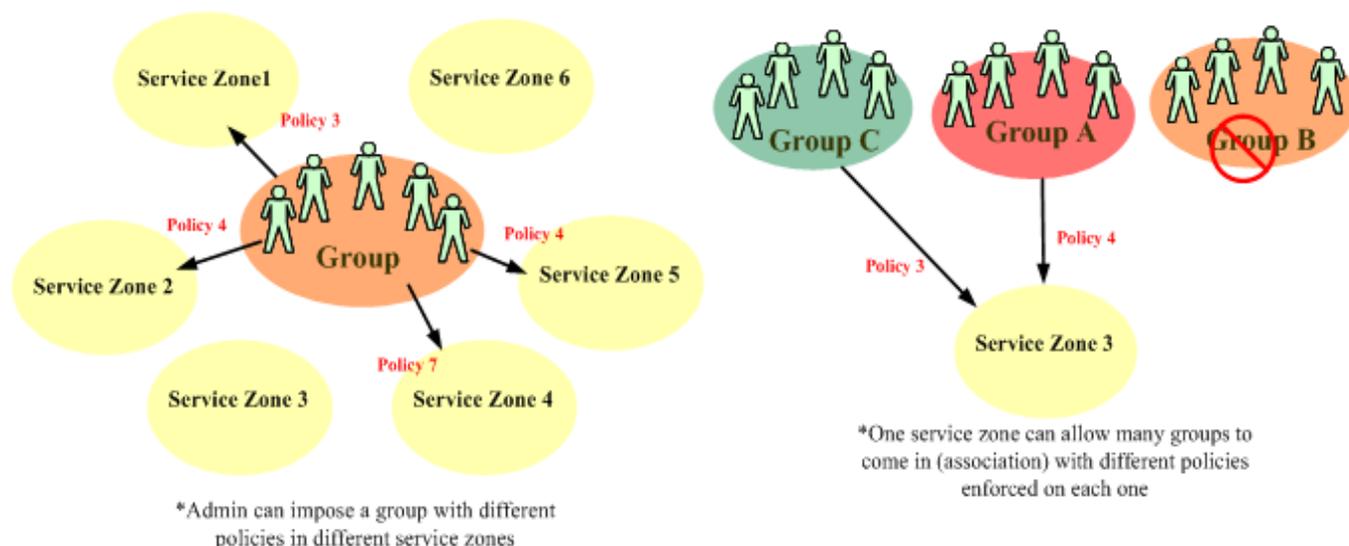
ポリシーとは、ファイアウォールルール、ログインスケジュール、ルーティングルール、セッション許容値など、ユーザーに適用されるネットワーク管理上の制約のプロファイルです。グローバルポリシーがあり、ユーザーがどのポリシーにもバインドされていないグループに属している場合に適用されます。ポリシープロファイルの数はモデルによって異なります。

グループプロファイルとポリシープロファイルが分離されているため、より柔軟性が高くなっています。これにより、同じグループのユーザーは、管理者が定義するグループサービスゾーンのアクセス許可マッピング設定に従って、異なるポリシーにバインドできるようになります。例えば、グループ 1 のユーザーは、サービスゾーン 1 のポリシー 1 によって課されますが、サービスゾーン 3 に移動するとポリシー 3 によって課されます。

● グループ、ポリシー、およびサービスゾーンの関係



最初の図は、グループとポリシーの関係、および各カテゴリで定義できる属性を示しています。管理者は、ポリシー、グループ、およびサービスゾーン間の関係を2つの視点から定義できます。グループをサービスゾーンにマッピングする視点と、その逆の視点です。以下の視覚的な説明を参照してください。



5.2 グループとポリシーの実用的な設定

このセクションでは、Edgecore EWS コントローラの WMI でグループとポリシーの実用的な設定をする方法のスクリーンショットを示します。

- グループ概要

設定パス : [Main Menu >> Users >> Groups >> Overview](#)

Group Overview (グループ概要) の表には、対応する各グループで使用される認証サーバーの概要が表示されます。オンデマンド認証データベースの請求プランに割り当てられたユーザーグループもここに表示されます。

Group Name	Authentication Type
Group 1	Local Billing Plan 1 Trial POP3-Server 4 RADIUS-Server 2-Default LDAP-Server 3-Default SIP-Server 1
Group 2	Billing Plan 2
Group 3	Billing Plan 3
Group 4	Billing Plan 4
Group 5	
Group 6	
Group 7	

- **グループ設定**

設定パス : [Main Menu >> Users >> Groups >> Configuration](#)

Group Configuration – Group x (グループ設定 — グループ x) は、グループに対して定義するポリシー設定のための表です。複数のデバイスログイン (オンデマンドを除く) は、ここで有効にすることができます。

Zone Permission Configuration & Policy Assignment – Group x (ゾーンのアクセス許可設定とポリシーの割り当て — グループ x) の表を使用すると、管理者はグループ、ポリシー、およびサービスゾーンの関係を確認できます。

Group Configuration

Select Group

Group Name

Remark

Number of devices which are allowed to login
(0 to 9999 devices, 0: Unlimited)
For On-Demand accounts, number of devices is configured individually per different billing plans. The number is for the following types: LOCAL, POP3, RADIUS, LDAP, and NT Domain.

Allow to logout other devices when exceeding the maximum amount of devices Enabled Disabled
For On -Demand accounts, allowing to logout others devices is always enabled. This setting id for the following types: LOCAL, POP3, RADIUS, LADP, and NT Domain.

Zone Permission Configuration & Policy Assignment

Enabled	Zone Name	Time Span 1	Time Span 2
		<input type="text" value="Schedule 1"/>	<input type="text" value="Schedule 1"/>
<input checked="" type="checkbox"/>	Service Zone : Default	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ1	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ2	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ3	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ4	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ5	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ6	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ7	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Service Zone : SZ8	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>
<input checked="" type="checkbox"/>	Remote VPN : IKEv2	<input type="text" value="Policy 1"/>	<input type="text" value="Policy 1"/>

ステータスチェックボックスにチェックを入れて、このグループのユーザーが対応するサービスゾーンにアクセスできるようにしてください。サービスゾーンの観点から設定するには、サービスゾーン設定の Access Permission and Authorization（アクセス権限と認可）を参照してください。

Authentication Settings

Authentication

Enable Disable Suspend

When Authentication is set to Suspended, users would see a suspend message from General Settings.

Access Permission and Authorization

Configure

Default Policy

Policy 1

To set up policies, please go to Users > Policies.

MAC Authentication

Enabled Disabled

RADIUS Authentication using MAC address

PPP Authentication

Enabled Disabled

SIP Interface Configuration

Enabled Disabled

WISPr Settings

Configure

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enable
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>

Group Overview - SZ1

Name	Status	Time Span 1	Time Span 2	Time Span 3
Group 1	<input checked="" type="checkbox"/>	Policy 1	Policy 1	Policy 1
Group 2	<input checked="" type="checkbox"/>	Policy 2	Policy 2	Policy 2
Group 3	<input checked="" type="checkbox"/>	Policy 3	Policy 3	Policy 3
Group 4	<input checked="" type="checkbox"/>	Policy 4	Policy 4	Policy 4
Group 5	<input checked="" type="checkbox"/>	Policy 5	Policy 5	Policy 5
Group 6	<input checked="" type="checkbox"/>	Policy 6	Policy 6	Policy 6
Group 7	<input checked="" type="checkbox"/>	Policy 7	Policy 7	Policy 7
Group 8	<input checked="" type="checkbox"/>	Policy 8	Policy 8	Policy 8
Group 9	<input checked="" type="checkbox"/>	Policy 9	Policy 9	Policy 9

● ポリシー設定

設定パス : [Main Menu >> Users >> Policies >> Policy Configuration](#)

1. **Select Policy** を使用すると、管理者は設定するポリシープロファイルを選択できます。
2. **Firewall Profile** は、サービスプロトコル、ユーザーファイアウォールルール、および IPv6 ファイアウォールルールを定義するためのものです。
3. **Privilege Profile** (権限プロファイル) では、オンデマンドアカウント作成、パスワード変更権限、および最大同時セッション数を設定します。
4. **QoS プロファイル** を使用すると、管理者はトラフィック設定を編集できます。
5. **Specific Route Profile** (特定のルートプロファイル) では、管理者が特定の宛先にトラフィ

ックを転送するルーティングノードを静的に割り当てることができます。

6. **IPv6 traffic class and 802.1p mapping** (グローバルポリシーのみ) は、IPv6 トラフィックが VLAN IPv4 ネットワークに転送されているときに、IPv6 トラフィッククラスを 802.1p にマッピングします。

ドロップダウンリストで1つのポリシーを選択し、**Configure** をクリックして各属性の設定を開始してください。設定後、必ず **Apply** をクリックして変更を保存してください。グローバルポリシーは、ポリシープロファイルによって明示的に管理されていないすべてのサービスゾーンのすべてのユーザーに適用されるポリシーであることに注意してください。

- **スケジュール**

設定パス : [Main Menu >> Users >> Schedule](#)

スケジュールとは、時計の時間から 1 時間単位でユーザーのログインが許可されている期間を割り当てたものです。チェックされていないタイムスロットは、このポリシーの下にあるユーザーがその特定の時間間隔でログインできないことを意味します。

Schedule Permitted Login Hours - Profile 1

Select Schedule

Schedule Name

	Time	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<input type="checkbox"/>	SUN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
<input type="checkbox"/>	MON	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																					
<input type="checkbox"/>	TUE	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																					
<input type="checkbox"/>	WED	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																					
<input type="checkbox"/>	THU	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																					
<input type="checkbox"/>	FRI	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																					
<input type="checkbox"/>	SAT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					

Log off authenticated users during unauthorized periods

定義済みのスケジュールは、グループ設定に適用されます。

- **ユーザーのグループ化**

グループは、認証サーバー、クラス (RADIUS)、属性 (LDAP)、またはアカウント (ローカル、オンデマンド) によって決定されます。

通常、グループは認証オプションのすべてのユーザーに割り当てられます。

Users > Authentication > Auth Option > Group

ただし、次のような柔軟性があります。

- ローカルアカウントは、作成時にアカウントごとにグループを割り当てるか、既存のアカウントの次のパスから割り当てることができる。Users > Authentication > Local > Configure > [Local User List](#) > [username](#) (管理者が **Applied Group** 行を使用して属性を決定する)
- オンデマンドアカウントは、作成時にアカウントごとに個別にグループを割り当てることができる。
- RADIUS ユーザーは、RADIUS クラスに基づいて異なるグループに割り当てられるユーザーを持つことができる。Users > Authentication > RADIUS > Configure > [Class-Group Mapping](#) > [Configure](#) でマッピングを設定できる
- LDAP ユーザーは、LDAP 属性に基づいて異なるグループに割り当てることができる。Users > Authentication > LDAP > Configure > [Map LDAP Attributes to Group](#) でマッピングを設定できる

- ポリシーの優先度

ポリシーは、グループサービスゾーンのアクセス許可マッピングとサービスゾーンプロファイルで設定できます。

Authentication Settings

Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Suspend <small>When Authentication is set to Suspended, users would see a suspend message from General Settings.</small>
Access Permission and Authorization	Configure
Default Policy	Policy 1 ▾ <small>To set up policies, please go to Users > Policies.</small>
MAC Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <small>RADIUS Authentication using MAC address</small>
PPP Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
SIP Interface Configuration	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
WISPr Settings	Configure

ポリシー強制の優先順位は次のとおりです。

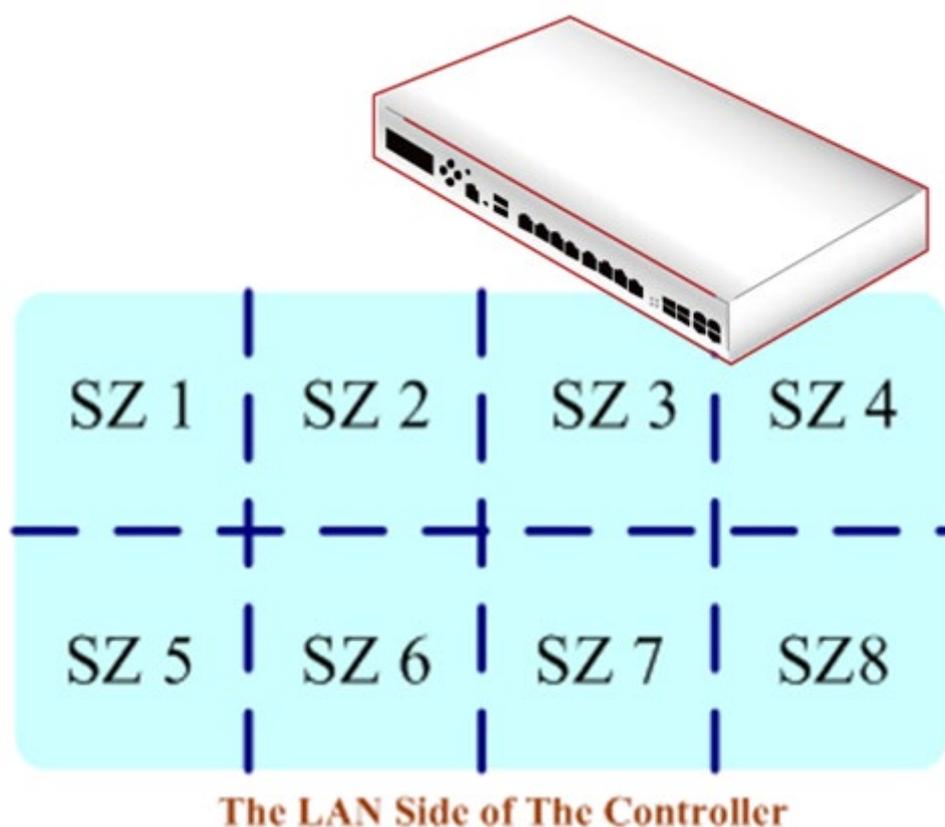
グループサービスゾーンマッピング > サービスゾーンのデフォルトポリシー > グローバルポリシー

したがって、管理者が特定のユーザーの設定階層でグループまたはポリシーを指定しない場合、システムはグローバルポリシーによって管理します。

第6章 基本的なサービスゾーン設定

5.3 サービスゾーンの概念

サービスゾーンは、Edgecore コントローラの物理 LAN 側の仮想パーティションです。VLAN と同様に、個別に管理および定義でき、独自のユーザーランディングページ、ネットワークインターフェース設定、DHCP サーバー、認証オプション、ポリシー、セキュリティ設定などを設定できます。固有の VLAN タグ（タグベースの場合）と SSID をサービスゾーンに関連付けることで、管理者は有線ネットワークと無線ネットワークを柔軟に分離できます。



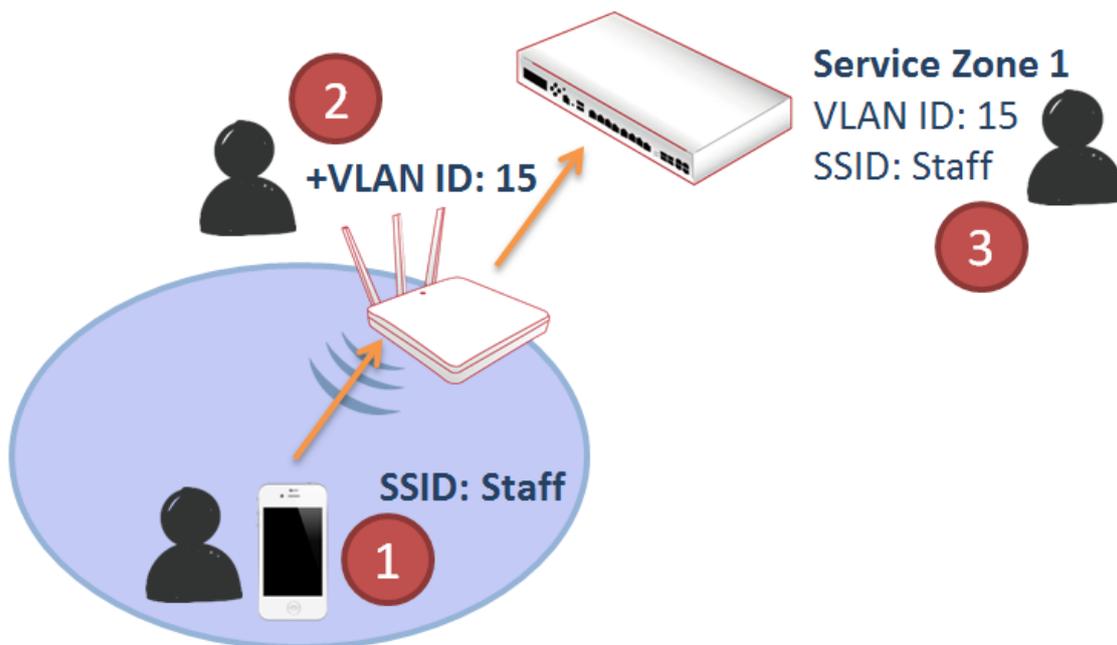
5.4 サービスゾーンの設定

6.2.1. タグベースまたはポートベースのサービスゾーン

Edgecore EWS コントローラは、物理 LAN ポートとサービスゾーンのマッピングに、ポートベースモードとタグベースモードの2つのモードを提供しています。直観的には、ポートベースモードは、各 LAN ポートが1つのサービスゾーンにサービスを提供するか、またはサービス

を提供しないことを意味します。したがって、サービスゾーンの最大数は、Edgecore EWS コントローラ上の LAN ポートの数に相当します。

逆に、タグベースのサービスゾーンは、LAN ポートに関係なく、管理者が事前に定義した VLAN タグ ID によって指定されるため、ポートの数に制限されません。下の図には、簡単なコンセプトが表示されています。



図に示すように、会社のスタッフは、アクセスポイントによる特定の SSID ブロードキャストに関連付けられています。この SSID は、VLAN ID 15 の VAP に属するとします。したがって、コントローラに転送された AP のトラフィックは、スタッフアクセス用の設定を使用してサービスゾーン 1 にマッピングされます。

設定のマッピング

設定パス : [Main Menu >> System >> LAN Ports](#)

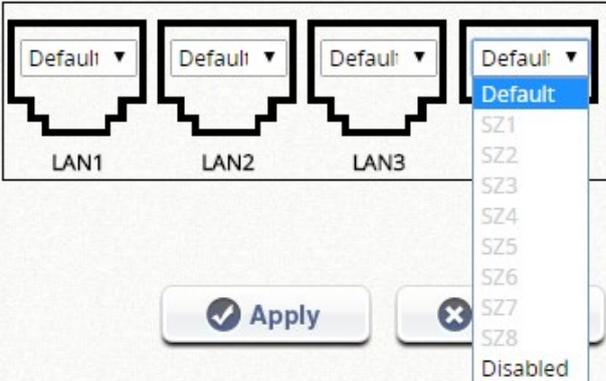
管理者は、サービスゾーンのタイプを変更できます。無効になっているため、一部のサービスゾーンがグレー表示されています。したがって、管理者はまず「System > Service Zones > Configure」の順に選択して、必要なサービスゾーンを有効にする必要があります。

LAN Ports

LAN Port Mode Port-Based Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping



LAN1 LAN2 LAN3

Apply Cancel

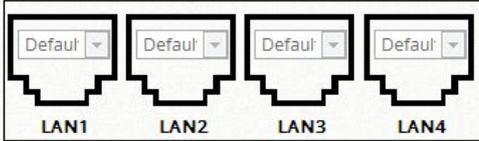
設定を **Tag-based** に変更すると、サービスゾーンとポートの対応がグレー表示されます。各サービスゾーンには、1~4096 の範囲で固有の VLAN ID を割り当てる必要があります。

LAN Ports

LAN Port Mode Port-Based Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

Port - Service Zone Mapping



LAN1 LAN2 LAN3 LAN4

デフォルトサービスゾーンは、ローカルアクセスポイントを管理し、タグ付けされていないトラフィックを処理するためにタグなしに設計されていることに注意してください。

6.2.2. NAT モードまたはルータモード

設定パス : [Main Menu >> System >> Service Zones >> Configure](#)

NAT は、アップリンクネットワークに転送する前に、コントローラの LAN 側のデバイスのプライベート IP アドレスをルーティング可能な IP に変換する Network Address Translation の頭字語です。プライベート IP アドレスは、コントローラの WAN 側のデバイスまたはルータには見えません。NAT を配置しているコントローラだけが対応する変換を認識します。このモードは、LAN 上のユーザーが外部デバイスから「見え」されないように保護するだけでなく、制限されたパブリック IP の問題も解決します。

ルータモードは、名前が示すように、コントローラへのアドレス変換なしで動作するネットワークです。ルータモードは、パブリック IP を使用する場合、またはダウンストリームデバイスがアップストリームルータへのルーティング可能な IP アドレスを必要とする場合に選択されます。

6.2.3. サービスゾーンネットワークインターフェース

設定パス : [Main Menu >> System >> Service Zones >> Configure](#)

IP address は、このサービスゾーンに接続されたユーザーへのコントローラ IP として機能します。**Subnet mask** は、サービスゾーンネットワークのサイズを定義し、このサービスゾーンにアクセスできる IP の範囲を定義します。ユーザーが範囲外のアドレスを使用できるようにするには、**Network Alias List** に IP を入力し、**Enable** (有効) にチェックを入れてください。完了したら、必ず **Apply** をクリックしてください。

システムがタグベースモードに設定されている場合、次の 3 つのアイソレーションオプションがあります。**Inter-VLAN Isolation**、**Clients Isolation**、および **None** です。

- **Inter-VLAN Isolation (VLAN 間アイソレーション)** : 同じ VLAN 内の 2 つのクライアントが、異なるポートから入ってくる时候お互いを見ることはありません。アイソレーションは、トラフィックがゲートウェイを通過するときに行われることに注意してください。スイッチまたは AP を配置する場合は、AP/スイッチでステーションアイソレーション

ンを有効にする必要があります。

- Clients Isolation : 同じレイヤ 2 ネットワーク上のすべてのクライアントは、このサービスゾーンで互いにアイソレーションされます。
- None (無し) : このサービスゾーンのクライアントにはアイソレーションが適用されません。

「None」(無し) を選択すると、スイッチでループ保護が有効で、かつ 1 つのサービスゾーンに属している VLAN が 2 つ以上ある場合、EWS の LAN ポートに接続しているスイッチポートがシャットダウンされることがあります。

メモ

1. Default のサービスゾーンは無効化できません。

6.2.4.DHCP サーバーオプション

設定パス : [Main Menu >> System >> Service Zones >> Configure](#)

動的ホスト構成プロトコル (DHCP) とは、特定のネットワークに対して設定された定義された数値の範囲 (スコープ) からサーバーが自動的にコンピュータに IP アドレスを割り当てることを可能にするネットワークプロトコルです。Edgecore EWS コントローラは、サービスゾーンプロファイルごとに独立した DHCP 設定をサポートします。オプションには、DHCP オプションを無効にする、組み込みの DHCP サーバーを有効にする、または DHCP リレーを有効にするなどがあります。

DHCP Enable DHCP Server

DHCP Server Configuration for Service Zone Default

No	Active	DHCP Scope	Start IP Address	End IP Address	Preferred DNS Server	Alternate DNS Server	Domain Name	Lease Time (mins)	WINS Server	Disregard Client's Name
1	<input checked="" type="checkbox"/>	Scope 1	192.168.1.1	192.168.1.100	192.168.1.254		domain.com	1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
2	<input type="checkbox"/>	Scope 2						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
3	<input type="checkbox"/>	Scope 3						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
4	<input type="checkbox"/>	Scope 4						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
5	<input type="checkbox"/>	Scope 5						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable
6	<input type="checkbox"/>	Scope 6						1440		<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Reserved IP Address List

DHCP Lease Protection Enable Disable

1. DHCP Server Configuration (DHCP サーバーの設定) — DHCP サーバーのデフォルト設定は「Enabled」(有効)です。ドロップダウンリストから他のオプションを選択してください。
2. DHCP サーバー (ビルトイン) の有効化を使用する場合に発行する IP 範囲を定義してください。設定には、合計 6 つの DHCP プールがあります。
3. 各プールでの DHCP リース時間は、アイドルタイムアウトの 2 倍の値より小さくすることはできません。
4. Reserving IP addresses (IP アドレスの予約) — DHCP サーバー IP 範囲内の特定の IP を、内部ファイルサーバーなどの特定のデバイス用に予約するための設定リストです。
5. DHCP lease protection (DHCP リース保護) — これは、有効にすると、リース期限切れの IP が現在オンラインになっているかどうかを確認するためのコントローラのオプションのチェックメカニズムです。はいの場合、コントローラはユーザーセッションが終了するまでこの IP アドレスの発行を停止します。
6. 「Apply」をクリックして変更を有効にしてください。

6.2.5. 認証オプション

設定パス : [Main Menu >> System >> Service Zones >> Configure](#)

管理者が Main Menu で認証サーバーを正しく設定すると、各サービスゾーンは、ダウンストリームクライアントに優先されるログイン用の認証オプションを選択できます。デフォルトでは、認証は常に有効になっていることに注意してください。

1. Databases

管理者は、使用する設定済みの認証サーバーを指定できます。複数の認証サーバーがサービスに対して有効になっている場合、接尾辞は認証サーバー識別子として使用されます。

Authentication Options					
Auth. Option	Auth. Database	Postfix	Default	Enabled	
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	
Server 2	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>	
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>	
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>	
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>	
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>	

2. Portal URL

ここで必要なランディングページの仕様を設定できます。有効にすると、管理者はユーザーの初回ログイン後に開いたブラウザの URL を設定できます。

Authentication Settings

Authentication Enable Disable Suspend
When Authentication is set to Suspended, users would see a suspend message from General Settings.

Access Permission and Authorization

Default Policy Policy 1 ▼
To set up policies, please go to Users > Policies.

Portal URL Specific Original None

*
(e.g. http://www.example.com)

MAC Authentication Enabled Disabled
RADIUS Authentication using MAC address

PPP Authentication Enabled Disabled

SIP Interface Configuration Enabled Disabled

WISPr Settings

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>

3. MAC address authentication (MAC アドレス認証)

RADIUS MAC 認証機能が有効になると、接続されたデバイスに設定された RADIUS サーバーに MAC アドレスが入力されている場合、コントローラは自動的に認証され、認証が成功する

とすぐにアクセスを許可します。ユーザーは、透過的なログインを経験します。

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input type="radio"/>	<input checked="" type="checkbox"/>

4. PPP dial-up authentication (PPP ダイアルアップ認証)

ポイントツーポイントプロトコル (PPP) とは、2つのネットワークノード間の直接接続を確立するために一般的に使用されるデータリンクプロトコルです。この機能がサービスに対して有効になっている場合、エンドユーザーは有効なユーザー名とパスワードを使用してダイアルアップ接続設定を設定できます (ローカルユーザーと RADIUS ユーザーのみをサポートします)。ダイアルアップ接続が確立されると、ユーザーは UAM ログインなしで正常に認証されます。

Authentication Settings

Authentication Enable Disable Suspend
When Authentication is set to Suspended, users would see a suspend message from General Settings.

Access Permission and Authorization

Default Policy Policy 1
To set up policies, please go to Users > Policies.

MAC Authentication Enabled Disabled
MAC Auth Server Server 2(radius)
RADIUS Authentication using MAC address

PPP Authentication Enabled Disabled

Assign IP Address From 172.50.0.1

Authentication Options

Auth Option	Auth Database	Postfix	Enable
Local	LOCAL	local	<input checked="" type="checkbox"/>
Server 2	RADIUS	radius	<input type="checkbox"/>

IP Address Range Assignment (IP アドレス範囲の割り当て) フィールドは、PPP がダイヤルアップ仮想インターフェースに IP アドレスを割り当てることができる開始 IP 範囲を設定します。割り当てられたインターフェース IP アドレスは、トンネルの両側のネットワーク間のルーティングに使用されます。

6.2.6. キャプティブポータルのカスタマイズ

設定パス : [Main Menu >> System >> Service Zones >> Configure](#)

各サービスゾーンには、固有のログインページまたはメッセージページを持つように設定できます。ログインページには 3 つのタイプがあります。一般ログインページ、PLM オープンタイプログインページ (ポートロケーションマッピングの無料アクセス用)、および PMS 請求プラン選択ページです。必要に応じて、サービス免責事項ページを有効にできます。これらのページは完全にカスタマイズ可能で、管理者には完全な柔軟性を提供します。メッセージページはカスタマイズでき、メッセージページには以下が含まれます。ログイン成功ページ、オンデマンドユーザーのログイン成功ページ、ログイン失敗ページ、デバイスログアウトページ、ログアウト成功ページ、ログアウト失敗ページ、およびオンラインデバイスリストです。

Login Page Customization

Service Disclaimer	Default	<input checked="" type="radio"/> Default <input type="radio"/> Customize with Template <input type="radio"/> Upload Your Own <input type="radio"/> Use External Page
General Login Page	Default	Enable Disclaimer <input type="checkbox"/> <input type="button" value="Preview"/>
PLM Open Type Login Page	Default	
PMS Billing Plan Selection Page	Default	

Theme for Template

Button Color: Grey Orange Green Blue Black

Upload Logo: No file selected.
 No File

The recommended dimension of the image is 360x120 with a size limit of 512 kB. It will be adjusted if the dimension does not fit.

Edgecore のデフォルトページとは別に、いくつかのカスタマイズオプションがあります。Customize with Template（テンプレートでのカスタマイズ）、Upload Your Own（独自のアップロード）、Use External Page（外部ページの使用）、Editor を使用できます。

Edgecore Default：ゲートウェイには、Edgecore ロゴが付いた標準の Edgecore デフォルトログインページがあり、管理者は必要に応じてサービス免責事項を有効にすることができます。

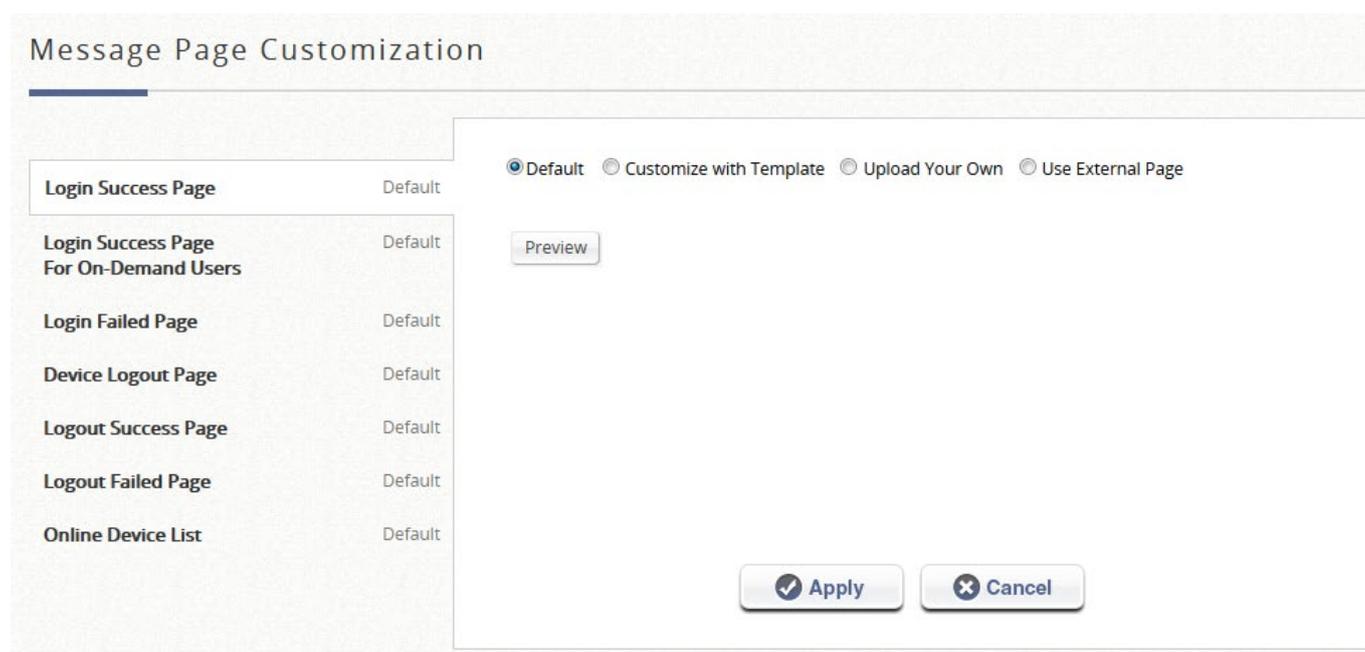
Customize with Template（テンプレートでのカスタマイズ）：このオプションでは、管理者が簡単にカスタマイズできるようにテンプレートが用意されています。一般的なレイアウトは管理者用に設定されていますが、内容は自分の好みに合わせてカスタマイズできます。カラーテーマとロゴをアップロードし、サービス免責事項などのコンテンツフィールド、テキストカラーをテンプレート内のレイアウトに入力することができます。

Upload Your Own（独自のアップロード）：管理者には、ログインページとして html ファイルをアップロードするオプションがあります。「Download HTML Sample File」（HTML サンプルファイルのダウンロード）では、編集元となるサンプル HTML コードを管理者に提供します。このサンプル HTML コードをダウンロードしたら、任意のブラウザでファイルを開き、右クリックして「View Page Source」（ページソースの表示）を選択してください。ファイルが.html 形式で保存されていれば、任意のテキストエディタで HTML コードを編集できます。

Use External Page（外部ページの使用）：ログインページには、定義済みの外部 URL を指定できます。このオプションでは、メッセージページと連携する URL パラメータの使用に関する広範な知識が必要であり、慎重に編成する必要があります。外部ログインページのカスタマイズの詳細については、ユーザーマニュアルの付録 C を参照してください。

Editor（エディタ）：ログインページは、見たままが得られる（WYSIWYG）エディタで編集することができます。エディタを使用すると、管理者はシンプルで直感的な方法でページ内の要素を追加、削除、または構成できます。現時点では、このオプションは一般ログインページでのみ使用できます。

カスタムページのプレビューを表示するには、「Apply」をクリックし、「Preview」ボタンをクリックしてください。同様に、メッセージページにもその 4 つのオプションを使用できます。



Message Page Customization

Login Success Page	Default
Login Success Page For On-Demand Users	Default
Login Failed Page	Default
Device Logout Page	Default
Logout Success Page	Default
Logout Failed Page	Default
Online Device List	Default

Default Customize with Template Upload Your Own Use External Page

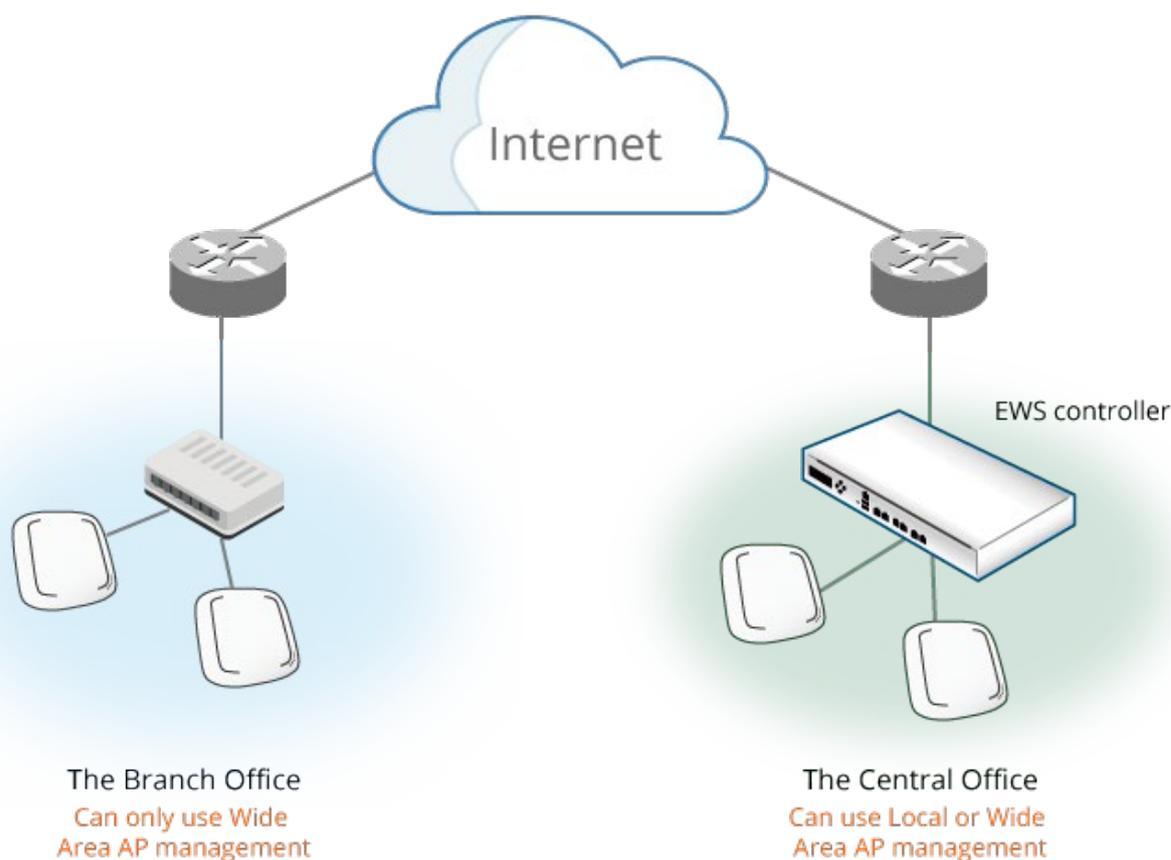
Preview

Apply Cancel

第7章 基本的な AP 管理

7.1. はじめに

アクセスポイントの管理は、ネットワーク管理者にとって常に重要です。したがって、Edgecore はそれを実現するためのシンプルでわかりやすい管理ツールセットを提供しています。一般的には、WAN 側と LAN 側の両方でアクセスポイントを担当するコントローラを備えた集中型ネットワークをお勧めします。インターネットやイントラネットの拡張性を考慮して、WAN 側の AP 管理を「ワイドエリア AP 管理」と呼び、LAN 側の AP 管理を「ローカルエリア AP 管理」と呼びます。以下は、これら 2 つの管理タイプの概念を示しています。



【ワイドエリアとローカル AP 管理図】

Edgecore EWS モデルは、Edgecore アクセスポイントによって管理性が異なります。つまり、管理者は、お使いの Edgecore EWS コントローラがサポートする AP モデルを確認する必要があります。

ローカル AP 管理用の管理可能な Edgecore アクセスポイントは、次の場所から確認できます。

[Main Menu >> Devices >> Local Area AP Management >> Overview](#)

AP Type List

AP Type	No. of AP	Online	Offline	No. of Client
EAP100	0	0	0	0
ECW100	0	0	0	0
ECW5210-L	0	0	0	0
ECW5211-L	0	0	0	0
ECW5410-L	0	0	0	0
ECW05210-L	0	0	0	0
ECW05211-L	0	0	0	0
ECW05212-L	0	0	0	0
ECW05213-L	0	0	0	0
OAP100	0	0	0	0
OAP100e	0	0	0	0
Others	0	0	0	0

ワイドエリア AP 管理用の管理可能な Edgecore アクセスポイントは、次の場所から確認できます。

[Main Menu >> Devices >> Wide Area AP Management >> Overview](#)

AP List

Type: All
Status: All
Tunnel: None

Name: Search

Refresh Interval: 60 seconds Refresh

Add Delete Add to Map / Floor Plan Backup Config Restore Config Upgrade Apply Settings Reboot Export Import

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number	Repair Method	From Template/Config
------	------	----	-----	-----	----------	--------	------------	--------	--------------	--------	---------	---------------	---------------	----------------------

大規模な AP 配置の場合、個別の AP 設定は非常に時間がかかり、実用的ではありません。

ローカルエリア AP 管理では、各 AP モデルに対して最大 8 つのテンプレートを使用できます。これには、主に無線バンド、データレート、送信電力、データレートなどの設定属性が含

まれます。AP を自動または手動で管理するために適用でき、AP を 1 つずつ設定する面倒なプロセスを回避できます。

ワイドエリア AP 管理には、管理者が集中管理で AP を設定するためのテンプレートもあります。

この章では、AP 管理の観点から無線ネットワーク環境を設定する方法について詳しく説明し、AP の検出と追加、一般的な AP 設定などの側面について説明します。このセクションでは、「不正 AP 検出」や「AP ロードバランシング」などの高度な設定ではなく、さまざまな一般的な AP 管理設定の明確な設定プロセスのみを扱っています。リファレンスガイドでは、上位レベルのアプリケーションについて紹介しています。

メモ

- 1.AP をサービスゾーンに追加する前に、管理者は事前にゾーンに一般的なワイヤレス環境を設定する必要があります。その環境は、ローカルで管理された AP にのみ適用されます。
- 2.各 AP には、管理下に 1 つの固有の IP アドレスも割り当てられます。タグベースモードでは、AP アドレスはデフォルトサービスゾーンの DHCP サーバーによって与えられます。ポートベースモードでは、AP は関連サービスゾーンの DHCP サーバーによって IP アドレスを割り当てられます。

7.2 ローカルエリア AP 管理 (EWS101、EWS5203、EWS5204、EWS5207)

設定パス : [Main Menu >> Devices >> Local Area AP Management](#)

このセクションでは、Edgecore EWS コントローラの LAN 側のアクセスポイントの管理について説明します。まず、コントローラの AP 管理リストにアクセスポイントを追加する方法論から始めます。その管理された AP にコントローラ上で適用できるユーティリティに至るまで、すべての方法を網羅しています。

メモ

1. LAPM 関連機能は Wi-Fi 6 AP ではサポートされていません。

7.2.1 AP リスト

設定パス : [Main Menu >> Devices >> Local Area AP Management >> AP List](#)

システム管理下のサポート対象の AP がすべてリストに表示されます。必要な AP タイプのチェックボックスにチェックを入れて、Apply をクリックすると、AP リストに表示されます。ドロップダウンリストから選択して、AP 名、IP アドレス、MAC アドレス、チャンネルに基づいて検索を行うことができます。さらに、テンプレート (ID) による検索の強化により、目的のテンプレートを採用した配備済み AP がフィルタリングされます。AP 名がハイパーリンクとして表示されます。管理対象の各 AP のハイパーリンクをクリックして、AP をさらに設定してください (一般設定、LAN 設定、無線 LAN、レイヤ 2 ファイアウォール)。AP の詳細ステータス情報 (システムステータス、サービスゾーンステータス、ワイヤレスステータス、アクセス制御ステータス、および関連付けられたクライアントステータス) を表示するには、表示されている各管理対象 AP のハイパーリンクをクリックしてください。

AP List

Type: All
Status: All
Tunnel: None
Template: 11 Search

Refresh Interval: 60 seconds Refresh

Add Delete Add to Map / Floor Plan Backup Config Restore Config Upgrade Apply Settings Reboot Export Import Users

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number	Repair Method	From Template/Config
<input type="checkbox"/>	EAP100	192.168.2.166	68:21:5F:2D:9C:8A	Overview	11	Online	1	Edit	System Overview Go	RUN	3.45.0000	EC1947004733	Disabled	

管理者は、必要な AP モデルを選択して AP リストをフィルタリングできます。AP タイプの AP モデルを確認し、「Apply」をクリックしてフィルタを適用してください。

1 つの AP または複数の AP を追加するには、「Add」ボタンをクリックしてください。これは、セクション 7.2.2 の AP の追加と検出で詳しく説明しています。

AP の有効化または無効化、テンプレートおよびサービスゾーンの適用などのオプションは、AP リストの左側にあるチェックボックスにチェックを入れ、それぞれのボタンをクリックす

ることで行うことができます。AP テンプレートの設定の詳細については、セクション 7.2.3 のテンプレートの設定を参照してください。監視には、更新間隔オプションがあり、管理者は各管理対象 AP の正確なステータスを把握できます。

すべてのファームウェアバージョンが EWS の AP 管理機能と完全に互換性があるわけではありません。「Status」列で互換性を確認してください。

7.2.2 AP の追加と設定の適用

設定パス : [Main Menu >> Devices >> Local Area AP Management >> AP List >> Add](#)

すべての AP が正しく接続されると、管理者は管理リストへの追加を開始できます。これは、AP リスト上にある「Add」をクリックすることで実現できます。AP は個別に、または一括で追加できます。これは「Add Method」（追加方法）によって決まります。ドロップダウンリストから「Add AP」を選択して AP を個別に追加するか、「Find Multiple APs」を選択して一括で追加してください。

AP を追加するには、AP 名を指定し、その IP アドレスと MAC アドレスを入力してください。赤いアスタリスクが付いた行は、必須の情報です。すべてのフィールドに入力したら、ページ下部にある **Apply** をクリックして AP を追加してください（AP を追加するには、必ずしもオンラインである必要はありません）。**AP List** をチェックして、追加を確認します。

Add Method Add AP ▾

Add An AP

AP Type ECW100 ▾

AP Name *

Admin Password

IP Address *

MAC Address *

Apply AP Template TEMPLATE1 ▾

Channel

RF Card A Default ▾

RF Card B Default ▾

APを一括で追加するには、管理者は IP アドレス範囲 をスキャンし、同じタイプの AP をまとめて検出します。

1. 「Factory Default」（工場出荷時のデフォルト）スキャン — 管理者が AP の設定を変更していない場合に使用します。そして、どのフィールドにも記入する必要はありません。**Scan Now** をクリックするだけです。
2. 「Manual」（手動）スキャン — AP の IP アドレスが 192.168.1.1 以外のアドレスに変更された場合に使用します。スキャンする IP アドレスの範囲を入力し、**Scan Now** をクリックしてください。

Find Multiple APs

AP Type ECW100 ▾

Service Zone Default ▾

Admin Settings Used to Discover

Factory Default

Manual

IP Address: ~

Login ID:

Password:

Scan Now

Discovery Results（検出結果）表には、現在生きているすべての AP が表示されます。AP を見つけたら、管理者は適用するテンプレートと動作チャンネルをさらに設定し、さらに有効にした特定のサービスゾーンに AP を配置できます。

メモ

1. コントローラが AP を検出するまでに時間がかかる場合があります。スキャン対象の AP が **Discovery Results**（検出結果）リストに表示されるまで、しばらくお待ちください。
2. 検出リスト上にある **Background** を有効にすると、管理者の設定に基づいて、一定時間ごとにワイヤレス環境をスキャンできます。**Configure** をクリックして、機能を設定してください。

それ以降の AP 設定の変更は、AP 名の下にあるハイパーリンクから行うことができます。[AP 名](#)のいずれかをクリックして、**一般設定**、**LAN インターフェース設定**、**ワイヤレスインターフェース設定**などの設定ページにアクセスしてください。

また、**再起動**、**有効化**、**無効化**、**削除**、**テンプレートの適用**、**サービスゾーン別に適用**、**デフォルトにリセット**を示すボタンが並んでおり、AP リストの内容を変更するための名前としては非常に直感的です。事前に 1 つまたは複数の AP を選択し、1 つの機能を実行してください。

Applying template（テンプレートの適用）は、管理者が事前に用意した基本的な無線パラメータなどの AP 設定を初期化するために設計されています。Edgecore のローカルエリア AP 管理機能は、管理者が実用的な使用期間を経て、SSID 名やワイヤレスセキュリティ事前共有キーなどの VAP 設定を変更したい場合に、設定を適用するための別のオプション、すなわち **Applying by Service Zone**（サービスゾーン別に適用）機能を提供しています。VAP が選択したサービスゾーンにマッピングされているかどうかを確認するだけです。

The image shows two side-by-side configuration panels. The left panel, titled 'Apply Template', features a dropdown menu with 'LAPM5211-L' selected, 'Apply', and 'Cancel' buttons. Below this is a table for the template configuration:

Template: LAPM5211-L	
Band	802.11g+802.11n / 802.11a+802.11n
Subnet Mask	255.255.0.0
Gateway	192.168.1.254

A red note below the table reads: "Note: If the Band of the template cannot match current Channel, the Channel will be changed to 'Auto'." The right panel, titled 'Apply by Service Zone', has a 'Service Zone' dropdown set to 'Default'. It includes fields for 'SSID' (containing 'SSID0'), 'Authentication' (set to 'Shared Key'), and 'Encryption' (set to 'WEP'). Under 'Encryption', there are fields for 'Key Length' (128 bits), 'Key Format' (ASCII), and 'Key Index' (Key1). Below these are four input fields for 'Key1', 'Key2', 'Key3', and 'Key4'. At the bottom are 'Apply' and 'Cancel' buttons.

7.2.3 テンプレートの設定

設定パス : [Main Menu >> Devices >> Local Area AP Management >> Templates](#)

冒頭で述べたように、管理者は AP 設定のテンプレートを使用して、面倒な AP 設定タスクを 1 つずつ排除できます。サブネットマスクやデフォルトゲートウェイなどの詳細な設定を表示するには、**Configure** をクリックしてください。異なるテンプレート名を持つレガシー AP と新世代 AP の両方に対応するテンプレートを、AP モデルごとに最大 8 つまで保存できます。

「Add Template」 ボタンをクリックしてテンプレートを増やし、Action 列の下に表示される「編集」アイコンをクリックして設定を編集してください。

Template AP Setting

Select Product Type: New Generation
Select Template: 1: vin1_6
Template Name: vin1_6
Country: United States
Radio: Configure
Wireless Network: Configure

Template AP Setting

Select Product Type: Legacy
Select Template: 1: vin1_5
Template Name: vin1_5
Country: USA
General Settings: Configure
VAP Configuration: Configure

AP Template

AP Model: ECW5211 Add Template

Template Name	Copy Settings from	Remark	Action
TEMPLATE1	NONE	Template 1	
TEMPLATE2	NONE	Template 2	

ここでは、AP のデフォルトゲートウェイなどの一般的な設定を行います。ワイヤレス設定と該当するサービスゾーン/SSID もここで設定できます。

Wireless

Band

Short Guard Interval

Channel Width

Data Rate

Short Preamble

Transmit Power

Beacon Interval (ms) (Default: 100; Range: 100 ~ 500)

VAP Configuration

Status	Profile Name	VLAN ID	Service Zone	SSID	WLAN Encryption	Action
<input checked="" type="checkbox"/>	VAP-1	0	Default	Default	NONE	 
<input checked="" type="checkbox"/>	VAP-2	0	Default	Default	NONE	 

Add VAP

SSID とワイヤレスセキュリティは、サービスゾーンごとに指定できます。配置のニーズによっては、個々のサービスゾーンの管理対象 AP デバイスにアクセスフィルタリングが課される場合があります。VAP Configuration (VAP 設定) リストの下にある Wireless Settings (ワイヤレス設定) セクションでは、Access Control (アクセス制御) リストを含むワイヤレス設定を指定できます。

管理者は、サービスゾーンごとに、認証と暗号化を含むワイヤレスセキュリティプロファイルを設定できます。利用可能なオプションは、オープンシステム、共有キー、WPA、WPA2 または WPA/WPA2 混合です。

WEP : 認証がオープンシステムまたは共有キーの場合、WEP が有効になります。

WPA2 : 認証が WPA の場合、WPA パーソナルまたは WPA エンタープライズは、WPA のオプションになります。WPA パーソナルでは、事前共有キーとしてパスフレーズまたは HEX を選択できます。

WPA/WPA2 混合 : 認証が WPA の場合、WPA パーソナルまたは WPA エンタープライズは、WPA のオプションになります。WPA パーソナルでは、事前共有キーとしてパスフレーズまたは HEX を選択できます。

MAC address フィールドは、管理者が拒否または許可する MAC アドレスを入力するためのフィールドです。ステータス「Denied」(拒否) は、ブラックリストを設定したことを意味しま

す。「Allowed」（許可）は、ホワイトリストを設定したことを意味します。「Disable」（無効）は、以下に設定されている MAC エントリに関係なく、アクセスフィルタリングが課されないことを意味します。

Status	MAC Address	コントローラによって実行されるアクション
Disabled（無効）		コントローラは、このサービスゾーンの AP に MAC ACL を適用しない
Allowed（許可）	Enabled（有効）	AP では、これらのアドレスを持つデバイスだけが、このサービスゾーンの AP に関連付けることを許可します。
Allowed（許可）	Disabled（無効）	AP では、これらのアドレスを持つデバイスがこのサービスゾーンの AP に関連付けることを許可しません。
Denied（拒否）	Disabled（無効）	これらのアドレスを持つデバイスは、このサービスゾーンの AP に関連付けることができません。
Denied（拒否）	Enabled（有効）	AP では、これらのアドレスを持つデバイスがこのサービスゾーンの AP に関連付けることを許可しません。

7.2.4.AP ファームウェア管理

強化された標準/機能のためにソフトウェアの強化の多くが定期的にリリースされているため、ファームウェアのアップグレードは重要です。Edgecore では、コントローラの AP 管理インターフェースから簡単にファームウェアのアップグレードプロセスが提供されるため、管理者は複数の AP デバイスを一度にアップグレードできます。



1. まず、ファームウェアを追加し、[Devices >> Local Area AP Management >> Firmware](#) でファームウェアファイルを選択し、行の横にある **Upload** をクリックして、AP ファームウェアをコントローラ内に保存してください。
2. [Devices >> Local Area AP Management >> Upgrade](#) で必要な AP をアップグレードし、バージョンをインポートしたい AP を選択してください。選択が完了したら、ページの下部にある **Upgrade** をクリックしてください。

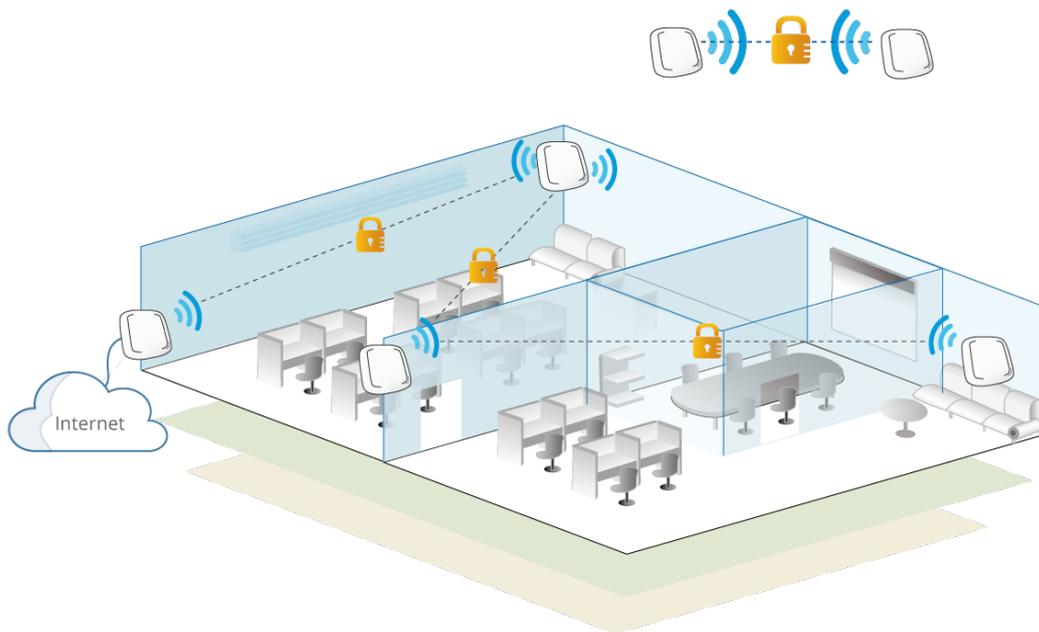
メモ

1. 予期せぬ結果を避けるため、各 AP ファームウェアのリリースノートをお読みください。

7.2.5 WDS リンク

設定パス : [Main Menu >> Devices >> Local Area AP Management >> WDS Management](#)

WDS は、Wireless Distribution System の頭字語で、追加の AP でネットワークの無線範囲を拡張する機能です。



【WDS 接続を示すシンプルなコンセプト図】

WDS 管理機能を使用すると、管理者は、管理された AP を使用して WDS ネットワークの「ツリー」構造を計画およびセットアップできます。

WDS Status

Refresh Interval Disable Auto Refresh ▼

WDS Tree	Security	Channel	Edit
No current WDS connection.			

WDS Update

Add WDS Connection

New Parent AP

New Child AP

Security Type None ▼

Move WDS Connection

Update Parent AP

Update Child AP

Delete WDS Link

WDS Status : WDS ツリーに追加された AP を、Security と Channel の設定とともに表示します。ネットワークには複数の WDS ツリーを設定できます。関連する WDS ツリーの WDS 接続設定を変更するには、Edit をクリックしてください。このリストは、一定の間隔（10 秒、20 秒、30 秒、40 秒、50 秒、60 秒）で自動的に更新されるように設定できます。

WDS Update : 新しい WDS 接続を追加するには、それぞれのドロップダウンリストから New Parent AP（新しい親 AP）と（新しい子 AP）を選択し、Add（追加）をクリックしてください。選択した親 AP が現在の WDS ツリーのいずれにもない場合、新しい WDS ツリーが追加されることに注意してください。現在の WDS ツリーを更新するには、それぞれのドロップダウンリストから Update Parent AP（親 AP を更新）と Update Child AP（子 AP を更新）を選択し、Move（移動）をクリックしてください。選択した更新子 AP の元の親 AP へのリンクが削除されることに注意してください。WDS リンクを削除するには、ドロップダウンリストから AP を選択し、Delete（削除）をクリックします。子 AP への WDS 接続を含め、選択した AP のすべての WDS 接続が削除され、有線接続のない子 AP には到達できなくなりますのでご注意ください。

7.2.6 不正 AP スキャン

不正 AP 検出は、ネットワーク環境を保護するもう 1 つの重要な方法です。ローカル AP 管理は、近くに存在する許可されていないアクセスポイントの検出をサポートします。

許可されていないアクセスポイントは、ワイヤレス干渉の観点から問題が発生する可能性があります。[Main Menu >> Devices >> Enter Local Area AP Management >> Rogue AP Detection](#) の順に選択して、この機能を設定してください。管理者は、スキャン間隔を決定し、スキャンジョブのための AP をセンサーとして選択し、安全なソースとして手動で識別できる場合は、疑わしい不正 AP リストに表示されている AP を信頼できるリストに追加する必要があります。

General Configuration

Rogue AP Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Apply
Scanning Interval	<input type="text" value="0"/> minutes	
Sensor List	0/0	Configure
Trusted APs	0/40	Configure

Rogue AP List

Add to Trusted AP List Delete

ESSID Search

<input type="checkbox"/>	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	RSSI	Report Time
--------------------------	----	----------------	-------	------	---------	------------	------	-------------

(Total:0) First Prev Next Last Go to Page (Page:1/1)

Row per Page:

検出されたアクセスポイントが一時的に不正 AP リストに入れられます。ハイパーリンクされている BSSID のいずれかをクリックすると、その詳細情報が表示されます。ただし、管理者が、リストされた AP の一部を信頼できると認識した場合は、BSSID 列の前のチェックボックスにチェックを入れて、**Add to Trusted AP List**（信頼できる AP リストに追加）をクリックしてください。このアクションは、**Trusted AP Configuration**（信頼できる AP 設定）に記録されます。

7.2.7 AP ロードバランシング機能

これは、管理対象 AP が過負荷にならないようにする機能です。システムは、状況において、AP の関連クライアント数が事前に定義されたしきい値を超えていることを検出し、同じグループ内の他の AP がまだしきい値を下回っている場合、バランシング機能は、過負荷の AP の送信電力を減少させ、他の利用可能な AP の送信電力を増加させるためにアクティブにされ、これにより、他の利用可能な AP が関連付けられる可能性が高くなります。システムは、管理対象 AP をグループに分割し、グループしきい値、および AP ロードバランシングをトリガーする時間間隔を定義できます。

ローカルエリア AP 管理機能は、さまざまな管理対象 AP のグループ化をサポートし、送信電力管理を実行して、同じグループの AP 間でネットワークの負荷をできるだけ均等に分散させます。

管理者は、AP ロードバランシング機能を適用する基準を指定できます。独自のロードバラン

シング開始基準を作成するためにカスタマイズできる属性には、強制間隔および関連するクライアントしきい値が含まれます。

LAPM Load Balancing

Load Balancing Enable Disable

Balance Interval minute(s)

Cluster 0/3

Device List

Add to AP Type

<input type="checkbox"/>	Cluster	Device Name	MAC Address	IP Address	Power Level	Clients	Log
--------------------------	---------	-------------	-------------	------------	-------------	---------	-----

AP デバイスのグループ化は、Device List ページで行うことができます。

7.3 ワイドエリア AP 管理

設定パス : [Main Menu >> Devices >> Wide Area AP Management](#)

ここでは、Edgecore EWS コントローラから WAN 上のアクセスポイントを集中管理する方法について説明します。WAN 側の AP には、インターネット上でルーティング可能なパブリック IP アドレスがあることが想定されていることは注目に値します。

ワイドエリア AP 管理の主な利点 :

- クロスレイヤ 3 IP ネットワーク管理
- 分散リモート AP サイトの一元化されたトラフィック転送。
- 簡単な参照と配置計画のためのグラフィカルマップユーティリティ。
- サードパーティの AP デバイスのトラフィック送信統計情報。
- CAPWAP サポート、完全なトンネルおよびスプリットトンネル。
- 指定した AP のオンラインユーザーを表示します。

ワイドエリア管理対象アクセスポイントの概要は、AP リストに記載されています。

設定パス : [Main Menu >> Access Points >> Wide Area AP Management >> AP List](#)

The screenshot displays the 'AP List' management interface. It includes filter controls for Type, Status, and Tunnel, a search bar, and a table of APs. Below the table is the 'AP Online All Users' section with a search bar and a table of active users.

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number	Repair Method	From Template/Config	
<input type="checkbox"/>	EAP100	EAP100	192.168.2.166	68:21:5F:2D:9C:8A	Overview	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	EC1947004733	Disabled	
<input type="checkbox"/>	EAP101(U.S)	EAP101	192.168.231.55	90:3C:B3:2D:34:BD	Overview	2	Offline	0	N/A	Go	N/A	12.4.0-959	EC2117003227	Disabled	
<input checked="" type="checkbox"/>	EAP101(U.S)	EAP101-vc_home	192.168.231.68	90:3C:B3:BB:21:0B	Overview	2	Online	1	N/A	Go	RUN	12.4.0-959	EC2107003706	Disabled	

User Name	IP Address	MAC Address	Host Name	SSID	Radio	Channel	Bytes In/Bytes Out	RSSI	SNR	Idle	Access From	Connected Time	Client OS	Log out
N/A	192.168.12.196	B4:F6:1C:5D:78:80	TSOU-tekii-iPad	VC-test-eap101-5G	5GHz	149	38M/1.746G	-50	52	16	EAP101-vc_home	64 hr 17 min 56 sec	iOS	Logout

1. ワイドエリア AP 管理を使用すると、コントローラの WAN 側と LAN 側に物理的に配置された AP を管理できます。
2. 各 AP の WAPM 機能の詳細については、ユーザーマニュアルの「付録 F」を参照してください。
3. インポート機能は、CAPWAP が有効なレガシーデバイスにのみ対応しています。レガシーデバイスについては、ユーザーマニュアルの付録 F を参照してください。

7.3.1. アクセスポイントの追加

設定パス : [Main Menu >> Access Points >> Wide Area AP Management >> AP List >> Add](#)

追加ページでは、管理者は、ステータスに関係なく、1つのアクセスポイントを管理リストに直接追加できます。デバイスの IP アドレス、名前、ログイン資格情報を設定し、SNMP コミュニティ文字列を設定し、Apply ボタンをクリックするだけです。

7.3.2. AP 検出による複数のアクセスポイントの検出

設定パス : [Main Menu >> Access Points >> Wide Area AP Management >> AP List >> Add](#)

AP 検出機能を使用すると、管理者は IP アドレスに到達できる限り、物理的な場所に関係なく AP をスキャンできます。IP スキャン範囲を設定できます。対象デバイスタイプを選択し、ス

キャン IP 範囲と管理者設定を定義して、「Discover」（検出）をクリックしてください。検出プロセスの後、新しく検出された AP が Device Results（デバイスの結果）に表示されます。管理者は、個々の AP デバイス名と SNMP コミュニティ文字列を指定できます。Add ボタンを選択し、クリックすると、検出された AP がリストに追加されます。

Discovery AP

Device Type

Admin Settings Used to Discover

Start IP Address	<input type="text"/>
End IP Address	<input type="text"/>
Login ID	<input type="text" value="admin"/>
Password	<input type="text" value="admin"/>

Device Results

<input type="checkbox"/>	Device Type	IP Address	Device Name	SNMP Community
--------------------------	-------------	------------	-------------	----------------

7.3.3 テンプレートを使用する AP 設定

テンプレートを使用した設定は、ワイドエリア AP 管理用に選択したモデルでサポートされています。

設定パス : [Main Menu >> Devices >> Wide Area AP Management >> Template](#)

Template AP Setting

Select Product Type	Legacy	▼	
Select Template	1: Template 1	▼	
Template Name	Template 1		Apply
Country	USA	▼	
General Settings	Configure		
VAP Configuration	Configure		
Security Settings	Configure		
Advanced Wireless Settings	Configure		
Hotspot 2.0 Settings	Configure		
Firewall Settings	Configure		
Linkyfi's Location Engine	Configure		
Copy Settings to	None	▼	Apply

テンプレートが用意されており、アクセスポイントの無線で設定可能なすべての機能をテンプレートから設定することができます。各モデルハードウェアのテンプレート数の詳細については、ユーザーマニュアルの付録 A を参照してください。

選択できるテンプレートには、2つの製品タイプがあります：**Legacy**と**New Generation**です。

● Legacy

アクセスポイントの**General Settings**（一般設定）には、バンド、チャネル、送信電力、送信レートなどの基本的なワイヤレス設定が含まれます。**VAP Settings**（VAP 設定）を使用すると、管理者は VAP を有効/無効にし、ESSID を指定し、必要に応じて対応するトンネルの有無に VLAN ID を割り当てることができます。必要に応じて、WEP、802.1X、WPA-Personal、WPA-Enterprise などの**Security Settings**（セキュリティ設定）を設定してください。

Advanced Wireless Settings（高度なワイヤレス設定）を使用すると、管理者はアクセスポイントのパフォーマンスと効率を微調整して、関連付けられたクライアントのワイヤレス接続品質を良好に維持できます。**Hotspot 2.0 Settings**（ホットスポット 2.0 の設定）は、異なるサービスプロバイダの無線 LAN ネットワーク間のローミングをサポートするためのものです。

Firewall Settings（ファイアウォールの設定）では、プロキシ ARP 機能を有効/無効にできます。**Linkyfi's Location Engine**（Linkyfi のロケーションエンジン）については、RTLS と DPI DNS を有効にして、Linkyfi のロケーションエンジンと統合してユーザートラッキングを行うこ

とができます。

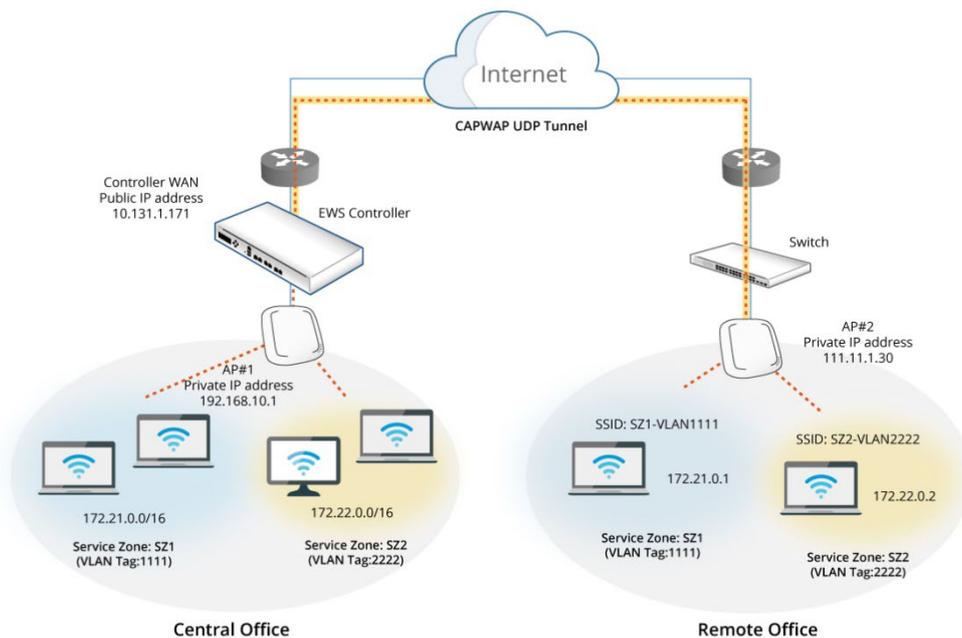
Template AP Setting	
Select Product Type	New Generation
Select Template	8: Template 8
Template Name	Template 8 Apply
Country	United States
Radio	Configure
Wireless Network	Configure
VLAN Settings	Configure
LAN Settings	Configure
Ethernet Settings	Configure
Services	Configure
User Accounts	Configure
Copy Settings to	None Apply

● New Generation

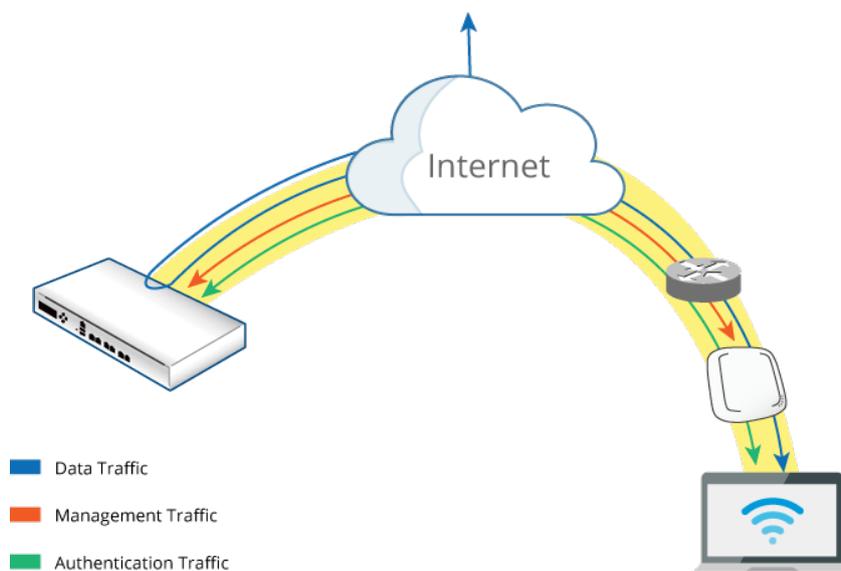
国名は、アクセスポイントと同じ国番号を選択します。アクセスポイントの Radio には、Band、Channel、Transmit Power などの基本的な無線設定が含まれています。ワイヤレスネットワークでは、VAP の有効/無効、SSID の指定、WPA-Personal/Enterprise、WPA2-Personal/Enterprise、WPA3 Personal/Enterprise、WPA3 Personal/Enterprise Transition、WPA3 Enterprise 192bit、OWE などのセキュリティの割り当てが可能です（必要な場合）。VLAN Settings は、SSID や他のインターフェースに使用する VLAN ID を作成するためのものです。LAN 設定 ローカルネットワークとゲストネットワークの LAN 設定を行います。Ethernet Settings は、Ethernet ポートのネットワーク動作を設定します。サービスでは、iBeacon の有効/無効を設定することができます。さらに、SSH、SNMP、NTP、マルチキャスト DNS など、関連するサービスもこのページで設定することができます。

7.3.4 CAPWAP を使用した AP の自動検出と設定

CAPWAP は、EWS コントローラが無線アクセスポイントの集合を管理できるようにする標準の相互運用可能なプロトコルです。トンネリングオプションには、完全なトンネルとスプリットトンネルの 2 つがあります。

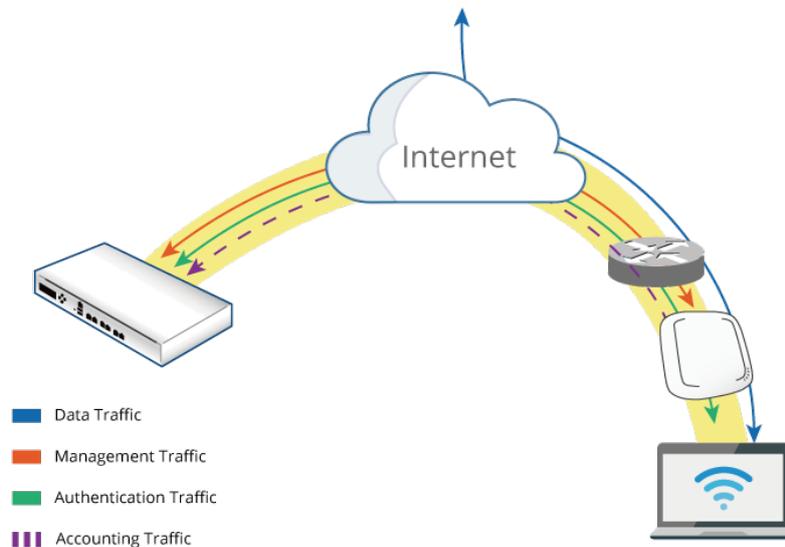


コンプリートトンネルは CAPWAP プロトコルを使用してアクセスポイントと通信します。これにより、提供されるサービスエリア AP からのすべての管理トラフィック、認証トラフィック、およびデータトラフィックが、データトラフィックをインターネットに転送する前に、コントローラに転送されます。EWS コントローラは、レイヤ 3 ネットワーク上で役割ベースのポリシーを実装でき、リモートサイトでユーザーアクセス制御を利用できます。この機能により、Edgecore EWS コントローラは、一元化された AP 管理とユーザー管理を完全にサポートできます。



スプリットトンネルの場合、ユーザー認証に関連するトラフィックだけがコントローラに送り

返されます。認証されたユーザーの場合、データトラフィックはローカルネットワーク経由でインターネットに直接送られます。ユーザーデータは、より短いパスで送信することができ、コントローラのネットワーク負荷も低減することができます。



設定手順：

1. Edgecore コントローラで、次の操作を行います。 [Main Menu >> Devices >> Wide Area AP Management >> CAPWAP](#) から CAPWAP を有効にします
2. コントローラの CAPWAP 設定で、同じ CA によって発行されたセキュリティ証明書が使用されていることを確認します。コントローラでの証明書管理については、このガイドの後続の章を参照してください。

Main > Device Management > Wide Area AP Management > CAPWAP

CAPWAP Configuration

CAPWAP Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Apply Certificate to APs	DEFAULT ▼
Trusted Certificate Authority(CA)	DEFAULT ▼
IP Address For Control Channel	100.64.145.254
IP Netmask For Control Channel	255.255.255.0 (253) ▼
Control Channel IP Range	100.64.144.1 ~ 100.64.145.253

3. コントローラが CAPWAP 検出および加入要求を検証するために、必要なセキュリティ証明

書を AP にアップロードします。

4. テンプレートの VAP Settings (VAP 設定) から CAPWAP テンプレートを設定します。VAP トラフィックは、コントローラの有効な SZ プロファイルにトンネリングされるように選択できます。トンネルインターフェースには 3 つのタイプがあります。**Disabled** (無効) はトンネルを確立しません。**Complete Tunnel** (コンプリートトンネル) は、すべてのデータをコントローラに転送するトンネルを作成します。一方、Split Tunnel は管理トラフィックと認証トラフィックのみをコントローラに転送します。管理者が各 VAP の Service Zone を選択する必要があるのは、後者の 2 つのトンネルインターフェースだけです。

VAP Configuration - 1: Template 1

Profile Name	RF Card A : VAP-1
VAP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Profile Name	VAP-1
ESSID	4ipnetAP-A1
Network Mode	Bridge
Uplink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
Downlink Bandwidth	0 Kbits/s *(1-1048576, 0:Disable)
VLAN ID	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
	VLAN ID 1234 *(1 - 4094)
CAPWAP Tunnel Interface	Split Tunnel
Service Zone	Default
Service Schedule	24/7 Service
Access Control Type	<input checked="" type="radio"/> Disable <input type="radio"/> MAC ACL Allow List <input type="radio"/> MAC ACL Deny List

5. On the AP side: レガシーデバイスの場合は、システム >> CAPWAP から CAPWAP 機能を有効にします。新世代デバイスの場合は、システム >> システム設定 >> 管理から EWS-Series Controller を選択し、管理者は有効化すべきいくつかの検出方法を確認できます：

(1) DNS SRV 検出

このタイプの検出では、DNS サーバーを使用して検出方法を完了します。取得した DNS SRV 記録を通じて、AP は CAPWAP 加入要求を送信するコントローラを認識します。

(2) DHCP オプション検出

AP が、接続しようとしている Edgecore EWS コントローラのサブネットと同じサブネットにある IP アドレスを取得するには、管理者が CAPWAP 機能とコントローラの DHCP サ

ーバーを有効にする必要があります。

(3) ブロードキャストの検出

AP は、サブネット内のすべての IP アドレスにブロードキャスト要求を送信します。

Edgecore EWS コントローラおよびその他のゲートウェイでは、ブロードキャストがサブネットワークを経由することを許可しません。機能を有効にする場合は、コントローラが AP と同じサブネットにあることを確認してください。

(4) マルチキャスト検出

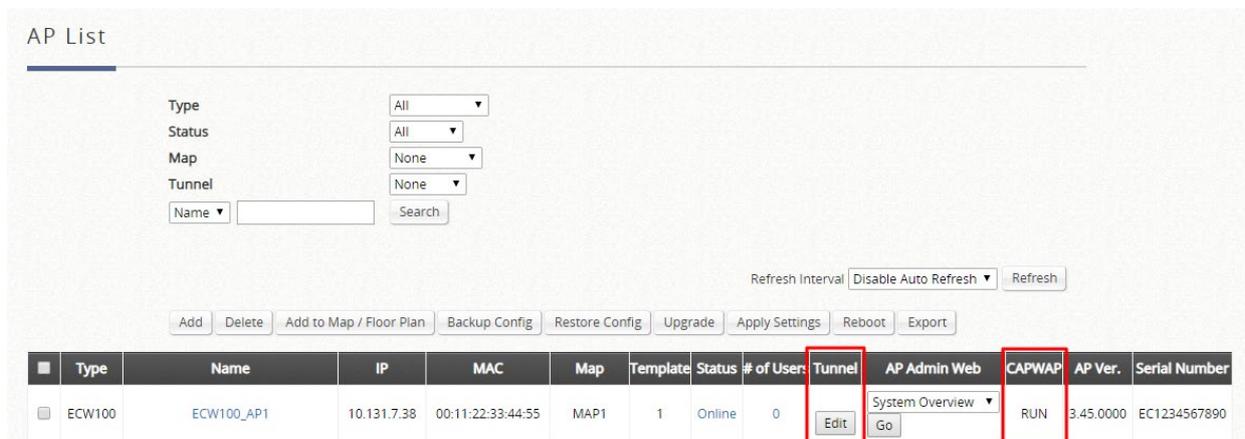
マルチキャスト検出は、正しいコントローラが応答することを期待して、ネットワークにマルチキャスト検出パケットを送信することによって機能します。この機能は、AP のルーティングパスに適切に設定する必要があります。関連する設定を有効にしてください。

(5) 静的検出

静的検出は、事前設定なしで直感的に実装できるため、最も推奨される検出方法です。機能を有効にして、この AP を接続する Edgecore EWS コントローラの IP アドレスを入力するだけです。

CAPWAP の加入に成功すると、次に示すように、AP が管理対象の AP list に表示されます。

CAPWAP 列には「RUN」ステータスが表示され、VAP がコントローラにトンネリングされるように設定されている場合、トンネルのステータスはクリック可能な「edit」ボタンが黒色で表示されます。



Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
ECW100	ECW100_AP1	10.131.7.38	00:11:22:33:44:55	MAP1	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	EC1234567890

AP WMI は、VAP が有効で、トンネルのステータスもシステム概要ページに表示されます。

- Legacy

LAN Interface

MAC Address	00:1F:D4:06:F1:1D
IP Address	10.73.7.38
Subnet Mask	255.255.0.0
Gateway	10.73.1.254

AP Status

RF Card Name : RF Card A ▼

Profile Name	BSSID	ESSID	Security Type	Online Clients	TUN
VAP-1	00:1F:D4:06:F1:1F	Guest Network	Open	0	

CAPWAP

Status	Run(10.71.1.81)
Data Channel	Active

IPv6

Status Disabled

AP WMI の VAP Configuration (VAP 設定) には、異なる VAP で動作している CAPWAP Tunnel Interface の種類も表示されます。

System Wireless Firewall Utilities Status

VAP Overview General VAP Config Security Repeater Advanced Access Control Hotspot 2.0

Home > Wireless > VAP Configuration

VAP Configuration

Profile Name : RF Card A : VAP-1 ▼

VAP : Disable Enable

Profile Name : VAP-1

ESSID : Guest Network

Network Mode : Bridge ▼

Uplink Bandwidth : 10 Kbits/s *(1-1048576, 0:Disable)

Downlink Bandwidth : 10 Kbits/s *(1-1048576, 0:Disable)

VLAN ID : Disable Enable
VLAN ID : 12 *(1 - 4094)

Uplink 802.1p : Best Effort (BE) ▼

CAPWAP Tunnel Interface : Split Tunnel ▼

Service Zone : SZ0 ▼

SAVE CLEAR

- 次世代

SERVICES

NAME	STATUS	MORE INFO
Edge-core Networks Cloud Agent Status	⊘ Disabled	The cloud agent (mgmtd) service is currently disabled.Go to system settings to enable it.
Hotspot (Chilli)	⊘ Disabled	The hotspot service is currently disabled. Included interfaces: <i>(no interfaces)</i>
Edge-core Networks EWS-Series Controller	● Enabled	The capwap service is running., CAPWAP status: RUN (10.131.5.110), Data Channel: Active

AP WMI の SSID Configuration は、異なる SSID でどの種類の CAPWAP Tunnel Interface が動作しているかも表示します。

NETWORK SETTINGS

Network Behavior	Route to Internet	▼
Network Name	Default local network	▼
CAPWAP Tunnel Interface	Disable	▼

メモ

1. CAPWAP テンプレートが VAP を選択して有効にし、SZ にトンネリングした場合、AP トンネルは自動的に確立されます。
2. CAPWAP 検出プロセスが失敗した場合は、コントローラで使用されている証明書設定と、AP にアップロードされた証明書を確認してください。
3. コントローラ CAPWAP ログは、トラブルシューティングプロセス中に参照されることがあります。

7.3.5 トンネリングされた VAP ロケーションマッピングの設定

設定パス : [Main Menu >> Devices >> Wide Area AP Management >> List](#)

リモート AP からコントローラにトンネリングされる VAP の場合、管理者は、NAS 識別子を割り当てるとともに、サービス用の IP プールを指定することもできます。

Wide Area AP Management の管理対象 AP List では、管理者は NAS 識別子を割り当て、管理対象 AP の VAP ごとにサービス用の IP プールを指定できます。これは、AP とコントローラの

間にトンネルを確立するときに設定できます。

AP List

Type: All
Status: All
Tunnel: None
Name: Search

Refresh Interval: Disable Auto Refresh Refresh

Add Delete Add to Map Backup Config Restore Config Upgrade Apply Settings Reboot Export

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
ECW5211-L	ECW5211-L	10.71.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	EC1912000687

(Total 1) First Prev Next Last Go to Page Row per Page 20

ECW5211-L: VAP Status

RF1				
Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-A1	1000	Configure	Default
RF2				
Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-B1	1000	Configure	Default

Tunnel Port Location Mapping Setup

Service Zone / Prefer DHCP Pool: Default / None

User Limitation: (Blank is for unlimited.)

ESSID: ECW5211-L-A1

Room Number / Location ID: *

Room Description / Location Name:

NAS Identifier:

Class:

HTTP Parameter:

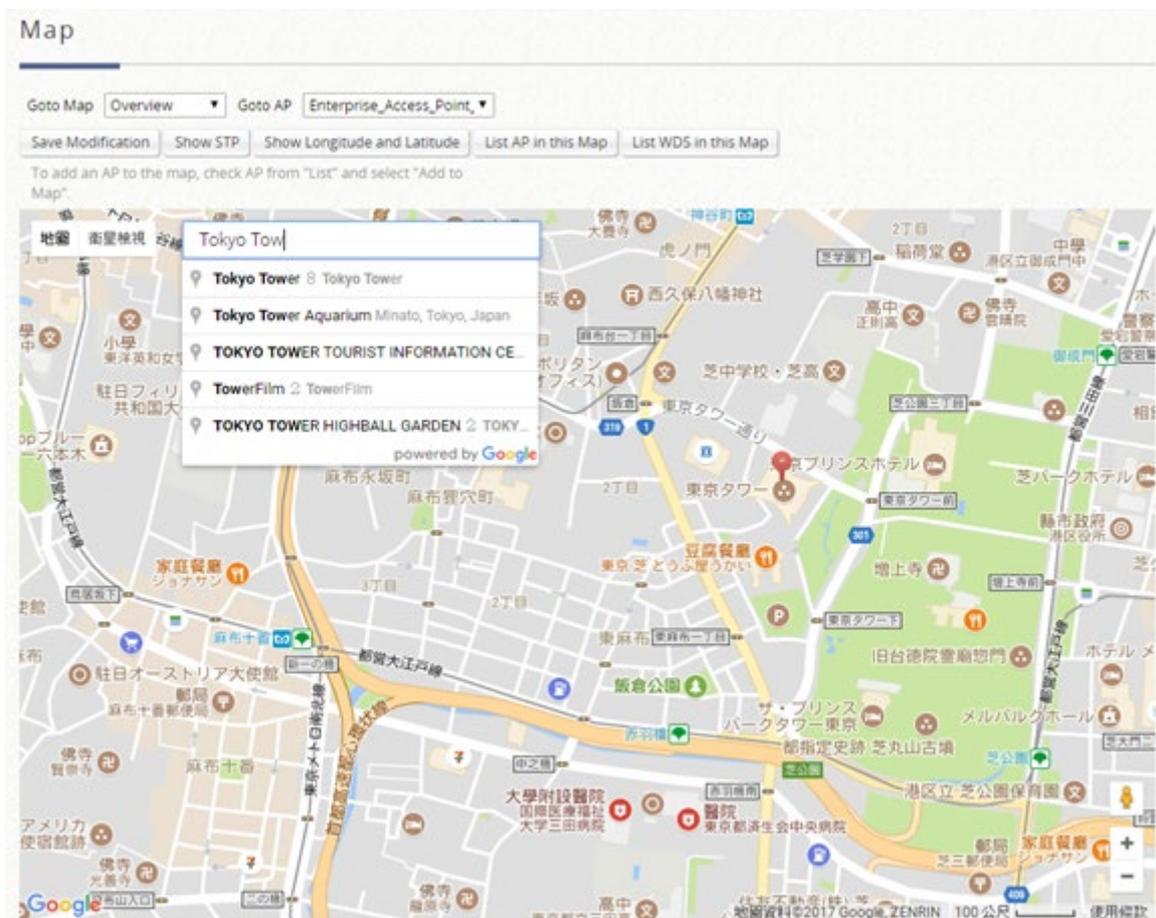
VAP がトンネリングバック、完全なトンネル、またはスプリットトンネルを PLM (Port Location Mapping) で設定すると、リモートサイトは PMS システムや、ロケーション属性や情報を必要とする、集中管理されたホットスポット操作の恩恵を受けることができます。

1. 本機能はレガシーデバイスにのみ対応しています。レガシーデバイスについては、ユーザーマニュアルの付録Fをご参照ください。

7.3.6 Google マップでのアクセスポイントの監視

マップは Google マップ API バージョン 3 で実装されており、管理者はワイドエリア AP 管理 (WAPM) の下にあるすべての AP の所在を一目で確認できます。この機能は、ネットワークの計画と管理に関して役立ちます。

管理者が管理リストに AP を追加すると、以下のように Google マップ API でこれらの AP にタグを付けたり、マークを付けたりして、その地理的位置を示すことができます。



マップを作成する手順は次のとおりです。

- ステップ1 ISP からパブリック IP アドレスを取得し、このアドレスを WAN インターフェイスに設定します。

ステップ2 Google Maps Registration key（Google マップ登録キー）を申請します。

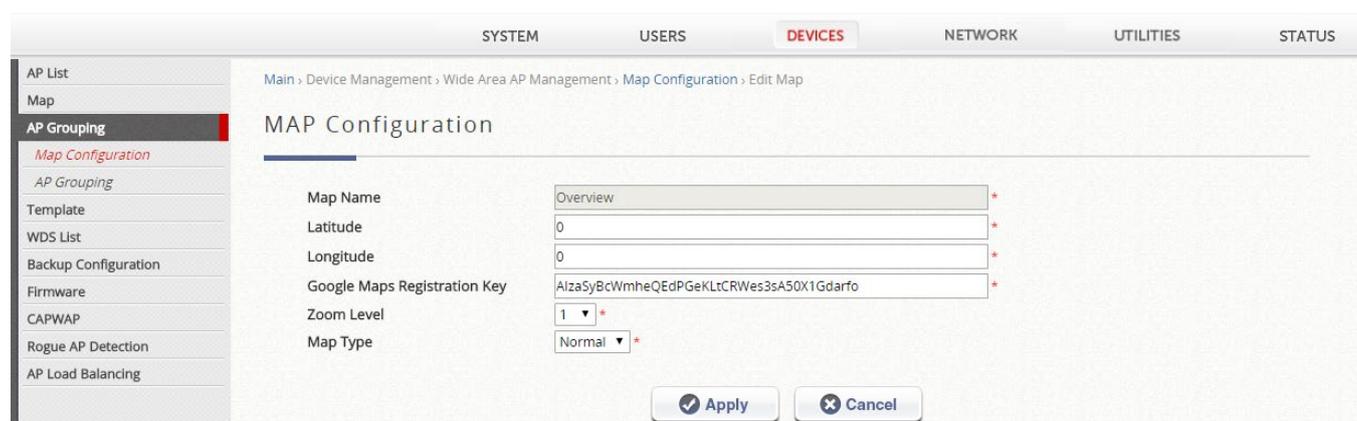
ステップ3 Map ページの Add a New Map（新しいマップを追加）ボタンをクリックします。Map Name（マップ名）と登録キーを設定します。

ステップ4 AP を検出し、これらの AP を管理対象リストに追加します。

ステップ5 List ページで、作成したマップにいくつかの AP を追加します。

AP 情報を使用してマップを構成するために必要な手順については、以降のセクションで説明します。

ワイドエリア AP 管理で新しい地図を追加する前に、Google アカウントにサインアップする必要があります。このアカウントは、Google マップ API v3 キーの申請に使用されます。詳細については、<https://developers.google.com/maps/documentation/javascript/v2/introduction> の Google の指示に従って、Maps API v3 キーを入手してください。Map Configuration（マップ設定）ページの「Google Maps Registration Key」（Google マップ登録キー）フィールドにキー情報を入力してください。



The screenshot shows the 'MAP Configuration' page in a web interface. The page has a navigation bar with tabs for SYSTEM, USERS, DEVICES, NETWORK, UTILITIES, and STATUS. The left sidebar contains a menu with items like AP List, Map, AP Grouping, Template, WDS List, Backup Configuration, Firmware, CAPWAP, Rogue AP Detection, and AP Load Balancing. The main content area is titled 'MAP Configuration' and contains the following fields:

Map Name	Overview
Latitude	0
Longitude	0
Google Maps Registration Key	AlzaSyBcWmheQEdPGeKltCRWes3sA50X1Gdarfo
Zoom Level	1
Map Type	Normal

At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

この Map Configuration（マップ設定）ページでは、このマップの Map Name（マップ名）と、Longitude（経度）と Latitude（緯度）で定義されている地理的位置を設定することもできます。表示する Zoom Level と Map Type も選択してください。

AP をマップに追加するには、まず AP List に移動し、AP 名をクリックして AP の緯度と経度を定義する必要があります。緯度と経度は、対象マップの位置を中心にしてください。このページでは、管理者は各 AP のマップ上に表示されるリンクや備考を設定することもできます。

Device : Enterprise_Access_Point

Device Name: Enterprise_Access_Point *

SNMP Community: public *modify snmp setting will reboot the AP

SNMP Write Community: private *modify snmp setting will reboot the AP

Latitude: 0 *-85 ~ 85

Longitude: 0 *-180 ~ 180

Remark:

Link 1: Name: Description: URL:

Link 2: Name: Description: URL:

Link 3: Name: Description: URL:

Apply Cancel

各 AP の場所を定義したら、AP List ページに戻ってください。マップ上にマークしたい AP を選択し、「Add to Map」(マップに追加) ボタンをクリックし、これらの AP をマークするマップの名前を選択し、「OK」ボタンをクリックしてください。

AP List

Type: All Status: All Map: None Tunnel: None Name: Search

Refresh Interval: Disable Auto Refresh Refresh

Add Delete **Add to Map / Floor Plan** Backup Config Restore Config Upgrade Apply Settings Reboot Export

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
<input checked="" type="checkbox"/>	ECW5211-L	ECW5211-L	10.71.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	Edit System Overview Go	RUN	3.45.0000	EC1912000685

(Total 1) First Prev Next Last Go to Page 1 Row per Page 20

Add to Map / Floor Plan

Add AP(ECW5211-L)

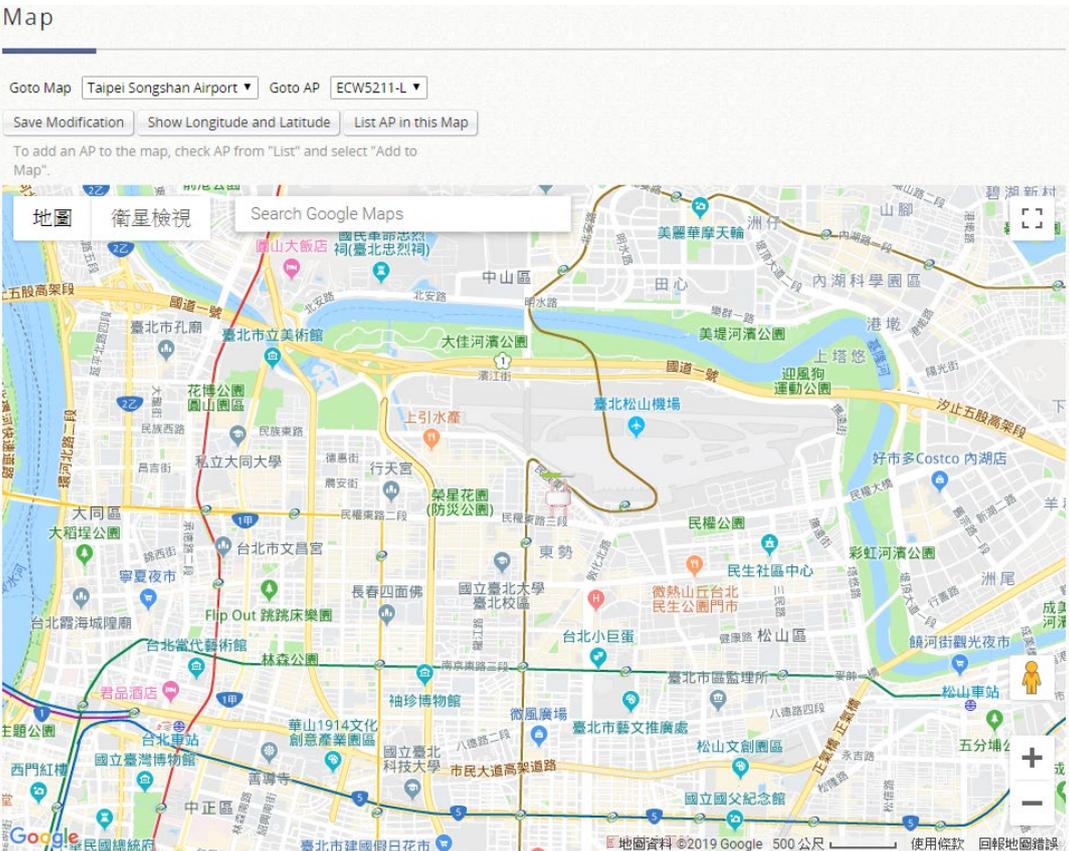
Add into a map

Select Map Taipei Songshan Airport ▾

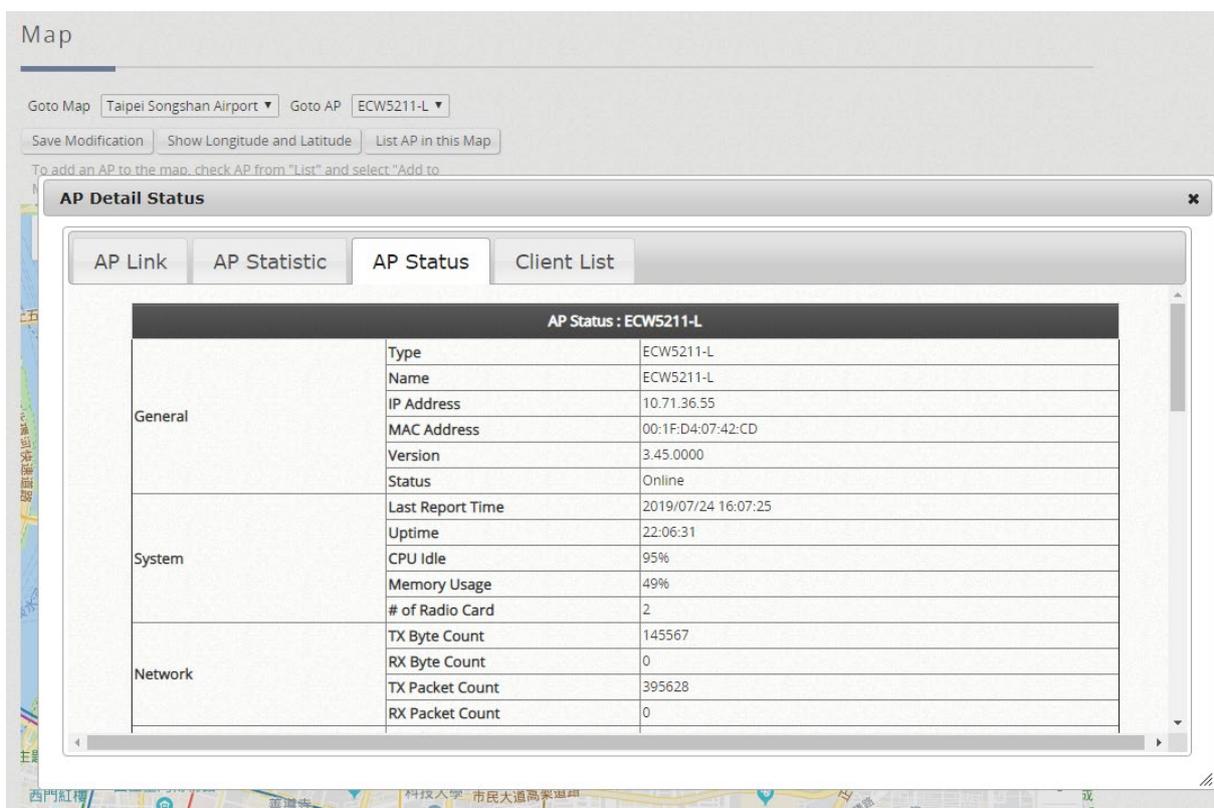
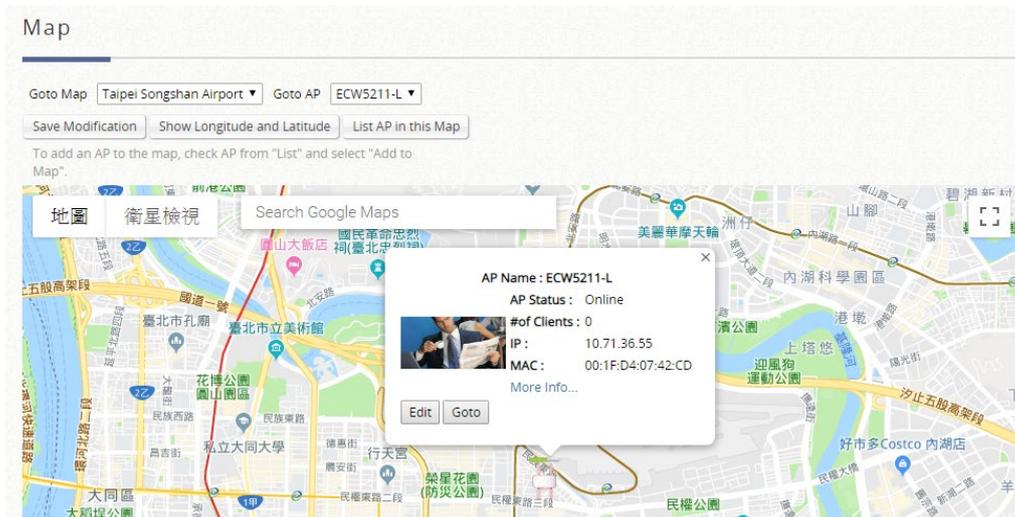
Add into a floor plan

Floor Plan Name Select an Option ▾

選択した AP は、以下に示すように、設定された物理座標でマーカイメージとしてマップ上に表示されます。



管理者は AP アイコンをクリックすると、設定済みの追加情報やリンクに関するダイアログボックスが表示されます。さらに、管理者は more info リンクをクリックすると、SNMP 経由でリモート AP から収集された AP Link、AP Statistic (AP 統計)、AP Status、Client List、WDS List、およびこの AP に関連する Links に関する情報が表示されます。



メモ

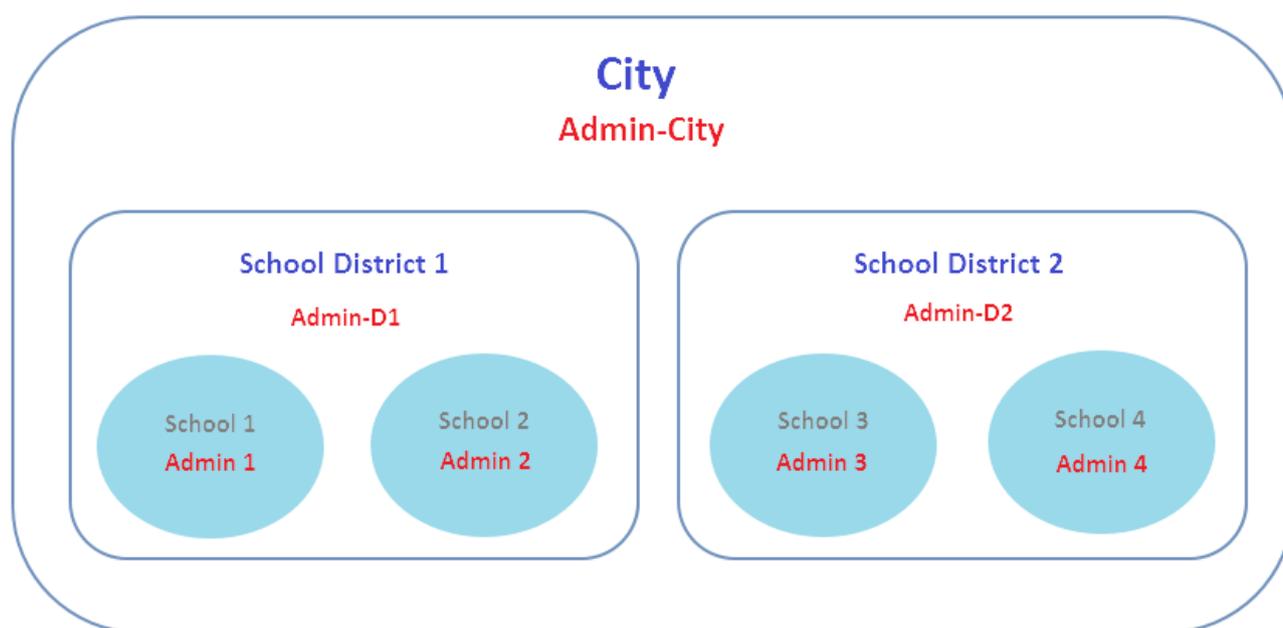
1. 「Overview」 マップは、システムのデフォルトマップです。このマップは、すべての管理対象 AP の概要を示します。
2. 管理リストに追加される AP は、「Overview」 マップに属します。
3. AP をマップに追加した後も、AP を「Overview」 マップで監視できます。

7.3.7 AP のグループ化

設定パス : [Main Menu >> Devices >> Wide Area AP Management >> AP Grouping >> Map Configuration](#)

Wide Area AP Management では、すべての管理対象 AP を、マップによって AP グループに指定する必要があります。各 AP は、マップに属するように設定する必要があります。すべての AP がデフォルトマップに追加されます。または、新しい AP を追加する前に、選択用の新しいマップを作成することもできます。

AP のグループ化を使用すると、異なるレベルの管理者が異なる AP グループで AP を管理できます。AP グループには、複数のマップと AP テンプレートを含めることができます。一方、マップを異なる AP グループに含めることができます。異なる管理者グループには、AP グループごとに異なる読み取り/書き込み権限を割り当てることができます。



【AP のグループ化の簡単な概念図】

AP のグループ化機能を使用するには、[Main Menu >> Devices >> Wide Area AP Management >> AP Grouping >> AP Grouping List](#) の順に選択して、AP グループを追加または削除してください。

AP Grouping

Add Delete

<input type="checkbox"/>	AP Group	Map	Template
<input type="checkbox"/>	456	123	1 3 5

Add をクリックして AP グループを追加してください。各 AP グループには、管理対象のマップとテンプレートを含めることができます。

AP Grouping Add

AP Group Name

test *

Map

Selectable

Selected

Overview
123

Template

Selectable

Template2
Template4
Template5
Template7
Template8

Selected

Template1
Template3
Template6

AP グループを作成したら、管理者グループを Administrator Group List に追加することによって、各 AP グループにアクセス許可を割り当てることができます。

Administrator Group List

Add Del

<input type="checkbox"/>	name	remark
<input type="checkbox"/>	Super Group	remark
<input type="checkbox"/>	Manager	remark
<input type="checkbox"/>	Operator	remark
<input type="checkbox"/>	On Demand	remark
<input type="checkbox"/>	Custom 1	remark
<input type="checkbox"/>	Custom 2	remark
<input type="checkbox"/>	Custom 3	remark

AP グループへの権限の割り当ててください。

	Disabled	▼	SZ7
	Disabled	▼	SZ8
AP GROUP	Disabled	▼	Select All
	Disabled	▼	456
AP Management	Read Only		
	Read/Write		
	Disabled	▼	Select All
Switch Management	Disabled	▼	Local Area AP Management
	Disabled	▼	Wide Area AP Management
	Disabled	▼	

7.3.8 不正 AP スキャン

不正 AP 検出は、ネットワーク環境を保護するもう 1 つの重要な方法です。ワイド AP 管理は、近くに存在する許可されていないアクセスポイントの検出をサポートします。

許可されていないアクセスポイントは、ワイヤレス干渉の観点から問題が発生する可能性があります。[Main Menu >> Devices >> Enter Local Area AP Management >> Rogue AP Detection](#)の順に選択して、この機能を設定してください。管理者は、スキャン間隔を決定し、スキャンジョブのための AP をセンサーとして選択し、安全なソースとして手動で識別できる場合は、疑わしい不正 AP リストに表示されている AP を信頼できるリストに追加する必要があります。

General Configuration

Rogue AP Detection Enable Disable

Scanning Interval minutes

Channel Switching Enable Disable

Sensor List 0/0

Trusted APs 0/40

Rogue AP List

ESSID

<input type="checkbox"/>	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	RSSI	Report Time
--------------------------	----	----------------	-------	------	---------	------------	------	-------------

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1)

Row per Page:

検出されたアクセスポイントが一時的に不正 AP リストに入れられます。ハイパーリンクされている BSSID のいずれかをクリックすると、その詳細情報が表示されます。ただし、管理者が、リストされた AP の一部を信頼できると認識した場合は、BSSID 列の前のチェックボックスにチェックを入れて、**Add to Trusted AP List**（信頼できる AP リストに追加）をクリックしてください。このアクションは、**Trusted AP Configuration**（信頼できる AP 設定）に記録されます。

メモ

1. 本機能はレガシーデバイスにのみ対応しています。レガシーデバイスについては、ユーザーマニュアルの付録 F をご参照ください。

7.3.9 AP ロードバランシング機能

これは、管理対象 AP が過負荷にならないようにする機能です。システムは、状況において、AP の関連クライアント数やネットワークトラフィックが事前に定義されたしきい値を超えていることを検出し、同じクラスタ内の他の AP がまだしきい値を下回っている場合、バランシング機能は、過負荷の AP の送信電力を減少させ、他の利用可能な AP の送信電力を増加させるためにアクティブにされ、これにより、他の利用可能な AP が関連付けられる可能性が高くなります。システムは、管理対象 AP をクラスタに分割し、しきい値、および AP ロードバラ

ンシングをトリガーする時間間隔を定義できます。クラスタを決定するために、Auto と Manual の 2 つのオプションがあります。方法が Auto の場合、システムは管理された AP をクラスタに分割することができ、距離の閾値と AP ロードバランシングをトリガーする時間間隔を定義することができます。方法が Manual の場合、管理されている AP を手動でクラスタに分割することができます。



ワイドエリア AP 管理機能は、さまざまな管理対象 AP のクラスタ化をサポートし、送信電力管理を実行して、同じクラスタの AP 間でネットワークの負荷をできるだけ均等に分散させます。

管理者は、AP ロードバランシング機能を適用する基準を指定できます。独自のロードバランシング開始基準を作成するためにカスタマイズできる属性には、強制間隔および関連するクライアントまたはトラフィックのしきい値が含まれます。

WAPM Load Balancing

Load Balancing Enable Disable

Method

Interval minute(s)

Threshold Number of Clients clients
 Number of Packets

Map Cluster Setting

Add to Cluster AP Type

<input type="checkbox"/>	Cluster	Device Name	IP Address	RF	Power Level	# of Users	Log
<input type="checkbox"/>	● None	ECW5211-L	10.131.5.12	1	Level 1 (20 dBm)	1	View
<input type="checkbox"/>	● None	ECW5211-L	10.131.5.12	2	Level 1 (20 dBm)	0	View
<input type="checkbox"/>	● None	EAP101	10.132.5.14	1	20 dBm	0	View
<input type="checkbox"/>	● None	EAP101	10.132.5.14	2	22 dBm	1	View
<input type="checkbox"/>	● None	EAP104ZZZZ	10.132.5.111	1	20 dBm	0	View
<input type="checkbox"/>	● None	EAP104ZZZZ	10.132.5.111	2	22 dBm	0	View

● Manual

方法が Manual に選択されている場合、リストで管理対象 AP を選択し、Apply ボタンをクリックして AP ロードバランシングクラスターに参加します。

WAPM Load Balancing

Load Balancing Enable Disable

Method

AP Distance meter(s)

Interval minute(s)

Threshold Number of Clients clients
 Number of Packets

Map Cluster Setting

Map

Cluster 0

Cluster	Device Name	IP Address	RF	Power Level	# of Users	Log
---------	-------------	------------	----	-------------	------------	-----

● Auto

方法が Auto に選択されている場合、AP ロードバランシングクラスターを作成するには、管理者がマップに AP を追加する必要があります。同じロードバランシングクラスター内の AP は、同じマップに存在する必要があります。AP をマップに追加した後、Main Menu >> Devices >> Wide Area AP Management >> AP Load Balancing で、Map Cluster Setting でマップを選択します。次に、「Create」ボタンをクリックすると、AP の各ペア間の距離に基づいて、このマップ上にクラスターが自動的に生成されます。クラスターが作成されたら、Configure ボタンをクリックして、各クラスターの AP ロードバランシング機能の有効/無効を設定することができます。

AP の場所が変更された場合（AP アイコンをマップ上の別の場所にドラッグし、「Save Modification」（変更を保存）ボタンをクリックするなど）、AP は自動的に再クラスター化されません。管理者は、まずマップ上の既存のクラスターを削除し、Create ボタンをクリックして、更新された位置情報に従ってクラスターを生成する必要があります。

一方、「AP Distance」（AP の距離）を変更すると、既存のクラスターは自動的に削除されます。クラスター化の更新された基準に基づいてクラスターを生成するには、Create ボタンをクリックする必要があります。

最後に、クラスターで AP ロードバランシング機能を有効にすると、各 AP の送信電力管理アクションのログを確認できるようになります。

第8章 ネットワーク環境の詳細設定

8.1 IPv4/IPv6 デュアルスタックネットワーク

設定パス : [Main Menu >> System >> IPv6](#)

Edgecore EWS コントローラは、IPv6 ネットワーク環境での動作をサポートします。IPv6 設定オプションが有効になっている場合、管理者は IPv4 IP アドレスと IPv6 アドレスをネットワークインターフェースの WAN1 または WAN2 のいずれかに割り当てることができます。選択

した WAN インターフェースに IPv6 アドレスを設定するには、Static、6to4、および go6 という 3 つの方法があります。ご使用の環境に適用できるオプションを選択してください。

IPv6 Setting

IPv6 Enable Disable

Interface WAN1 WAN2

Type Static (Use the following IPv6 settings)
 Use 6to4 transition
 Use go6 transition

Mode: Automatic Configured

IPv6 Address:

Prefix Length:

Preferred DNS Server:

Alternate DNS Server:

- **6to4** : 6to4とは、IPv4からIPv6に移行するためのインターネットの移行機構で、明示的なトンネルを設定することなく、IPv4ネットワーク（一般的にはIPv4インターネット）上でIPv6パケットを送信できるようにする仕組みです。6to4オプションは、選択したWANインターフェースに静的IPv4アドレスが設定されている場合にのみ選択できます。

- **IPv4/IPv6 ネットワークユーティリティ**

ネットワークユーティリティを設定するには、次の順に選択してください。 [Main Menu](#)
[>> Utilities >> Network Utilities](#)

システムには、管理者が簡単にネットワークを管理するのに役立つネットワークユーティリティが用意されています。

Network Utilities

Type IPv4 IPv6 Sniff IP Discovery

Ping

Trace Route

ARPing Interface

VLAN ID

ARP Table

Status

Result

Network Utilities

Type IPv4 IPv6 Sniff IP Discovery

Sniff

Controls:

The Sniff tool is for the administrator to capture packets from the selected "Interface".

The "Packet" field is to determine how many packets to capture.

If the information of the link layer is to be displayed, check the "Link Layer" box.

If the packet information is to be displayed in hexadecimal format, check the "Hex" box.

To further filter the types of packets, please enter the filtering "Expression" below following the syntax of Linux tcpdump command.

Example 1, to capture only TCP related packets occurring at port 23, type in "tcp port 23"

Example 2, to capture only ARP related packets, type in "arp"

Example 3, to capture only ICMP related packets, type in "icmp"

Interface Packet Link Layer Hex

Expression

Status

Result

項目	説明
IPv4	<ul style="list-style-type: none"> ▪ Ping : 管理者が IP アドレスやホストドメイン名を使用してデバイスを検出し、それが応答しているかどうかを確認することができます。 ▪ Trace Route : 管理者は、IP アドレスまたはホストドメイン名を使用して、ゲートウェイから宛先へのパケットの実際のパスを回復することができます。 ▪ ARPing : 管理者が特定の IP アドレスまたはドメイン名に対する ARP 要求を送信できるようにします。 ▪ ARP Table : 管理者は、アドレス解決プロトコル (ARP) で使用される、IP から物理アドレスへの変換表を表示できます。
IPv6	<ul style="list-style-type: none"> ▪ Ping : 管理者が IPv6 アドレスやホストドメイン名を使用してデバイスを検出し、それが応答しているかどうかを確認することができます。 ▪ Trace Route 6 : 管理者は、IPv6 アドレスまたはホストドメイン名を使用して、ゲートウェイから宛先へのパケットの実際のパスを回復することができます。 ▪ Neighbor Discovery (近隣検出) : 管理者は、この機能を使用して、同じ IP セグメントまたはドメイン名にある IPv6 近隣ノードを知ることができます。 ▪ Neighbor Cache (近隣キャッシュ) : ノードは、近隣キャッシュ内の近隣の情報を管理します。この機能により、管理者はシステムの近隣キャッシュに格納されている情報を表示できます。
Sniff	<p>この機能を使用すると、管理者は選択したインターフェースからのパケットをリッスンできます。管理者は、Expression フィールドの tcpdump コマンドを使用して、キャプチャするパケットのタイプをさらにフィルタリングできます。</p>

IP Discovery (IP 検出)	この機能を使用すると、コントローラは同じレイヤ2 ネットワーク内で接続されている AP の IP アドレスを検出できます。管理者は、検出された AP の IP 設定を変更することもできます。
Status	管理者がネットワークユーティリティ機能を実行している場合、操作の状態がここに表示されます。
Result (結果)	操作結果が表示されます。

8.2 ユーザーアクセス制御

ネットワークオペレータは、認証や関連付けから特定のアカウントやデバイスのアクセス性を制限したい場合があります。このセクションでは、ユーザーまたはデバイスの制限を実現する方法について説明します。

8.2.1 ブラックリスト

設定パス : [Main Menu >> Users >> Black List](#)

ブラックリストは、ユーザーアクセス制御のためのツールです。各ブラックリストには、ネットワークアクセスが拒否される特定のユーザーアカウントを保持できます。管理者は、プルダウンメニューを使用して、編集するブラックリストプロファイルを選択できます。

Select Blacklist 1: Blacklist1

Blacklist Settings

Blacklist Name: Blacklist1 [Apply]

[Add] [Delete]

User Name	Remark
(Total:0/40) *First *Prev Next* Last* Go to Page (Page:1/1) Row per Page: 10	

Adding User(s) to Blacklist1

40 users can be added to this Blacklist.

No.	Username	Remark
1	<input type="text" value="User1"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

Username の空白フィールドにユーザー名を入力し、**Remark** の空白フィールドに関連情報を入力（必須ではありません）したら、**Apply** をクリックしてユーザーを追加してください。

ブラックリストからユーザーを削除するには、ユーザーの **Delete** ハイパーリンクを選択して、そのユーザーをブラックリストから削除してください。

Select Blacklist 1: Blacklist1 ▼

Blacklist Settings

Blacklist Name

<input type="checkbox"/>	User Name	Remark
<input checked="" type="checkbox"/>	User1	

ブラックリストのセットアップが完了したら、必要な認証サーバーでブラックリストを選択すると、ブラックリストが有効になります。

Local Authentication

User Postfix	local
Blacklist	1 : Blacklist1
Local User List	Configure
Account Roaming Out	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
802.1X Authentication	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

8.2.2 MAC ACL

設定パス : [Main Menu >> Users >> Additional Controls](#)

MAC ACL は、アクセスフィルタリングのために特定の MAC アドレスを許可または拒否することができる MAC アドレスアクセス制御リストです。MAC ACL 許可ユーザーには、引き続きユーザー認証が必要です。**Configure** をクリックして、**MAC アドレス制御** リストに入ってください。**Add MACs** をクリックして必要な MAC アドレスを入力し、**Allow** (許可) または **Deny** (拒否) を選択して **Apply** をクリックしてください。

MAC Access Control List

MAC Access Control List

Configure

MAC Access Control is used to grant or deny permission to access the User Login Page.

List Type Allow Deny Disable

Access Control List

Add MACs Delete

No.	MAC Address
-----	-------------

(Total:0/400) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1)

Row per Page: 20

メモ

1. MAC アドレスの形式は xx:xx:xx:xx:xx:xx または xx-xx-xx-xx-xx-xx です。コロンは、システムによって自動的に挿入されます。

8.3 認定

設定パス : [Main Menu >> Utilities >> Certificate](#)

EWS アクセスコントローラは、プライベートネットワークで管理する AP に証明書を発行できません。管理者は、システムのルート CA が発行する証明書に署名し、管理された AP にこれらの証明書をロードすることができます。これらのセキュリティ証明書は、AP と AC の間の CAPWAP 検出要求の ID と信頼性の検証に使用されます。また、ローミングアウトする組み込み RADIUS サーバーのユーザーの認証にも使用できます。「Certificate Management」(証明書管理)には、利用可能な証明書と現在使用中の証明書の概要が表示されます。

Certificate Management

Cert Name	Common Name	Used by
System Certificate 		
Default Certificate	CN=gateway.example.com	WEB Server, Built-in RADIUS, CAPWAP
Internal Root CA 		
Internal Root CA	N/A	
Internally Issued Certificate 		
N/A	N/A	
Trusted Certificate Authorities (CA) 		
N/A	N/A	

設定に入るには、各カテゴリの左上隅にある「編集」アイコンをクリックしてください。

8.3.1. システム証明書

これは、システムを識別する証明書です。これらの証明書は、HTTPS ログイン、CAPWAP などのアプリケーションに使用できます。コントローラには、削除できない出荷時デフォルト証明書 (gateway.example.com) が組み込まれていますが、証明書のアップロードは許可されています。Re-generate (再生成) ボタンを使用すると、管理者はゲートウェイの MAC アドレスに基づいて独自の証明書を自動的に生成できます。証明書の詳細を表示するには、対応する View (表示) ボタンをクリックしてください。

System Certificate

Cert Name	Common Name	Operation	
Factory Default Certificate			
Factory Default Certificate	CN=gateway.example.com	View	Regenerate
Internally Issued Certificate			
N/A	N/A	View	Delete
Uploaded Certificate			
N/A	N/A	View	Delete Upload Intermediate/Root CA Verify

Certificate

DEFAULT	
Subject	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com
Issuer	C=US ST=US L=CA O=EXAMPLE,INC CN=gateway.example.com
Validity	2020/08/13 10:36:37
<input type="button" value="Get CERT"/> <input type="button" value="Get Key"/>	

証明書と公開キーをローカルディスクにダウンロードするには、「Get CERT」（証明書を取得する）と「Get Key」（キーを取得する）をクリックしてください。

証明書/秘密キー/中間 CA をアップロードするには、「Browse」（参照）をクリックして適切なファイルを選択し、Upload Files（ファイルをアップロードする）をクリックしてください。

Upload System Certificate

Certificate	<input type="text"/>	<input type="button" value="Browse..."/>
Private Key	<input type="text"/>	<input type="button" value="Browse..."/>
Intermediate CA	<input type="text"/>	<input type="button" value="Browse..."/>
Certification Path Verification	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
<input type="button" value="Upload Files"/>		

8.3.2.内部ルート CA

管理者は、内部ルート CA をアップロードし、またはプライベート用にルート CA を生成することができます。作成されたルート CA 証明書をダウンロードして、システムによって生成された証明書に署名するために使用できます。システムでは、内部ルート CA を 1 つしか作成できないことに注意してください。

Generate Root CA

Common Name	<input type="text"/>
Email Address	<input type="text"/>
Country Name	<input type="text"/>
State or Province Name	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Key Type	RSA ▾
Key Length	512 ▾

内部ルート CA をアップロードするには、Browse（参照）をクリックしてローカルディスクから証明書と一致する秘密キーを選択し、「Upload Files」（ファイルをアップロードする）をクリックしてください。

内部ルート CA がアップロード/生成されると、詳細は次の形式で表示されます。

Internal Root CA

Cert Name	Common Name	Operation
Internal Root CA		
Root CA	CN=4ipnet.com	<input type="button" value="View"/> <input type="button" value="Delete"/>

証明書の詳細を表示するには、View（表示）ボタンをクリックしてください。

8.3.3. 内部発行証明書

内部発行証明書は、このページで生成できます。内部発行の証明書に署名する前に、内部ルート CA を最初に作成する必要があることに注意してください。Certificate Information（証明書情報）は、現在発行されているすべての内部発行証明書を表示する概要です。証明書の詳細を表示するには、対応する View（表示）ボタンをクリックしてください。

Certificate Information

Cert Name	Common Name	Operation
Internally Issued Certificate		
cert1	CN=4iptest.com	View Delete

Use Internal Root CA to generate certificate

Common Name	<input type="text"/>
Email Address	<input type="text"/>
Country Name	<input type="text"/>
State or Province Name	<input type="text"/>
Locality Name	<input type="text"/>
Organization Name	<input type="text"/>
Organization Unit Name	<input type="text"/>
Key Type	RSA ▾
Key Length	512 ▾

[Generate Certificate](#)

8.3.4. 信頼できる証明書発行者

自己署名証明書とシステムのルート CA とは別に、管理者は、他の CA エンティティまたは信頼できる CA によって署名された他の証明書をシステムにアップロードすることもできます。これらの信頼できるルート CA 証明書は、コントローラが外部支払いゲートウェイおよび/または CAPWAP 対応 AP の証明書を認識し、信頼するためのものです。信頼できる CA をアップロードするには、browse（参照）をクリックして証明書を選択し、Upload Files（ファイルをアップロードする）をクリックしてください。証明書の詳細を表示するには、対応する View（表示）ボタンをクリックしてください。

Trusted Certificate Authorities (CA)

Cert Name	Common Name	Operation
Certificate Authorities (CA)		
N/A	N/A	<input type="button" value="View"/> <input type="button" value="Delete"/>

Upload Trusted CAs

Certificate

8.4 管理アクセス

設定パス : [Main Menu >> System >> General >> Management IP Address](#)

EWS アクセスコントローラでは、管理者は WAN または LAN の両方から特定の IP アドレスまたは IP アドレスの範囲をリストで指定することで、Web 管理インターフェースへのアクセスを許可できます。例えば、「192.168.3.1」と「192.168.1.0/24」を入力すると、192.168.3.1 のデバイスと 192.168.1.0～192.168.1.255 の範囲のデバイスだけが Web 管理インターフェースに到達できることを意味します。

Remote Console が有効になっている場合、コンソールインターフェースにリモートでアクセスできます。セキュリティ上の理由から、コンソールアクセスはデフォルトで無効になっており、悪意のあるユーザーがシステムにアクセスできないようにしています。

第9章 コントローラ管理用ユーティリティ

9.1 EWS コントローラ管理

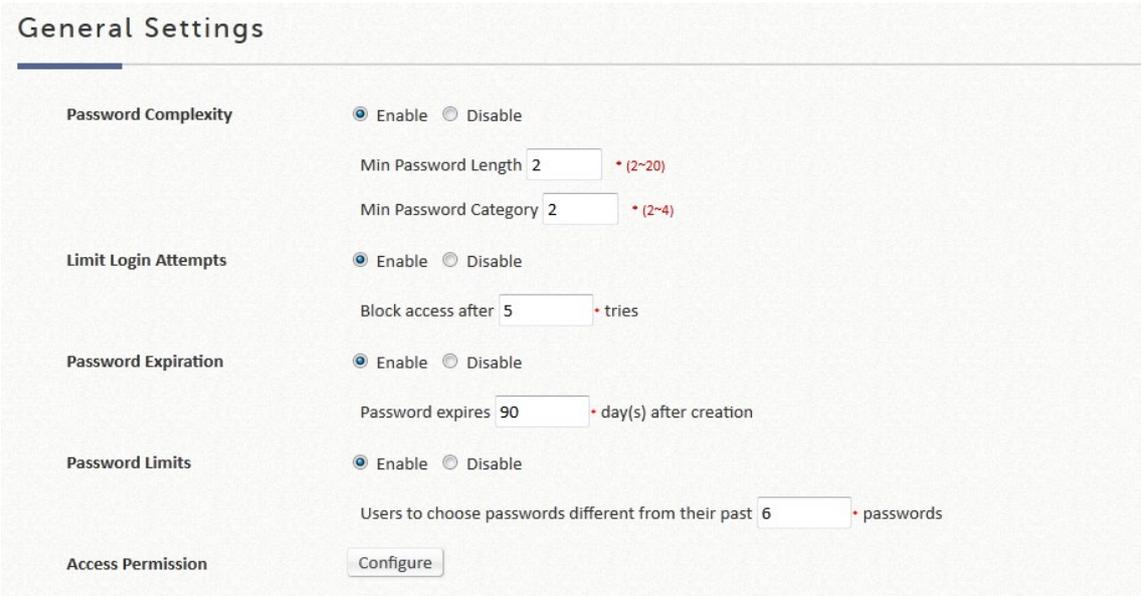
設定パス : [Main Menu >> Utilities >> Administrator Account](#)

EWS コントローラのルート管理アカウントは、フルアクセス、変更、アプリケーションの特権と権限を持つ「管理者」アカウントです。ただし、管理担当者が指定した権限領域にアクセスするために作成できる、権限の低い第2階層のアカウントがあります。これは、複数の管理担当者を必要とする大規模な展開に必要な機能です。

この設定パスは、権限プロパティを割り当てるページと、ネットワークのニーズに合わせてカスタマイズ可能な他の管理アカウントを生成するためのページにつながります。

デフォルトの状態では管理アカウントが1つだけです。**Group Permission Settings**（グループのアクセス許可設定）では、特定の管理グループに対してアクセス可能な WMI ページをカスタマイズし、そのグループの管理アカウントを作成できます。

ステップ1：パスワードの安全設定



The screenshot shows the 'General Settings' page with the following configuration options:

- Password Complexity:** Enable Disable
Min Password Length: 2 (range 2-20)
Min Password Category: 2 (range 2-4)
- Limit Login Attempts:** Enable Disable
Block access after: 5 tries
- Password Expiration:** Enable Disable
Password expires: 90 day(s) after creation
- Password Limits:** Enable Disable
Users to choose passwords different from their past: 6 passwords
- Access Permission:**

パスワードの安全性を有効にして、Web 管理インターフェースを権限のない担当者から保護することができます。これらの設定はデフォルトで無効になっています。

ステップ 2 : グループアクセスプロパティの設定

Main > Utilities > Administrator Accounts > Administrator Group > Administrator Group Edit

Administrator Group Edit

Admin Group Name	Custom 1 *
Remark	
Service Zone	Disabled ▼ Select All
	Disabled ▼ Default
	Disabled ▼ SZ1
	Disabled ▼ SZ2
	Disabled ▼ SZ3
	Disabled ▼ SZ4
	Disabled ▼ SZ5
	Disabled ▼ SZ6
	Disabled ▼ SZ7
	Disabled ▼ SZ8
AP GROUP	
AP Management	Disabled ▼ Select All
	Disabled ▼ Local Area AP Management
	Disabled ▼ Wide Area AP Management
Switch Management	Disabled ▼
On-Demand API	<input type="checkbox"/> Enable administrator to create On-Demand Account through external interfaces
Setup Wizard	Disabled ▼

コントローラは、カスタマイズ可能な管理アカウントタイプ（スーパーグループ、マネージャ、オンデマンドマネージャ、オペレータなど）をサポートします。管理者は、すべてのアクセス権限と設定権限を持つ、スーパーグループに分類されます。スーパーグループメンバーのみが、他の管理アカウント（マネージャー、オンデマンドマネージャー、オペレータ）を生成できます。すべての管理アカウントの権限設定をカスタマイズできます。スーパーグループメンバーを除き、他の管理アカウントは、読み取り/書き込みアクセス権または読み取り専用アクセス権を持つように設定できます。

ステップ 3 : 管理者アカウントリストを使用して、管理者アカウント情報とそのステータスを表示できます。「Add」をクリックし、必要なアカウント名、パスワード、および割り当てられた権限グループを入力してアカウントを作成してください。**Apply** をクリックした後、新しく生成されたアカウントが下表に表示されます。

Administrator Accounts

[Add ...](#) [Delete](#) [Lock Admin](#) [Unlock](#) [Backup List](#) [Restore List](#)

<input type="checkbox"/>	Name	IP Address	MAC Address	Group	Status
<input type="checkbox"/>	admin	10.29.129.162	DC:0E:A1:27:F4:63	Super Group	Current Page: /Utilities/MlaUser.shtml
<input type="checkbox"/>	admin	10.30.42.168		Super Group	Current Page: /SystemConfiguration/SCAPList.shtml?sz_id=0

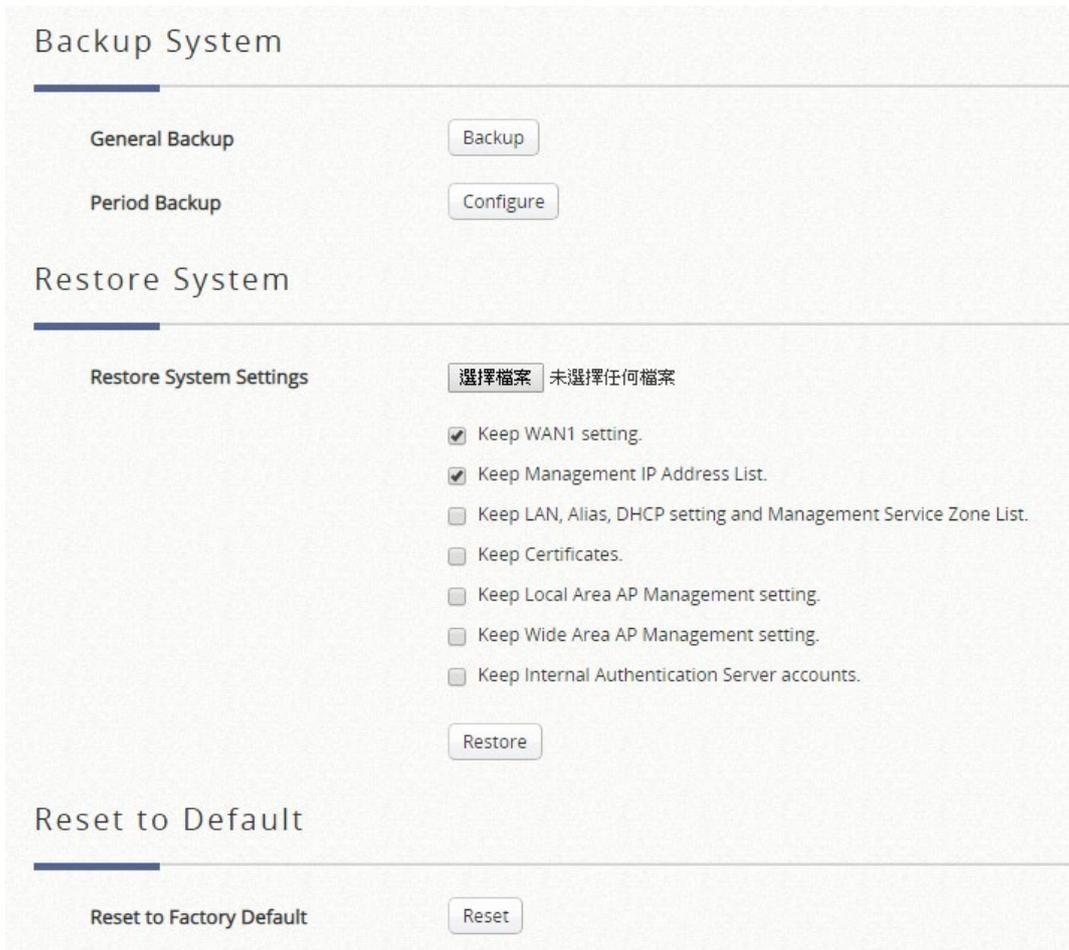
メモ

1. パスワードの安全設定には、管理アカウントの作成またはパスワードの変更時に従う必要がある制約または規則が含まれています。
2. このアカウントが現在 WMI にアクセスしている場合、管理者リストには、既存のすべての管理アカウントとログイン状態が表示されます。
3. 管理者アカウントはルートアカウントであり、削除したり、権限を変更したりすることはできません。

9.2 設定のバックアップと復元

設定パス : [Main Menu >> Utilities >> Backup & Restore](#)

この機能は、EWS コントローラの設定をバックアップ/復元するために使用します。バックアップは FTP 経由で定期的に行うことができます。さらに、EWS コントローラを工場出荷時の設定に戻すことが可能です。



メモ

1. General Backup（一般バックアップ）機能を使用すると、db ファイルの保存を求め
るポップアップウィンドウが表示されます。
2. この操作をリモートで実行する場合、WMI 接続の損失を防ぐために WAN 設定を保
持するなどのオプションを使用して、以前の db 設定の復元を実行できます。
3. 工場出荷時のデフォルトにリセットすると、すべての設定が消去され、コントロー
ラが工場出荷時の設定に復元します。このアクションには、重要な設定を保持する
ための追加オプションもあります。

9.3ファームウェアのアップグレード

設定パス : [Main Menu >> Utilities >> System Upgrade](#)

管理者は、Edgecore のウェブサイトまたは Edgecore のサポートチームから最新のファームウェアを入手し、システムをアップグレードすることができます。**Browse**（参照）をクリックしてローカルドライブ上のファームウェアファイルを検索し、**Apply** をクリックしてファームウェアをアップグレードしてください。アップグレードプロセスが完了するまでに数分かかる場合があります。その後、新しいファームウェアをアクティブ化するためにシステムを再始動する必要があります。FTP ファームウェアのアップグレードもオプションで、FTP サーバーの IP アドレス、FTP サーバーポート、および FTP アカウント名とパスワードを入力し、最後に、システムのアップグレードに使用する FTP サーバーに格納されている完全なファームウェアファイル名を指定してください。

アップグレードを実行する前に、システムはバージョンの互換性をチェックし、システムの健全性を確認します。バージョンの互換性については、Edgecore サポートチームにお問い合わせください。

The screenshot shows the 'System Firmware Upgrade' web interface. It features a title bar at the top. Below it, there are several sections: 'Current Version' showing '3.00.00', 'Upload New Firmware' with a text input field, a 'Browse...' button, and an 'Apply' button, and 'Upgrade Firmware Via FTP' with radio buttons for 'Anonymous' (set to 'Yes') and 'No', input fields for 'IP Address', 'Port', and 'File Name' (with a placeholder 'File Name or Dir/File Name'), and an 'Apply' button.

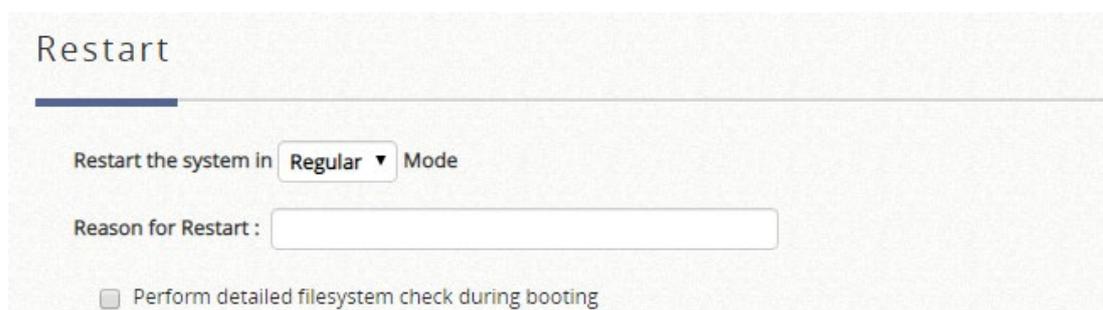
メモ

ファームウェアのアップグレード後に工場出荷時のデフォルトにリセットする前に、システムを再始動する必要があります。

9.4再始動

設定パス : [Main Menu >> Utilities >> Restart](#)

この機能により、管理者は EWS コントローラを安全に再始動でき、処理が完了するまで数分かかる場合があります。**Apply** をクリックして、EWS コントローラを再始動してください。電源を切る必要がある場合は、まず EWS コントローラを再始動し、再始動プロセスの完了後に電源を切ることを強くお勧めします。管理者は、保守のために再始動の理由を入力できます。



Restart

Restart the system in **Regular** Mode

Reason for Restart :

Perform detailed filesystem check during booting

メモ

1. システムの再始動中に、システムすべてのオンラインユーザーの接続が切断されます。

第10章 監視用のレポートとログ

10.1 システム関連のステータス

10.1.1 ダッシュボード

このページには、一般的なシステム設定、ネットワークインターフェース、オンラインユーザーなどを含む、管理者が把握する必要がある重要なシステム関連情報が表示されます。ドロップダウンメニューを使用して、このページの情報更新レートを選択できます。または、「Refresh」ボタンをクリックして手動で更新することもできます。

画面右上の「Display Mode」（表示モード）ボタンを使用すると、管理者はダッシュボードに表示される項目を決定できます。

右上隅の Download ボタンは、システム設定をキャプチャするツールです。これは、メンテナンスまたはトラブルシューティングの目的で使用されます。



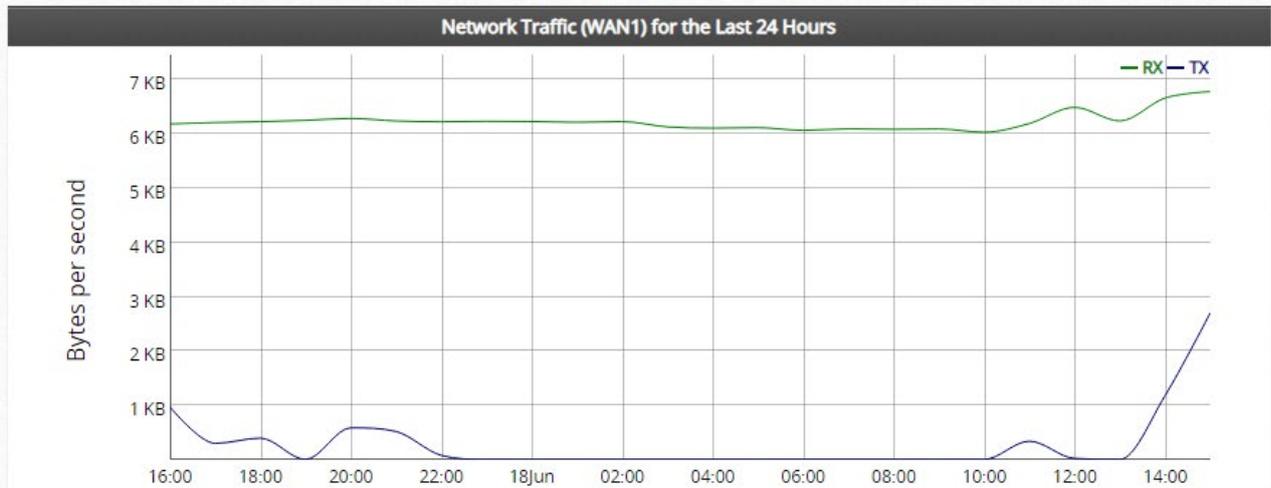
10.1.2 システムの概要

設定パス : [Main Menu >> Status >> System Summary](#)

システムステータスページには、システムファームウェアバージョン、設定されたレポートサーバー、WAN オプション設定、ユーザーログプロファイル、システム時間、セッション制御設定などの目次が表示されます。この概要は、主要な設定項目用に設計されています。詳細なステータスについては、対応する設定ページに進んでください。

System Summary

[See Reports](#)



General

System Name	EWS101	Firmware Version	3.45.0000
System Up Time	14 days, 23 hours, 27 min	Build Number	1.36-1.9737
System Time	2019/06/18 15:20:58 +0800	NTP Server	ntp1.pads.ufrj.br
Preferred DNS Server	8.8.8.8	Alternate DNS Server	N/A
Proxy Server	Disabled	APM Version	3.45.0000
SNMP	Enabled	Warning of Internet Disconnection	Disabled
Idle Timeout	10min	Traffic Direction for Idle Timeout	Uplink & Downlink
Num of Current Users	0	Num of Maximum Users	400

Report

SYSLOG server 1		N/A:N/A
SYSLOG server 2		N/A:N/A
User Logs	Retained Days	30 days
	Receiver E-mail Address(es)	N/A
		N/A
		N/A
		N/A

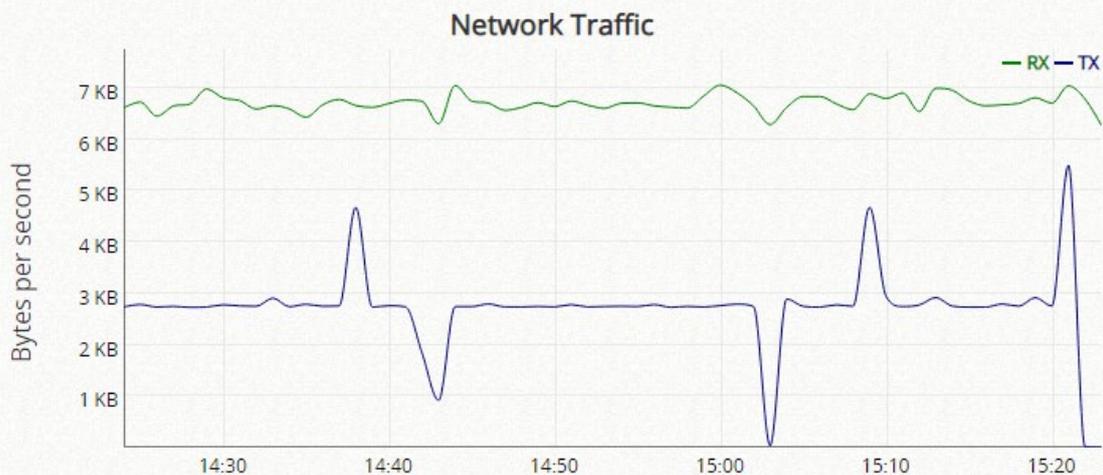
See Reports (レポートを表示する) ボタンをクリックすると、レポートを選択できません。これらのレポートは、インターフェースと間隔に基づいてソートできます。

System Report

Item

Interface

Display Interval



10.1.3 ネットワークインターフェース

設定パス : [Main Menu >> Status >> Interface](#)

このセクションでは、**WAN1**、**WAN2**、**SZ デフォルト**、**SZ1～SZ8** など、管理者が検査する各ネットワークインターフェースの詳細を説明します。

表示するネットワークインターフェースを選択してください。選択されたインターフェースが有効になっている場合は、対応するネットワーク設定が表示されます。ページをスクロールダウンすると、トラフィックの概要、その日のトラフィック、月のトラフィック、上位 10 日間のトラフィックなど、さまざまなスケールのトラフィック統計がグラフィカルに表示されます。

Select Interface: WAN1

Network Interface: WAN1

WAN1			
Mode	STATIC	IP Address	10.29.42.101
MAC Addr	00:10:F3:23:D3:54	Subnet Mask	255.255.0.0
IPv6 Addr	N/A	IPv6 Prefix	N/A
Auto-negotiation	On	Speed / Duplex	100Mb/s Full

summaryTraffic

today

rx: 9.09 MiB
tx: 7.08 MiB
= 16.17 MiB
2.84 kbit/s

yesterday

rx: 18.74 MiB
tx: 11.45 MiB
= 30.18 MiB
2.86 kbit/s

all time

rx: 1.29 GiB
tx: 697.30 MiB
= 1.97 GiB

since 01/11/13

rx: 366.76 MiB
tx: 153.05 MiB
= 519.81 MiB
7.54 kbit/s

Feb '13

rx: 953.68 MiB
tx: 544.25 MiB
= 1.46 GiB
4.58 kbit/s

Jan '13

dailyTraffic

day	rx	tx	total	avg. rate
01/12/13	7.48 MiB	516 KiB	7.99 MiB	0.76 kbit/s
01/13/13	7.49 MiB	507 KiB	7.99 MiB	0.76 kbit/s
01/14/13	55.38 MiB	35.24 MiB	90.62 MiB	8.59 kbit/s
01/15/13	26.90 MiB	46.95 MiB	73.85 MiB	7.00 kbit/s
01/16/13	241.00 MiB	54.98 MiB	295.98 MiB	28.06 kbit/s
01/17/13	109.16 MiB	42.05 MiB	151.22 MiB	14.34 kbit/s
01/18/13	59.43 MiB	25.99 MiB	85.42 MiB	8.10 kbit/s
01/19/13	10.43 MiB	415 KiB	10.83 MiB	1.03 kbit/s
01/20/13	8.86 MiB	328 KiB	9.18 MiB	0.87 kbit/s
01/21/13	55.97 MiB	27.50 MiB	83.48 MiB	7.91 kbit/s
01/22/13	19.56 MiB	17.41 MiB	36.97 MiB	3.51 kbit/s
01/23/13	12.89 MiB	9.13 MiB	22.02 MiB	2.09 kbit/s
01/24/13	25.80 MiB	25.10 MiB	51.90 MiB	4.92 kbit/s
01/25/13	21.04 MiB	39.55 MiB	60.59 MiB	5.74 kbit/s
01/28/13	35.32 MiB	84.39 MiB	119.70 MiB	11.35 kbit/s
01/29/13	62.02 MiB	10.35 MiB	72.36 MiB	6.86 kbit/s
01/30/13	44.33 MiB	24.44 MiB	68.77 MiB	6.52 kbit/s
01/31/13	62.56 MiB	22.97 MiB	85.52 MiB	8.11 kbit/s
02/01/13	58.17 MiB	22.20 MiB	80.36 MiB	7.62 kbit/s
02/02/13	52.07 MiB	9.17 MiB	61.24 MiB	5.81 kbit/s
02/03/13	51.87 MiB	9.07 MiB	60.94 MiB	5.78 kbit/s
02/04/13	58.45 MiB	22.98 MiB	81.43 MiB	7.72 kbit/s
02/05/13	41.68 MiB	15.80 MiB	57.48 MiB	5.45 kbit/s
02/05/13	215 KiB	579 KiB	794 KiB	0.07 kbit/s
02/07/13	12.53 MiB	26.12 MiB	38.65 MiB	3.66 kbit/s
02/06/13	13.70 MiB	11.40 MiB	25.11 MiB	2.38 kbit/s
02/07/13	48.57 MiB	15.24 MiB	64.31 MiB	6.15 kbit/s
02/06/13	1.57 MiB	0.98 MiB	2.55 MiB	0.24 kbit/s
02/06/13	18.74 MiB	11.45 MiB	30.18 MiB	2.86 kbit/s
02/07/13	9.09 MiB	7.08 MiB	16.17 MiB	2.84 kbit/s
estimated	16 MiB	12 MiB	28 MiB	

monthlyTraffic

month	rx	tx	total	avg. rate
Jan '13	953.68 MiB	544.25 MiB	1.46 GiB	4.58 kbit/s
Feb '13	366.76 MiB	153.05 MiB	519.81 MiB	7.54 kbit/s
estimated	1.53 GiB	655 MiB	2.17 GiB	

top10Traffic

#	day	rx	tx	total	avg. rate
1	01/16/13	241.00 MiB	54.98 MiB	295.98 MiB	28.06 kbit/s
2	01/11/13	88.07 MiB	75.49 MiB	163.56 MiB	15.51 kbit/s
3	01/17/13	109.16 MiB	42.05 MiB	151.22 MiB	14.34 kbit/s
4	01/28/13	35.32 MiB	84.39 MiB	119.70 MiB	11.35 kbit/s
5	01/14/13	55.38 MiB	35.24 MiB	90.62 MiB	8.59 kbit/s
6	01/31/13	62.56 MiB	22.97 MiB	85.52 MiB	8.11 kbit/s
7	01/18/13	59.43 MiB	25.99 MiB	85.42 MiB	8.10 kbit/s
8	01/21/13	55.97 MiB	27.50 MiB	83.48 MiB	7.91 kbit/s
9	02/04/13	58.45 MiB	22.98 MiB	81.43 MiB	7.72 kbit/s
10	02/01/13	58.17 MiB	22.20 MiB	80.36 MiB	7.62 kbit/s

メモ

1. 長期保存のために統計を保存する必要がある場合は、外部サーバーでのネットワークトラフィックの送信と保存の手順について、「レポートと通知」セクションを参照してください。

10.1.4 ルーティング

設定パス : [Main Menu >> Status >> Routing Tables >> IPv4/IPv6](#)

このステータスページには、すべてのポリシールートルールが表示され、グローバルポリシールートルールがここに表示されます。これは、管理者が異なるポリシーに属するユーザーのルーティングルールの適用状況を確認するための迅速な参照ウィンドウを提供します。また、各ネットワークインターフェースに指定されたシステムルートルールも表示されます。

IPv6 はグローバルポリシーで使用できます。また、そこで構成されたルールは、IPv6 トラフィックのシステムインターフェース設定とともに IPv6 ルーティングテーブルページにも表示されます。

10.1.5 DHCP サーバー

設定パス : [Main Menu >> Status >> DHCP Leases](#)

DHCP IP リース統計情報は、このページの **Show** Statistics List をクリックすると表示できます。

- **提供リストの統計**

ここには、**Last 10 Minutes** (分)、**Hours** (時間)、および **Days** (日間) の有効なリース数が表示されます。ヘッダー1~10 は単位乗数です。例えば、列 2 の下の数字は過去 20 分/時間/日間のリース数を示し、列 3 の下の数字は過去 30 分/時間/日間のリース数を示します。

- **期限切れリストの統計**

ここには、**Last 10 Minutes** (分)、**Hours** (時間)、および **Days** (日間) に期限切れになったクライアントへの IP リースが表示されます。ヘッダー1~10 は単位乗数です。例えば、列 2 の下の数字は過去 20 分/時間/日間の期限切れ数を示し、列 3 の下の数字は過去 30 分/時間/日間の期限切れ数を示します。

IPs Offered

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	1	0	0	0	0	0	0	0	0	0
Last 10 Hours	1	0	0	0	0	0	0	0	0	0
Last 10 Days	1	0	0	0	0	0	0	0	0	0

IPs Expired

Refresh Refresh Disable ▾

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	0	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	0	0	0	0	0	0	0	0	0
Last 10 Days	0	0	0	0	0	0	0	0	0	0

- **DHCP リースリスト**

DHCP サーバーから発行された有効な IP アドレスと、この IP アドレスを使用するクライアントの関連情報がここに表示されます。

DHCP Leases

Statistics List Show
DHCP Lease Log Show

DHCP Lease List

Refresh Delete Refresh Disable ▾

<input type="checkbox"/>	No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires
<input type="checkbox"/>	1	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	3154	2013/02/08 11:08:14

(Total:1) [First](#) [Previous](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

10.2 クライアント関連のステータス

10.2.1 オンラインユーザー

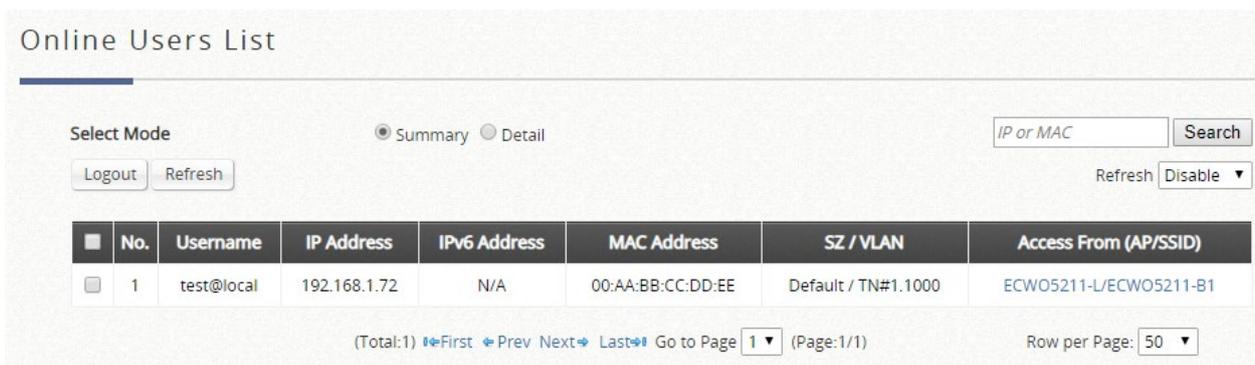
ページパス : [Main Menu >> Status >> Monitor Users >> Online Users](#)

このページに表示されるユーザーは、LAN またはリモートでトンネリングされたサイト

の管理対象ネットワークで、このコントローラによって認証されたユーザーです。

メモ

1. 非トンネル構成時にはオンラインユーザーリストに接続端末情報が表示されません。



Online Users List

Select Mode: Summary Detail

Logout Refresh

IP or MAC Search Refresh Disable

No.	Username	IP Address	IPv6 Address	MAC Address	SZ / VLAN	Access From (AP/SSID)
1	test@local	192.168.1.72	N/A	00:AA:BB:CC:DD:EE	Default / TN#1.1000	ECW05211-L/ECW05211-B1

(Total:1) First Prev Next Last Go to Page 1 (Page:1/1) Row per Page: 50

選択できるモードは2つあります。「Detail」を選択すると、Pkts In/Out、Bytes In/Outなどの詳細情報が表示され、インスタンスのクライアント認証タイプも表示されます。管理者は、**Kick Out**をクリックして特定のオンラインユーザーを強制退出させたり、**Access From**（アクセス元）のAP名のハイパーリンクをクリックしてユーザーアクセスのAPステータスを確認することができます。特定のオンラインユーザーのIPアドレスまたはMACアドレスを検索するための「Search」（検索）ツールが用意されています。**Refresh**をクリックして現在のユーザーリストを更新するか、このページの右下隅にあるドロップダウンボックスから自動更新の時間間隔を選択できます。



Online Users List

Select Mode: Summary Detail

Logout Refresh

No.	Username	IP Address	IPv6 Address	MAC Address	SZ / VLAN	Group / Policy	Auth. Database	Auth. Method	Pkts In/Out	Bytes In/Out
1	049226DBFF14	10.131.5.78	N/A	04:92:26:DB:FF:14	Default / TN#1.3000	N/A / N/A	EXRADIUS	802.1X Transparent	0 / 0	0 / 0

(Total:1) First Prev Next Last Go to Page 1 (Page:1/1)

10.2.2 関連付けられた非ログインユーザー

ページパス : [Main Menu >> Status >> Monitor Users >> Non-Login Devices](#)

このページには、システムの DHCP サーバーから IP アドレスを取得している、LAN ま

たはリモートでトンネリングされたサイトで認証されていないユーザーが表示されま
す。この機能は、管理者がシステムのリソースが枯渇しないように管理するために設計
されています。リストには、クライアントの **MAC Address**、**IP Address**、および関連
付けられた **VLAN ID**、**Service Zone**、クライアントがワイヤレス接続を使用している場
合の **Associated AP**（関連付けられた AP）が表示されます。

Non-Login Devices List

Refresh Refresh Disable ▾

MAC Address	IP Address	VLAN ID	Service Zone	Associated AP/SSID
D0:13:FD:45:5B:07	IPv4:192.168.1.72 IPv6:N/A	TN#1.1000	Default	Seb05211/Seb05211-B1

(Total:1) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

10.2.3 クロスゲートウェイローミングユーザー

ページパス : [Main Menu >> Status >> Monitor Users >> Roaming In Users](#)

このページには、物理的にこのコントローラの下にある、ローミングピアコントローラ
によって認証されているユーザーが表示されます。ここにリストされているユーザー
は、自分のホームコントローラにトンネリングされ、インターネットに転送されます。

Cross Gateway Roaming In Users

Refresh Refresh Disable ▾

Name	IP Address	MAC Address	VLAN ID	Home	Detail
------	------------	-------------	---------	------	--------

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

10.2.4 オンデマンドローミングアウトユーザー

ページパス : [Main Menu >> Status >> Monitor Users >> Roaming Out Users](#)

このページには、このコントローラのオンデマンドデータベースを RADIUS データベ
ースとして使用して、他のコントローラによって認証されたユーザーが表示されます。

On-Demand Roaming Out Users

Refresh Refresh Disable

Name	IP Address	MAC Address	NAS ID	Session Time	Bytes In / Out	Login Time
					Pkts In / Out	Last Update Time

(Total:0) First Previous Next Last Go to Page (Page:1/1) Row per Page: 50

10.2.5 MAC ログインデバイス

ページパス : [Main Menu >> Status >> Monitor Users >> MAC Login Devices](#)

このページには、それ自体で MAC 認証を完了できないデバイスが表示されます。管理者は、デバイスを選択し、「MAC Authenticate」(MAC 認証) ボタンをクリックすると、手動で認証を行うことができます。認証結果は、このページのテキスト領域に表示されます。

Main > Status > User Monitor > MAC Login Devices

MAC Login Devices List

MAC Authenticate Refresh Refresh Disable

No.	MAC Address	IP Address	Service Zone
-----	-------------	------------	--------------

Result

(Total:0) First Prev Next Last Go to Page (Page:1/1) Row per Page: 50

10.2.6 認証されたユーザー

ページパス : [Main Menu >> Status >> Monitor Users >> Authenticated Users](#)

このページには、コントローラに対して不明な IP 情報を持つ認証完了ユーザーが表示されます。一部のタイプの認証 (802.1X、MAC 認証、PPP 認証、CoA ログイン) では、ユーザーはネットワークアクセスを許可する前にネットワークアクセスを認証する必要

があります。したがって、ユーザーは、認証が完了した後にのみ DHCP 経由で IP アドレスを要求できます。認証されたユーザーが IP アドレスを取得し、ネットワークの使用を開始すると、認証されたユーザーリストからオンラインユーザーリストに移動されます。

管理者は、ユーザーを選択し、「Logout」ボタンをクリックすると、認証されたユーザーをログアウトできます。

Main > Status > User Monitor > Authenticated Users

Authenticated Users List

Logout Refresh Refresh Disable ▾

No.	Username	MAC Address	Auth. Database	Auth. Method
-----	----------	-------------	----------------	--------------

(Total:0) ⏪First ⏩Prev Next⏩ Last⏪ Go to Page ▾ (Page:1/1) Row per Page: 50 ▾

10.2.7 スマートログインユーザー

ページパス : [Main Menu >> Status >> Monitor Users >> Smart Login Users](#)

スマートログインは、オンデマンドユーザーにとって便利な機能です。スマートログインを有効にしたとき、オンデマンドユーザーがログインに成功すると、デバイスがログアウトしていても、定義された期間内に自動的にログインされます。

このページには、スマートログイン期間内のオンデマンドユーザーが表示されます。このリストのユーザーは、次回ネットワークにアクセスしたときに自動的にログインします。

管理者は、スマートログインユーザーリストでユーザーを削除できます。削除されたユーザーは、次回手動でログインする必要があります。

Smart Login User Information

Delete All Delete

	MAC	Name	Last Login
--	-----	------	------------

(Total:0/2000) ⏪First ⏩Prev Next⏩ Last⏪ Go to Page ▾ (Page:1/1) Row per Page: 10 ▾

10.2.8 セッションリスト

設定パス : [Main Menu >> Status >> Sessions](#)

このページでは、管理者はクライアントとシステムの間で現在確立されているセッションを検査できます。各結果には、送信元と宛先の IP とポートの値が表示されます。フィルタ条件を定義し、希望する結果のみを表示できます。

Session List

Filter					
Address Family	Protocol	Source IP	Port	Destination IP	Port
IPv4 ▾	All ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Filter

Display Mode: ALL ▾

No	Protocol	Source IP	Port	Destination IP	Port	State	Timeout
1	udp	10.29.129.110	17500	10.29.255.255	17500	UNREPLIED	29
2	udp	10.29.36.203	17500	10.29.255.255	17500	UNREPLIED	5
3	udp	10.29.13.1	50119	10.29.255.255	8765	UNREPLIED	9
4	udp	10.29.43.131	35811	10.29.42.101	5246	ASSURED	179
5	tcp	10.28.128.188	54547	10.29.42.101	80	TIME_WAIT	38
6	udp	10.29.42.101	57930	10.29.43.131	161	ASSURED	148

10.3 ログとレポート

10.3.1 システム関連

設定パス : [Main Menu >> Status >> Logs and Reports](#)

このページには、システムの起動後にシステムのローカルログとユーザーイベントが表示されます。管理者は、さまざまなイベントのログエントリを調べることができます。ただし、これらの情報はすべて揮発性メモリに格納されるため、再起動/再始動操作中に失われます。したがって、ログ情報を文書化する必要がある場合は、管理者が手動でバックアップを作成する必要があります。

- **CAPWAP Log** : このページには、コントローラと CAPWAP 対応の AP 間で通信される CAPWAP メッセージが表示されます。
- **Configuration Change Log** : このページには、コントローラの WMI 設定を変更したユーザーのアカウントと IP が表示されます。
- **Local Monthly Usage** : このページには、ローカルユーザーの集計統計が表示され、その月の送信トラフィックが表示されます。
- **Local Web Log** : このページには、コントローラ組み込み Web サーバー上でアクセスされた Web ページが表示されます。
- **On-Demand User Billing Report Log** : このページには、オンデマンドアカウントの取引概要が表示されます。
- **RADIUS Server Log** : このページには、コントローラを通過する RADIUS メッセージが表示されます。
- **SIP Call Usage** : ログには、開始時刻、発信者、着信者、期間（秒）などの SIP クライアント（デバイスおよびソフトクライアント）のログインおよびログアウトアクティビティが表示されます。
- **System Log** : このページには、イベントトレース用のシステム関連のログが表示されます。
- **UAMD Log** : UAM デーモンから出力される UAM 関連情報を表示します。
- **Alarm** : 選択した項目のエラーメッセージまたは警告メッセージを表示します。障害が解決されるまで、アラームメッセージはアラームリストに残ります。アラーム項目

は、「Alarms & Events Settings」 ページで設定できます。

- **Management Event** : 選択した管理イベントのログを表示します。管理イベントは、「Alarms & Events Settings」 ページで設定できます。

10.3.2 ユーザーイベント

設定パス : [Main Menu >> Status >> Logs and Reports >> User Events](#)

このページには、すべてのユーザーログとイベントがまとめられています。ユーザーログとイベントは、最大 40 日間保存できます。管理者の好みに合わせてカスタマイズ可能なすべてのユーザー関連情報を表示します。管理者は、ページごとに表示する行数 (20、40、60、80、100) を選択できます。カレンダーから「開始」と「終了」の日付を選択して、不要なユーザーイベントをフィルタリングしてください。開始日と終了日を選択したら、「Display」 をクリックして、選択した日付内のすべてのユーザーイベントを表示します。

「Download」 ボタンでは、表示されたユーザーイベントをカンマ区切りの.txt ファイルにダウンロードできます。ダウンロードしたデータをセルにソートするには、.csv 拡張子を付けて新しいファイルとして保存してください。「Clear」 ボタンでは、ユーザーインターフェースに表示されている現在のユーザーイベントを削除できます。

User Events

Display Mode

From

To

User Type Local On-Demand Trial Roaming Out Roaming In External

Date	Type	Event	Name	Policy	IP	MAC	Source
2013-02-07 06:08:35 +1000	Local - Mobile	Login	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 06:18:12 +1000	Local - Mobile	Admin-Reset	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:22:41 +0900	Local - Mobile	Login	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:23:03 +0900	Local - Mobile	Logout	duncan@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:23:58 +0900	Local - Mobile	Login	example@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-07 14:34:03 +0900	Local - Mobile	Idle-Timeout	example@local	1	192.168.1.89	68:09:27:A4:48:80	
2013-02-06 11:38:17 +0800	Ondemand	Create_OD_User	28v2		0.0.0.0	00:00:00:00:00:00	WEB:PLM3154

Display Mode の「Configure」 ボタンを使用すると、管理者はユーザーイベントに表示される列を変更できます。

ユーザータイプが異なると、ユーザー情報が異なることに注意してください。ユーザータイプに適用できない場合、カテゴリは空白のままになります。

ローカルユーザーに適用可能なユーザーイベントカテゴリ：

Date、Type、Name、IP、IPv6、MAC、Pkts In、Bytes In、Pkts Out、Bytes Out、VLAN ID、Group、Policy、MaxDnLoad、MaxUpload、ReqDnLoad、RequPload。

オンデマンドユーザーに適用可能なユーザーイベントカテゴリ：

Date、System Name、Type、Name、Unit、Price、Total Price、IP、IPv6、MAC、Pkts In、Bytes In、Pkts Out、Bytes Out、Activation Time、1st Login Expiration Time、Account Valid Through、Remark、VLAN ID、Group、Policy、MaxDnLoad、MaxUpload、ReqDnLoad、RequPload。

ローミングアウトユーザーの適用可能なユーザーイベントカテゴリ：

Date、Type、Name、NSID、NASIP、NASPort、UserMac、SessionID、SessionTime、Bytes In、Bytes Out、Pkts In、Pkts Out、Message。

ローミングインユーザーに適用可能なユーザーイベントカテゴリ：

Date、Type、Name、NSID、NASIP、NASPort、UserMac、UserIP、SessionID、SessionTime、Bytes in、Bytes Out、Pkts In、Pkts Out、Message。

10.4 レポートと通知

設定パス：[Main Menu >> Status >> Reporting](#)

EWS コントローラは、設定された電子メールアドレス、SYSLOG サーバー、または FTP サーバーに、ユーザーおよび/またはシステム関連のさまざまなレポートを自動的に送信できます。

Notification Settings

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
	1	2	3	4	5				Detail / Test
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	N/A	1 Hour ▼
High Availability Mode Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼
Wide Area AP Report									<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
<input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associated Clients <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic						N/A	N/A	<input type="checkbox"/>	
Switch Status	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼
Switch Report									<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
<input type="checkbox"/> PoE overview	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	
Local HTTP Web Log						N/A	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
HTTP Web Log						N/A	<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	1 Hour ▼
DHCP Server Log						N/A	<input type="checkbox"/>	N/A	N/A
DHCP Lease Log						N/A	N/A	<input type="checkbox"/>	1 Hour ▼
System Report									<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
<input type="checkbox"/> CPU Loading <input type="checkbox"/> CPU Temperature <input type="checkbox"/> Memory Usage <input type="checkbox"/> Storage Usage <input type="checkbox"/> Network Traffic <input type="checkbox"/> Online User <input type="checkbox"/> Successful Login <input type="checkbox"/> Session <input type="checkbox"/> DHCP Lease <input type="checkbox"/> DNS Query						N/A	N/A	<input type="checkbox"/>	
Traffic Report (Text)						N/A	N/A	<input type="checkbox"/>	1 Hour ▼
<input type="checkbox"/> Service Zone <input type="checkbox"/> VLAN						N/A	N/A	<input type="checkbox"/>	

- ▶ **SMTP Settings** : 5つの受信者の電子メールアドレスと、さまざまなユーザー関連のログを送信する必要なメールサーバー設定を設定できます。
- ▶ **SYSLOG Settings** : 選択したユーザーログとシステムログが送信される2つの外部SYSLOGサーバーの設定を許可できます。
- ▶ **FTP Settings** : 選択したユーザーログとシステムログが送信される外部FTPサーバーの設定を許可できます。
- ▶ **Notification Settings** : 選択可能なすべてのユーザーおよびシステムログの概要を示します。

選択したログは、カスタマイズ可能な時間間隔で、選択した場所（電子メール、SYSLOG、FTP）に送信できます。

- ▶ **Alarms & Events Settings** : 選択可能な管理イベントのリストが表示されます。項目を管理イベントとして選択すると、関連ログが管理イベントページとダッシュボードに記録されます。項目をアラームとして選択すると、関連する障害が発生したときに、警告メッセージまたはエラーメッセージが表示されます。障害が解決されると、メッセージはアラームから削除され、管理イベントとして記録されます。

第11章 ホットスポットアプリケーション

11.1 オンデマンド請求プラン

設定パス : [Main Menu >> Users >> Internal Authentication >> On-Demand >> Billing Plans](#)

請求プランプロファイルは、ゲストのインターネットアクセスの利用規約を定義します。**請求プラン番号**のリンクをクリックして、選択した請求プランプロファイルの設定ページに入ってください。請求プランプロファイルの設定が完了したら、**Billing Plans**（請求プラン）の画面に戻り、**Active** チェックボックスにチェックを入れ、**Apply** をクリックして有効にしてください。

No	Plan Type	Quota	Price	Active	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	<input checked="" type="checkbox"/>	Group 1	Reset
2	N/A			<input type="checkbox"/>	Group 1	Reset
3	N/A			<input type="checkbox"/>	Group 1	Reset
4	N/A			<input type="checkbox"/>	Group 1	Reset
5	N/A			<input type="checkbox"/>	Group 1	Reset

- **Plan** : 選択した請求プランプロファイルの番号。
- **Plan Type** : このプランで選択されたアカウントタイプ。アカウントの種類によって、プロパティが異なります。ゲストの使用要件に最も適した、適切なアカウントタイプを選択する必要があります。
- **Quota** : オンデマンドユーザーがネットワークへのアクセスを許可する量または期間に関する使用条件。
- **Price** : それぞれの請求プランの単価。
- **Active** : チェックボックスにチェックを入れて、請求プランを有効にできます。無効化された請求プランは、オンデマンドゲストアカウントの生成には使用できません。
- **Group** : それぞれの請求プランに関連付けられたオンデマンドユーザーのグループ割り当て。
- **Function** : Reset ボタンをクリックして、選択した請求プランプロファイルの設定をクリアできます。

11.2 オンデマンド請求プランのタイプ

11.2.1 使用時間（有効期限あり）

残りのクォータ（使用可能時間）でアカウントが有効である限り、ユーザーはインターネットにアクセスできます。ユーザーは、ログインして、所定の期間内に購入したアカウントを有効にする必要があります。これは、コーヒーショップや空港ターミナルなどの短期的な使用に最適です。クォータは使用中のみ減らされます。ただし、有効期限へのカウントダウンは、ログインまたはログアウトに関係なく継続されます。**有効期間**が使い切れたり、クォータが枯渇したりすると、アカウントは期限切れになります。

- **Quota** は、オンデマンドユーザーがネットワークへのアクセスを許可されている期間の合計（xx days yy hrs zz mins）です。引き換え後も合計最大のクォータは「364Days 23hrs 59mins 59secs」です。
- **Account Activation** は、ユーザーが最初のログインを実行する必要がある期間です。Account Activation で設定した期間内にそれを行わないと、アカウントの有効期限が切れず。
- **Valid Period** は使用するための有効期間です。この期間が過ぎると、クォータが残っていても、アカウントは期限切れになります。
- **Price** はこのプランの単価です。
- **Group** はこのプランから作成されたユーザーに適用されたグループです。
- **Reference** フィールドでは、管理者は追加情報を入力できます。

Billing Plan Configuration

Plan Number: 1

Plan Type: Usage-time

Activation: User's First time login must be done within 0 day(s) 2 hour(s)
The value for hour(s) has to be between 0~23; Day(s) and hour(s) cannot be both zeros.

Expiration: Enable Disable
 Account will expire in 7 day(s) after activation

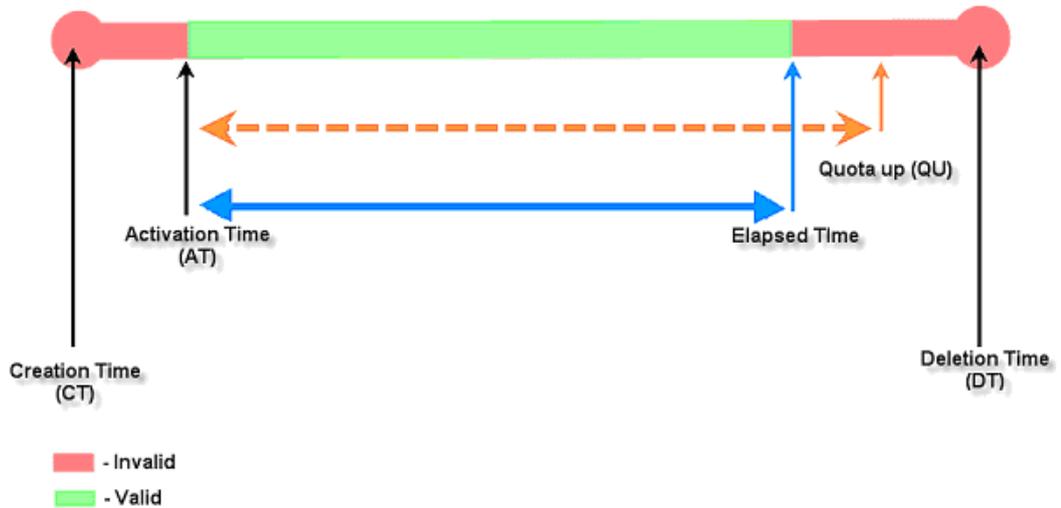
Quota: 0 day(s) 2 hr(s) 0 min(s)
The value for day(s) cannot exceed 364; The value for hr(s) has to be 0~23; The value for min(s) has to be between 0~59.

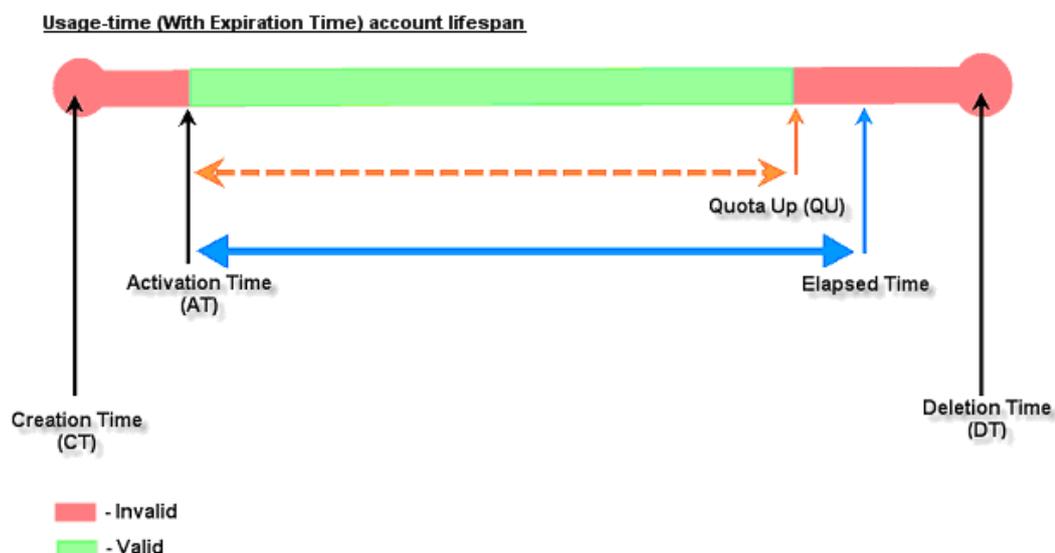
Unit Price: 1.99
The unit price cannot exceed 100000, and can take values up to two decimal places.

Group: Group 1

Reference:

Usage-time (With Expiration Time) account lifespan





11.2.2.使用時間（有効期限なし）

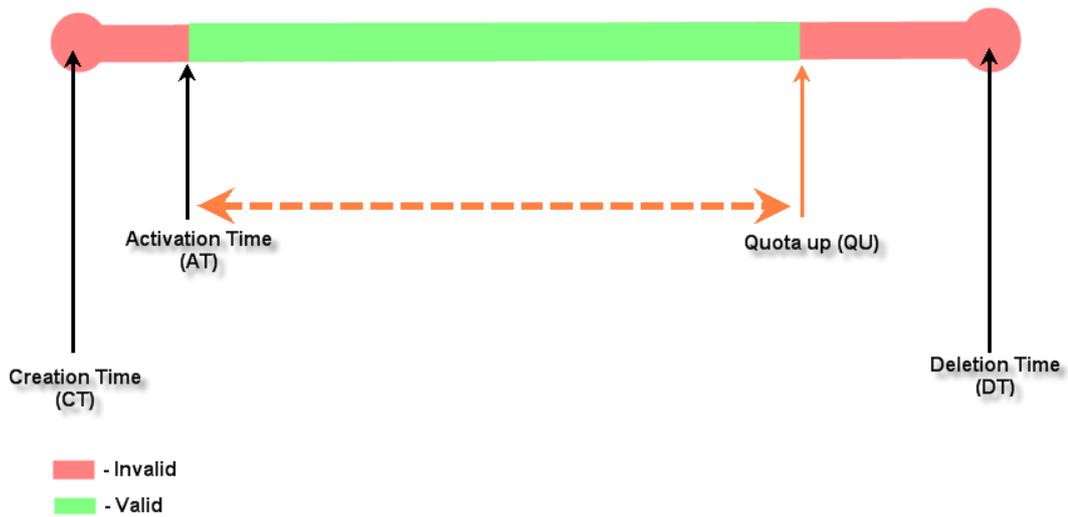
アカウントのクォータ（使用可能時間）が残っている限り、ユーザーはインターネットにアクセスできます。ユーザーは、ログインして、所定の期間内に購入したアカウントを有効にする必要があります。これは、コーヒーショップや空港ターミナルなどの短期的な使用に最適です。クォータは使用中のみ減らされます。クォータが枯渇した場合のみアカウントが失効します。

- **Quota** は、オンデマンドユーザーがネットワークへのアクセスを許可されている期間の合計（*xx days yy hrs zz mins*）です。引き換え後も合計最大のクォータは「364Days 23hrs 59mins 59secs」です。
- **Account Activation** は、ユーザーが最初のログインを実行する必要がある期間です。Account Activation で設定した期間内にそれを行わないと、アカウントの有効期限が切れます。
- **Price** はこのプランの単価です。
- **Group** はこのプランから作成されたユーザーに適用されたグループです。
- **Reference** フィールドでは、管理者は追加情報を入力できます。

Billing Plan Configuration

Plan Number	1
Plan Type	Usage-time
Activation	User's First time login must be done within 0 day(s) 2 hour(s) <small>The value for hour(s) has to be between 0~23; Day(s) and hour(s) cannot be both zeros.</small>
Expiration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Quota	0 day(s) 2 hr(s) 0 min(s) <small>The value for day(s) cannot exceed 364; The value for hr(s) has to be 0~23; The value for min(s) has to be between 0~59.</small>
Unit Price	1.99 <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1
Reference	

Usage-time (No Expiration) account lifespan



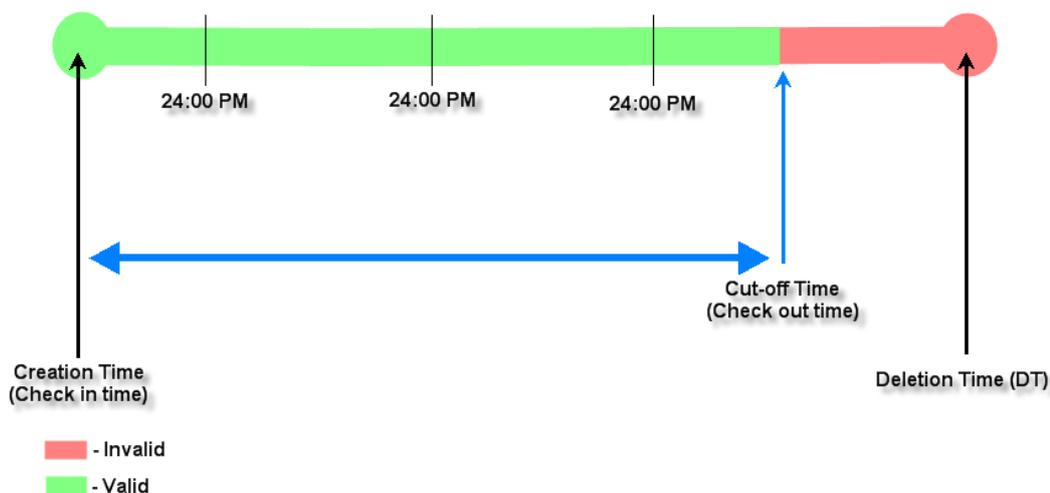
11.2.3.ホテルカットオフ時間

ホテルカットオフ時間とは、翌日または何日後にシステムによってオンデマンドアカウントが遮断される（有効期限が切れる）時計の時間（通常はチェックアウト時間）です。このプランのアカウント作成 UI で、オペレータは顧客の滞在時間に応じてカットオフまでの日数である単位値を入力できます。例えば、次のようになります。単位=2 日間、カットオフ時間=13:00 の場合、アカウントは2 日後の 13:00 に期限切れになります。**Grace Period**（猶予期間）は、アカウントが切断された後の短期間の追加期間で、ユーザーは追加料金を支払うことなく、オンデマンドアカウントを使用してインターネットにアクセスし続けることができます。**Number of Devices** は、アカウントごとに同時にログインできるデバイスの数を定義できます。**Unit Price** は、この請求プランの1 日あたりの価格です。これは、主に宿泊時間に応じてインターネットサービスを提供するために、ホテルの会場で使用されています。**Group** はこのプランから作成されたユーザーに適用されたグループです。**Reference** フィールドでは、管理者は追加情報を入力できます。

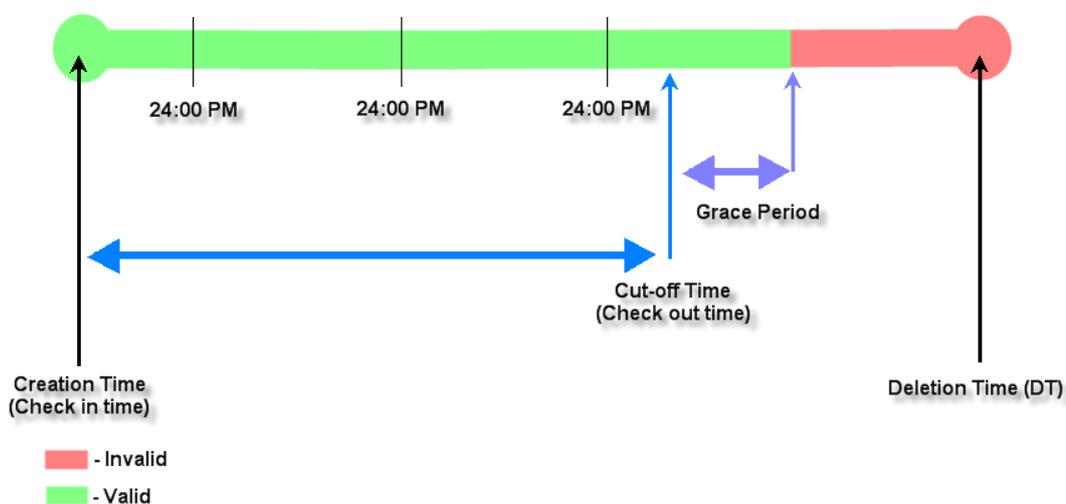
Billing Plan Configuration

Plan Number	1
Plan Type	Hotel Cut-off time ▾
Cut-off Time	<input type="text"/> : <input type="text"/> <small>The cut-off time has to be between 00:00~23:59 in the form of hh:mm.</small>
Grace Period	0 ▾ hour(s) after Cut-off
Number of devices	1 <input type="text"/> device(s) <small>Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).</small>
Unit Price	11 <input type="text"/> per day <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1 ▾
Reference	<input type="text"/>

Hotel Cut-off-time account lifespan (3 night stay example)



Hotel Cut-off-time account lifespan (3 night stay example with Grace Period)



11.2.4.ボリューム

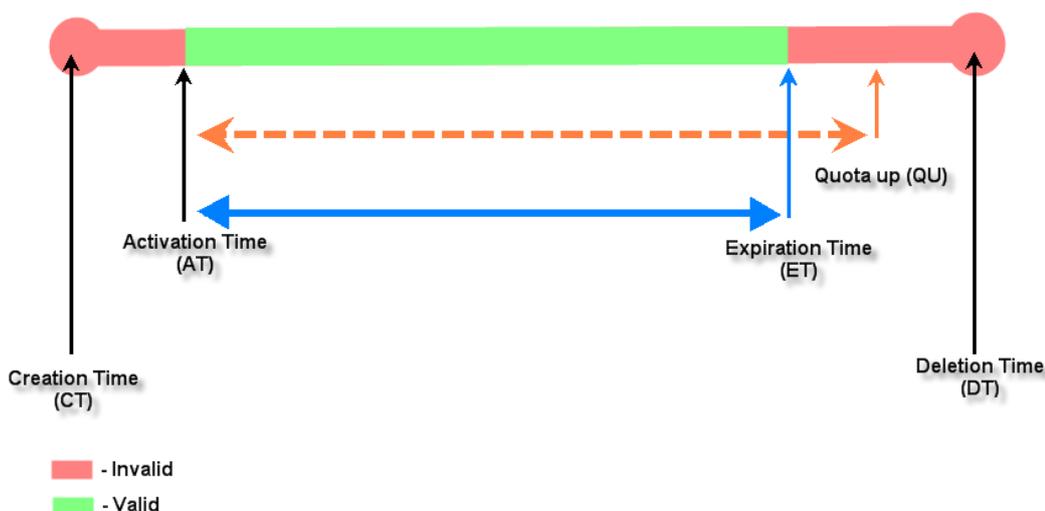
残りのクォータ（トラフィック量）でアカウントが有効であれば、ユーザーはインターネットにアクセスできます。有効期間が使い切れたり、クォータが枯渇したりすると、アカウントは期限切れになります。これは、メールの送受信やファイルの転送など、少量アプリケーションに最適です。有効期間のカウントダウンは、ログインまたはログアウトに関係なく継続されます。

- **Account Activation** は、ユーザーが最初のログインを実行する必要がある期間です。Account Activation で設定した期間内にそれを行わないと、アカウントの有効期限が切れます。
- **Expiration** は使用するための有効期間です。この期間が過ぎると、クォータが残っていてもアカウントは期限切れになります。
- **Quota** は、オンデマンドユーザーがネットワークへのアクセスを許可されている M バイトの合計（1~1000000）です。
- **Number of Devices** は、アカウントごとに同時にログインできるデバイスの数を定義できます。（0：無制限）
- **Unit Price** はこのプランの単価です。
- **Group** はこのプランから作成されたユーザーに適用されたグループです。
- **Reference** フィールドでは、管理者は追加情報を入力できます。

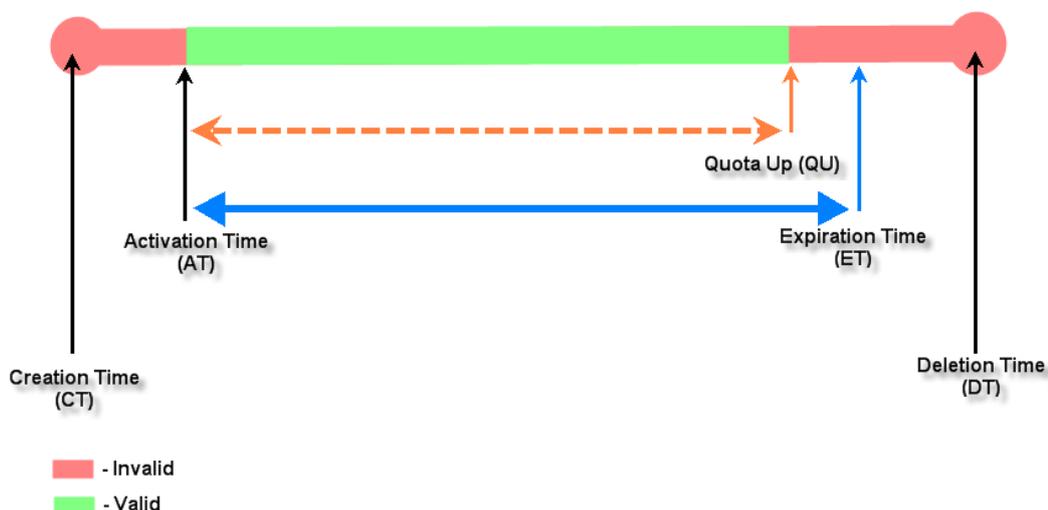
Billing Plan Configuration

Plan Number	1
Plan Type	Volume ▾
Activation	User's First time login must be done within <input type="text" value="0"/> day(s) <input type="text" value="2"/> hour(s) The value for hour(s) has to be between 0-23; Day(s) and hour(s) cannot be both zeros.
Expiration	Account will expire in <input type="text" value="7"/> day(s) after activation
Quota	<input type="text" value="100"/> MByte(s) *(Range : 1 ~ 1000000)
Number of devices	<input type="text" value="3"/> device(s) Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).
Unit Price	<input type="text" value="2"/> The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1 ▾
Reference	<input type="text"/>

Volume account lifespan



Volume account lifespan



11.2.5.経過時間を含む継続時間

アカウントは、アカウントの作成時にアクティブ化されます。カウントダウンは、アカウントが作成された直後に開始され、ログインまたはログアウトに関係なく継続されます。*経過時間*に達すると、アカウントは期限切れになります。これは、特定の期間を通じてアカウント作成直後にインターネットサービスを提供するのに理想的です。

- **Begin Time**（開始時間）は、アカウントが使用可能になる時間です。アカウント作成時間に設定されています。
- **Elapsed Time**（経過時間）は、アカウントがインターネットアクセスに対して有

11.2.6. カットオフ時間付き継続時間

カットオフ時間は、システムによってオンデマンドアカウントがその日に切断される（期限切れ）時計の時間です。例えば、ショッピングモールが 23:00 に閉じられるように設定されている場合、オンデマンドチケットを販売する事業者は、このプランを使用して 23:00 に切れるようにチケットセットを作成できます。この種類のアカウントが「カットオフ時間」の後に作成されると、そのアカウントは自動的に期限切れになりません。

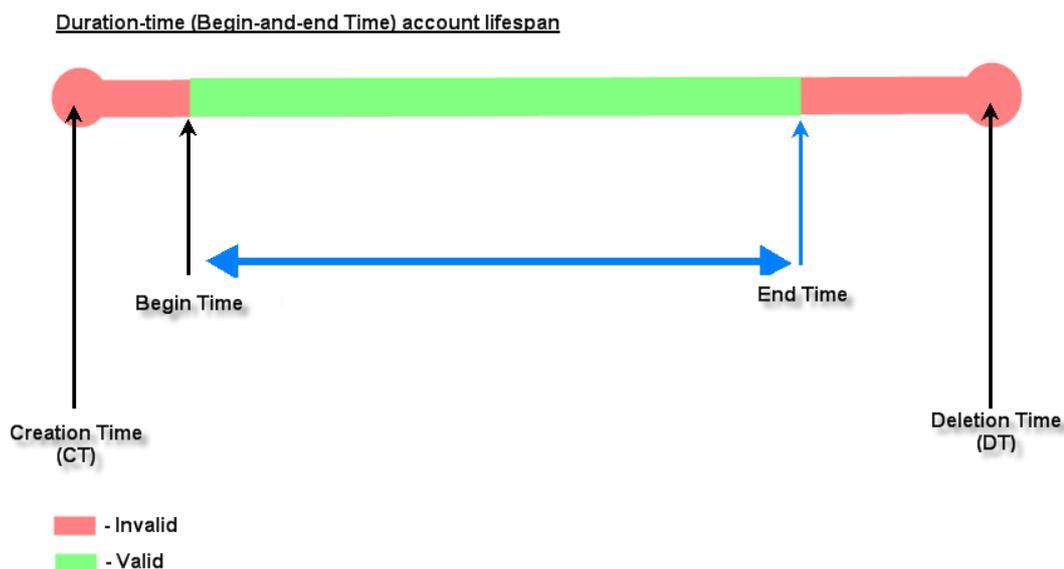
- **Begin Time**（開始時間）は、アカウントが使用可能になる時間です。アカウント作成時間に設定されています。
- **Cut-off Time**（カットオフ時間）は、アカウントの有効期限が切れる時計の時間です。
- **Number of Devices** は、アカウントごとに同時にログインできるデバイスの数を定義できます。
- **Price** はこのプランの単価です。
- **Group** はこのプランから作成されたユーザーに適用されたグループです。
- **Reference** フィールドでは、管理者は追加情報を入力できます。

Billing Plan Configuration

Plan Number	1
Plan Type	Duration-time ▼
Duration Type	<input type="radio"/> Elapsed Time <input type="radio"/> Begin-and-End Time <input checked="" type="radio"/> Cut-off Time
Begin Time	Upon Account Creation
Cut-off Time	<input type="text"/> : <input type="text"/> <small>The cut-off time has to be between 00:00~23:59 in the form of hh:mm.</small>
Number of devices	<input type="text" value="1"/> device(s) <small>Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).</small>
Unit Price	<input type="text" value="11"/> <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1 ▼
Reference	<input type="text"/>

Billing Plan Configuration

Plan Number	1
Plan Type	Duration-time
Duration Type	<input type="radio"/> Elapsed Time <input checked="" type="radio"/> Begin-and-End Time <input type="radio"/> Cut-off Time
Begin Time	-- : -- , -- --
End Time	-- : -- , -- --
Number of devices	1 device(s) <small>Number of devices is an integer from 0 to 9999, representing the number of simultaneous logged-in devices allowed per account (0: Unlimited).</small>
Unit Price	11 <small>The unit price cannot exceed 100000, and can take values up to two decimal places.</small>
Group	Group 1
Reference	



11.3 POS プリンタのセットアップ

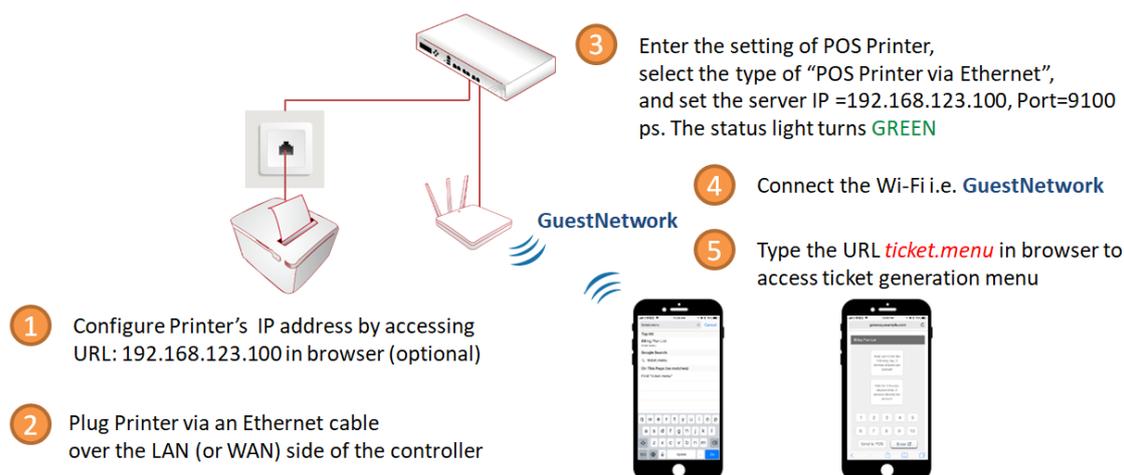
ネットワークチケットジェネレーターの概要

オンデマンドアカウント生成をサポートするように設計された EC-PP200 は、Edgecore 無線

LAN コントローラに組み込まれたオンデマンド請求プラン機能を使用してチケットを印刷できます。注目すべきことは、EC-PP200 は、追加の機器なしでイーサネットを介して 4pnet コントローラに接続できることです。

ネットワークへの EC-PP200 の組み込み

次の図は、ネットワークで EC-PP200 を利用するための簡単なユースケースと簡単なセットアップを示しています。



1. EC-PP200 の IP アドレスを設定します。
2. コントローラ付き EC-PP200 をイーサネットケーブルで接続します。
3. コントローラのターミナルサーバーページで、EC-PP200 の IP アドレスとポートを入力します。
4. Wi-Fi またはイーサネット経由でネットワークを接続します。
5. コントローラの Web 管理インターフェースにアクセスして、チケット生成メニューにアクセスします。

Web 管理インターフェースでの EC-PP200 の管理

EC-PP200 は、すべての Edgecore ゲートウェイ/コントローラと連携して動作するように特別に設計されています。EC-PP200 を Edgecore ゲートウェイ/コントローラに接続する前に、いくつかの設定手順が必要です。

EC-PP200 の関連設定については、Web 管理インターフェース（WMI）を参照してください。
デフォルト値は次のとおりです。

IP アドレス : 192.168.123.100

サブネットマスク : 255.255.255.0

使用するコンピュータの TCP/IP 設定は、EC-PP200 と同じサブネットの下にある静的 IP アドレスで設定することを忘れないでください。例えば、192.168.123.20 です。

The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) - Content' dialog box. The 'General' tab is selected. The text reads: '如果您的網路支援這項功能，您可以取得自動指派的 IP 設定。否則，您必須詢問網路系統管理員正確的 IP 設定。' (If your network supports this feature, you can get automatically assigned IP settings. Otherwise, you must ask the network system administrator for the correct IP settings.)

Options for IP address assignment:

- 自動取得 IP 位址(O) (Obtain IP address automatically)
- 使用下列的 IP 位址(S): (Use the following IP address)

Fields for static IP configuration (highlighted with a red box):

- IP 位址(I): 192 . 168 . 123 . 20
- 子網路遮罩(U): 255 . 255 . 255 . 0
- 預設閘道(D): 192 . 168 . 123 . 1

Options for DNS server assignment:

- 自動取得 DNS 伺服器位址(B) (Obtain DNS server address automatically)
- 使用下列的 DNS 伺服器位址(E): (Use the following DNS server address)

Fields for DNS servers:

- 慣用 DNS 伺服器(P): . . .
- 其他 DNS 伺服器(A): . . .

Buttons: 進階(V)... (Advanced...), 確定 (OK), 取消 (Cancel). A checkbox for '結束時確認設定(L)' (Show advanced settings on completion) is also present.

EC-PP200 の WMI では、「Configure Interface」ページで IP 設定を変更してください。「Fixed IP Address」（固定 IP アドレス）が設定されていることを確認してください。

Ethernet WebConfig Version 1.00

Interface Status
Printer Status
Configure Interface

Reboot

Configure Interface
Settings for the Ethernet Interface .

IP Address: DHCP Client:
DHCP Timeout (s) 90

Fixed IP Address:
Device IP Address 192.168.1.123
Subnet Mask 255.255.0.0
Gateway Address 192.168.1.254

Restore Default Save Exit

EC-PP200 を再起動した後、新しい IP アドレスを使用して WMI にアクセスし、EC-PP200 の「Interface Status」が正しいことを確認してください。

Ethernet WebConfig Version 1.00

Interface Status
Printer Status
Configure Interface

Reboot

Interface Status
View the current status of the interface module.

Mac Address 0-71-80-146-86-140
IP Address 192.168.1.123
Subnet Mask 255.255.0.0
Gate Way 192.168.1.254
DHCP Disabled
DHCP Timeout 90

Refresh

Edgecore ゲートウェイ/コントローラでの EC-PP200 の設定

設定パス : [Main Menu >> Users >> Internal Authentication >> On-Demand Authentication >> POS Printer Configuration](#)

Edgecore ゲートウェイ/コントローラは、複数の POS プリンタの管理をサポートします。EC-PP200 を使用してアカウントチケットを印刷するには、管理者がプリンタの IP アドレスをコントローラのリストに追加する必要があります。EC-PP200 を管理するには、以下の手順に従

ってください。

1. 請求プランを作成して有効にします。（11.1 および 11.2 を参照）
2. POS チケットテンプレートを構成します。（11.4 を参照）
3. 「POS Printer via Ethernet」（イーサネット経由の POS プリンタ）を選択し、Server IP フィールドに POS プリンタの IP アドレスを入力します。チケットテンプレートを選択し、有効にする請求プランを確認してください。

メモ

1. EC-PP200 を POS プリンタリストに追加する場合は、Port を **9100** にする必要があります。

Main > Users > Internal Authentication > On-Demand Authentication > POS Printer Configuration

POS Printer Configuration

Printer Type POS Printer with Wireless Smart Device Serve POS Printer via Ethernet

Status	Item	USB Printer ID	type	Remark	Ticket template	Billing plan
●	1		USB		Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>

(Total: 1) [First](#) [Prev](#) [Next](#) [Last](#)

Status	Item	Server IP	Port	Remark	Ticket template	Billing plan
●	1	10.73.36.123	9100		Template 1 ▼	1 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	2				Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	3				Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/>

11.4 POS チケットのカスタマイズ

設定パス：[Main Menu >> Users >> Internal Authentication >> On-Demand >> POS Tickets](#)

ホットスポットでの配置を柔軟にするために、テンプレートを使用した POS チケットのカスタマイズは EWS コントローラでサポートされています。最大 5 つのチケットテンプレートをシステムに保存できます。

POS Tickets

Templates	Template 1 ▾
Image	Upload
Width	2" ▾
Languages	English ▾
length of password	<input checked="" type="radio"/> 4 characters <input type="radio"/> 8 characters
Ticket Type	Type I ▾ <input type="button" value="Restore"/>
	For Usage-Time with expiration time & Volume

- 必要に応じて、TMB 形式で画像（会社のロゴなど）をアップロードできます。
- 幅は 2 種類あり、EC-PP200 には 3"が推奨されます。
- 構成済みのチケットテンプレートの言語を選択してください。EWS は、英語、フランス語、ドイツ語、日本語、スペイン語、簡体字中国語、繁体字中国語をサポートしています。
- チケットメニューで生成されたアカウントの場合、パスワードはランダムですが、管理者は 4 文字と 8 文字のパスワードを選択できます。
- 設定されている請求プランに応じて、適切なチケットタイプを選択してください。

Type I

Parameters	<div style="border: 1px solid #ccc; padding: 2px;"> \$remain ▼ <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> \$remain \$username \$username_without_postfix \$password \$usage \$price \$extid \$activationtime \$expiretime \$expire_time \$duration \$remark \$image \$unit \$date \$quota \$price \$sprice \$qr \$max_user </div> </div>	<input type="button" value="Insert Parameters"/>
<pre> Username: \$username Password: \$password Quota: \$quota Price: \$price ESSID: Activation: Before \$expire_time Expiration: \$duration days after activation </pre>	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> SN:\$remain </div>	
<input type="button" value="Preview"/>		

POS チケットのカスタマイズは、下のウィンドウから手動で入力するか、上記の例に示すように、ドロップダウンリストからパラメータを挿入して開始できます。

これが完了したら、ターミナルサーバーへの請求プランとチケットテンプレートの割り当てを開始できます。

Terminal Server Configuration						
Status	Item	Server IP	Port	Remark	Ticket template	Billing plan
●	1	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	2	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	3	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>
●	4	<input type="text"/>	<input type="text"/>	<input type="text"/>	Template 1 ▼	1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 0 <input type="checkbox"/>

管理者は、ドロップダウンリストから特定のチケットジェネレーターに必要なチケットテンプレートを選択できるようになりました。

QR コードログインの申込み

```
-----
Username : $username
Password : $password
Quota : $usage
Total Price : $price
External ID : $extid
-----
ESSID : $wlan_ess_id
Wireless Key : $wep_key
-----
Your first time login must be
done before $expire_time
-----
The account is valid within
$duration days
after your first login.
-----

QR Code Login
Scan the QR code your device to login automatically
-----
```

チケットジェネレーターを使用したオンデマンドアカウント生成は、ホットスポットプロバイダにとって非常に一般的な配置です。面倒なのは、アカウントのユーザー名とパスワードを手動で入力することです。特に、小さなキーボードで入力する必要があるモバイルデバイスでは、目に優しいとは言えません。

ユーザー名、パスワード、使用量、価格などを含むログイン資格情報は、すべて QR コードに埋め込まれています。

SSID に関連付けて、QR コードをスキャンするだけで、インターネットを閲覧する準備が整いました！

QR コードをサポートするための Web チケットの設定

する必要があります。

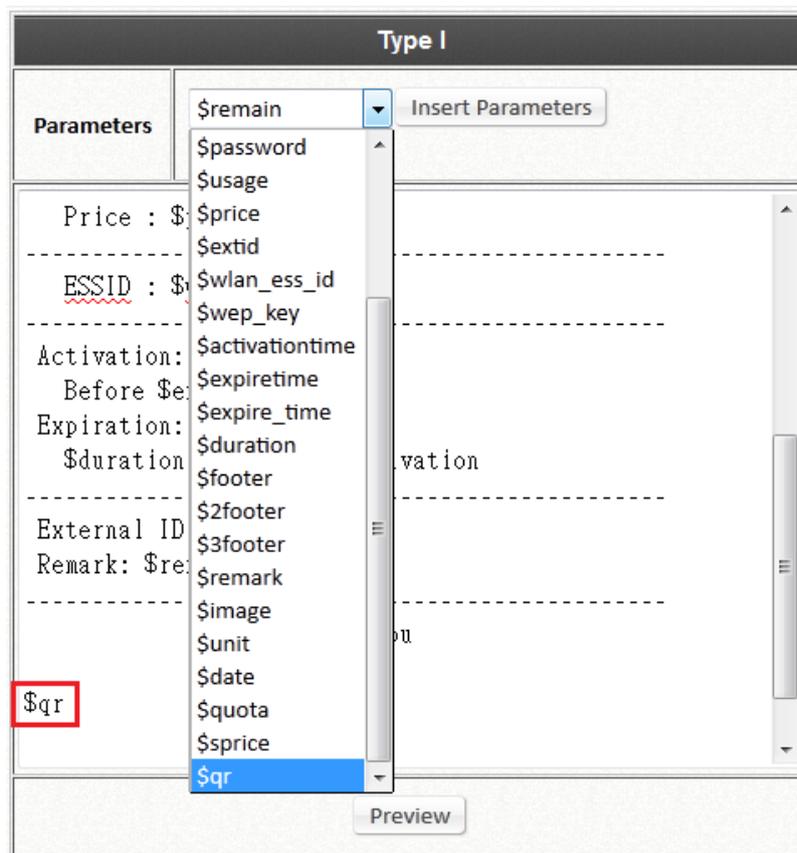
QR コードの印刷をサポートするには、チケットをカスタマイズす

Main Menu >> Users >> Authentications の順に選択し、**On-Demand User** と **Configure** をクリックして、チケットテンプレートのカスタマイズを設定してください。

POS Tickets

Templates	Template 1 ▼
Image	Upload
Width	3" ▼
Languages	English ▼
length of password	<input checked="" type="radio"/> 4 characters <input type="radio"/> 8 characters
Ticket Type	Type I ▼ <input type="button" value="Restore"/>

For Usage-Time with expiration time & Volume



利用された請求プランでは、QRコードをサポートするように対応するチケットテンプレートをカスタマイズする必要があります。

- 1) 幅を3"に変更する必要があります（デフォルト値=2"）。
- 2) パラメータを追加するには、テンプレートに「\$qr」を入力するか、ドロップダウンメニューから「\$qr」を選択して Insert Parameters（パラメータを挿入する）をクリックしてください。

11.5 アカウントの作成

設定パス：[Main Menu >> Users >> On-Demand Accounts >> Accounts Creation](#)

管理者は、単一のアカウントを作成することも、一括でアカウントを作成することもできます。販売のためのゲストアカウントを事前に生成したい潜在的なホットスポットオペレータのために、オンデマンド機能には、一括作成機能があり、オンデマンドページへのアクセス権限を持つ管理者またはオペレータが一括で有効な請求プランの複数のアカウントを作成し、POS

プリンターに送信して販売用の物理的なチケットのプリントアウトを生成することができます。

On-Demand Account Creation

Plan	Account Type	Quota	Price (円)	Group	Function
1	Usage-time	1 min(s) of connection time quota with expiration	11	1	Create Single Create Batch
2	N/A				Create Single Create Batch
3	N/A				Create Single Create Batch
4	N/A				Create Single Create Batch
5	N/A				Create Single Create Batch
6	N/A				Create Single Create Batch
7	N/A				Create Single Create Batch
8	N/A				Create Single Create Batch
9	N/A				Create Single Create Batch
0	N/A				Create Single Create Batch

管理者は、一括でオンデマンドアカウントを作成するときに、ランダムに生成されたユーザー名とパスワードを使用するか、カスタム作成するかを選択できます。ランダムに生成されたパスワードの場合、ショート（4文字）またはロング（8文字）を使用できます。

Creating Batch On-Demand Accounts

Plan : Account Type 1 : Usage-time

Quota 2 hr(s) of connection time quota with expiration

Numbers Number of tickets to batch create

Account Creation System created Manual created

Username

Prefix: *(A-z/0-9 and max length is 5)

Serial Number: *(1~5 digits and max length is 5)

Postfix: *(A-z/0-9 and max length is 5)

*(Total length is less than 10)

Password Randomly Same as username Admin Assign

Valid Period After activation, the account will be expired in 7 day(s)

Total Price 1.99

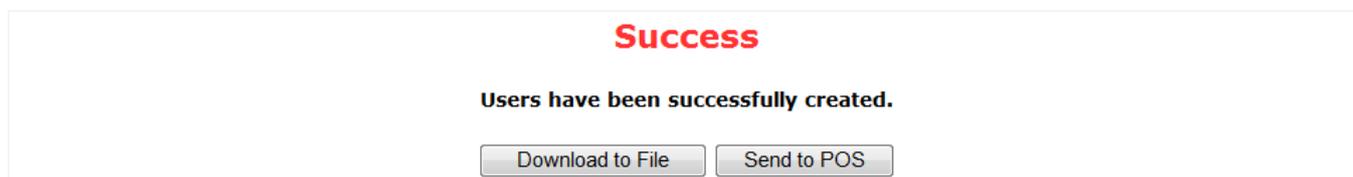
Unit Number of units per ticket

Group Group 1

Please confirm the information and press Create button to create accounts.

カスタムユーザー一名を作成する場合、アカウントのシリアル番号は1つのインクリメントになりますが、接頭辞と接尾辞は一定に保たれます。

生成されたアカウントは、安全に保管するためにダウンロードするか、一括印刷のためにプリンタに送信することができます。



11.6 ユーザーセルフサービス

外部支払いゲートウェイ経由のクレジットカード

設定パス : [Main Menu >> Users >> Authentication >> On-Demand User >> External Payment Gateway](#)

EWS コントローラは、オペレータが所有するアカウントの種類に応じて異なるタイプの支払いゲートウェイオプションをサポートしています。例えば、Authorize.NET、PayPal、SecurePay、WorldPay、PELECard があります。

最も一般的に使用される PayPal は、以下の図の例のように使用されています。

「PayPal」を設定する前に、ホットスポットの所有者が有効な PayPal 「ビジネスアカウント」を持っている必要があります。

PayPal ビジネスアカウントを開設した後、ホットスポットの所有者は、「PayPal Payment Page Configuration」（PayPal 支払いページ設定）を続行するために、この PayPal アカウントの「Identity Token」（ID トークン）を見つける必要があります。

支払いページ設定に必要なマーチャントアカウントの資格情報を入力してください。コントローラの WAN IP が NAT の下にある場合、支払いエンドユーザーが取引結果を受け

取るには、Instant Payment Notification (IPN) フィールドで IP 転送情報を設定する必要があります。

External Payment Gateway

Selection

Disable Authorize.Net PayPal SecurePay WorldPay PeleCard

Number of SMS quota *(1~10) **SMS gateway configure**

The function to send SMS after purchasing an account is not ready.This is the given SMS quota to the client when multiple messages are required, either for multiple devices or if the SMS needs to be re-sent.

PayPal Payment Page Configuration

Business Account *

Payment Gateway URL *

Identity Token *

Instant Payment Notification (IPN) Enable Disable

Behind NAT

Verify SSL Certificate Enable Disable

▼

エンドユーザーが支払ゲートウェイを通じて自己購入することを許可する、有効な請求プランを選択してください。

Choose Billing Plan for PayPal Payment Page

Plan	Activation	Quota	Price	Remark
1	<input type="checkbox"/>	2 hr(s) of connection time quota with expiration	1.99	<input type="text"/>
2	<input type="checkbox"/>	Valid until 5:01 the following day	1	<input type="text"/>
3	<input type="checkbox"/>			<input type="text"/>
4	<input type="checkbox"/>			<input type="text"/>
5	<input type="checkbox"/>			<input type="text"/>
6	<input type="checkbox"/>			<input type="text"/>
7	<input type="checkbox"/>			<input type="text"/>
8	<input type="checkbox"/>			<input type="text"/>
9	<input type="checkbox"/>			<input type="text"/>
0	<input type="checkbox"/>			<input type="text"/>

Web ページのカスタマイズを設定することで、サービスの免責事項をカスタマイズすることができます。

外部支払いゲートウェイの設定後、ログインページには、有効なクレジットカードでア

アカウントを購入するためのエンドユーザーを段階的に案内するハイパーリンクが表示されます。

ユーザーがオンラインで新しいアカウントを購入した後に SMS 経由でアカウント情報を取得し、次回ログイン時にユーザー名とパスワードが忘れられるリスクを排除するために、管理者は SMS ゲートウェイと支払いゲートウェイを統合することができます。

External Payment Gateway

Selection

Disable Authorize.Net PayPal SecurePay WorldPay PeleCard

Number of SMS quota *(1~10) [SMS gateway configure](#)

The function to send SMS after purchasing an account is not ready.This is the given SMS quota to the client when multiple messages are required, either for multiple devices or if the SMS needs to be re-sent.

PayPal Payment Page Configuration

Business Account *

Payment Gateway URL *

Identity Token *

Instant Payment Notification (IPN) Enable Disable

Behind NAT

Verify SSL Certificate Enable Disable

▾

正常にセットアップされると、**Number of SMS Quota**（SMS クォータの数）フィールドが使用可能になります。

External Payment Gateway

Selection

Disable Authorize.Net PayPal SecurePay WorldPay PeleCard

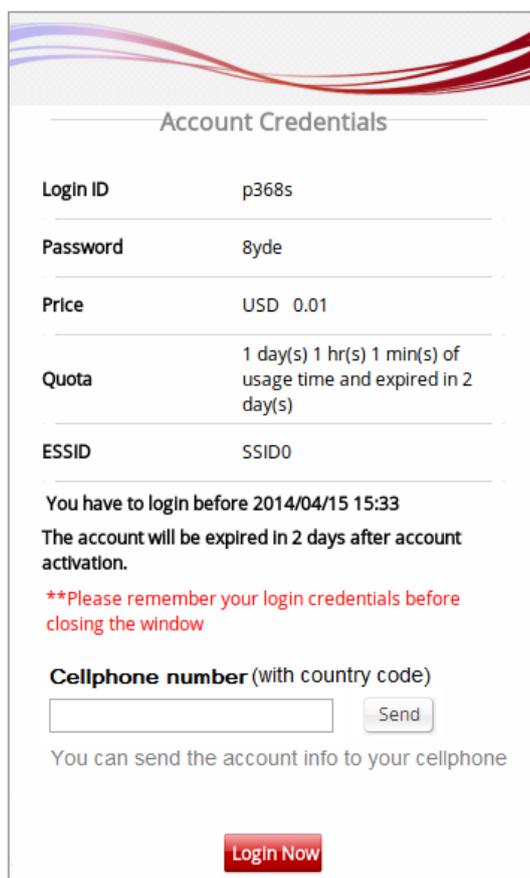
Number of SMS retry [SMS gateway configure](#)

The function to send SMS after purchasing an account is ready

アカウントの購入者は、オンラインでアカウントの料金を支払った後、携帯電話番号を入力します。アカウントの購入者は、設定された番号を超えないように SMS を再送信

することができます。

外部支払いポータルをプレビューするには、ページの下部にある **Web Page Customization** の「Configure」をクリックしてください。システム内のすべてのカスタマイズ可能な Web ページと同様に、このページは、テンプレートによるカスタマイズ、html のアップロード、または外部ページの使用もサポートしています。SMS ゲートウェイで外部支払いゲートウェイを使用した場合に表示される内容の例を以下に示します。



The screenshot shows a web form titled "Account Credentials". It contains the following fields and values:

Login ID	p368s
Password	8yde
Price	USD 0.01
Quota	1 day(s) 1 hr(s) 1 min(s) of usage time and expired in 2 day(s)
ESSID	SSID0

Below the fields, there is a warning message: "You have to login before 2014/04/15 15:33. The account will be expired in 2 days after account activation." followed by a red reminder: "**Please remember your login credentials before closing the window".

There is a section for "Cellphone number (with country code)" with an input field and a "Send" button. Below this is the text "You can send the account info to your cellphone".

At the bottom, there is a red "Login Now" button.

PMS セルフサービス

VLAN ネットワークを計画し、ポートロケーションマッピングの設定をすべて完了したら、設定が正しく機能しているかどうかを確認する必要があります。設定されたポートタイプに従って、ユーザーが VLAN マッピングされた部屋からインターネットにアクセスしようとする、表示されるページまたはメッセージは次のようになります。

ユーザーが部屋からインターネットにアクセスしようとする、ブラウザは利用可能な

プランとサービス契約のリストを含むログインページを表示します。サービス契約本文は、適用されたサービスゾーンのカスタムページ設定で設定できます。ユーザーは請求プランを選択し、Confirm ボタンをクリックすると、生成されたアカウント名とパスワードが表示されます。すでにユーザーアカウントをお持ちの場合は、「[here](#)」リンクをクリックして、所有しているユーザーアカウントでログインできます。

here to login.'" data-bbox="295 229 752 583"/>

Plan (s)	Price ()	Unit
<input checked="" type="radio"/> 2 hr(s) of usage time and expired in 10 day(s)	0.99	<input type="text"/>
<input type="radio"/> Valid until 23:00 the following day; 40 devices allowed per account	1.49	<input type="text"/>
<input type="radio"/> Valid for 3 day(s) elapsed time; 40 devices allowed per account	1.99	<input type="text"/>

Service Agreement

Please kindly note that there will be no refund once connectivity is confirmed. Please click Confirm to accept the usage charge. The selected service charge will be posted directly into your guest folio.

Confirm

If you already have an user account, please click [here](#) to login.

第12章 PMS 統合

ここでは、PMS 統合で使用されるポートロケーションマッピング機能について説明します。この機能は、サービスゾーンの下に複数の VLAN 分割を（別々の LAN ポートであるかのように）作成し、これらの VLAN を別の場所に個別にマッピングするように設計されています。この機能は、MTU/MDU 配置で、個別のクライアントに VLAN 接続を提供するためにゲートウェイの下に VLAN スイッチを配置する、個別のクライアントに VLAN を提供するために利用できます。

ポートロケーションマッピング機能は、おもてなしの場では、客室や公共エリアのインターネットサービスを管理するために一般的に使用されています。さらに、サードパーティのホスピタリティアプリケーションと連携して動作することができ、ゲートウェイと一般的な高速インターネットアクセス（HSIA）ハードウェアとフロントオフィスシステム（FOS）ソフトウェアとのシームレスな統合を提供する Net Retriever ミドルウェアでテストされています。

各ポートロケーションマッピングエントリは、エントリの VLAN タグに対応するロケーションで、課金（シングルまたはマルチユーザー）、無料またはブロックされたインターネットサービスを提供するように設定できます。有料サービスをご利用いただくには、少なくとも1つまたは複数のオンデマンド請求プランが作成され、ユーザーがインターネットアクセス料金を支払うための希望プランを選択することが必要がありますのでご注意ください。

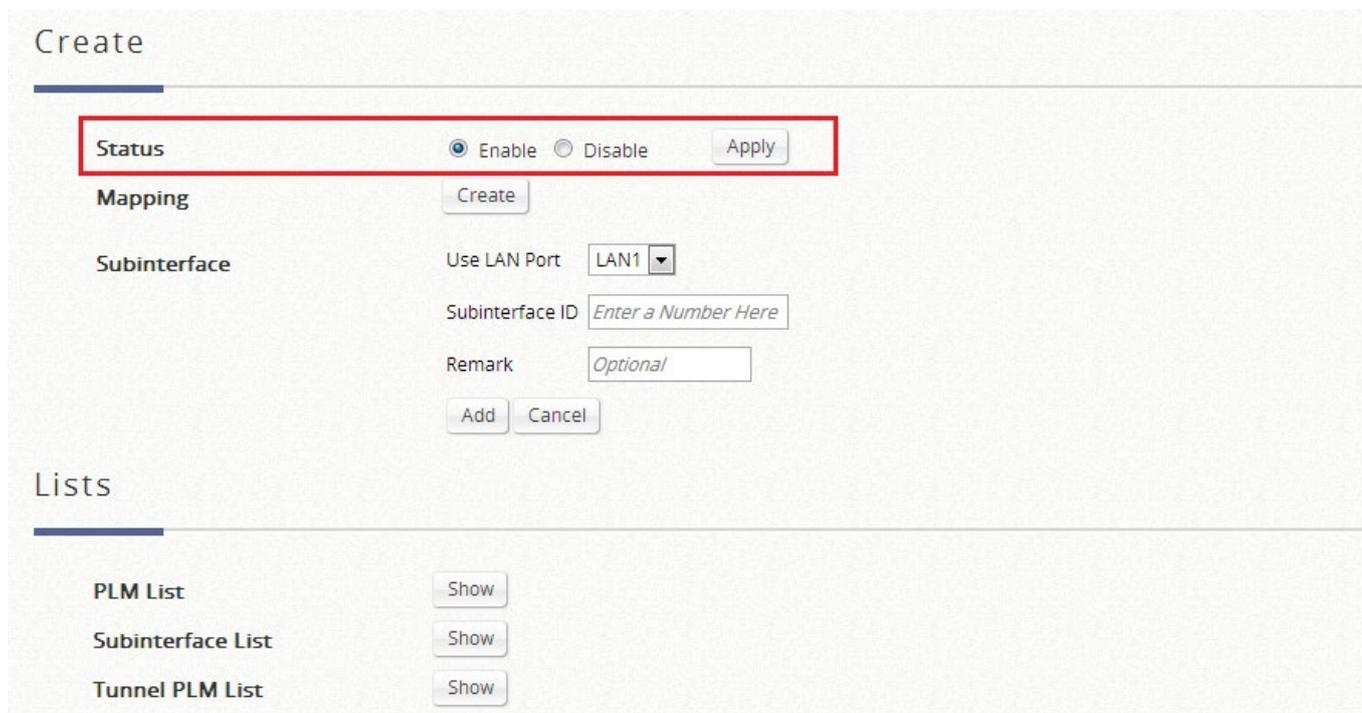
メモ

1. EWS コントローラは、デフォルトで Micros PMS、InnKeyPMS、および IDS インターフェースをサポートします。お客様独自のインターフェース・ホスピタリティソフトウェアを作成またはカスタマイズする際に、専用のサポートが必要な場合は、Edgecore 営業担当者までお問い合わせください。

12.1 ホテルの部屋ロケーションマッピング

設定パス：[Main Menu >> System >> Port Location Mapping](#)

ポートロケーションマッピング機能を使用すると、各サービスゾーンが複数の VLAN を所有し（各 VLAN がポートであるかのように）、クライアントの送信元を識別できます。PMS ミドルウェアの設定、またはサービスゾーンへの VLAN の追加を行う前に、まずポートマッピング機能を有効にする必要があります。



The screenshot shows a web interface for configuring port location mapping. The 'Create' section is highlighted with a red box, indicating the 'Status' is set to 'Enable' and the 'Apply' button is visible. Below this, there are fields for 'Mapping' (Create), 'Subinterface' (Use LAN Port: LAN1, Subinterface ID: Enter a Number Here, Remark: Optional), and 'Lists' (PLM List, Subinterface List, Tunnel PLM List, each with a Show button).

管理者は、ポートロケーションマッピング機能を使用して、ロケーション（ホテルの部屋など）を VLAN スイッチまたは DSLAM デバイスの VLAN ポートにマッピングできます。各部屋は VLAN タグにマッピングされます。また、各部屋を異なるサービスゾーンに割り当てて、異なるポリシーを取得することができます。さらに、アプリケーションに応じて、異なるポートタイプの部屋を設定することができます。**Open**、**Block**、または **Auth.Required** です。

- **Open** というポートタイプは、ユーザーがこの部屋で無料でインターネットにアクセスできることを意味します。
- 部屋のインターネットアクセスを提供したくない場合は、部屋のポートタイプを「**Block**」に変更できます。ユーザーがブラウザを開いてインターネットにアクセスしようとする、ブロックメッセージがポップアップしてユーザーに通知されます。
- **Auth.Required** というポートタイプは、主にユーザーに課金するためのホスピタリティアプリケーションで使用されます。ユーザーがブラウザを開いてインターネットに

アクセスしようとする、免責事項と請求プランのオプションを含むページが表示されます。ユーザーは、希望するプランを選択し、confirm ボタンをクリックしてアカウントを購入することができます。アカウント費用は PMS に送信され、設定されたミドルウェアを介してホテルの請求書に追加されます。

メモ

1. VLAN ポートは 1 つずつ作成することも、一度に一括作成することもできます。その後の変更は、ポートタイプの変更設定ボックスで行えます。
2. ポートロケーションマッピングで設定された VLAN タグは、各サービスゾーンに割り当てられている VLAN タグと競合してはいけません。

Port Location Mapping List には、VLAN ID、Room Num/Location ID、Port Type、Service Zone などの情報を含むすべてのプロファイルエントリが表示されます。**Delete** リンクをクリックすると、個々のポートロケーションマッピングプロファイルが消去されます。**Delete All** ボタンをクリックすると、ポートロケーションマッピングプロファイルがすべて消去されます。

Port Location Mapping List

Delete Export List Import List Change All Port Types All Search

<input type="checkbox"/>	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
<input type="checkbox"/>	100	1000		Single User	LAN1	Default	●
<input type="checkbox"/>	101	1001		Single User	LAN1	Default	●
<input type="checkbox"/>	102	1002		Single User	LAN1	Default	●
<input type="checkbox"/>	103	1003		Single User	LAN1	Default	●
<input type="checkbox"/>	104	1004		Single User	LAN1	Default	●
<input type="checkbox"/>	105	1005		Single User	LAN1	Default	●
<input type="checkbox"/>	106	1006		Single User	LAN1	Default	●
<input type="checkbox"/>	107	1007		Single User	LAN1	Default	●
<input type="checkbox"/>	108	1008		Single User	LAN1	Default	●
<input type="checkbox"/>	109	1009		Single User	LAN1	Default	●
<input type="checkbox"/>	110	1010		Single User	LAN1	Default	●

12.2 PMS 設定

設定パス : [Main Menu >> System >> PMS Interface](#)

PMS Interface Configuration ページで、管理者はサイトのホスピタリティ管理システムまたは PMS システムと互換性のあるインターフェースタイプを選択できます。

PMS Interface Configuration

PMS Interface Type Disable Micros Opera InnKeyPMS IDS

PMS IP Address

PMS Port

Account Credentials Username Password

Room Bill Description

Login Error Message

User Account Log

Synchronize Data with PMS

PMS External Page Customization API Disable Enable

External Page Validity Verification Username Password

Sample External Login Page

Micros Opera/IDS

インターフェースタイプが Micros Opera または IDS の場合、PMS システム側で設定された PMS IP および Port を入力してください。管理者は、RN（部屋番号）、GN（ゲスト名）、G#（ゲスト番号）、G+（プロファイル名）の組み合わせを使用して、ユーザーアカウントの資格情報を定義し、ユーザー名とパスワード情報を伝送するためのプロトコル・パラメータを指定できます。Micros Opera ユーザーに関する詳細は、オンデマンドアカウントリストから監視することもできます。

On-Demand Account List

Buttons: Delete, Restore List, Backup List, Delete Expired, Delete Out of Quota, **PMS Micros Opera**, Search

■	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
<input type="checkbox"/>	1	16 hr(s) 9 min(s) 8 sec(s)	Expired	Group 1			
<input type="checkbox"/>	pf3k	Until 2013/10/29-12:30	Expired	Group 1	roomN-100-9C:EB:E8:0B:76:8B		
<input type="checkbox"/>	8krm	Until 2013/10/29-22:11	Expired	Group 1	122		
<input type="checkbox"/>	gtum	Until 2013/10/29-22:11	Expired	Group 1	aaaa		
<input type="checkbox"/>	6uw5	Until 2013/10/29-22:11	Expired	Group 1	111		
<input type="checkbox"/>	42s7	Until 2013/10/29-22:11	Expired	Group 1	xx		
<input type="checkbox"/>	qr6e	Until 2013/10/29-22:11	Expired	Group 1	aaq		

Micros Opera User List

Buttons: On-Demand Account List, Search

G#	GN	RN	Username	Password	Remaining Quota	Status	Group
0123456789	0123456789	102	102	0123456789	Until 2013/11/06-22:11	Normal	Group 1

Innkey PMS

インターフェースタイプが Innkey PMS の場合、クエリ API、ポスト API、および PMS システムの共有キーが統合に必要な情報です。部屋番号とゲスト番号は、ユーザーアカウントの資格情報になります。

外部ログインページ用の PMS API

PMS API は、ログイン情報、選択された請求プラン、購入単位などにアクセスプロセスを完了することができ、カスタマイズされたログインページを備えた柔軟な実装を管理者に提供します。管理者は、独自のユーザー名とパスワードを使用して、外部 Web サーバーと EWS コントローラ間の API プロトコルを保護することもできます。さらに、管理者が簡単に変更できるダウンロード可能な例があります。

外部ログインページ用の PMS API は、Micros Opera および IDS インターフェースでのみ利用可能です。

第13章 アカウントローミング

13.1 ローミング関連

ローミング機能は、他の ISP 加入者がより多くの利益源を生成するためにネットワークアクセスを提供しようとする事業者にとって、大規模な配置やアライアンス協力を不可欠な機能です。

EWS コントローラは、Boingo、iPass Connect などの市場におけるほとんどのローミングブローカーとのローミング関係を確立するために必要な WISPR 属性をサポートします。

通信事業者の互換性および技術評価に関する詳細なサポートについては、Edgecore サポートチームにお問い合わせください。

13.2 ISP ローミング用の WiSPr

設定パス : [Main Menu >> System >> Service Zones >> Service Zone Configuration](#)

WiSPr (「whisper」と発音される)、無線インターネットサービスプロバイダローミングというプロトコルは、Wi-Fi Alliance に提出された草案で、携帯電話ユーザーがキャリア間でローミングできるようにするために使用されるのと同様の方法で、ユーザーが無線インターネットサービスプロバイダ間でローミングできるようにするものです。

RADIUS サーバーは、加入者の資格情報を認証するために使用されます。

RADIUS サーバーが構成されている場合、RADIUS 認証中に使用される WISPr 属性をこのサービスゾーンで定義できます。

WISPr Configuration

WISPr Smart Client	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Smart Client Black List	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
	<input type="text"/>
	<small>(Separate by comma)</small>
WISPr Location ID	ISO Country Code <input type="text"/> <small>(e.g. US)</small>
	E.164 Country Code <input type="text"/> <small>(e.g. 1)</small>
	E.164 Area Code <input type="text"/> <small>(e.g. 408)</small>
	Network (SSID/ZONE) <input type="text"/> <small>(e.g. MYWIFI)</small>
WISPr Location Name	Hotspot Operator <input type="text"/> <small>(e.g. MYISP)</small>
	Location <input type="text"/> <small>(e.g. Lobby_of_Airport)</small>
WISPr Billing Time	<input type="text" value="0"/> : <input type="text" value="0"/> <small>(HH:MM)</small>

WISPr Smart Client : WISPr エージェント (iPass、WiFi Skype、Boingo など) のローミングアカウントをお持ちのお客様がインターネットにアクセスできるようにする場合は、Enable を選択してください。クライアントのデバイス上のローミングソフトウェアが正しく動作するためには、System >> General の HTTPS Protected Login (HTTPS 保護されたログイン) フィールドを有効にしてください。

Smart Client Black List : WISPr エージェント名を入力し、その特定の WISPr ローミングエージェントからユーザーのインターネットへのアクセスをブロックすることを有効にしてください。例えば、「ipassconnect」を入力した場合、iPass クライアントはネットワーク内のローミングアクセスを拒否されます。

WISPr Location ID : これらの属性は、無線ホットスポットプロバイダが Web ポータルをカスタマイズできるようにするもので、クライアントデバイスの位置情報に基づいており、RADIUS ベンダー固有属性 (VSA) となっています。

WISPr Location Name : これらの属性は、無線ホットスポットプロバイダが Web ポータルをカスタマイズできるようにするもので、クライアントデバイスの位置情報に基づいており、RADIUS ベンダー固有属性 (VSA) となっています。

WISPr Billing Time : RADIUS アカウントの請求時間を設定してください。

13.3 クロスゲートウェイローミング

設定パス : [Main Menu >> Network >> Client Mobility](#)

クロスゲートウェイローミング機能により、エンドユーザーは、複数のコントローラが存在している大規模なネットワーク配置をシームレスに移動できます。通常、ユーザーがエッジ AP から、別のコントローラで管理されている別のエッジ AP に移動すると、ネットワークが切断され、ネット閲覧を続けるために再ログインが必要になります。

クロスゲートウェイローミングを有効にすると、エンドユーザーはネットワークの中断を経験しません。トラフィックは、インターネットに転送するために元のコントローラにトンネリングされます。

採用されたクロスゲートウェイローミングアーキテクチャ設計は、1つのマスターノードが最大 15 のスレーブノードピアを持つことができるスタートポロジ設計です。マスターノードという用語は、単にこのノードがスタートポロジの中心に位置することを意味します。

役割の決定は、管理者の設定に完全に依存します。ローミングパートナーシップを確立するには、コントローラをマスターノードに、別のコントローラをスレーブノードに設定してください。秘密キーと両方のコントローラの WAN インターフェースがルーティング可能であることを確認してください。

スレーブノードの IP アドレスと秘密キーを設定してください。

Cross Gateway Roaming

Mode Disable Master Mode Slave Mode

Status

Slave Nodes Setting	No.	Active	Remote IP Address*	Secret Key*	Remark
	1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

スレーブノードのマスターノードと秘密キーを設定してください。

Cross Gateway Roaming

Mode Disable Master Mode Slave Mode

Status

Master Node Setting

Remote IP Address *

Secret Key *

Remark

13.4 ローカル/オンデマンドアカウントのローミングアウト

EWS コントローラのローカルおよびオンデマンドの組み込みユーザーアカウントデータベースは、外部 RADIUS 認証データベースとして他のコントローラに使用できます。

このアプリケーションは、認証プロセス中にアカウントの資格情報を検索するために単一の中央コントローラを参照する機能を提供し、複数の支店を持つ企業やビジネスに最適です。

ローカルユーザーデータベースを別のコントローラの RADIUS データベースとして使用するには、次の手順で行います。

設定パス : [Main Menu >> Users >> Internal Authentication >> Local](#)

Local Authentication

User Postfix *

Blacklist

Local User List

Account Roaming Out Enable Disable

802.1X Authentication Enable Disable

オンデマンドユーザーデータベースを別のコントローラの RADIUS データベースとして使用するには、次の手順で行います。設定パス : [Main Menu >> Users >> Internal](#)

On-Demand Authentication

User Postfix:

Billing Plans:

Currency: None \$ USD € EUR £ GBP

This is used when the currency is not defined in the Paypal account. Or input another desired monetary unit (max. 3 letters) in the blank field.

Expired Account Cache: day(s)

Out-of-quota Account Cache: day(s)

On-Demand Access Code: Enable to login with an On-Demand Access Code, not only an On-Demand Account

Smart Login: Enable to allow On-Demand users to login automatically within Days

Set Ticket's Serial Number:

Web Printout:

This will be applied to the regular printer printout when creating a single On-Demand account.

POS Tickets:

Number of Tickets: 1 2

This will be applied to printouts from the POS ticket printer. Templates can be edited for customization.

POS Printer:

Payment Gateway:

SMS Gateway:

Email Verification:

Account Roaming Out: Enable Disable

Blacklist:

RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out	<input type="text" value="10.30.40.45"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text" value="••••"/>	<input type="text"/>
2	Disable	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
3	Roaming Out	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
4	802.1X DM & CoA	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
5	Disable	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
6	Disable	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
7	Disable	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>
8	Disable	<input type="text"/>	<input type="text" value="255.255.255.255 (/32)"/>	<input type="text"/>	<input type="text"/>

ローカルまたはオンデマンドのローミングアウト機能を有効にしたら、RADIUS Client Device Settings（RADIUS クライアントデバイスの設定）ハイパーリンクをクリックし

てください。リダイレクトされたページでは、管理者は、RADIUS クライアントとして動作し、このコントローラの有効なユーザーデータベースに対して認証できるコントローラ IP を指定できます。

メモ

1. ユーザーデータベースの接尾辞が、2つのコントローラ上で互いに競合しないよう設定されていることを確認してください。
-

第14章 VPN

14.1 サイト間

設定パス : [Main Menu >> Network >> VPN](#)

EWS コントローラは、2 つ以上の EWS コントローラに対して**サイト間 VPN** をサポートし、WAN ネットワーク経由で相互に VPN トンネルを作成します。例えば、EWS コントローラが 2 つある場合、1 つの EWS コントローラのサブネットが別の EWS コントローラのサブネットにアクセスできるようにする VPN トンネルを作成できます。

Site-to-Site VPN

Local Sites

Add... Delete

<input type="checkbox"/>	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Test Tunnel to Remote IP
--------------------------	-----	-------------------	-----------------	--------------------	--------------------	--------------------------

Remote Sites

Add... Delete

<input type="checkbox"/>	No.	Name	IP Address	Pre-shared Key
--------------------------	-----	------	------------	----------------

Apply Cancel

まず、少なくとも 1 つのリモートサブネットを持つリモートサイトを追加する必要があります。

Remote Site Configuration

Name	<input type="text"/>									
IP Address	<input type="text"/>									
Authentication Method	Pre-shared Key ▾									
Pre-shared Key	<input type="text"/>									
Phase1 Proposal	Encryption AES256 ▾ Authentication SHA-1 ▾									
Diffie-Hellman Group	<input type="checkbox"/> Group 1 <input type="checkbox"/> Group 2 <input type="checkbox"/> Group 5									
IKE Life Time	8 <input type="text"/> h ▾ (The time is a 5-digit number; e.g. 36h stands for 1 day and 12 hours)									
Dead Peer Detection	DPD Delay 10 <input type="text"/> (second) DPD Timeout 15 <input type="text"/> (second)									
Remote Subnet	<table border="1"><thead><tr><th>No.</th><th>Network</th><th>Mask</th></tr></thead><tbody><tr><td>1</td><td><input type="text"/></td><td>255.255.255.255 (/32) ▾</td></tr><tr><td>2</td><td><input type="text"/></td><td>255.255.255.255 (/32) ▾</td></tr></tbody></table>	No.	Network	Mask	1	<input type="text"/>	255.255.255.255 (/32) ▾	2	<input type="text"/>	255.255.255.255 (/32) ▾
No.	Network	Mask								
1	<input type="text"/>	255.255.255.255 (/32) ▾								
2	<input type="text"/>	255.255.255.255 (/32) ▾								

メモ

1. 両方のサイトの IPSec 設定は同じである必要があります。

次に、リモートサイトにマッピングするためのサブネットを持つローカルサイトを作成します。例えば、EWS コントローラ_A の「192.168.11.0/24」 >> EWS コントローラ_B の「192.168.111.0/24」のように、トンネルが作成されると、これら 2 つのサブネット内のユーザーは互いに到達できます。

Local Site Configuration

Local Interface	WAN1 ▾
Remote VPN Gateway	▾ Edit Host Add a New Host
Local Host/Subnet	<input checked="" type="radio"/> Host <input type="radio"/> Subnet
Remote Host/Subnet	▾
Phase2 Proposal	Encryption AES256 ▾ Authentication SHA-1 ▾
Key Life Time	24 <input type="text"/> h ▾ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
Rekey	<input type="checkbox"/> Enable Rekey Rekey Margin 9 <input type="text"/> m ▾ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
Perfect Forward Secrecy	<input checked="" type="checkbox"/> Enable PFS PFS Group Group 2 ▾

1. 複数のVPNトンネルを作成できますが、1つのIPセグメントに2つのルーティングルールを設定できないため、IPセグメントマッピングは重複できません。

14.2 リモートクライアント

設定パス : [Main Menu >> Network >> VPN](#)

EWS コントローラは、リモートエリアからシステムへのユーザーログインのためのリモートVPNをサポートしています。ユーザーがWANの外部ネットワークからシステムにログインすると、EWS コントローラへのログインがローカルでサービスゾーンの下にあることがユーザーに表示されます。リモートユーザーとコントローラの間で転送されるデータは、IKEv2 VPNトンネルで暗号化されます。また、ポリシーを適用することができ、ユーザーはネットワークにアクセスするためにシステムによって制御されます。

Remote VPN IKEv2

Function Enable Disable

Allocate IP Address from IP Address * Subnet Mask ▼

Certificate ▼

WISPr

Authentication Options

Auth Option	Auth Database	Postfix	Enable
Server 1	LOCAL	local	<input type="checkbox"/>
Server 2	RADIUS	.	<input type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="checkbox"/>
Server 4	LDAP	ldap	<input type="checkbox"/>
Server 5	POP3	pop3	<input type="checkbox"/>

すべての設定は、サービスゾーンの設定に似ています。リモートVPNは、専用サブネット、証明書、WISPr設定、認証オプションを使用して設定することもできます。

リモートVPNを有効にすると、ユーザーはクライアントデバイス上のVPNツールを使用して、有効化された認証オプションのユーザー名とパスワードを使用してVPNリンクをセットアップできます。

メモ

1. リモート VPN クライアントは、[Main Menu >> Users >> Groups >> Configuration](#) のページで異なるユーザーポリシーによって適用できます。
-

第15章 スイッチ管理

EWS コントローラは、Edgecore スイッチを管理するための包括的なインターフェースを提供します。

15.1 スイッチリスト

設定パス : [Main Menu >> Devices >> Switch Management >> Switch List](#)



EWS コントローラの WAN ポートまたは LAN ポートに接続されたスイッチは、手動で、または検出によって追加できます。

The screenshot shows the 'Add Switch' form. At the top, there is a dropdown menu for 'Add Method' set to 'Add Switch'. The form fields are as follows:

Field Name	Value / Status
Device Type	ECS2100-10P
Device IP	[Empty] *
Device MAC	[Empty] *
Device Name	[Empty] *
Login ID	admin
Password	[Empty] *
SNMP Community Read	[Empty] *

スイッチがリストに正常に追加されると、そのステータスが表示されます。

Switch List

Status

<input type="checkbox"/>	Name	Type	Status	IP address	MAC address	Total allocated/Used/Max supply power [W]	Switch UI
<input type="checkbox"/>	TestSW	ECS2100-10P	Offline	10.73.36.210	AA:BB:CC:DD:EE:FF	Switch Offline	<input type="button" value="Go to"/>

Switch List には、スイッチ名、スイッチタイプ、ステータス、IP アドレス、MAC アドレス、パワーバジェット、およびスイッチ管理 Web インターフェースへのショートカットリンクが表示されます。

15.2 PoE スケジュールテンプレート

設定パス : [Main Menu >> Devices >> Switch Management >> PoE Schedule Template](#)

PoE スケジュールテンプレートを使用すると、管理者は、管理対象スイッチの割り当てられたポートに電力を供給するスケジュールを設定できます。この機能は、管理対象スイッチから PoE によって電力供給される場合に、AP スケジュールを制御するために使用できます。

Main > Switches > PoE Template

PoE Schedule Template

Template Name	Copy Settings From	Remark	Action
<input type="text" value="Default"/>	<input type="text" value="NONE"/>	<input type="text"/>	

テンプレートは、鉛筆アイコンをクリックして追加またはカスタマイズできます。

■	Day	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<input type="checkbox"/>	Sun	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Mon	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Tue	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Wed	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Thu	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Fri	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Sat	<input checked="" type="checkbox"/>																							

Apply to

Refresh

■	Port	PoE Mode	Connected Device	■	Port	PoE Mode	Connected Device
<input type="checkbox"/>	1			<input type="checkbox"/>	13		
<input type="checkbox"/>	2			<input type="checkbox"/>	14		
<input type="checkbox"/>	3			<input type="checkbox"/>	15		
<input type="checkbox"/>	4			<input type="checkbox"/>	16		
<input type="checkbox"/>	5			<input type="checkbox"/>	17		
<input type="checkbox"/>	6			<input type="checkbox"/>	18		
<input type="checkbox"/>	7			<input type="checkbox"/>	19		
<input type="checkbox"/>	8			<input type="checkbox"/>	20		
<input type="checkbox"/>	9			<input type="checkbox"/>	21		
<input type="checkbox"/>	10			<input type="checkbox"/>	22		
<input type="checkbox"/>	11			<input type="checkbox"/>	23		
<input type="checkbox"/>	12			<input type="checkbox"/>	24		

15.3 バックアップ設定

設定パス : [Main Menu >> Devices >> Switch Management >> Backup Configuration](#)

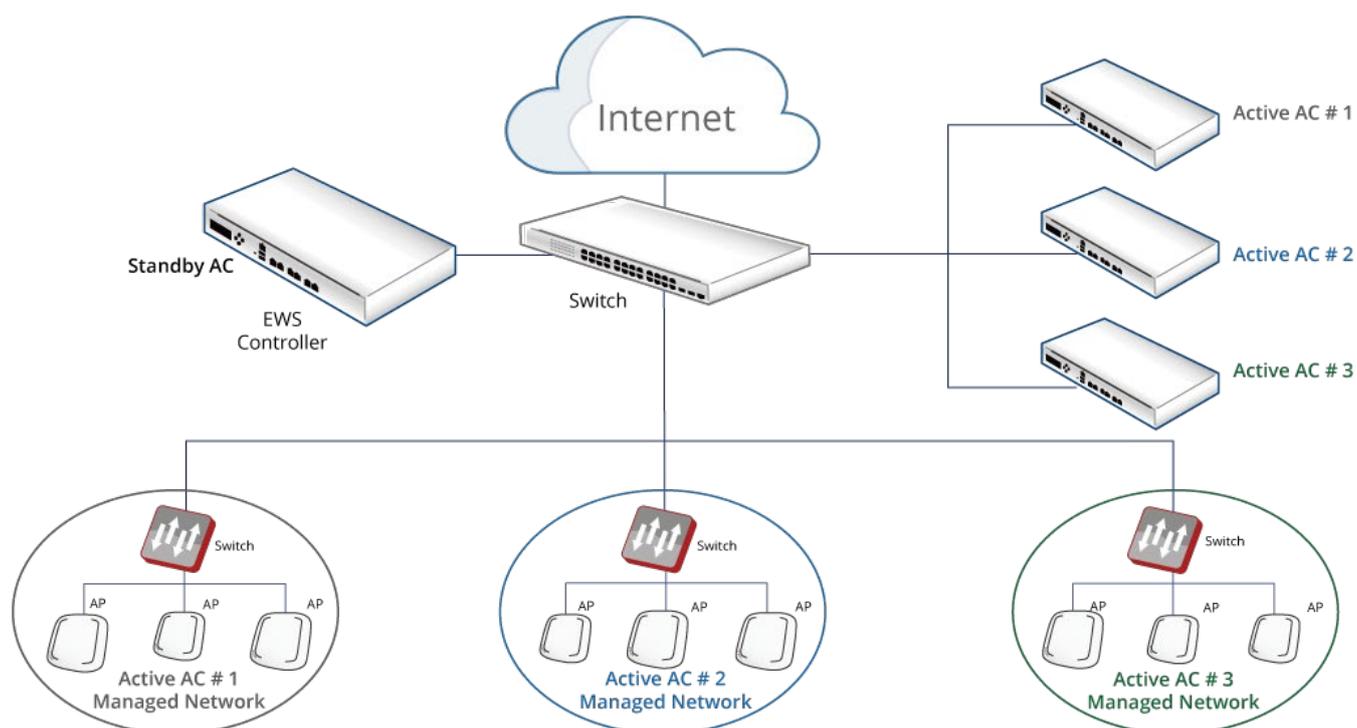
Backup Configuration には、管理対象スイッチからバックアップされた設定のリストが表示されます。スイッチを選択して「Backup」をクリックすると、設定をこのリストに保存できます。

第16章 プラットフォームに依存する機能

16.1 高可用性 (HA) (EWS5203、EWS5204、EWS5207)

Edgecore HA の設計原則は、冗長性を使用して可用性を高め、サービス移行時の影響を最小限に抑えることです。Edgecore HA アプローチでは、AC (アクセスコントローラ) 間に専用のメッセージリンクを実装し、N が ≤ 3 の N+1 冗長システムを作成します。HA リンクが確立されると、アクティブ AC はすべてのネットワークトラフィックにサービスを提供しますが、スタンバイ AC はホットスタンバイ状態になり、アクティブ AC がサービスを提供できなくなった場合に備えて、ネットワークサービスを引き継ぐ準備が整います。

設定パス : [Main Menu >> System >> High Availability](#)



機能の説明 :

1. Edgecore HA 機能は、ソフトウェアによって決定された機能で、有効または無効にすることができます。

ソフトウェアによって決定されたイーサネットの役割 :

- 有効にすると、LAN1 ポートが専用の HA ポートになります。

- 無効にすると、LAN1 は LAN ポートとして通常の機能のままになります。
2. Web UI には、HA 機能が有効になっている場合に、この AC を「Active」または「Standby」として指定するための構成項目があります。
 3. すべての HA 設定は手動で適用されます。これには、アクティブまたはスタンバイとしての AC の役割と、AC がダウンした後の HA ペアの復元が含まれます。

Configuration

Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Number of Active(s)	2 ▼
Mode	<input checked="" type="radio"/> Active <input type="radio"/> Standby
HA Port IP Address	172.31.0.1 *
HA Port Subnet Mask	255.255.0.0 *
Peer IP Address	10.1.2.3 *
Shared Key *

Configuration

Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Number of Active(s)	2 ▼
Mode	<input type="radio"/> Active <input checked="" type="radio"/> Standby
HA Port IP Address	172.31.0.3 *
HA Port Subnet Mask	255.255.0.0 *
#1 Peer IP Address	10.1.2.1 *
#2 Peer IP Address	10.1.2.2 *
Shared Key *
Switch Support	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

4. HA リンクが確立されると、すべてのシステム構成、ユーザーデータベース、ユーザーオンラインステータス、システムリソースステータス、管理対象 AP プロファイルをアクティブ AC からスタンバイ AC に同期します。
5. HA リンクが確立されると、スタンバイ AC による HA リンク監視メカニズムがあります。このリンク監視モジュールは、アクティブ AC のステータスをチェックします。アクティブ AC が応答していないイベント中、このモジュールは、この AC をサービスを提供しなくなったと見なし、ネットワークサービスを引き継いでいます。
6. HA リンク確立時には、アクティブ AC による HA リンク監視メカニズムがあります。この監視モジュールは、アクティブ AC の WAN1 ポートのステータスを確認します。(Target for Detecting Internet Connection に記載の) IP アドレスやドメイン名への Ping に失敗すると、このモジュールはアクティブ AC はこれ以上サービスを提供できないと判断し、スタンバイ AC がネットワークサービスを引き継ぎます。もともとのアクティブ AC はスタンバイ AC になります。

Target for Detecting Internet Connection

8.8.8.8

Enter IP Address/Domain Name Here

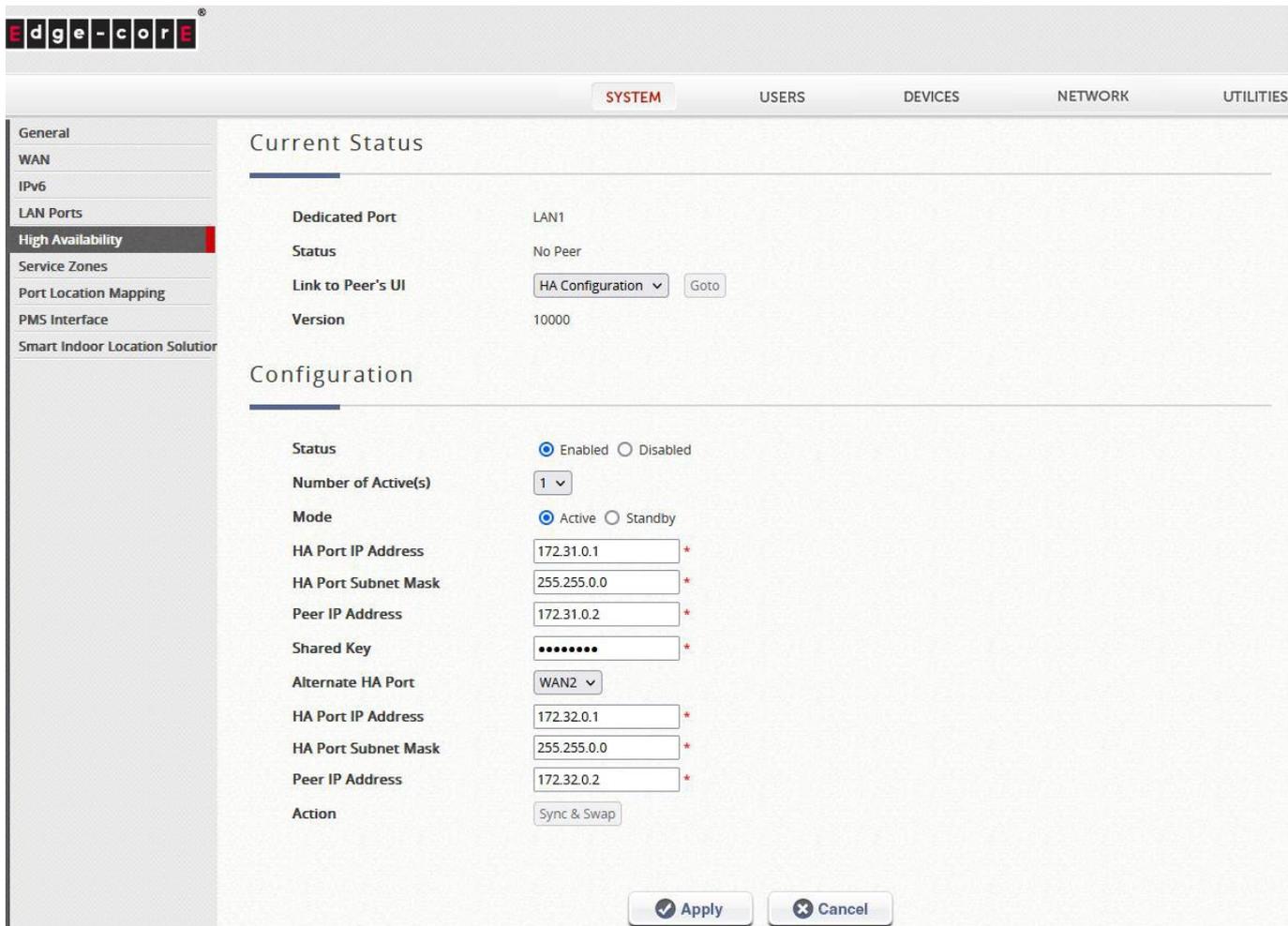
Enter IP Address/Domain Name Here

Warning of Internet Disconnection

When the addresses for detecting internet connection are unreachable, this message will be shown on the browser.

Sorry! The service is temporarily unavailable.

7. ローカル APM 管理対象 AP は、L2 デバイスであるため、ネットワークの中断はほとんど発生しません。ローカルで管理される AP に関連付けられたクライアントは、サービススイッチオーバー中に、有線クライアントと同じシナリオ（ネットワークの中断がほとんどまたはまったく発生しません）が発生します。
8. トンネルが確立された L3 デバイス上のワイドエリア管理対象 AP（手動または CAPWAP 経由）は、サービススイッチオーバー後、最大 5 分（概算）以内に AP 管理能力をフルに確保してサービスを再開できます。
9. HA ステータスの変更電子メール通知は、Status > Reporting > Notification Settings > High Availability Mode Change で設定できます。HA N+1 の場合、サービスを提供するために新しいアクティブ AC が入れ替わったときに、新しいアクティブ AC によって電子メールが送信されます。また、HA がすでに有効になっているときにスタンバイ AC が検出されない場合、アクティブ AC から Standby-AC-is-DOWN のメールが送信されます。
10. HA 機能は、同じブランドおよび同じ FW バージョンおよびビルド番号の最大 3 つの AC に対してのみ有効にできます。
11. ユーザーは WAN2 をセカンダリ HA 検出ポートとして設定でき、プライマリ HA ポートが故障した場合、セカンダリ HA ポートがチェックされます。プライマリとセカンダリの両方のポートに障害が発生した場合、HA スワップイベントがトリガーされます。
12. 以下のトラップを HA イベント発生時のユーザーアラートに追加します：
 - a. slavetoMaster : スタンバイからアクティブへの HA フェイルオーバー
 - b. slaveDown: HA スタンバイダウン
 - c. HAPortDown : HA ポートダウン
 - d. AlternatePortDown : HA 代替ポートダウン
 - e. InternetWAN1DOWN/InternetUP: インターネット接続の Ping テストに失敗/成功



メモ

1. 冗長構成時には、管理 IP アドレスリストに Active 機の IP アドレスを入れなければ Standby 機にアクセスできなくなります。
2. スタンバイ機がアクティブ機に同期できていないという情報は表示されません。また、通知もされません。現在のステータスの「ピア UI ヘリンク」の実行ボタンからスタンバイ機の管理画面へアクセスできない場合スタンバイ機がアクティブ機に同期できていない状態になります。
3. HA モードでは、コントローラが FW をアップグレードする必要がある場合、FW をアップグレードする前に HA を無効化する必要があります。

16.2 WiFi モニター（EWS5203、EWS5204、EWS5207）

WiFi モニターを使用すると、仮想エリアでも、実際の管理対象 AP 信号カバレッジでも、管理者はアクセスポイントの WiFi 信号カバレッジをシミュレートできます。また、管理対象 AP の

AP ステータスおよび統計情報も監視します。

これは、管理者がネットワーク調査、初期設置段階での計画およびパフォーマンスの向上、および既存の配置の管理対象 AP の監視に役立つように設計されています。

フロアプランには、次の 3 つのタイプがあります。仮想、ローカル、ワイドです。

16.2.1.フロアプランを追加する

WiFi モニターは、AP を配置する場所と、AP の数が初期設置時にスループット要件を満たすかどうかを管理者が決定できるように設計されています。まず、.jpg 形式のマップまたはフロアプランが必要です。パーティションは.xml 形式または.osm 形式で描画されます。

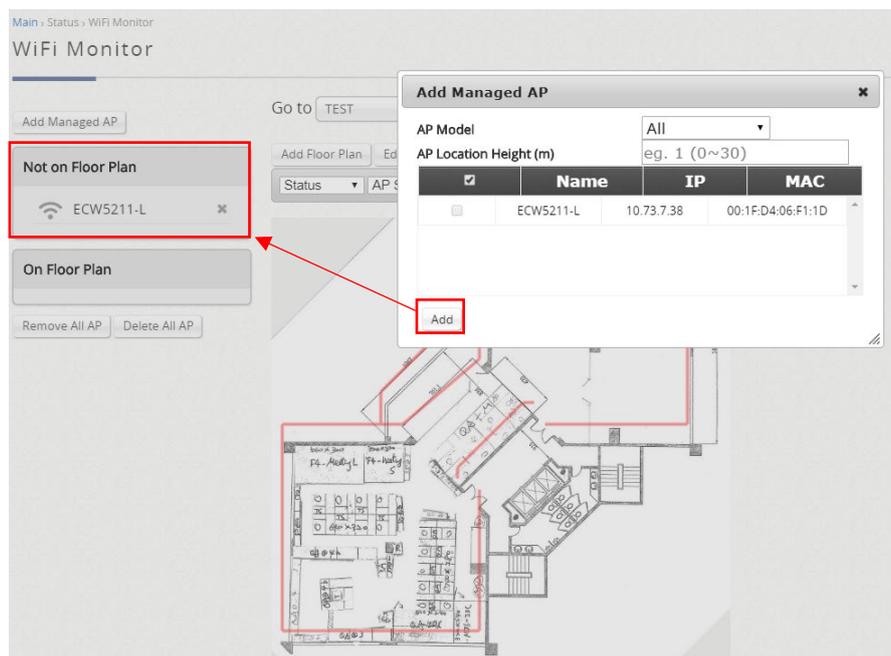
The image shows two screenshots of a web interface. The top screenshot is the 'WiFi Monitor' page, which has a navigation menu on the left and a main content area. The 'Add Floor Plan' form is overlaid on the main content area. The bottom screenshot is a close-up of the 'Add Floor Plan' form, showing the following fields and values:

Field	Value	Notes
Floor Plan Type	Local	Dropdown menu
Floor Plan Name	WiFi Monitor Testing	Required (*)
Floor Plan (.jpg)	House-Design...lans-011.jpg	Selected from file manager, Required (*), Under 256k, JPG
Wall (.xml)	floor.xml	Selected from file manager, Required (*)
Map Width (m)	79	Required (*), Range (1-200)
Map Length (m)	79	Required (*), Range (1-200)
Country Code	USA	Dropdown menu
Height of Receiving Device (m)	1	Required (*), Range (1-10)

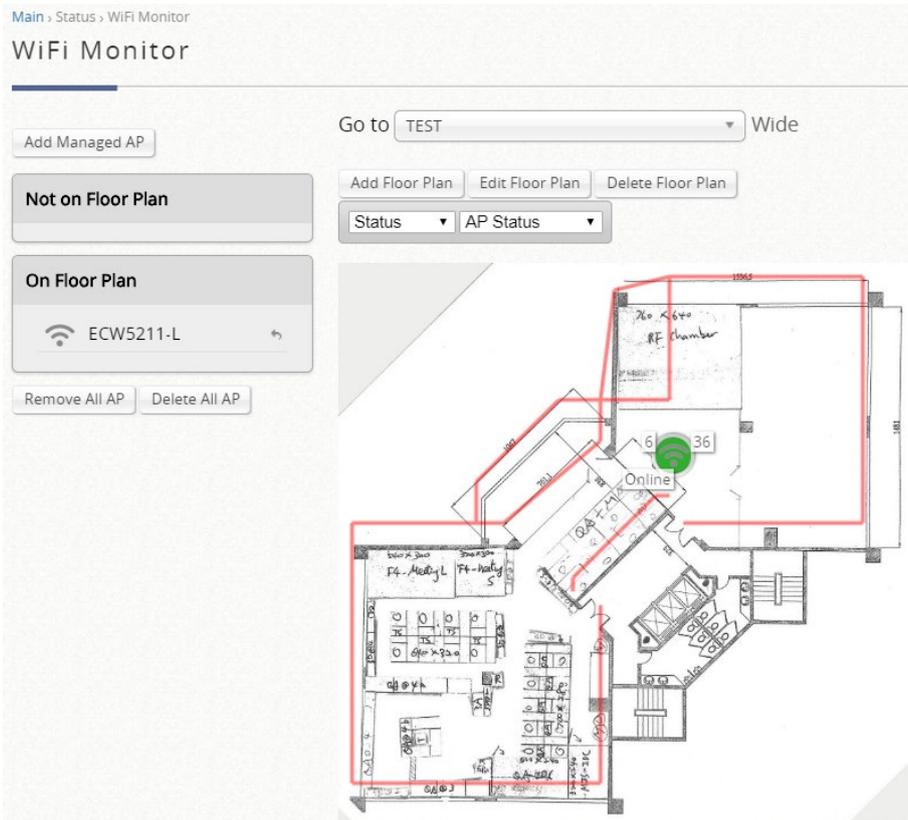
On the right side of the form, there is a preview of a floor plan with a red border. Below the preview, there are navigation controls (back, forward, home, search, zoom in, zoom out) and a note: "Original size of floor plan is twice of this displayed sample". At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

管理対象 AP シミュレーションは、場所に基づいてアクセスポイントの監視に利用されます。管理対象 AP シミュレーションのフロアプラン上の AP は、コントローラ上の実際の管理対象アクセスポイントです（ローカル AP 管理またはワイド AP 管理のいずれか）。

このアクセスポイントは、EWS コントローラによって管理される AP にリンクされており、IP アドレス、MAC アドレス、関連クライアント番号などの実際の AP 情報を見ることができます。これにより、管理者は AP の位置を基準に無線ネットワークを簡単に視覚化できます。



これらの管理対象 AP を作成したら、これらの AP をフロアプランにドラッグ&ドロップするだけです。2.4GHz は青色、5GHz は赤色で信号強度を示します（したがって、両方のバンドが重なっている場合は紫色）。



管理対象 AP の信号強度とカバレッジは、AP モデル、送信電力、AP の高さなどの要因によって異なります。



16.2.2. シミュレーション AP

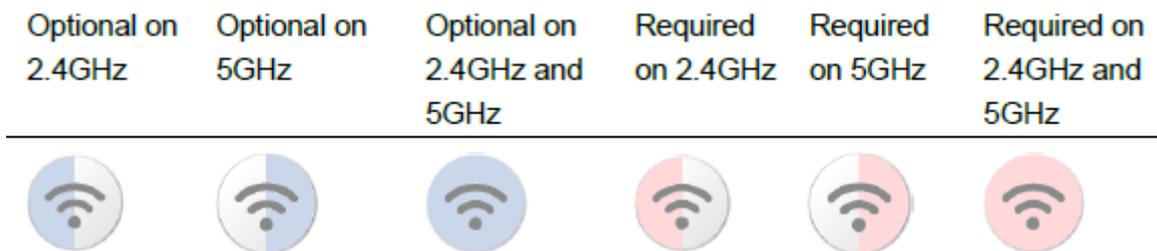
WiFi モニターは、Edgecore AP をシミュレートし、フロアプランに配置し、最適化で関連する設定をチェックすることができます。一方、シミュレーション AP の信号強度とカバレッジは、AP モデル、送信電力、AP の高さなどの要因によって異なります。

フロアプランとパーティションを配置すると、以下に示すように、シミュレーション用のフロ

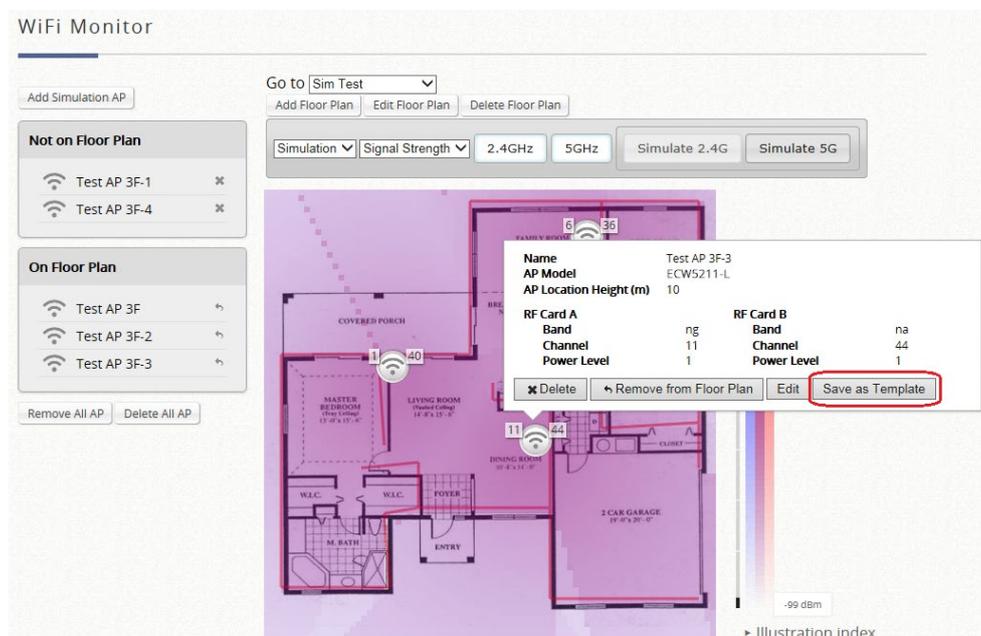
アプランにシミュレーション AP を追加できるようになりました。



「Simulate 2.4G」または「Simulate 5G」をクリックして、配置された AP が要件に適切かどうかを確認してください。



シミュレーションが正常に完了すると、推奨チャンネル割り当てがシミュレーション AP の横に表示されます。

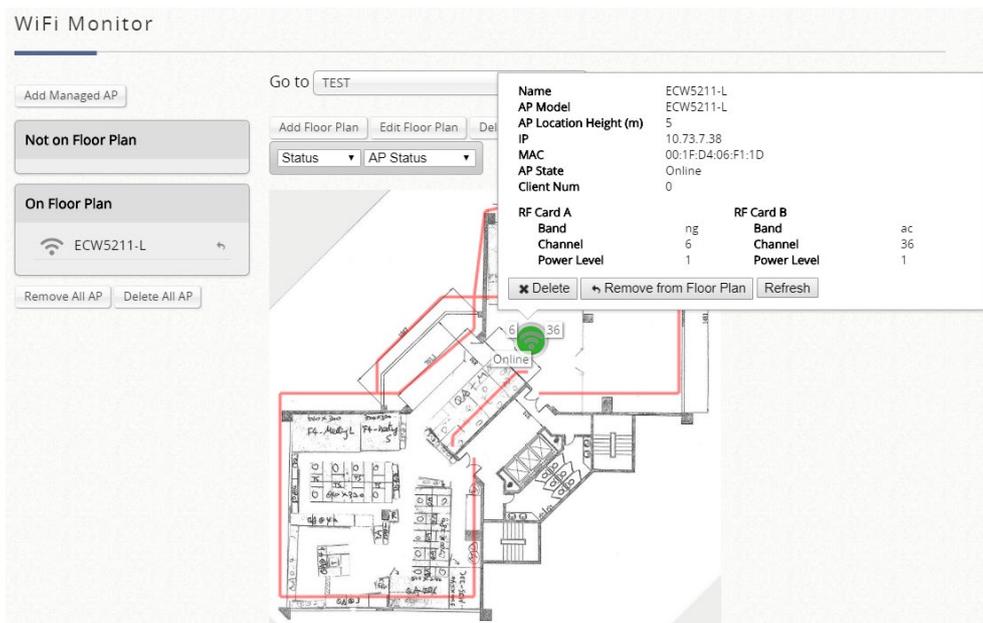


この設定は、AP 管理に使用するテンプレートに便利に保存できます。

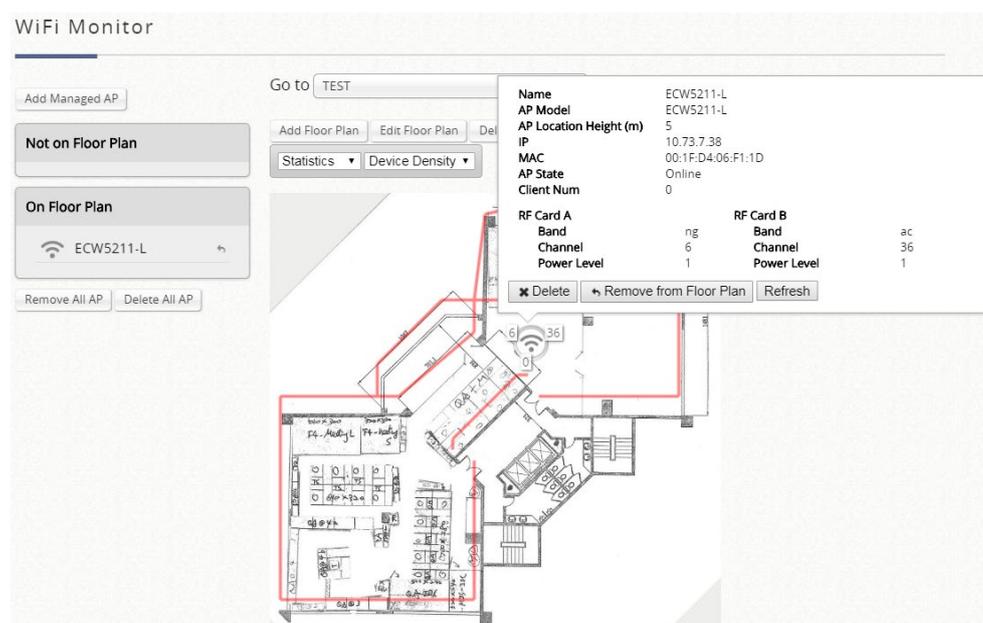
16.2.3.フロアプランの AP 監視

AP が動作しているエリアでは、管理者は作成したフロアプランから AP ステータスを表示できます。

AP ステータスは「Online」、「Offline」または「Disabled」と表示されます。また、AP がワイドエリア AP 管理によって管理されている場合、管理者は CPU アイドル状態とメモリ使用量を取得することもできます。



APがワイドエリアAP管理を使用して管理されている場合、AP密度やAP平均トラフィック、AP平均トラフィックなどのAP統計情報もサポートされます。



付録A EWS モデルと設置

付録 A-1 EWS の機種と設置方法

EWS コントローラ容量表

容量	EWS101	EWS5203	EWS5204	EWS5207
フォームファクタ	7.5 インチ デスクトップ	19 インチ (1U)	19 インチ (1U)	19 インチ (2U)
WAN	1 x GbE	2 x GbE または 2 x 1G SFP	2 x GbE 2 x 1G SFP	2 x GbE、 2 x 10Gb SFP+
LAN	4 x GbE	8 x GbE	6 x GbE 2 x 1G SFP	6 x GbE、 2 x 10Gb SFP+
ローカルアカウント	2000	10000	30000	50000
オンデマンドアカウント	2000	10000	30000	50000
管理対象 AP 容量 (ローカルとワイド併用)	50	300	1000	3000
最大同時ユーザー数	200	3000	10000	30000
管理可能な AP モデル	リリースノートをご参照ください。			
監視対象 AP	100	250	500	500
サービスゾーン	デフォルト + 8	デフォルト + 8	デフォルト + 32	デフォルト + 64
ユーザーグループ	8	16	24	24
ユーザーポリシー	グローバル + 12	グローバル + 24	グローバル + 40	グローバル + 40

*1: さまざまな展開シナリオに対応するイーサネットポート割り当てオプション

*表の内容は予告なく変更する場合があります。

ハードウェアの概要

EWS101 ハードウェア

1	リセット/再始動ボタン	リセットボタンを 3 秒以上押し続けると、フロントパネルの LED の状態が点滅し始めます。この段階でボタンを放すとシステムを再始動します。リセットボタンを 10 秒以上押し続けると、フロントパネルの LED の状態が点滅から消えます。この段階
---	-------------	--

		で放すと、システムをデフォルト設定にリセットします。
2	コンソール	システムは、シリアルコンソールポートを介して設定できます。管理者は、Microsoft の Hyper Terminal などの端末エミュレーションプログラムを使用して、設定コンソールインターフェースにログインし、管理者パスワードを変更したり、システムステータスを監視したりすることができます。
3	LAN1~LAN4	クライアントマシンまたはスイッチは、LAN ポート（10/100/1000 Base-T RJ45）を介して EWS コントローラに接続します。
4	WAN1	ISP（インターネットサービスプロバイダ）からの ADSL ルータなどの外部ネットワークへのアップリンク接続用の WAN ポート（10/100/1000 Base-T RJ45）。
5	USB	将来の使用のために備えた機能。
6	LED ディスプレイ	電源 ：電源がオンになると、電源 LED が一定の緑色に点灯します。 ステータス ：点滅は、システム OS が起動していることを示します。システムが動作可能な状態になると、LED は常に点灯します。

EWS5203 ハードウェア

1	リセット/再始動ボタン	リセットボタンを約 5 秒間押し続けると、システムを再始動する前にフロントパネルの LED の状態が点滅し始めます。 リセットボタンを 10 秒以上押し続けると、フロントパネルの LED の状態が点滅し始めてから、システムをデフォルト設定にリセットします。
2	USB	将来の使用のために備えました。
3	WAN1/WAN2 (SFP)	ISP（インターネットサービスプロバイダ）からの ADSL ルータなどの外部ネットワークへのアップリンク接続用の 2 つのコンボ WAN ポート（SFP）。
4	WAN1/WAN2 (RJ45)	ISP（インターネットサービスプロバイダ）からの ADSL ルータなどの外部ネットワークへのアップリンク接続用の 2 つのギガビット WAN ポート（10/100/1000 Base-T RJ45）。
5	コンソール	システムは、シリアルコンソールポートを介して設定できます。管理者は、Microsoft の Hyper Terminal などの端末エミュレーションプログラムを使用して、設定コンソールインターフェースにログインし、管理者パスワードを変更したり、システムステータスを監視したりすることができます。
6	LED インジケータ	電源 ：電源がオンになると、電源 LED が一定の緑色に点灯します。 ステータス ：点滅は、システム OS が起動していることを示します。システムが動作可能な状態になると、LED は常に点灯します。
7	LAN1~LAN8	LAN トラフィックを処理するための 8 つのギガビット LAN ポート（10/100/1000 Base-T RJ45）。

EWS5204 ハードウェア

1	液晶ディスプレイ	ネットワーク管理者は、ネットワークインターフェース、SZ 構成などの重要なシステム設定を確認することができます。左から右へのナビゲーションボタンは、それぞれ「Esc」、「Up」、「Down」、「Enter」です。
2	LED インジケータ	2つの LED インジケータ、電源、HDD（ハードディスク）があり、システムの異なるステータスを示します。
3	再始動ボタン	再始動ボタンを約 5 秒間押し続けると、システムが再始動します。
4	コンソール	システムは、シリアルコンソールポートを介して設定できます。管理者は、Microsoft の Hyper Terminal などの端末エミュレーションプログラムを使用して、設定コンソールインターフェースにログインし、管理者パスワードを変更したり、システムステータスを監視したりすることができます。
5	USB	将来の使用のために備えました。
6	WAN1/WAN2 (RJ45)	2つの WAN ポート（10/100/1000 Base-T RJ45）は、ISP（インターネットサービスプロバイダ）から ADSL ルータなどの外部ネットワークに接続されています。
7	LAN1~LAN6 (RJ45)	クライアントマシンは、これらの LAN ポート（10/100/1000 Base-T RJ45）を介して EWS コントローラに接続します。
8	WAN1/WAN2 (SFP)	2つのコンポ WAN ポート（SFP）が ISP（インターネットサービスプロバイダ）から ADSL ルータなどの外部ネットワークに接続されています。
9	LAN1/LAN2 (SFP)	クライアントマシンは、これらの LAN ポート（SFP）を介して EWS コントローラに接続します。

EWS5207 ハードウェア

1	LED インジケータ	<p>ERR（電源エラー）： PSU の状態が正常であれば消灯し、いずれかの電源が故障した場合はオレンジ色のライトが点灯します。</p> <p>STBY（システムスタンバイ）： システムの準備ができている場合は、オレンジ色のライトが常に点灯します。</p> <p>HDD（ハードディスク）： データが転送されない場合は消灯し、HDD の読み取り/書き込みが行われている場合は緑色のライトが点滅します。</p> <p>PWR（電源）： 電源を入れると緑のライトが点灯。</p>
2	液晶ディスプレイ	ネットワーク管理者は、ネットワークインターフェース、SZ 構成などの重要なシステム設定を確認することができます。左から右へのナビゲーションボタンは、それぞれ「Esc」、「Up」、「Down」、「Enter」です。
3	コンソール	システムは、シリアルコンソールポートを介して設定できます。管理者は、Microsoft の Hyper Terminal などの端末エミュレーションプログラムを使用して、設定コンソールインターフェースにログインし、管理者パスワードを変更したり、システムステータスを監視したりすることができます。

4	USB	将来の使用のために備えました。
5	MGMT ポート	管理者が EWS コントローラを管理するためのものです。
6	再始動ボタン	再始動ボタンを約 5 秒間押し続けると、システムが再始動します。
7	WAN1/WAN2 (SFP+)	2 つの WAN ポート (10G SFP+) は、ISP (インターネットサービスプロバイダ) から ADSL ルータなどの外部ネットワークに接続されています。
8	LAN7/LAN8 (SFP+)	クライアントマシンは、これらの LAN ポート (10G SFP+) を介して EWS コントローラに接続します。
9	WAN1/WAN2 (RJ45)	2 つの WAN ポート (10/100/1000 Base-T RJ45) は、ISP (インターネットサービスプロバイダ) から ADSL ルータなどの外部ネットワークに接続されています。
10	LAN1~LAN6 (RJ45)	クライアントマシンは、これらの LAN ポート (10/100/1000 Base-T RJ45) を介して EWS コントローラに接続します。

設置手順

準備

1. EWS コントローラを開梱し、パッケージのチェックリストを確認します。
2. 前面パネルと背面パネルを確認し、ハードウェアと仕様セクションで説明されている各コントロールおよびネットワークインターフェースを識別します。
3. RJ-45 コネクタを備えたイーサネットケーブルを準備します。
4. Web 管理インターフェースにアクセスするための Web ブラウザを備えた PC を準備します。
5. ADSL、ケーブルモデム、その他のエッジデバイスなど、EWS コントローラがネットワークに接続するためのアップストリームデバイスを特定します。ISP から提供された DNS サーバーアドレスを収集します。

設置

- 1) 電源アダプタまたは電源ケーブルを背面パネルの電源ソケットに接続します。電源 LED が点灯し、正しく接続されていることを示します。
- 2) 前面パネルの WAN1 ポートにイーサネットケーブルを接続します。イーサネットケーブルのもう一方の端を、xDSL/ケーブルモデム、または内部ネットワークのスイッチ/ハブに接続します。このポートの LED が点灯し、正しく接続されていることを示します。
- 3) イーサネットケーブルを、前面パネルの LAN ポートに接続します。システムを設定するために、イーサネットケーブルのもう一方の端を管理者 PC に接続します。スイッチは、コントローラの LAN ポートに複数のデバイスを接続するために使用できます。

メモ

1. 最高の性能を保証するために、他のサプライヤーの部品を置き換えるのではなく、パッケージ内のすべての供給品を使用することを強くお勧めします。

付録 A-2 VEWS の機種と設置方法

VEWS コントローラー性能表

性能	VEWS5203	VEWS5204	VEWS5207	VEWS1000
ローカルアカウント数	10000	30000	50000	120000
オンデマンドアカウント	10000	30000	50000	120000
管理可能なAP数	300	1000	3000	10000
最大同時接続ユーザー数	3000	10000	30000	100000
管理可能なAPモデル	リリースノートをご参照ください。			
モニターAP	250	500	500	500
WAPM テンプレート	500	500	500	500

導入インストラクション

前提条件

- ・ Linuxシステム上で動作するOne Serverです。本書では Ubuntu v18.04 を例として使用します。
- ・ VEWS のイメージファイル (qcow2 形式)。イメージファイルの入手については、ecwifi@edge-core.com までお問い合わせください。
- ・ VM 環境の設定ファイル "V-EWS.xml"。テンプレートファイルの入手は、ecwifi@edge-core.com にお問い合わせください。
- ・ VEWS のバウチャーコード。対応するライセンスのバウチャーコードは、Edge-core 営業または ecwifi@edge-core.com までお問い合わせください。

ステップ 1. Ubuntu システムに KVM をインストールする

ターミナルを開いて "sudo apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virtinst" を実行してください。

```
root@v-ews:/# apt install qemu-kvm libvirt-daemon-system libvirt-clients bridge-utils virtinst
```

インストール後、libvirt デーモンが動作していることを確認するために、"systemctl is-active libvirtd" を実行します。

```
root@v-ews:/var/lib/libvirt/images# systemctl is-active libvirtd
active
```

ステップ 2. システムのネットワーク構成を変更する

VM が物理インターフェイス経由でネットワークにアクセスできるようにするには、物理イーサネットインターフェイスと仮想ネットワークインターフェイスをブリッジするブリッジインターフェイスを作成する必要があります。以下のスクリーンショットは、Netplan ツールでネットワークを構成する例を示しています。この例では、ブリッジ・インターフェースを **br0** と名付け、物理ネットワーク・インターフェースを **ens33** としています。

```
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens33:
      dhcp4: false
  bridge:
    br0:
      dhcp4: true
      interfaces:
        - ens33
  version: 2
```

ステップ **3.XML** ファイルを環境にあわせて編集する

- Modify □ <domain> <name> 要素の VM 名を変更します。

以下の画面は、「V-EWS」という名称を使用した例です。

```
<domain type='kvm'>
  <name>V-EWS</name>
  <memory unit='KiB'>1048576</memory>
  <currentMemory unit='KiB'>1048576</currentMemory>
  <vcpu placement='static'>2</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
```

- <domain> <device> <disk> <source> 要素の VM ディスクパスを変更します。ここには、VEWS のイメージファイルのパスを記入する必要があります。

以下のスクリーンショットは、VEWS イメージのパスが

"/var/lib/libvirt/images/Edgecore_V-EWS_3.43.S0_1.55.4.1-1.9481.2.33.2.38.qcow2" の場合の例です。

```
<disk type='file' device='disk'>
  <driver name='aemu' type='qcow2' />
  <source file='/var/lib/libvirt/images/Edgecore_V-EWS_3.43.V1_1.5-1.9481.2.46.4.8.qcow2' />
  <target dev='vda' bus='virtio' />
  <alias name='virtio-disk0' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0' />
</disk>
```

- <domain> <device> <interface> <source>要素で VM の NIC を変更します。

この例では、モードは「bridge」で、VM の NIC は br0 にブリッジされることとなります。

```
<interface type='bridge'>
  <source bridge='br0' />
  <target dev='vnet0' />
  <model type='virtio' />
  <alias name='net0' />
  <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0' />
</interface>
```

ステップ4. 画像ファイルをコピーする

VEWS のイメージファイルを「/var/lib/libvirt/images/」にコピーします。

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# ls -al
total 149132
drwx--x--x 2 root      root      4096   五  23 14:58 .
drwxr-xr-x 7 root      root      4096   五  23 13:27 ..
-rw-r--r-- 1 libvirt-qemu kvm 152698880   五  23 12:10 Edgecore_V-EWS_3.43.V1_1.5-1.9481.2.46.4.8.qcow2
-rw-r--r-- 1 root      root      1792   五  23 14:58 V-EWS.xml
root@vincent-Aspire-4752:/var/lib/libvirt/images#
```

ステップ 5. VM の作成と起動

- 以下のコマンドを使用して、**VM** を作成し、起動します。

virsh define V-EWS.xml を実行します。

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh define V-EWS.xml
Domain V-EWS defined from V-EWS.xml
```

V-EWS を起動します。

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh start V-EWS
Domain V-EWS started
```

virsh list (VM が起動していることを確認します。)

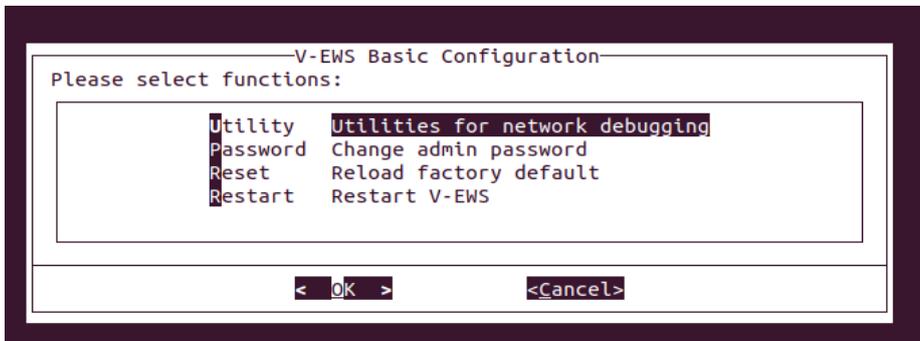
```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh list
 Id   Name                               State
-----
  1   V-EWS                              running
```

- ステップ 6.VM のコンソールからデフォルト **IP** を取得する

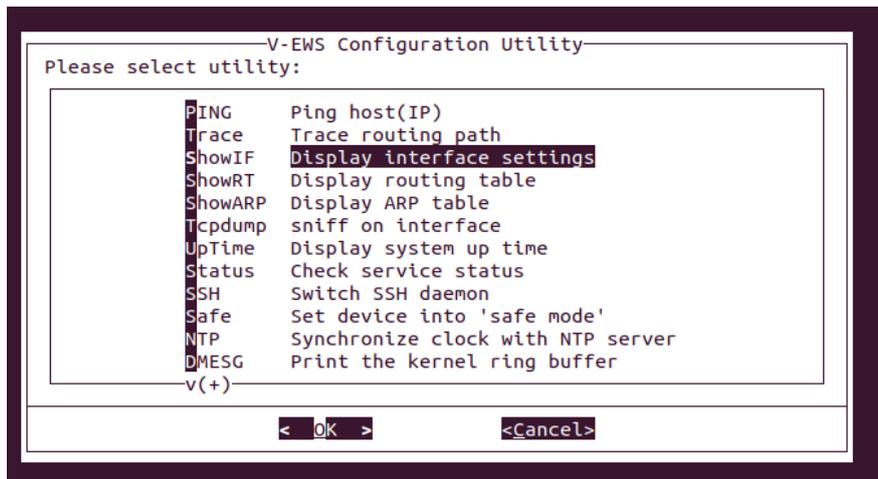
virsh console V-EWS」を実行し、コンソールモードにします。

```
root@vincent-Aspire-4752:/var/lib/libvirt/images# virsh console V-EWS
Connected to domain V-EWS
Escape character is ^]
```

"Enter "キーを押し、"Utility "を選択します。



- “ShowIF”を選択します。



- WAN1 の IP アドレスを確認する

```

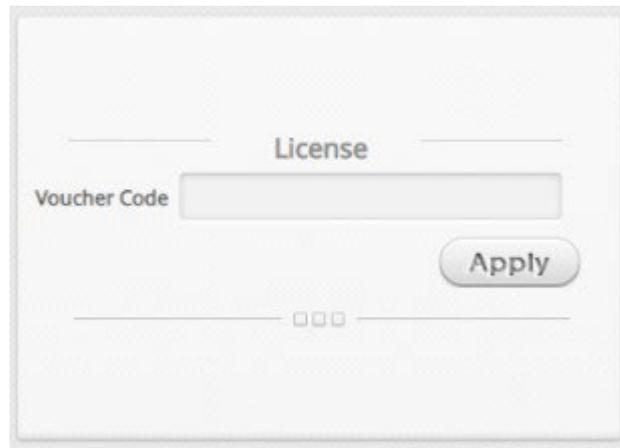
WAN1:
Link encap:Ethernet HWaddr 52:54:00:24:8C:86
inet addr:10.71.1.120 Bcast:10.71.255.255 Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1400 Metric:1
RX packets:5318 errors:0 dropped:633 overruns:0 frame:0
TX packets:403 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:510213 (498.2 KiB) TX bytes:58533 (57.1 KiB)

Default:
Link encap:Ethernet HWaddr FA:61:66:87:D7:E7
inet addr:192.168.1.254 Bcast:192.168.255.255 Mask:255.255.0.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

Press ENTER to continue

```

- ステップ 7.VEWS をアクティベートする
ブラウザを開き、<http://<WAN1 IP>/>に接続します。



License

Voucher Code

□□□

- ・クーポンコードを入力し、「適用」をクリックします。クーポンコードが有効な場合、ログインページにリダイレクトされます。



LOGIN

Username

Password

□□□

[Change password?](#)

[Forgot password?](#)

- ・デフォルトのユーザー名は "admin"、デフォルトのパスワードは "admin "を入力してください。指示に従ってパスワードを変更すると、新しいパスワードでログインできるようになります。



Edit New Password

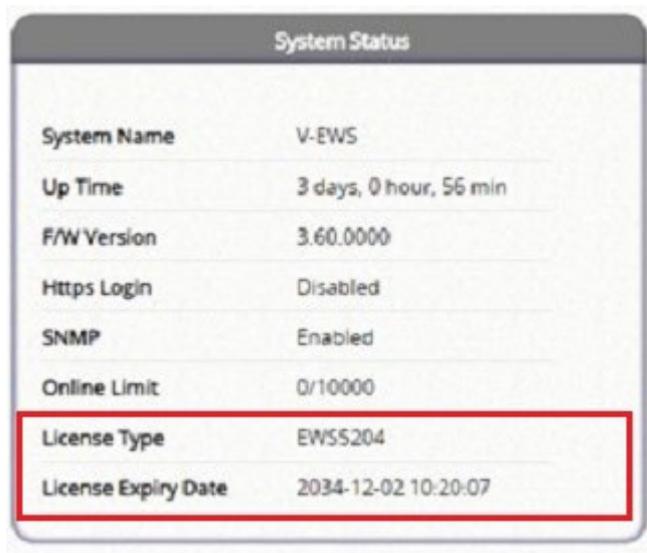
Name

Original Password

New Password

Verify Password

- ・ ライセンス情報はダッシュボードで確認することができます。



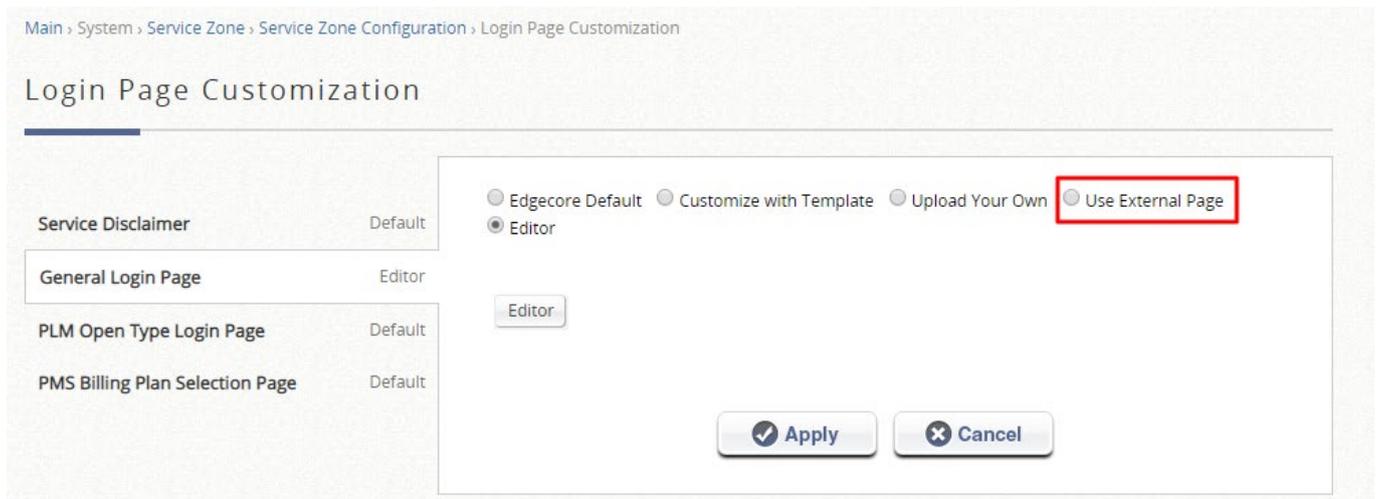
The image shows a 'System Status' dashboard with a table of system parameters. The 'License Type' and 'License Expiry Date' rows are highlighted with a red border.

System Status	
System Name	V-EWS
Up Time	3 days, 0 hour, 56 min
F/W Version	3.60.0000
Https Login	Disabled
SNMP	Enabled
Online Limit	0/10000
License Type	EWSS204
License Expiry Date	2034-12-02 10:20:07

付録B 外部ページ

外部ページのコセ

カスタムページに外部Webページを使用する場合は、External Pageを選択してください。外部WebページのURLを入力し、Previewボタンをクリックして到達可能かどうかを確認し、外部Webページがどのように表示されるかを見て、Applyボタンをクリックするだけです。



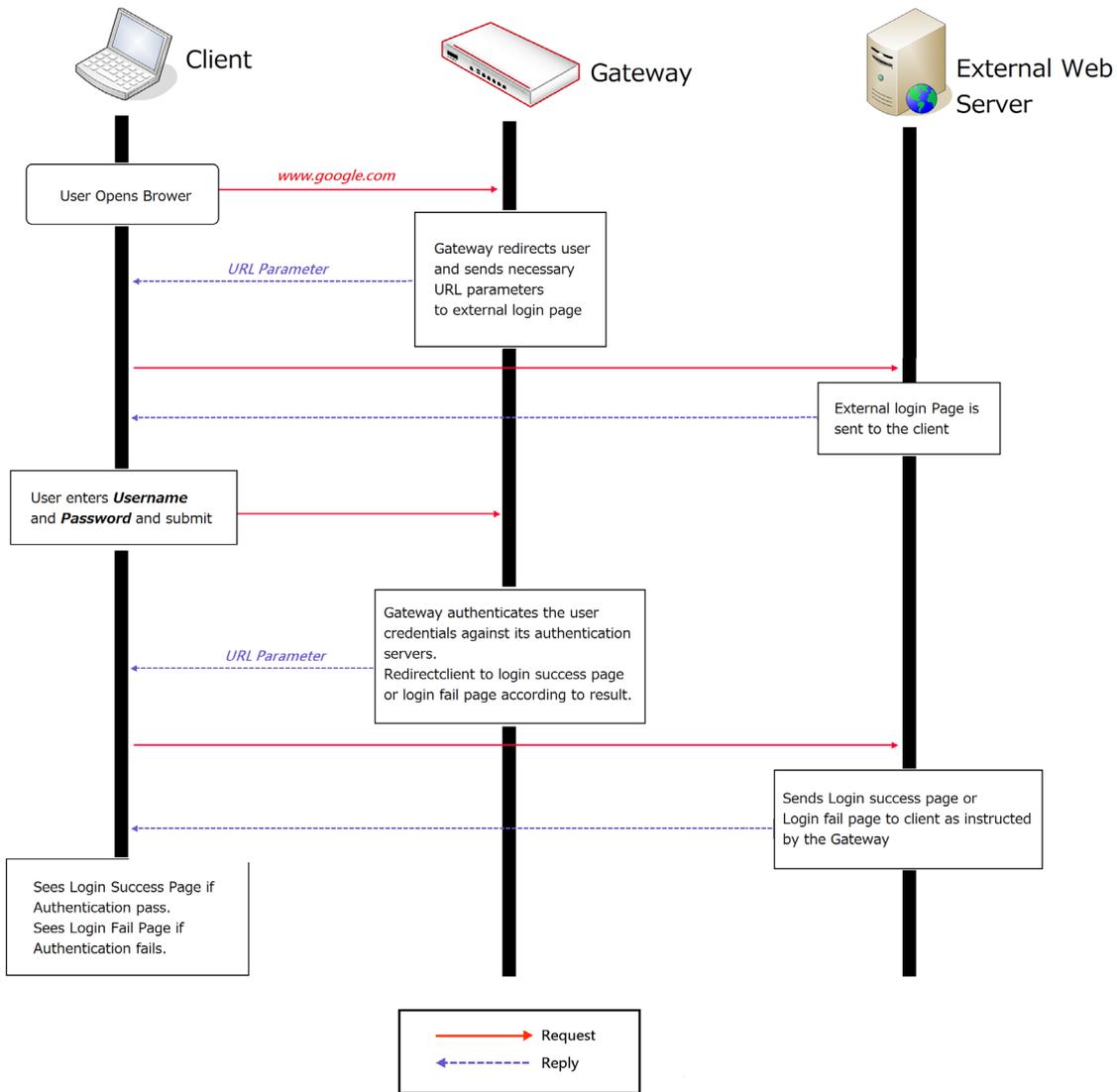
Main Menu>System>Service Zone>Service Zone Configuration>Login Page

ユーザーがこのサービスゾーンに接続し、Webブラウザを開いてインターネットにアクセスしようとするとき、システムは設定された外部ログインページにユーザーをアドレス指定します。外部Webページにユーザーをアドレス指定しながら、ゲートウェイは、操作に必要なURLパラメータ（ユーザー認証など）も送信します。したがって、自己定義の各外部ページ（ログイン、ログアウト、ログイン成功、ログアウト成功など）には、ゲートウェイとの間のURLパラメータを処理するためのコードが必要です。ログインページの簡単な例を以下に示します。ログイン成功ページなどの他のページに関連するURLパラメータについては、外部ログインページパラメータを参照してください。

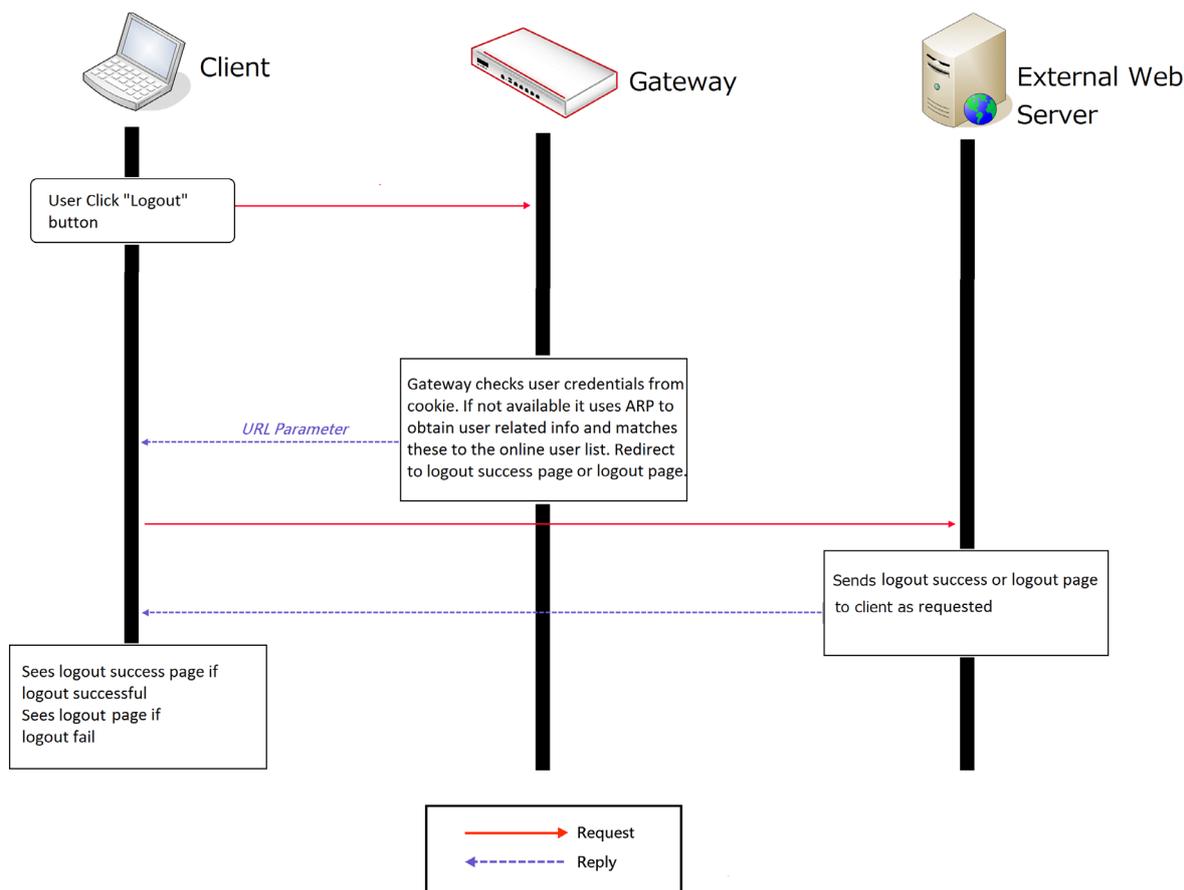
したがって、外部ページは、URLパラメータの使用に関する十分な知識を持つユーザーによって設計されていることが重要です。

次の図に、ユーザーのログイン/ログアウトフローを使用した外部ページの動作を示します。

ログイン：



ログアウト :



ゲートウェイから外部ログインページに送信されるURLパラメータは次のとおりです。

フィールド	値	説明
loginurl	文字列 (URL エンコード)	ユーザーがログインしたときに送信される URL。
remainingurl	文字列 (URL エンコード)	ユーザーが残りのクォータを取得したいときに送信される URL。
vlanid	整数 (1~4094)	VLAN ID
iface	整数 (0~8)	サービスゾーン ID。デフォルトのサービスゾーンは 0
gwip	IP 形式	ゲートウェイでアクティブ化された WAN IP アドレス
gwmac	MAC 形式 (':'で区切る)	ゲートウェイでアクティブ化された WAN MAC アドレス

client_ip	IP 形式	クライアント IP アドレス
ipv6_addr	IPv6 形式	クライアント IPv6 アドレス
umac	MAC 形式（':'で区切る）	クライアント MAC アドレス
session	文字列	暗号化されたセッション情報には、クライアント IP アドレス、MAC アドレス、日付、および戻り URL が含まれます。

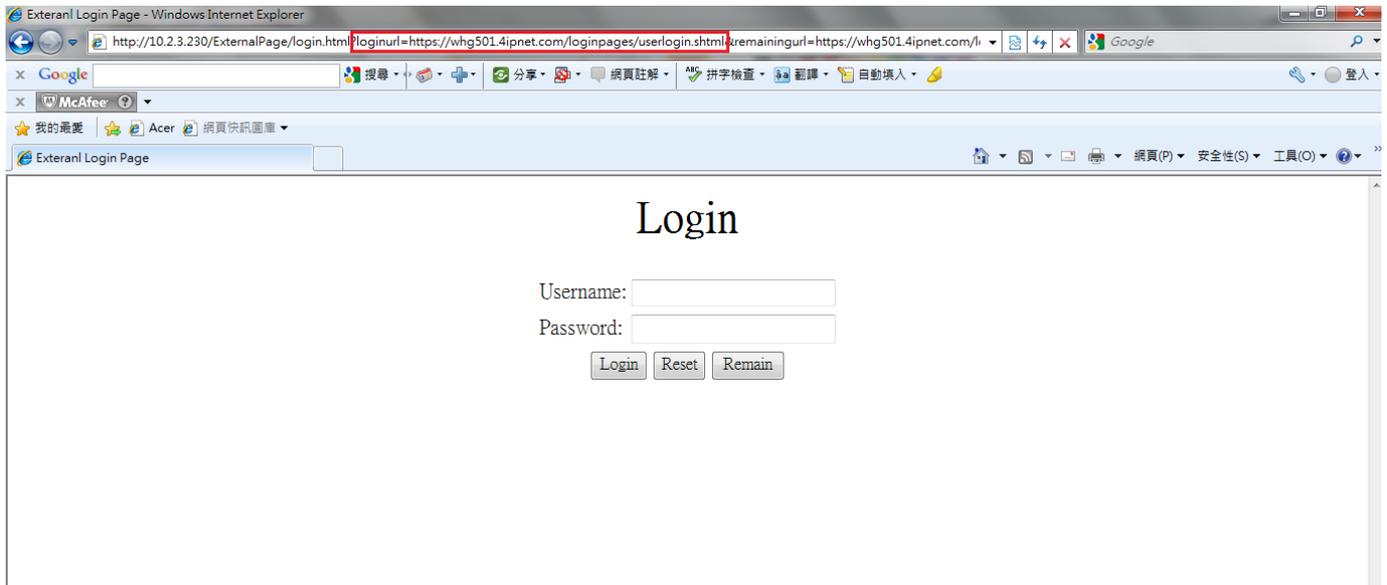
html コードで必要なパラメータを解析する必要があります。次の HTML コードセグメントは、自己定義の JavaScript 関数を使用して *loginurl* パラメータを解析する例です。

```
<FORM action="" method="post" name="form">
<script language="Javascript">
form.action = getVarFromURL(window.location.href, 'loginurl');
</script>
<INPUT type="text" name="myusername" size="25">
<INPUT type="password" name="mypassword" size="25">
<INPUT name="button_submit" type="submit" value="Enter">
<INPUT name="button_clear" type="button" value="Clear">
</FORM>
```

以下に、*loginurl* パラメータの解析に使用する、対応する自己定義の JavaScript 関数を示します。

```
function getVarFromURL(url, name) {
    if(name == "" || url == "") { return ""; }
    name = name.replace(/[%]/|"%%%"|").replace(/[%]/|"%%%"|");
    var regObj = new RegExp("[%?&]" + name + "(^[&#]*)");
    var result = regObj.exec(url);
    if(result == null) { return ""; }
    else { return decodeURIComponent(result[1]); }
}
```

ブラウザを起動したときにユーザーに表示される外部ページの例が表示され、システムから送信された URL パラメータが赤で強調表示されます。



外部ページデザイン変数

このセクションには、ゲートウェイからさまざまな外部ページに送信されるすべての URL パラメータが表示されます。適切に機能するためには、自己設計のユーザーページに対して正しい変数を使用することが不可欠です。

1. 外部ログインページ

変数：

フィールド	値	説明
loginurl	文字列 (URL エンコード)	ユーザーがログインしたときに送信される URL。
remainingurl	文字列 (URL エンコード)	ユーザーが残りのクォータを取得したいときに送信される URL。
vlanid	整数 (1~4094)	VLAN ID
iface	整数 (0~8)	サービスゾーン ID。デフォルトのサービスゾーンは 0
gwip	IP 形式	ゲートウェイでアクティブ化された WAN IP アドレス
gwmac	MAC 形式 (':'で区切る)	ゲートウェイでアクティブ化された WAN MAC アドレス
client_ip	IP 形式	クライアント IP アドレス
ipv6_addr	IPv6 形式	クライアント IPv6 アドレス
umac	MAC 形式 (':'で区切る)	クライアント MAC アドレス
nat_ip	IP 形式	スプリットトンネルからクライアントを識別するための内部 IP アドレス。

2. ログイン成功ページ

変数：

フィールド	値	説明
uid	文字列	ユーザー ID (接尾辞を含む)
original_uid	文字列	元のユーザー ID
utype	文字列 (LOCAL、RADIUS、)	認証サーバー名

	ONDEMAND、POP3、LDAP、SIP、NT Domain)	
umac	MAC 形式 (':'で区切る)	クライアント MAC アドレス
sessionlength	整数 (秒)	RADIUS ユーザーセッションの長さ (RADIUS ユーザーのみ使用可能)
byteamount	整数 (バイト)	RADIUS ユーザー容量制限 (RADIUS ユーザーのみ使用可能)
idletimeout	整数 (秒)	アイドルタイムアウト
acct-interim-interval	整数 (秒)	RADIUS アカウンティング中間更新間隔 (RADIUS ユーザーのみ使用可能)
logouturl	文字列 (URL エンコード)	ユーザーがログアウトするときに送信される URL。
change_passwd_url	文字列 (URL エンコード)	ユーザーがパスワードを変更したいときに送信される URL。(ローカルユーザーのみ使用可能)
ondemand_creation_url	文字列 (URL エンコード)	ユーザーがオンデマンドユーザーを作成するときに送信される URL。(ローカルユーザーのみ使用可能)
vlanid	整数 (1~4094)	VLAN ID
gwip	IP 形式	ゲートウェイでアクティブ化された WAN IP アドレス
client_ip	IP 形式	クライアント IP アドレス
ipv6_addr	IPv6 形式	クライアント IPv6 アドレス
sz	整数	サービスゾーン ID
group	整数	グループインデックス
policy	整数	ポリシーインデックス
available_plan	請求プラン：使用量、請求プラン：使用量	ローカルユーザーがオンデマンドユーザーを作成する場合
max_uplink	整数 (b/s)	最大アップリンクレート
max_downlink	整数 (b/s)	最大ダウンリンクレート
req_uplink	整数 (b/s)	最小アップリンクレート
req_downlink	整数 (b/s)	最小ダウンリンクレート
next_page	文字列	クライアントを URL に導く
CLASS	文字列	RADIUS クラス属性 (RADIUS ユーザーのみ使用可能)
WISPR-REDIRECTION-URL	文字列	クライアントを URL に導く
WISPR-SESSION-TERMINATE-TIME	文字列、形式：YYYY-MM-DDThh:mm:ssTZD	WISPr セッション終了時間属性 (RADIUS ユーザーのみ使用可能)
WISPR-SESSION-TERMINATE-END-OF-DAY	整数 (0/1)	WISPr セッション終了日付属性。終了ルールを示す 0 または 1。(RADIUS ユーザーのみ使用可能)
WISPR-BILLING-CLASS-OF-SERVICE	文字列	WISPr 請求クラス属性 (RADIUS ユーザーのみ使用可能)
WISPR-LOCATION-ID	文字列	WISPr ロケーション ID 属性 (RADIUS ユーザーのみ使用可能)
WISPR-LOCATION-NAME	文字列	WISPr ロケーション名属性 (RADIUS ユーザーのみ使用可能)
WISPR-BILLING-TIME	文字列、形式：HH:MM	WISPr 請求時間属性 (RADIUS ユーザーのみ使用可能)
split_tunnel	整数 (0/1)	クライアントがスプリットトンネルからの場合は 1、それ以外の場合は 0。
nat_ip	IP 形式	スプリットトンネルからクライアントを識別するための内部 IP アドレス。
custom	文字列	カスタマイズパラメータ

3.外部エラーページ

変数 :

フィールド	値	説明
msg	<p>文字列。以下を含む :</p> <p>The system is busy.Please try again later.</p> <p>Cannot find session related information.
Please enable the Cookie in the browser setting or open a website to get a Cookie.</p> <p>Invalid IP address.Please check the IP address and try again.</p> <p>Invalid MAC address.Please check the MAC address and try again.</p> <p>Sorry, your account is not usable, because the authentication option is currently disabled.
 Please contact your network administrator.</p> <p>Sorry, your account is not usable, because the authentication option (associated with the postfix) is not found.
Please contact your network administrator.</p> <p>Sorry, you are not allowed to log in, because your account is currently on the Black List.</p> <p>Sorry, you are not allowed to log in, because it is currently not the service hour for your account.</p> <p>You have already logged in.</p> <p>Sorry, there is a system problem checking the information of your account (XXX).
Please contact your network administrator.</p> <p>Invalid username or password.
Please check your username and password and try again.</p> <p>Cannot identify the policy for your account.
Please contact your network administrator.</p> <p>User of this device (the MAC address) is not allowed to use this account.
Please contact your network administrator.</p> <p>Sorry, the external authentication server is currently unreachable.
Please contact your network administrator.</p> <p>Sorry, you are not allowed to create a remote VPN connection.</p> <p>返信メッセージは RADIUS サーバーから送信されます。</p>	エラーメッセージ

	(RADIUS 属性 : 返信メッセージ)	
loginurl	文字列 (URL エンコード)	ユーザーログイン時に提出する URL。
remainingurl	文字列 (URL エンコード)	ユーザーが残りのクォータを取得したいときに送信されなければならない URL。
vlanid	整数 (1~4094)	VLAN ID
iface	整数	サービスゾーン ID。デフォルトのサービスゾーンは 0
client_ip	IP 形式	クライアント IP アドレス
gwip	IP 形式	ゲートウェイでアクティブ化された IP アドレス
ipv6_addr	IPv6 形式	クライアント IPv6 アドレス
umac	MAC 形式 (':'で区切る)	クライアント MAC アドレス
original_uid	文字列	元のユーザー ID
nat_ip	IP 形式	スプリットトンネルからクライアントを識別するための内部 IP アドレス。
custom	文字列	カスタマイズパラメータ

4.外部ログアウト成功ページ

変数 :

フィールド	値	説明
uid	文字列	ユーザー ID (接尾辞を含む)
original_uid	文字列	元のユーザー ID
vlanid	整数 (1~4094)	VLAN ID
gwip	IP 形式	ゲートウェイでアクティブ化された IP アドレス
used_time	整数	ユーザーの使用時間

5.外部オンデマンド/ゲストログイン成功ページ

変数 :

フィールド	値	説明
uid	文字列	ユーザー ID (接尾辞を含む)
original_uid	文字列	元のユーザー ID
utype	文字列 (LOCAL、RADIUS、ONDEMAND、POP3、LDAP、SIP、NT Domain)	認証サーバー名
umac	MAC 形式 (':'で区切る)	クライアント MAC アドレス
sessionlength	整数 (秒)	時間タイプのオンデマンドユーザーのクォータ
byteamount	整数 (バイト)	オンデマンドユーザーのボリュームタイプのクォータ
chargetype	文字列	ユーザーアカウントタイプ
idletimeout	整数 (秒)	アイドルタイムアウト
logouturl	文字列 (URL エンコード)	ログアウト URL
redeemurl	文字列 (URL エンコード)	引き換え URL
Vlanid	整数 (1~4094)	VLAN ID
gwip	IP 形式	ゲートウェイでアクティブ化された WAN IP アドレス

client_ip	IP 形式	クライアント IP アドレス
ipv6_addr	IPv6 形式	クライアント IPv6 アドレス
sz	整数	サービスゾーン ID
group	整数	グループインデックス
policy	整数	ポリシーインデックス
next_page	文字列	クライアントを URL に導く
max_uplink	整数 (b/s)	最大アップリンクレート
max_downlink	整数 (b/s)	最大ダウンリンクレート
req_uplink	整数 (b/s)	最小アップリンクレート
req_downlink	整数 (b/s)	最小ダウンリンクレート
nat_ip	IP 形式	スプリットトンネルからクライアントを識別するための内部 IP アドレス。

6. 外部ログアウト失敗ページ

変数 :

フィールド	値	説明
uid	文字列	ユーザーID
gwip	IP 形式	ゲートウェイでアクティブ化された WAN IP アドレス
vlanid	整数 (1~4094)	VLAN ID

外部ページデザイン変数

次のセクションでは、外部ページからコントローラが受け入れることができるすべての変数を収集し、表示します。いくつかは必須です。宛先パスは、デザイナーの参照用にも指定されています。

1. ユーザーログイン

パス :

(LAN IP アドレスまたは内部ドメイン名) /loginpages/userlogin.shtml

入力 :

フィールド	必須	値	説明
myusername 代替変数 : (username、user、account)	必須	文字列	ユーザーID
mypassword 代替変数 (passwd、password、pass)	必須	文字列	ユーザーパスワード
session	オプション	文字列	このセッションのいくつかの情報を含むエンコードされた文字列。デフォルトはクッキーから取得される。

出力 :

出力がない。ログイン成功ページに戻る。

2. ユーザーログアウト

パス :

(LAN IP アドレスまたは内部ドメイン名) /loginpages/logoff.shtml

入力 :

フィールド	必須	値	説明
uid	オプション	文字列	ユーザーID。デフォルトはクッキーから取得される

出力 :

出力がない。ログアウト成功ページに戻る。

3. 残枠 (クレジット残高)

パス :

(LAN IP アドレスまたは内部ドメイン名) /loginpages/reminder.shtml

入力 :

フィールド	必須	値	説明
myusername 代替変数 : (username、user、 account)	必須	文字列	ユーザー名
mypassword 代替変数 (passwd、password、 pass)	必須	文字列	パスワード
ret_url	オプション	文字列 (URL エンコード)	戻り URL。デフォルトは pop_reminder.shtml
command	オプション	文字列	getValue : コマンドが「getValue」に設定されている場合、戻り URL は無視され、ページは利用可能なクォータのみを出力する。

出力 :

コマンドが「getValue」に設定されている場合、出力は単に「値」になります。(ユーザータイプに応じて秒またはバイト)

コマンドが設定されておらず、ret_url が指定されていない場合、クライアントは pop_reminder.shtml ページに誘導され、残りのクォータを UI スタイルで表示します。ret_url が指定されている場合、クライアントは ret_url に返され、ゲートウェイは URL にこれらの 4 つの変数を追加します。

フィールド	値	説明
msg	文字列。以下を含む :	結果とエラーメッセージ

	Remaining Quota:XXX byte(s) Credit Balance:XXXXXX Sorry, this feature is available for On-Demand user only. Sorry, this account or password is incorrect. Sorry, this account is out of quota. Sorry, this account is expired. Sorry, this account is redeemed.	
value	整数（秒またはバイト） またはエラーNo. -1：アカウントが見つかりません。 -2：クォータが不足しています。 -3：期限切れしました。 -4：引き換えられました。	残りクォータ。ユーザーが時間タイプの場合、値は残り秒。ユーザーがボリュームタイプの場合、値は残りバイト。
uname	文字列	ユーザー名
type	文字列。以下を含む： TIME: Time type DATA: Volume type CUTOFF: Cut-off type	オンデマンドユーザー請求タイプ

4.パスワードの変更

パス：

(LAN IP アドレスまたは内部ドメイン名) /loginpages/user_change_password.shtml

入力：

フィールド	必須	値	説明
save	必須	1（1にする必要がある）	
opw	必須	文字列	古いパスワード
npw	必須	文字列	新しいパスワード
npwc	必須	文字列	確認済みの新しいパスワード
ret_url	必須	文字列（URL エンコード）	戻り URL

出力：

クライアントは ret_url に戻り、ゲートウェイはパスワードを変更した結果を示す ret_url に結果を追加します。

フィールド	値	説明
result	文字列。以下を含む： Change password successfully User password is incorrect	結果とエラーメッセージ

	Invalid password format	
--	-------------------------	--

5.引き換え（オンデマンドユーザー）

パス：

[\(LAN IP アドレスまたは内部ドメイン名\) /loginpages/redeemuserlogin.shtml](#)

入力：

フィールド	必須	値	説明
username	オプション	文字列	現在のユーザーID（指定されていない場合、クッキーに保存されているユーザー名がデフォルト値になる）
upassword	オプション	文字列	現在のユーザーパスワード（指定されていない場合、クッキーに保存されているパスワードがデフォルト値になる）
myusername	必須	文字列	引き換えのユーザーID
mypassword	必須	文字列	引き換えのユーザーパスワード
ret_url	オプション	文字列（URL エンコード）	戻り URL。ログイン成功ページがデフォルト値

出力：

ret_url が指定されていない場合、クライアントはログイン成功ページに導かれ、さらに、JavaScript ウィンドウがポップアップして結果を表示します。ret_url が指定されている場合、クライアントは ret_url に戻され、ゲートウェイは引き換えプロセスの結果を示すために、追加の変数 rmsg を追加します。

フィールド	値	説明
rmsg	文字列。以下を含む： Redeem process completed. Original user name cannot be found from the database. Redeem user name cannot be found from the database. Original user password is incorrect. Redeem user password is incorrect. Original user type and on demand user type do not match. Original user has not logged in. Redeem user logged in already. Had been redeemed before.	結果とエラーメッセージ

	<p>User has run out of quota.</p> <p>Maximum allowable time has exceeded.</p> <p>Maximum allowable memory space has exceeded.</p> <p>Wrong postfix please check it.</p> <p>This account is expired.</p>	
--	---	--

付録C 便利な管理および評価ツール

便利な管理ツール

ここでは、HP、IBM、CA、BMC の大きなスイートを置き換えるためにしっかりとした仕事をしているオープンソースの IT 管理製品のトップ 6 を紹介します。それぞれは、低コストのプロフェッショナルサービスとフリーソフトウェアのダウンロードを提供しています。これらは主に、提供する機能とサポートするオペレーティングシステムで異なります。

QUEST BIG BROTHER

この Web ベースのシステムとネットワークモニターは、ほとんどの Windows、Unix、Linux OS をサポートしており、さらにユーザーが作成したスクリプトのリポジトリを使用することで、ネットワークに合わせて簡単に Big Brother をカスタマイズすることができます。その GUI は、赤が悪く、緑が良いことを意味する普遍的に理解されたカラーコードを備えています。

GROUNDWORK MONITOR PROFESSIONAL

2004 年に発売されたこの製品は、最初のエンタープライズ規模のオープンソースネットワーク管理ソリューションの 1 つです。Nagios、Apache、NMap を含む 100 以上の優れたオープンソースプロジェクトを、Web ベースのインターフェースなどの追加機能を備えた 1 つのフレームワークに統合します。Monitor Professional は、Linux、Unix および Windows サーバー、アプリケーション、データベース、ネットワークボックスなどのエンタープライズネットワークを一元的に管理および監視します。

HYPERIC HQ ENTERPRISE

Hyperic のソフトウェアは、データセンターに向けて、ハードウェア、ミドルウェア、仮想化、Web およびオープンアプリケーションを含む Web インフラストラクチャのすべてのレイヤを管理および監視するために構築されています。また、トレンドと分析も行います。Apache、JBoss、Linuxなどをサポートしています。

OPENNMS

この Java ベースのネットワーク管理ツールは、サービスのポーリング、データ収集、イベントと通知の管理に重点を置いています。現在、Linux、Mandrake、Solaris、Mac OS X など様々なオープンオペレーティングシステムをサポートしています。OpenNMS 2.0 では Windows サポートが予定されています。

OPENQRM

同じくデータセンター管理を対象とする OpenQRM は、数千台の Linux サーバーと Windows サーバーを管理し、データセンターの使用状況や利用率を追跡できます。また、ポリシーベースの自動プロビジョニングも行います。こちらも監視のために Nagios を統合しています。

ZENOSS CORE

主に Python で書かれているこの管理プラットフォームは、サーバー、ネットワークデバイス、OS およびアプリケーションのイベント管理、可用性、パフォーマンス監視を提供します。Zenoss は Linux、FreeBSD、Mac OS X 上で動作し、VMPlayer と Zenoss 仮想アプライアンスを搭載した Windows 上で動作します。

評価ツール

Wireshark (パケットキャプチャおよびデバッグ分析用)

Wireshark は、世界有数のネットワークプロトコルアナライザです。これにより、コンピュータネットワーク上で実行されているトラフィックをキャプチャし、インタラクティブに閲覧することができます。これは、多くの業界や教育機関でデファクトスタンダード（時にはデジュールスタンダード）となっています。

Wireshark の開発は、世界中のネットワークング専門家の貢献のおかげで繁栄しています。1998 年に始まったプロジェクトの続きになります。

<http://www.wireshark.org/>

inSSIDer (ワイヤレススキャンおよび周波数アナライザ用)

inSSIDer は、近くの AP 信号と深度周波数を空中でスキャンし、配置サイトのチャンネル解析を行うための便利なツールです。

次のことが可能です。

- Wi-Fi と周囲のネットワークを検査する
- 近くの何百ものアクセスポイントをスキャンしてフィルタリングする
- 競合するアクセスポイントや Wi-Fi チャンネルに関するトラブルシューティング
- Wi-Fi が集中しているエリアのアクセスポイントを強調表示する
- 時間の経過とともに受信信号の強度を dBm で追跡する
- MAC アドレス、SSID、チャンネル、RSSI、最後に見た時間によって結果を並べ替える
- Wi-Fi および GPS データを Google Earth の KML ファイルにエクスポートする

<http://www.metageek.net/products/inssider/>

付録D オンデマンドアカウントタイプ

オンデマンドアカウントの種類には、主に次の4種類があります。

- **使用時間** (使用可能な時間クォータを購入する)
- **ボリューム** (使用可能なトラフィック量クォータを購入する)

プリペイド概念です。使用中のみクォータが減らされます。クォータが枯渇するか、アカウントの有効期限に達すると、アカウントは期限切れになります。

- **ホテルカットオフ** (有効なアカウントの時間間隔を購入する)
- **継続時間** (有効なアカウントの時間間隔を購入する)

使用時間間隔を定義します。カウントダウンは、アカウントがアクティブ化されたときに開始され、有効期限/日付に達したときに期限切れになります。

使用時間

- 残りのクォータでアカウントが有効である限り、ユーザーはインターネットにアクセスすることができ、ログインして所定の期間内に購入したアカウントを有効にする必要があります。

- 使用時間のアカウントは、次の項目を選択できます。

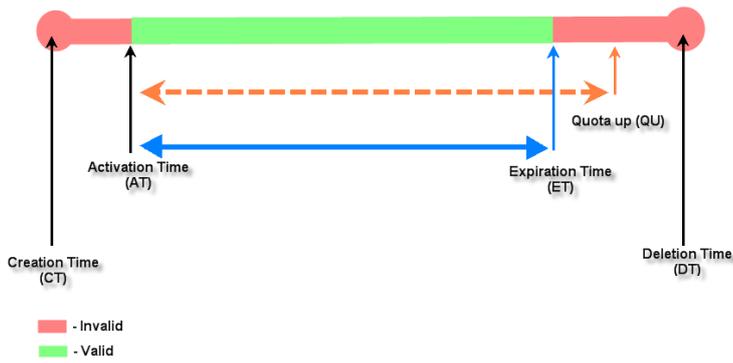
□ 有効期限あり

- カウントダウンは、最初のログインの直後に開始されます。有効期間が使い切れたり、クォータが枯渇したりすると、アカウントは期限切れになります。

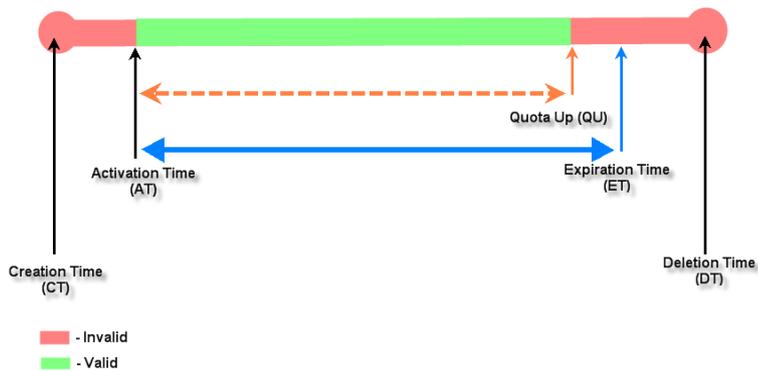
□ 有効期限なし

- アカウントは、クォータを使い切った場合にのみ有効期限が切れます。

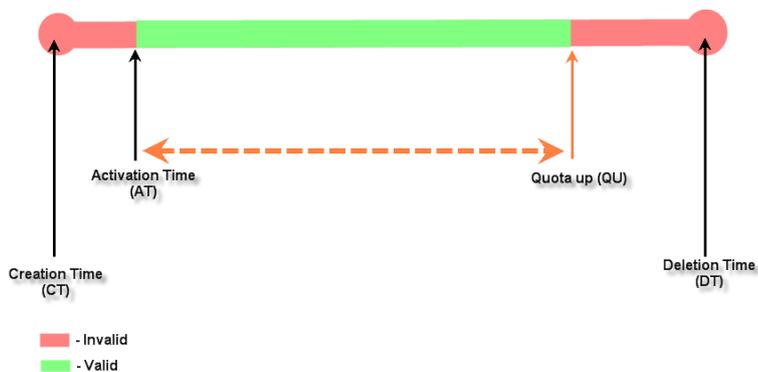
Usage-time account lifespan



Usage-time account lifespan

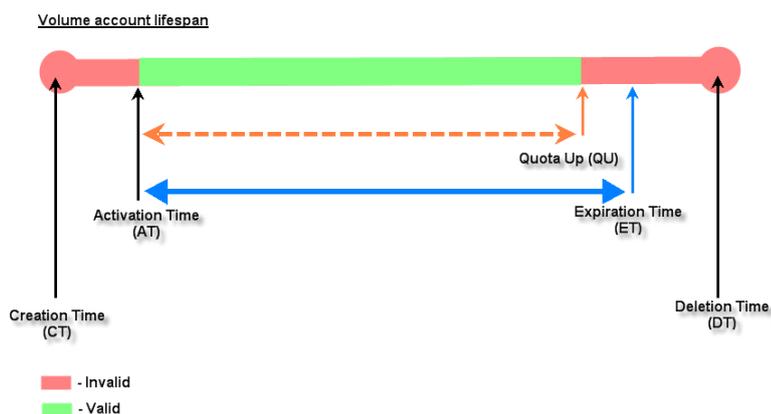
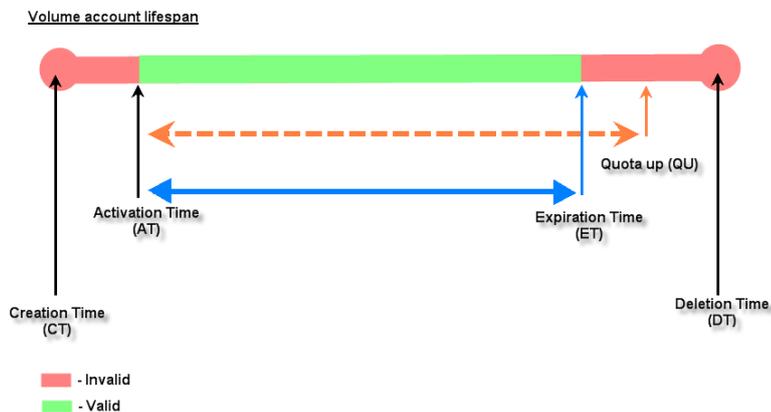


Usage-time account lifespan



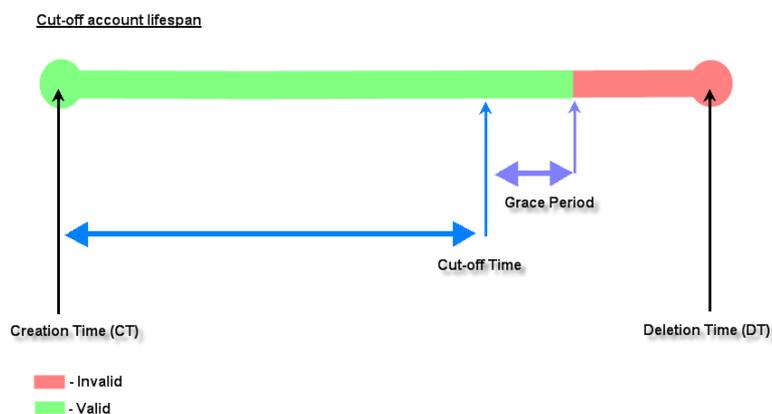
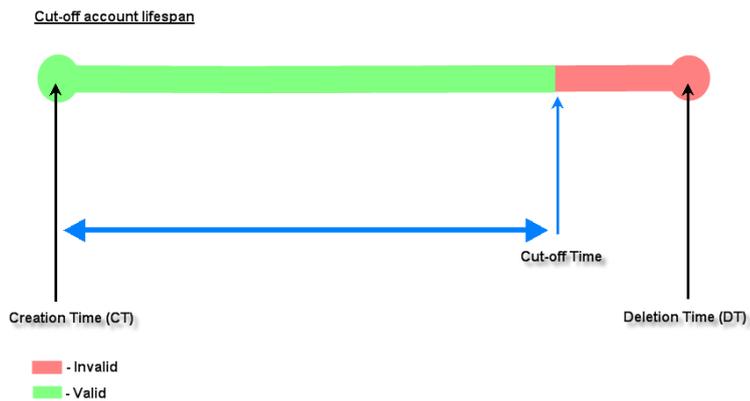
ボリューム

- 残りのクォータでアカウントが有効である限り、ユーザーはインターネットにアクセスすることができ、ログインして所定の期間内に購入したアカウントを有効にする必要があります。
- 有効期間が使い切れたり、クォータが枯渇したりすると、アカウントは期限切れになります。



ホテルカットオフ時間

- オペレータは、アカウントの有効期限が切れる時計の時間を設定できます。
- アカウントが作成されると自動的にアクティブになります。
- 単位は、「カットオフ」を実行する日数です。例えば、次のようになります。単位=2 日間、カットオフ時間=10:00 の場合、アカウントは作成時から 2 日後の午前 10:00 に期限切れになります。
- 猶予期間が付与されていない限り、カットオフ時間に達すると、アカウントの操作性は無効になります。
- 主に宿泊時間に応じてインターネットサービスを提供するために、ホテルの会場で使用されています。



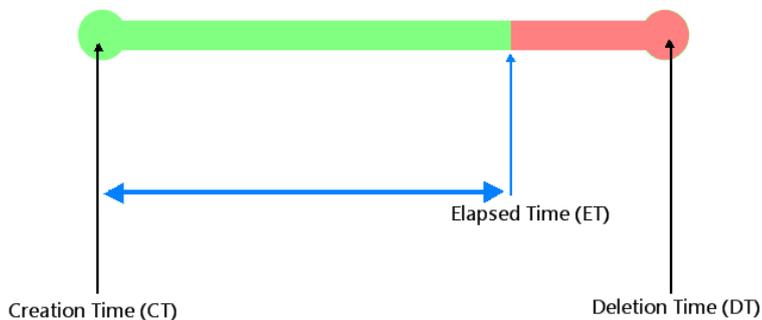
継続時間

- アカウントが有効な時間内であれば、ユーザーはインターネットにアクセスできます。カウントダウンは、アカウントがアクティブ化されると開始され、有効期限に達すると期限切れになります。
- 継続時間のアカウントはさらに次のように分類できます。
 - 経過時間
 - ・ アカウント作成時間であるアクティベーション時間を基準にしています。有効期限に達すると、アカウントは有効期限が切れます。
 - 開始終了時間
 - ・ アカウントの開始時間と終了時間を明示的に定義します。アカウントは、終了時間に達すると有効期限が切れます。

□ カットオフ時間

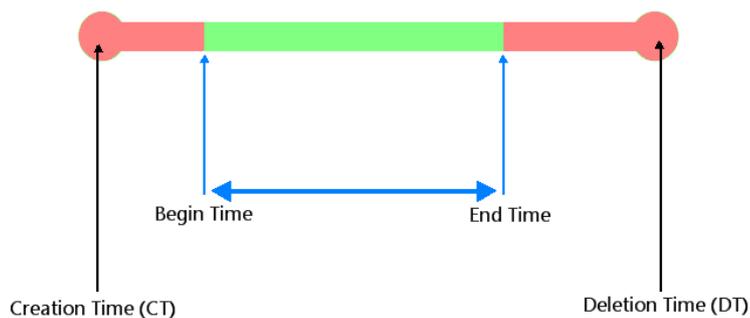
- 作成日以内に「カットオフ」する時計の時間を明示的に定義します。

Duration-time Elapsed account lifespan



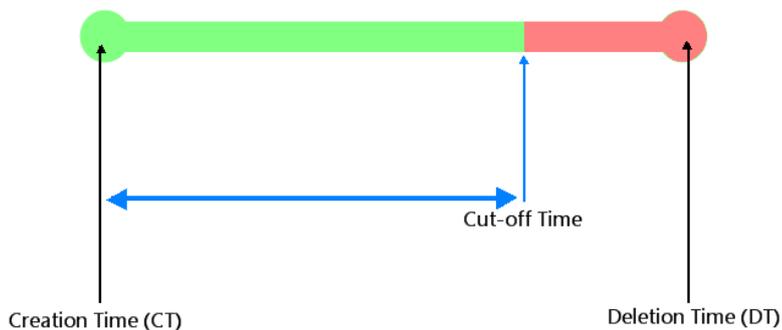
■ - Invalid
■ - Valid

Duration-time Begin-End Account lifespan



■ - Invalid
■ - Valid

Duration-time Cut-off account lifespan



■ - Invalid
■ - Valid

1. 請求プランは 10 個しかないため、同じタイプで異なるクォータのアカウントを作成する場合は、Unit フィールドを使用して作成することができます。

On-Demand Account Creation

Plan	Account Type	Quota	Price	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	1	Create Single Create Batch
2	Hotel Cut-off-time	Valid until 5:01 the following day	1	1	Create Single Create Batch



Creating an On-Demand Account

Plan : Account Type 1 : Usage-time

Quota 2 hr(s) of connection time quota with expiration

Account Creation System created Manual created

Valid Period After activation, the account will be expired in 7 day(s)

Total Price 1.99

Unit Units per ticket

Group Group 1

Reference Add a reference related to this account (for example, the customer's name)

External ID Enter an external ID such as a Library ID No.

Please confirm the information and press Create button to create an account.

ネットワークオペレータは、Unit フィールドの 1~9 の範囲の整数でクォータを乗算することができます。1 つのアカウントに対して複数ユニットクォータの生成をサポートするのは、使用時間、ボリューム、および継続経過時間のアカウントタイプのみです。



SN:xxxxxx

Welcome!



Username	xxxx@ondemand
Password	xxxxxxxx
Plan : Account Type	1 : Usage-time
Quota	xx hr(s) xx min(s)
Unit	Units
Total Price	1.99
Max User	1
Reference	Customer xxx
External ID	SSID0

ESSID : SSID0

Shared Wireless Key: None (Open System)

Your account is activated at

The account will be expired in 2019/06/25 15:33

You have to login before

The account will be expired in after account activation.

Thank You!

I. Dashboard

このページには、一般的なシステム設定、ネットワークインターフェース、オンラインユーザーなどを含む、管理者が把握する必要がある重要なシステム関連情報が表示されます。ドロップダウンメニューを使用して、このページの情報更新レートを選択できます。

右上隅にある「Download」ボタンは、システムステータスのスナップショットを提供するツールです。この情報は、メンテナンスまたはトラブルシューティングの目的で使用できます。

また、管理者は「Display Mode」（表示モード）を編集することで、ダッシュボードに表示する項目を選択できます。ダッシュボードは、必要な情報を表示するためにのみカスタマイズできます。



II.Setup Wizard

このウィザードは、セットアップ手順を簡易的に提供します。各ステップの指示に従って、システム管理者パスワードの変更、タイムゾーンの選択、WAN1 インターフェースの設定、およびローカルユーザーアカウントの作成を行ってください。セットアップ手順を完了したら、システムを再始動して設定を有効にする必要があります。再始動後、最小限の設定で動作可能な状態になっています。

The screenshot shows the 'General' configuration screen of the Setup Wizard. At the top, there is a progress bar with four steps: 1. FIRST STEP (Change Password), 2. SECOND STEP (Configure WAN), 3. THIRD STEP (Create A Local User), and 4. YOU'RE DONE (Restart the System). The first step is currently active. On the left side, a red vertical bar highlights a recommendation: 'It is recommended to change administrator's password and select an appropriate time zone for the system.' The main area is titled 'General' and contains three input fields: 'New Password' and 'Verify Password', both with masked characters (dots), and a 'Time Zone' dropdown menu currently set to '(GMT+08:00)Taipei'. At the bottom right, there are two buttons: 'Exit' and 'Next'.

A.System

System : このセクションは、システム構成に関するものです。これには、一般情報、WAN 構成、LAN ポート、サービスゾーンなどが含まれます。

1) General

The image shows two screenshots of a web interface. The top screenshot is titled "General Settings" and contains various configuration options. The bottom screenshot is titled "System Time" and shows time-related settings.

General Settings

System Name	<input type="text" value="EWS101"/>
Contact Information	<input type="text"/>
HTTPS Certificate	Default CERT ▼
User HTTPS Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <input type="checkbox"/> Secure
HTTPS Automatic Redirect	<input checked="" type="radio"/> Allow <input type="radio"/> Block <input type="radio"/> Bypass Allow HTTPS Automatic Redirect with Certification Security Alert
Internal Domain Name	<input checked="" type="checkbox"/> Use the name on SSL certificate <input type="text" value="mknhhi.example.com"/>
Portal URL Exceptions (User Agent)	<input type="text" value="IEMobile/7.0,XBLWP7"/> (e.g. IEMobile/7.0,XBLWP7, separate by comma)
User Log Access	<input type="text" value="Enter IP Address Here"/>
UAM Filter	<input type="button" value="Configure"/>
Management IP Address	<input type="button" value="Configure"/>
SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="button" value="Configure"/>
Suspend Warning Message	<input type="text" value="Sorry! The service is suspended."/> *
NMS Setting	<input type="button" value="Configure"/>

System Time

Current Time	2019/06/25 17:26:12
Time Zone	(GMT+08:00)Taipei ▼
Time Update	<input checked="" type="radio"/> NTP <input type="radio"/> Manually set up NTP Server 1: <input type="text" value="time.nist.gov"/> NTP Server 2: <input type="text" value="ntp1.fau.de"/> NTP Server 3: <input type="text" value="clock.cuhk.edu.hk"/> NTP Server 4: <input type="text" value="ntp1.pads.ufrj.br"/> NTP Server 5: <input type="text" value="ntp1.cs.mu.OZ.AU"/> <input type="checkbox"/> Use this controller as an NTP server

- **System Name** : これは、コントローラに付けることができるニーモニック名です。設定が完了すると、Web ブラウザのフレームに表示されます。

- **Contact Information** : これは、インターネット接続が切断された場合にクライアントの Web ブラウザに表示される電子メール、携帯電話、またはその他の連絡手段です。
- **HTTPS Certificate** : サイトの安全性の検証として、独自のネットワーク証明書を選択できます。証明書は、「Utilities > Certificates > System Certificate」でアップロードおよび管理できます。
- **User HTTPS Login** : HTTPS で認証されたエンドユーザーに対して、暗号化されたコンテンツ転送を許可するオプションを示します。「Secure」オプションは、「高」暗号化暗号スイートのみをサポートします。
- **HTTPS Automatic Redirect** : ユーザーが最初にネットワークに接続したときに HTTPS 要求を許可または拒否するオプションを提供します。有効にすると、HTTPS トラフィックはリダイレクトされますが、証明書のセキュリティ警告が表示されることがあります。HTTPS を無効にすると、すべての HTTPS トラフィックが拒否され、タイムアウトになります。このオプションを使用すると、ユーザーのデバイス上のすべてのセキュリティ警告が効果的に表示されなくなります。HTTPS リクエストがタイムアウトになると、一部のブラウザが HTTP Web ページをキャプティブポータルにリダイレクトするように自動的に要求することがあります。
 - **HTTPS Automatic Redirect を有効にする** : キャプティブポータルにアクセスする前に、HTTPS で閲覧しているユーザーに、証明書のセキュリティ警告が表示される場合があります。
 - **HTTPS Automatic Redirect をブロックする** : HTTPS で閲覧しているユーザーはタイムアウトになります。つまり、Web ページは宛先に到達しないため、空白になります。
 - **サインイン前に非 HTTP トラフィックをバイパスする** : ユーザーがキャプティブポータルで免責事項ページを受け入れていない場合や、サインインプロセスを完了していない場合でも、すべての HTTPS ウェブサイトの閲覧が許可されます。
- **Internal Domain Name** : システムの完全修飾ドメイン名 (FQDN) です。LAN インターフェースの IP アドレスを記憶する代わりに、コントローラにアクセスするのに最適です。管理者が Internal Domain Name フィールドに目的のドメイン名を入力すると、入力した内部ドメイン名は、LAN IP アドレスではなく、ログイン成功ページの URL に表示されます。また、HTTPS が有効になっている場合、アップロードされた証明書のドメイン名を入力すると、ログイン速度が向上し、ユーザーログインページの URL が変更されます。ソーシャルメディアログインでは、この内部ドメイン名は、ログインに成功したクライアントをログイン成功ページにリダイレクトするのに役立ちます。
- **Portal URL Exceptions (User Agent)** : ここに記載されている特定の開かれているブラウザを除き、ユーザーの初回ログイン後に目的のランディングページが表示される場合があります。
- **User Log Access IP Address** : 一度設定すると、入力された IP を介してのみユーザーログにアクセスできます。
- **UAM Filter** : Universal Access Method (UAM) フィルタは、過剰なトラフィックによるシステムの過負荷を防ぐために、認証の前にユーザーエージェントからのブラウザ以外の HTTP 要求をドロップします。
- **Management IP Address List** : この設定ボタンを使用すると、ネットワーク管理者は、Web 管理インターフェースの閲覧を許可された予約済みの IP アドレス/範囲を選択できます。リモートコンソールインターフェースは、デフォルトで無効になっています。
- **SNMP** : SNMP プロトコルを介したシステム情報の取得を有効または無効にするオプションを示します。管理者は、SNMP トラップメッセージを送信するために特定のポートを割り当てることができます。CPU 使用率、メモリ使用率、DHCP スコープ、ハートビート期間などの詳細なしきい値を設定できます。
- **Suspend Warning Message** : サービスゾーンのサービスが一時的に中断されたときに、管理者がユーザーにメッセージを入力するためのフィールドです
- **Time** : このセクションでは、システム時間を手動で設定するオプション、または外部 NTP サーバーを指定して自動で時間を同期させるオプションを示します。
 - **Current Time** : 以下の設定直後のシステム時間です。
 - **Time Zone** : システムがあるローカルタイムゾーンを選択するドロップダウンリストです。
 - **Time Update (NTP)** : システムは、NTP サーバー1~5 の順で外部 NTP サーバーを指定することにより、自動時刻同期を完了します。デフォルトでは、Use this controller as an NTP server チェックボックスがチェックされ、管理されている AP の時刻が同期されます。

- **Time Update (Manually Set Up)** : システム時刻は手動で設定されます。

Management Service

SSH Service Enable Disable
 Telnet Service Enable Disable

Management Service Zone List

Active	Status	Service Zone	IP Address/Segment
<input checked="" type="checkbox"/>		Default	192.168.1.254/255.255.0.0
<input checked="" type="checkbox"/>		SZ1	10.1.1.254/255.255.0.0
<input type="checkbox"/>		SZ2	10.2.1.254/255.255.0.0
<input type="checkbox"/>		SZ3	10.3.1.254/255.255.0.0
<input type="checkbox"/>		SZ4	10.4.1.254/255.255.0.0
<input type="checkbox"/>		SZ5	10.5.1.254/255.255.0.0
<input type="checkbox"/>		SZ6	10.6.1.254/255.255.0.0
<input type="checkbox"/>		SZ7	10.7.1.254/255.255.0.0
<input type="checkbox"/>		SZ8	10.8.1.254/255.255.0.0

Management IP Address List

No.	Active	IP Address/Segment
1	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0/0.0.0.0"/>
2	<input checked="" type="checkbox"/>	<input type="text" value="10.71.1.1/255.255.0.0"/>
3	<input type="checkbox"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>

- **Management Service** : リモートコンソール管理インターフェースを有効または無効にするオプションです。
 - **SSH Service** : ポート 22 の暗号化されたリモートコンソールインターフェースです。セキュリティ上の理由から、悪意のあるユーザーがシステムにアクセスするのを防ぐために、SSH サービスを無効にすることをお勧めします。ただし、Edgecore サポートチームによるリモートトラブルシューティングが必要な場合は、事前に有効にしておいてください。
 - **Telnet Service** : ポート 23 の暗号化されていないリモートコンソールインターフェースです。セキュリティ上の理由から、Telnet サービスはデフォルトで無効になっており、悪意のあるユーザーがシステムにアクセスできないようにしています。
- **Management Service Zone List** : 「System > Service Zone, chapter2.4」で設定されている有効なサービスゾーンがある場合、管理者は Active で IP アドレスの範囲に一致するデバイスがシステムの WMI にアクセスできるようにすることができます。
- **Management IP Address List** : リモートアクセスのために、IP アドレス/セグメントは、管理者がシステムの WMI にアクセスできるようにカスタマイズすることができます。チェックボックスにチェックを入れて、表のエントリがアクティブになっていることを確認してください。例えば、「192.168.3.1」と「192.168.1.0/24」を入力すると、192.168.3.1 のデバイスと 192.168.1.0~192.168.1.255 の範囲のデバイスだけが Web 管理インターフェースに到達できることを意味します。管理者が特定の IP アドレスを入力する場合は、セグメントを入力する必要はありません。(192.168.5.44/32 ではなく、192.168.5.44 と入力してください。)

2) WAN

WAN1 Configuration

Physical Mode:

Interface Type: Static (Use the following IP settings)

IP Address: *

Subnet Mask: *

Default Gateway: *

Preferred DNS Server: *

Alternate DNS Server:

Dynamic (IP settings assigned automatically)

PPPoE

PPTP

- **Physical Mode** : 管理者は、ドロップダウンリストを使用して、WAN 接続の速度と二重を選択できます。自動ネゴシエーションがオンの場合、システムはインターフェースに接続されたシステムとデバイスの両方がサポートする最高性能の伝送モード（速度/二重/フロー制御）を選択します。
- **Static** : WAN ポートの IP アドレスを手動で指定します。
- **Dynamic** : DHCP サーバーがアップストリームネットワークで使用可能なネットワーク環境にのみ適用されます。Renew ボタンを押すと自動的に IP アドレスが取得されます。
- **PPPoE** : ISP が提供する PPPoE ダイアルアップ接続のためのものであり、ISP は設定を完了するためにパスワード付きのアカウントを発行します。
- **PPTP** : 一部の IPS（ヨーロッパ諸国）は、ダイアルアップ接続に PPTP プロトコルを提供する場合があります。発行された PPTP アカウントと、PPTP サーバー用のパスワードが必要です。
- **Transmission Option** : (EWS5204、EWS5207 のみ) SFP ファイバポートを使用して設計された Edgecore キャリアグレードモデルです。次のように構成できます。
 - **Ether Port** : サービス用に銅線イーサネット WAN ポートを配置します。
 - **Fiber Port** : サービス用の SFP ファイバポートを配置します。
 - **Fiber Port and Ether Port** : ファイバポートとイーサネットポートの橋渡しをします。物理的には、SFP ポートまたはイーサポート経由で 1 つのアップリンクだけを接続します。
 - **Bonding** : サービス用に SFP ポートと銅線イーサネットポートの両方を配置します。このオプションは、2 つの接続を集約し、集約されたスループットが高くなります。

WAN2 Configuration

Physical Mode:

Interface Type: None

Static (Use the following IP settings)

Dynamic (IP settings assigned automatically)

Obtain DNS server address automatically.

Preferred DNS Server: *

Alternate DNS Server:

PPPoE

- **Physical Mode** : 管理者は、ドロップダウンリストを使用して、WAN 接続の速度と二重を選択できます。自動ネゴシエーションがオンの場合、システムはインターフェースに接続されたシステムとデバイスの両方がサポートする最高性能の伝送モード（速度/二重/フロー制御）を選択します。
- **None** : WAN2 インターフェースによるサービスの提供を無効にします。
- **Static** : WAN ポートの IP アドレスを手動で指定します。
- **Dynamic** : DHCP サーバーがアップストリームネットワークで使用可能なネットワーク環境にのみ適用されます。Renew ボタンを押すと自動的に IP アドレスが取得されます。
- **PPPoE** : ISP が提供する PPPoE ダイアルアップ接続のためのものであり、ISP は設定を完了するためにパスワード付きのアカウントを発行します。
- **Transmission Option** : (EWS5204、EWS5207 のみ) SFP ファイバポートを使用して設計された Edgecore キャリアグレードモデルです。次のように構成できます。
 - **Ether Port** : サービス用に銅線イーサネット WAN ポートを配置します。
 - **Fiber Port** : サービス用の SFP ファイバポートを配置します。
 - **Fiber Port and Ether Port** : ファイバポートとイーサネットポートの橋渡しをします。物理的には、SFP ポートまたはイーサポート経由で 1 つのアップリンクだけを接続します。
 - **Bonding** : サービス用に SFP ポートと銅線イーサネットポートの両方を配置します。このオプションは、2 つの接続を集約し、集約されたスループットが高くなります。

WAN Traffic Settings

Bandwidth Limitation Enable Bandwidth Limitation on WAN

Max Uplink Bandwidth Kbps

Max Downlink Bandwidth Kbps

Function of WAN2

Disable(None)

Load Balancing
The "Load Balancing" function when Enabled also acts as the "Failover" function when one of the WAN interfaces is down.

WAN Failover

Target for Detecting Internet Connection

Warning of Internet Disconnection

When the addresses for detecting internet connection are unreachable, this message will be shown on the browser.

- **Bandwidth Limitation** : デフォルトでは無効です。この制限は、WAN1 と WAN2 の両方で組み合わせられていますが、帯域幅は ISP オペレータのネットワーク速度によって制限されます。
- **Function of WAN2** : 次の機能は、WAN2 が有効になっている場合にのみ機能します。
 - **Disable** : WAN2 は、ロードバランシングと WAN フェイルオーバーなしでシステムの別のアップリンクとして動作します。
 - **Load Balancing** : 管理者がセッション、バイト、またはパケットを使用して計算された負荷の割合に基づいて、システムトラフィックを WAN1 ポートおよび WAN2 ポートに分散させる場合にこのオプションを選択します。
 - **WAN Failover** : WAN1 がダウンするたびに、WAN2 は WAN1 によって処理されたトラフィックを処理するオプションとして選択します。ネストされたオプションが選択されている場合、WAN1 リンクが再び立ち上がると、サービスは WAN1 リンクに戻されます。この機能は、ロードバランシングと同時に使用することはできません。
- **Address for Detecting Internet Connection** : アップリンクサービスが生きているかダウンし

ているかを検証するために、検出対象として最大3つのアウトバウンドサイトを指定できます。警告メッセージテキストのフィールドはカスタマイズできます。このフィールドは、3つの検出対象がすべて応答しなかった場合にユーザーの Web ブラウザに表示されます。

3) IPv6

IPv6 Setting

IPv6 Enable Disable

Interface WAN1 WAN2

Type Static (Use the following IPv6 settings)

IPv6 Address:

Prefix Length:

Default Gateway:

Preferred DNS Server:

Alternate DNS Server:

Use 6to4 transition

Use 6to4 transition

- **Status** : 選択した WAN インターフェースで IPv6 サポートを有効または無効にします。
- **Interface** : IPv6 アドレスで構成するデバイスの外部インターフェースを選択します。
- **Type** : 1つの IPv6 方式を選択します。
 - **Static** : 関連する IPv6 情報をすべて手動で入力します。赤いアスタリスクは必須フィールドです。お使いのインターネットパッケージに、ISP による静的な IPv6 アドレスの問題がある場合に最適です。
 - **6to4** : 6to4 とは、IPv4 から IPv6 に移行するためのインターネットの移行機構で、明示的なトンネルを設定することなく、IPv4 ネットワーク（一般的には IPv4 インターネット）上で IPv6 パケットを送信できるようにする仕組みです。6to4 オプションは、選択した WAN インターフェースに静的 IPv4 アドレスが設定されている場合にのみ選択できます。

4) LAN ポート

デフォルトでは、システム内の「サービスゾーン」には、組織内の有線および無線カバレッジエリアが含まれています。このページには、サービスゾーンのマッピングを識別するためのオプションがありません。

LAN Ports

LAN Port Mode Port-Based Tag-Based

When LAN Ports are set to Port-Based Mode, Service Zones will be differentiated by the respective LAN ports. When LAN Ports are set to Tag-Based Mode, VLANs are used to separate traffic to different Service Zones. This is needed for Port Location Mapping and Access Point Management.

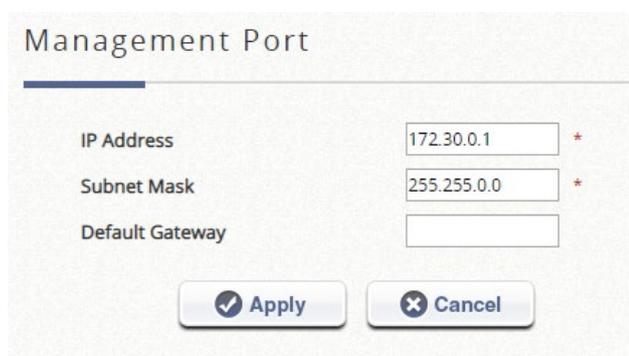
Port - Service Zone Mapping

Default	Default	SZ1	SZ1
LAN1	LAN2	LAN3	LAN4

- **LAN Port Mode** : ポートとサービスゾーンのマッピングを識別するオプションを選択します。
 - **Port-based** : 各物理 LAN ポートは、有効なサービスゾーンにマッピングすることも、サービスの提供を無効にすることもできます。実際にサービスを提供するために利用可能なサービスゾーンの最大量は、コントローラ上の LAN ポートの数によって決まることに注意してください。
 - **Tag-based** : 物理 LAN ポートに関係なく、異なるサービスゾーンが VLAN ID によって識別されます。つまり、タグベースモードは、トラフィックパケットにタグ付けされた VLAN ID に基づいて、クライアントをサービスゾーンに動的にマッピングします。
- **Port – Service Zone Mapping** : ポートベースモードが選択されている場合に、有効化されたサービスゾーンによる物理 LAN ポートの設定を行います。

5) MGMT Port

(EWS5207 で利用可能)



The image shows a web-based configuration form titled "Management Port". It contains three input fields: "IP Address" with the value "172.30.0.1", "Subnet Mask" with the value "255.255.0.0", and "Default Gateway" which is empty. Each of the first two fields has a red asterisk to its right. At the bottom of the form are two buttons: "Apply" with a checkmark icon and "Cancel" with an 'X' icon.

管理ポートの IP 設定は、このページで設定できます。

6) High Availability

(EWS5203、EWS5204、EWS5207 で利用可能)

Current Status

Dedicated Port	LAN1
Status	No Peer
Link to Peer's UI	HA Configuration ▼ <input type="button" value="Goto"/>
Version	10000

Configuration

Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Number of Active(s)	1 ▼
Mode	<input checked="" type="radio"/> Active <input type="radio"/> Standby
HA Port IP Address	<input type="text" value="172.31.0.1"/> *
HA Port Subnet Mask	<input type="text" value="255.255.0.0"/> *
Peer IP Address	<input type="text"/> *
Shared Key	<input type="text"/> *
Action	<input type="button" value="Sync & Swap"/>

Configuration :

- **Status** : この機能はここでオンとオフを切り替えることができます。
- **Number of Active(s)** : N+1 HA に対して最大 3 つのアクティブを選択します
- **Mode** : この特定のコントローラの役割は、ここで手動で決定する必要があります。
- **HA Port IP Address** : 専用の HA ポートに設定された IP アドレスです。すべてのコントローラの HA ポート IP が同じサブネットの下にあることを確認する必要があります。
- **HA Port Subnet Mask** : HA 通信用のサブネットマスクです。
- **Peer IP Address** : ピアコントローラの HA ポートの IP アドレスを入力します。
- **Shared Key** : 両方のコントローラに秘密の文字列を入力します。HA 接続を成功させるには、Shared Key (共有キー) が同じである必要があります。
- **Switch Support** : HA N+1、N=2 または 3 の場合には、HA 発生時に関連する LAN ポートと VLAN ID が自動的に変更できるため、Edgecore SW1024 を強く推奨します。管理者が SW1024 のポート 1、ポート 4、ポート 2 を VLAN 101、41、42 でそれぞれアクティブ AC に設定する場合は、#1 のアクティブ関連ポートに 1,4,2 を入力し、#1 のアクティブ LAN ポート VLAN ID に 101,41,42 と入力してください。
- **Action** : この機能は、プライマリコントローラでトリガーされ、サービスをセカンダリコントローラに手動で切り替えることができます。(1+1 HA でのみ使用可能)

Current Status :

- **Dedicated Port** : 現在、すべてのコントローラモデル用の LAN1 です。
- **Status** : HA リンクの現在のステータスを反映します。
- **Link to peer's UI** : ページを選択して、ピア Web UI にすばやくアクセスできます。アクティブなものでのみ使用できます。
- **Version** : HA 機能のリビジョンを表示します。

7) Service Zones

この表には、サービスゾーンと関連設定が一覧表示されます。

- **Status** : 各サービスゾーンのステータスです。デフォルトのサービスゾーンでは、常に「ON」です。
- **Service Zone Name** : サービスゾーンの名前です。
- **IP Address** : 各サービスゾーンのコントローラの IP アドレスです。
- **IPv6 Address** : 各サービスゾーンのコントローラの IPv6 アドレスです。
- **VLAN Tag** : (タグベースモードでのみ) 各サービスゾーンにマッピングされた VLAN タグ番号です。
- **LAN Port Mapping** : (ポートベースモードでのみ) LAN ポートとサービスゾーン間のマッピングです。
- **Default Auth.Option** : 各サービスゾーンに指定されているデフォルトの認証サーバーです。
- **Network Alias** : 各サービスゾーンのエイリアスサブネットです。
- **DHCP Pool** : DHCP サーバーのステータスまたは DHCP プールの IP 範囲です。

Service Zone Settings

Status	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
<input checked="" type="checkbox"/>	Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
<input type="checkbox"/>	SZ1	10.1.1.254	N/A	1	Server 1	N/A	10.1.1.1 ~ 10.1.1.100
<input type="checkbox"/>	SZ2	10.2.1.254	N/A	2	Server 1	N/A	10.2.1.1 ~ 10.2.1.100
<input type="checkbox"/>	SZ3	10.3.1.254	N/A	3	Server 1	N/A	10.3.1.1 ~ 10.3.1.100
<input type="checkbox"/>	SZ4	10.4.1.254	N/A	4	Server 1	N/A	10.4.1.1 ~ 10.4.1.100

Basic Settings

Service Zone Status Enabled Disabled

Service Zone Name

Network Interface VLAN Tag * (Range: 1 ~ 4094)

Tag-based Isolation Inter-VLAN Isolation Clients Isolation None

Note: When set to "None", the port on a switch connecting to the gateway's LAN port may be shut down if "Loop Protection" is enabled on the switch and there are 2 VLANs belonging to this Service Zone.

Operation Mode NAT Router

IP Address * Subnet Mask *

Network Alias List

This list defines other IP Addresses (range) that are routable in this Service Zone.

DHCP Enabled

ルータモード

Basic Settings

Service Zone Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Service Zone Name	<input type="text" value="SZ1"/>
Network Interface	VLAN Tag <input type="text" value="1"/> * (Range: 1 ~ 4094)
	Tag-based Isolation <input checked="" type="radio"/> Inter-VLAN Isolation <input type="radio"/> Clients Isolation <input type="radio"/> None
	Note: When set to "None", the port on a switch connecting to the gateway's LAN port may be shut down if "Loop Protection" is enabled on the switch and there are 2 VLANs belonging to this Service Zone.
	Operation Mode <input checked="" type="radio"/> NAT <input type="radio"/> Router
	IP Address <input type="text" value="172.21.0.254"/> * Subnet Mask <input type="text" value="255.255.0.0"/> *
	Network Alias List <input type="button" value="Configure"/>
	This list defines other IP Addresses (range) that are routable in this Service Zone.
DHCP	Enabled <input type="button" value="Configure"/>

NAT モード

- **Service Zone Status** : デフォルトのサービスゾーンを除き、各サービスゾーンを有効または無効にすることができます。
- **Service Zone Name** : サービスゾーンの名前をここに入力できます。

Network Interface :

- **VLAN Tag (タグベースモードのみ)** : サービスゾーンにマッピングされている VLAN タグ番号です。
- **Tag-Based Isolation (タグベースモードのみ)** : 管理者は、各サービスゾーンで異なるアイソレーションオプションを選択できます。
 - **Inter-VLAN Isolation** : 同じサービスゾーン内の 2 つのクライアントが、異なる VLAN および異なる LAN ポートから入ってくる时候お互いを見ることはありません。アイソレーションは、トラフィックがゲートウェイを通過するときに行われることに注意してください。スイッチまたは AP を配置する場合は、AP/スイッチでステーションアイソレーションを有効にする必要があります。
 - **Clients Isolation** : 同じレイヤ 2 ネットワーク上のすべてのクライアントは、このサービスゾーンで互いにアイソレーションされます。
 - **None** : このサービスゾーンのクライアントにはアイソレーションが適用されません。
- **Port-Based Isolation (ポートベースモードのみ)** : 管理者は、各サービスゾーンで異なるアイソレーションオプションを選択できます。
 - **Inter-Port Isolation** : 同じサービスゾーン内の 2 つのクライアントが、異なるポートから入ってくる时候お互いを見ることはありません。アイソレーションは、トラフィックがゲートウェイを通過するときに行われることに注意してください。スイッチまたは AP を配置する場合は、AP/スイッチでステーションアイソレーションを有効にする必要があります。
 - **Clients Isolation** : 同じレイヤ 2 ネットワーク上のすべてのクライアントは、このサービスゾーンで互いにアイソレーションされます。
 - **Until Auth.** : 同じレイヤ 2 ネットワーク上のすべてのクライアントは、認証の前に、このサービスゾーンで互いにアイソレーションされます。
 - **None** : このサービスゾーンのクライアントにはアイソレーションが適用されません。
- **Operation Mode**
 - **NAT** : Network Address Translation モードの頭字語です。アップリンクネットワークに転送する前に、コントローラの LAN 側のデバイスのプライベート IP アドレスをルーティング可能な IP に変換

します。プライベート IP アドレスは、コントローラの WAN 側のデバイスまたはルータには見えません。NAT を配置しているコントローラだけが対応する変換を認識します。このモードは、LAN 上のユーザーが外部デバイスから「見え」されないように保護するだけでなく、制限されたパブリック IP の問題も解決します。

- **Router** : コントローラへのアドレス変換を行わないネットワーク動作モードです。ルータモードは、パブリック IP を使用する場合、またはダウンストリームデバイスがアップストリームルータへのルーティング可能な IP アドレスを必要とする場合に選択されます。

- **IP Address** : このサービスゾーンの IP アドレスです。
- **Subnet Mask** : このサービスゾーンのサブネットマスクです。
- **IPv6 Settings** : このサービスゾーンの IPv6 アドレスと設定 (IPv6 が有効な場合のみ) です。
- **Network Alias List** : 管理者は、オプションでサービスゾーンに対して多数のエイリアスネットワークセグメントを設定できます。この機能により、1つのサービスゾーンを多数のサービスゾーンとして見ることができ、また、サービスゾーンのネットワークインターフェースの IP アドレスを隠すことができ、ある程度、LAN クライアントからの攻撃から保護することができます。 **Configure** ボタンをクリックして、Network Alias List ページを表示します。

Network Alias List - SZ1

Enable	No.	IP Address	Subnet Mask	Operation Mode
<input type="checkbox"/>	1	<input type="text"/>	255.255.255.255 (/32)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	2	<input type="text"/>	255.255.255.255 (/32)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	3	<input type="text"/>	255.255.255.255 (/32)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	4	<input type="text"/>	255.255.255.255 (/32)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	5	<input type="text"/>	255.255.255.255 (/32)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	6	<input type="text"/>	255.255.255.255 (/32)	<input checked="" type="radio"/> NAT <input type="radio"/> Router
<input type="checkbox"/>	7	<input type="text"/>	255.255.255.255 (/32)	<input checked="" type="radio"/> NAT <input type="radio"/> Router

- ◆ 目的のエイリアス IP アドレスを入力し、優先する Subnet Mask と Operation mode を選択し、Enable チェックボックスにチェックを入れ、 **Apply** ボタンをクリックして設定を有効にします。

- **DHCP** : ドロップダウンメニューから、この特定のサービスゾーンの DHCP サーバーは無効、有効、または中継することができます。
「Enable DHCP Relay」が有効になっている場合は、外部 DHCP サーバーの IP アドレスを入力すると、クライアントの IP アドレスは外部 DHCP サーバーによって割り当てられます。システムは、外部 DHCP サーバーから、このサービスゾーンのダウンストリームクライアントに DHCP 情報のみをリレーします。冗長 DHCP サーバーは、DHCP サーバーリレーモードに設定すると設定できます。コントローラは、DHCP サーバーと同じサブネットにある必要があることに注意してください。

DHCP Enable DHCP Server

DHCP Server Configuration for Service Zone SZ1

No.	Active	DHCP Pool	Start IP Address	End IP Address	Preferred DNS Server	Alternate DNS Server	Domain Name	Lease Time (mins)	WINS Server	Disregard Client's Name
1	<input checked="" type="checkbox"/>	Scope 1	172.21.0.1 *	172.21.0.100 *	172.21.0.254 *	<input type="text"/>	domain.com	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
2	<input type="checkbox"/>	Scope 2	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
3	<input type="checkbox"/>	Scope 3	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
4	<input type="checkbox"/>	Scope 4	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
5	<input type="checkbox"/>	Scope 5	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
6	<input type="checkbox"/>	Scope 6	<input type="text"/> *	<input type="text"/> *	<input type="text"/> *	<input type="text"/>	<input type="text"/>	1440	<input type="text"/>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Reserved IP Address List

DHCP Lease Protection

Enable Disable

- **Start IP Address/End IP Address** : DHCP サーバーに組み込まれている IP アドレスの範囲は、クライアントに割り当てられます。注：ネットワークインターフェースのデフォルト IP アドレスが変更された後に管理者が EWS コントローラ管理ページにアクセスできるように、管理 IP アドレスリストを適宜変更してください (System Configuration >> System Information >> Management IP Address List)。
 - **Preferred DNS Server** : このサービスゾーンで使用されるプライマリ DNS サーバーです。
 - **Alternate DNS Server** : このサービスゾーンで使用される代替 DNS サーバーです。
 - **Domain Name** : このサービスゾーンのドメイン名を入力します。
 - **WINS Server** : WINS サーバーがこのサービスゾーンに適用可能な場合の WINS (Windows インターネットネーミングサービス) サーバーの IP アドレスです。
 - **Lease Time** : これは、DHCP サーバーから発行された IP アドレスが有効かつ使用可能な期間です。
 - **Disregard Client Name** : 有効にすると、IP アドレスを要求しているデバイスの名前は記録されません。一方、無効を選択すると、システムは IP アドレスを発行するときにデバイスの名前を記録します。デバイス名 (ホスト名) は、**DHCP Lease** タブに表示されます。
 - **Reserved IP Address List** : 特定のデバイス (MAC) の DHCP サーバー IP 範囲内の特定の IP を予約するための構成リスト (内部ファイルサーバーなど) です。**Configure** ボタンをクリックして、予約済み IP リストを編集します。
 - **DHCP Lease Protection** : 有効にすると、リース期限切れの IP が現在オンラインになっているかどうかを確認するためのコントローラのオプションのチェックメカニズムです。はいの場合、コントローラはユーザーセッションが終了するまでこの IP アドレスの発行を停止します。
- **Assigned IP Address for AP Management** : LAPM によって新しく検出された AP がサービスゾーンに追加されるときに管理対象 AP に IP アドレスを割り当てるための IP セグメントです。

Assigned IP Address for AP Management

IP Range	Start IP Address	<input type="text" value="192.168.10.1"/>
	End IP Address	<input type="text" value="192.168.10.254"/>

This defines the range of IP addresses Access Points would use for Local Access Point Management.

Authentication Settings

システムは、いくつかの認証オプションをサポートしています。それは、ローカル、オンデマンド、ゲスト、ワンタイムパスワード、RADIUS、SIP、LDAP、NT ドメイン、POP3、ソーシャルメディアです。すべての認証オプションを有効にして同時に適用できます。これは、次のセクション「ユーザー」で強調します。

Authentication Settings

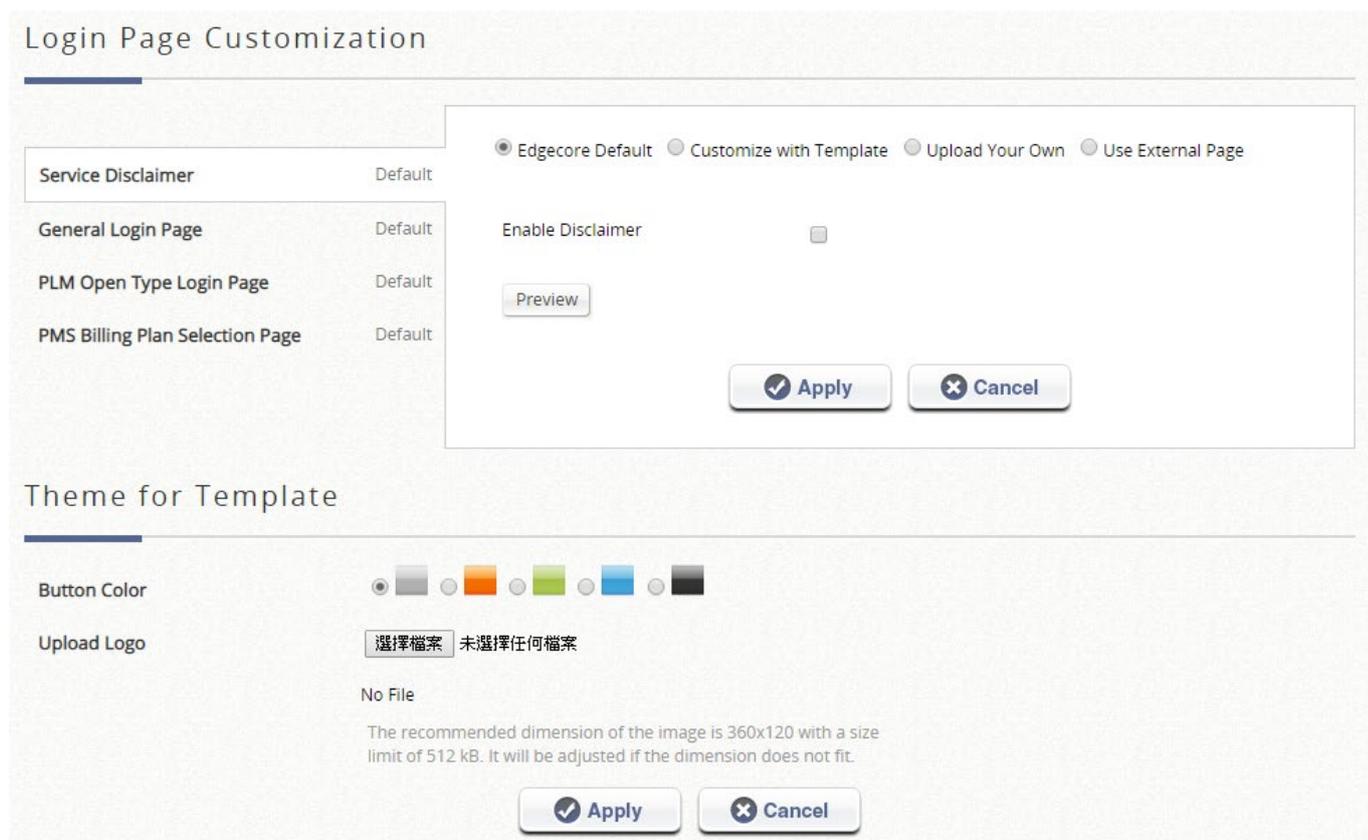
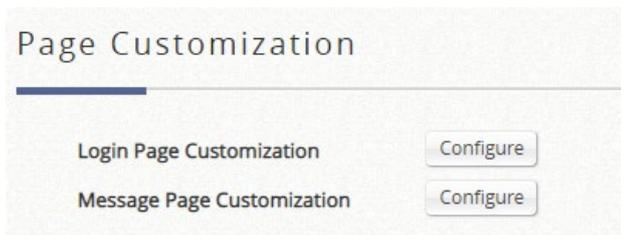
Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Suspend When Authentication is set to Suspended, users would see a suspend message from General Settings.																																																							
Access Permission and Authorization	<input type="button" value="Configure"/>																																																							
Portal URL	<input checked="" type="radio"/> Specific <input type="radio"/> Original <input type="radio"/> None <input type="text" value="http://www.google.com"/> * (e.g. http://www.example.com)																																																							
MAC Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled RADIUS Authentication using MAC address																																																							
PPP Authentication	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled																																																							
SIP Interface Configuration	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled																																																							
WISPr Settings	<input type="button" value="Configure"/>																																																							
Authentication Options	<table border="1"><thead><tr><th>Auth. Option</th><th>Auth. Database</th><th>Postfix</th><th>Default</th><th>Enabled</th></tr></thead><tbody><tr><td>Server 1</td><td>LOCAL</td><td>local</td><td><input checked="" type="radio"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td>Server 2</td><td>RADIUS</td><td>.</td><td><input type="radio"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td>Server 3</td><td>RADIUS</td><td>radius</td><td><input type="radio"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td>Server 4</td><td>LDAP</td><td>ldap</td><td><input type="radio"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td>Server 5</td><td>POP3</td><td>pop3</td><td><input type="radio"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td>On-Demand</td><td>ONDEMAND</td><td>ondemand</td><td><input type="radio"/></td><td><input checked="" type="checkbox"/></td></tr><tr><td>SIP</td><td>SIP</td><td>N/A</td><td><input type="radio"/></td><td><input type="checkbox"/></td></tr><tr><td>Guest</td><td>FREE</td><td>N/A</td><td><input type="radio"/></td><td><input type="checkbox"/></td></tr><tr><td>Social Media Login</td><td>SOCIAL</td><td>N/A</td><td><input type="radio"/></td><td><input type="checkbox"/></td></tr><tr><td>One Time Password</td><td>OTP</td><td>N/A</td><td><input type="radio"/></td><td><input type="checkbox"/></td></tr></tbody></table>	Auth. Option	Auth. Database	Postfix	Default	Enabled	Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	Server 2	RADIUS	.	<input type="radio"/>	<input checked="" type="checkbox"/>	Server 3	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>	Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>	Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>	On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>	SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>	Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>	One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>
Auth. Option	Auth. Database	Postfix	Default	Enabled																																																				
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>																																																				
Server 2	RADIUS	.	<input type="radio"/>	<input checked="" type="checkbox"/>																																																				
Server 3	RADIUS	radius	<input type="radio"/>	<input checked="" type="checkbox"/>																																																				
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>																																																				
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>																																																				
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>																																																				
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>																																																				
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>																																																				
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>																																																				
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>																																																				

- **Authentication Options** : 管理者は、使用する設定済みの認証サーバーを指定できます。複数の認証サーバーがサービスに対して有効になっている場合、接尾辞は認証サーバー識別子として使用されます。
- **Portal URL** : ここで必要なランディングページの仕様を設定できます。有効にすると、管理者はユーザーの初回ログイン後に開いたブラウザの URL を設定できます。
- **MAC Authentication** : RADIUS MAC 認証機能が有効になると、接続されたデバイスに設定された RADIUS サーバーに MAC アドレスが入力されている場合、コントローラは自動的に認証され、認証が成功するとすぐにアクセスを許可します。ユーザーは、透過的なログインを経験します。
- **PPP Authentication** : ポイントツーポイントプロトコル (PPP) とは、2つのネットワークノード間の直接接続を確立するために一般的に使用されるデータリンクプロトコルです。この機能がサービスに対して有効になっている場合、エンドユーザーは有効なユーザー名とパスワードを使用してダイヤルアップ接続設定を設定できます (ローカルユーザーと RADIUS ユーザーのみをサポートします)。ダイヤルアップ接続が確立されると、ユーザーは UAM ログインなしで正常に認証されます。
- **Assign IP Address From** : PPP がダイヤルアップ仮想インターフェースに IP アドレスを割り当てることのできる開始 IP 範囲です。割り当てられたインターフェース IP アドレスは、トンネルの両側のネットワーク間のルーティングに使用されます。

Page Customization

各サービスゾーンには、固有のログインページまたはメッセージページを持つように設定できます。ログインページには 3 つのタイプがあります。一般ログインページ、PLM オープンタイプログインページ (ポート

ロケーションマッピングの無料アクセス用)、および PMS 請求プラン選択ページです。必要に応じて、サービス免責事項ページを有効にできます。これらのページは完全にカスタマイズ可能で、管理者には完全な柔軟性を提供します。メッセージページはカスタマイズでき、メッセージページには以下が含まれます。ログイン成功ページ、オンデマンドユーザーのログイン成功ページ、ログイン失敗ページ、デバイスログアウトページ、ログアウト成功ページ、ログアウト失敗ページ、およびオンラインデバイスリストです。



Edgecore のデフォルトページとは別に、次の 3 つのカスタマイズオプションがあります。Customize with Template（テンプレートでのカスタマイズ）、Upload Your Own（独自のアップロード）、Use External Page（外部ページの使用）です。

- **Edgecore Default** : ゲートウェイには、Edgecore ロゴが付いた標準の Edgecore デフォルトログインページがあり、管理者は必要に応じてサービス免責事項を有効にすることができます。
- **Customize with Template** : このオプションでは、管理者が簡単にカスタマイズできるようにテンプレートが用意されています。一般的なレイアウトは管理者用に設定されていますが、内容は自分の好みに合わせてカスタマイズできます。カラーテーマとロゴをアップロードし、サービス免責事項などのコンテンツフィールド、テキストカラーをテンプレート内のレイアウトに入力することができます。
- **Upload Your Own** : 管理者には、ログインページとして html ファイルをアップロードするオプションがあります。「Download HTML Sample File」（HTML サンプルファイルのダウンロード）では、編集元となるサンプル HTML コードを管理者に提供します。このサンプル HTML コードをダウンロードしたら、任意のブラウザでファイルを開き、右クリックして「View Page Source」（ページソースの表示）を選択してください。ファイルが.html 形式で保存されていれば、任意のテキストエディタで HTML コードを編集できます。
- **Use External Page** : ログインページには、定義済みの外部 URL を指定できます。このオプションで

は、メッセージページと連携する URL パラメータの使用に関する広範な知識が必要であり、慎重に編成する必要があります。外部ログインページのカスタマイズの詳細については、テクニカルガイドを参照してください。

APs with VAP mapped to this Service Zone

AP Type

AP Type	AP Name	IP Address	MAC Address	Status
---------	---------	------------	-------------	--------

- **Managed AP(s)** : LAPM で管理され、サービスゾーンで動作する AP がここに表示されます。このリストは AP タイプ別に整理されています。AP は、AP 名のショートカットリンクをクリックして設定できます (Main > Access Points > Local Area AP Management > List > AP Configuration へのリンク)。これは概要のように機能し、管理者は一目で簡単にステータスをチェックできます。

8) Port Location Mapping

ポートロケーションマッピング機能を使用すると、各サービスゾーンが複数の VLAN を所有し (各 VLAN がポートであるかのように)、クライアントの送信元を識別できます。管理者は、ポートロケーションマッピング機能を使用して、ロケーション (ホテルの部屋など) を VLAN スイッチまたは DSLAM デバイスの VLAN ポートにマッピングできます。各部屋は VLAN タグにマッピングされます。また、各部屋を異なるサービスゾーンに割り当てて、異なるポリシーを取得することができます。さらに、アプリケーションに応じて、異なるポートタイプの部屋を設定することができます。**Authentication Required**、**Open** または **Block** です。

Create

Status Enable Disable

Mapping

Subinterface Use LAN Port

Subinterface ID

Remark

Lists

PLM List

Subinterface List

Tunnel PLM List

- **Open** : このポートタイプは、ユーザーがこの部屋で無料でインターネットにアクセスできることを意味します。

- **Block** : 部屋のインターネットアクセスを提供したくない場合は、部屋のポートタイプを「Block」に変更できます。ユーザーがブラウザを開いてインターネットにアクセスしようとする、ブロックメッセージがポップアップしてユーザーに通知されます。
- **Auth.Required** : このポートタイプは、主にユーザーに課金するためのホスピタリティアプリケーションで使用されます。ユーザーがブラウザを開いてインターネットにアクセスしようすると、免責事項と請求プランのオプションを含むページが表示されます。ユーザーは、希望するプランを選択し、confirm ボタンをクリックしてアカウントを購入することができます。アカウント費用は PMS に送信され、設定されたミドルウェアを介してホテルの請求書に追加されます。

➤ Create Single Mapping

The screenshot shows a web form titled 'Create One' under the 'Method' 'Create Single Mapping'. The form contains the following fields:

Port Type	Open
Choose LAN Port	LAN1
Service Zone	Default
DHCP Scope	None
Assign VLAN ID	Range from 1 - 4094 *
Location ID	A number
Location Description	Optional
User Limit	Unlimited if left blank
NAS Identifier	NAS Identifier
Class	
HTTP Parameter	

- **Port Type** : 部屋のデフォルトの状態は、次のようになります。Open、Block、または Auth.Required です。
- **Choose LAN Port** : トラフィックを受信する LAN ポートを選択します。
- **Service Zone** : 対応する場所にインターネットサービスを提供するために使用されるサービスゾーンプロファイルです。
- **DHCP Scope** : 対応するサービスゾーンから使用する DHCP プールを選択します。
- **Assign VLAN ID** : VLAN ID です。
- **Location ID** : 数値の ID 番号（通常は部屋番号）です。
- **Location Description** : 参照用の説明（オプション）です。
- **User Limit** : 対応するポートのバッチ内の最大ユーザー数です
- **NAS Identifier** : RADIUS 属性のオプションパラメータです。
- **Class** : RADIUS 属性のオプションパラメータです。
- **HTTP Parameter** : 外部ログインページが設定され、追加の HTTP パラメータが必要な場合にのみ使用されます。

➤ Create Multiple Mappings

Method Create Multiple Mappings ▼

Create Batch

Port Type	<input type="text" value="Open"/>
Choose LAN Port	<input type="text" value="LAN1"/>
Service Zone	<input type="text" value="Default"/>
DHCP Scope	<input type="text" value="None"/>
Assign VLAN ID From	<input type="text" value="Range from 1 - 4094"/> *
Number of VLANs	<input type="text" value="A number"/> *
Location ID From	<input type="text" value="A number"/>
Location Prefix	<input type="text" value="Optional"/>
Location Postfix	<input type="text" value="Optional"/>
User Limit Per Port	<input type="text" value="Unlimited if left blank"/>
NAS Identifier From	<input type="text" value="Optional"/>
NAS Identifier Prefix	<input type="text" value="Optional"/>
NAS Identifier Postfix	<input type="text" value="Optional"/>

- **Port Type** : 部屋のデフォルトの状態は、次のようになります。Free、Block、Single User、Multiple User です。
- **Choose LAN Port** : トラフィックを受信する LAN ポートを選択します。
- **Service Zone** : 対応する場所にインターネットサービスを提供するために使用されるサービスゾーンプロファイルです。
- **DHCP Scope** : 対応するサービスゾーンから使用する DHCP スコープを選択します。
- **Assign VLAN ID From** : 開始 VLAN ID です。
- **Number of VLAN** : VLAN の合計数です。
- **Location ID** : 数値の ID 番号（通常は部屋番号）です。
- **Location ID Prefix** : (部屋番号の) 接頭辞です。
- **Location ID Postfix** : (部屋番号の) 接尾辞です。
- **User Limit Per Port** : 対応するポートのバッチ内の最大ユーザー数です。
- **NAS Identifier From/Prefix/Postfix** : オプションの RADIUS 属性です

➤ Subinterface

サブインターフェース ID を入力すると、複数の VLAN ヘッダーを 1 つのイーサネットフレームに組み込むことができます。この機能は、さらなる分離のために複数の VLAN ヘッダーを必要とする大規模なネットワークでよく使用されます

➤ Port Location Mapping List

Port Location Mapping List

<input type="checkbox"/>	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
<input type="checkbox"/>	100	1000		Single User	LAN1	Default	●
<input type="checkbox"/>	101	1001		Single User	LAN1	Default	●
<input type="checkbox"/>	102	1002		Single User	LAN1	Default	●
<input type="checkbox"/>	103	1003		Single User	LAN1	Default	●

Port Location Mapping List には、VLAN ID、Room Num/Location ID、Port Type、Service Zone などの情報を含むすべてのプロファイルエントリが表示されます。

- **Delete** : 個々のポートロケーションマッピングプロファイルを消去します。
- **Export List** : 存在していたポートロケーションマッピングリストをバックアップします。
- **Import List** : ポートロケーションマッピングリストを復元します。
- **Change All Port Type** : すべての部屋にポートタイプを設定します。Free、Block、Single User、Multiple User です。

➤ Tunnel PLM List

<input type="checkbox"/>	ESSID	Location ID	Location Description	Port Type	From	Service Zone
--------------------------	-------	-------------	----------------------	-----------	------	--------------

(Total:0) [First](#) [Prev](#) [Next](#) [Last](#) (Page:1/1)

リモート AP からコントローラにトンネリングされる VAP の場合、管理者は、NAS 識別子を割り当てるとともに、サービス用の IP プールを指定することもできます。

Wide Area AP Management の管理対象 AP List では、管理者は NAS 識別子を割り当て、管理対象 AP の VAP ごとにサービス用の IP プールを指定できます。これは、AP とコントローラの間トンネルを確立するときに設定できます。

9) PMS Interface

PMS インターフェースへの接続を設定することにより、システムは、PMS サーバーからの特定のメッセージをリッスンすることができます。ホテルのゲストがインターネットアクセスのために客室料金プランを購入すると、システムは PMS サーバーに記録を転記します。

PMS Interface Configuration

PMS Interface Type	<input type="radio"/> Disable <input checked="" type="radio"/> Micros Opera <input type="radio"/> InnKeyPMS <input type="radio"/> IDS
PMS IP Address	<input type="text"/>
PMS Port	<input type="text"/>
Account Credentials	Username <input type="text"/> RN ▼
	Password <input type="text"/> RN ▼
Room Bill Description	<input type="text" value="Wireless Access"/>
Login Error Message	<div style="border: 1px solid #ccc; padding: 5px;">An error has occurred during login. Please contact the front desk for assistance.</div>
User Account Log	<input type="button" value="View"/>
Synchronize Data with PMS	<input type="button" value="Sync"/>
PMS External Page Customization API	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
External Page Validity Verification	Username <input type="text"/>
	Password <input type="text"/>
Sample External Login Page	<input type="button" value="Download"/>

- **PMS Interface Type** : 統合する PMS インターフェースタイプを選択します。

Micros Opera/IDS

- **PMS IP** : Micros Opera PMS が使用する IP を入力します。
- **PMS ポート** : Micros Opera PMS が使用するポートを入力します。
- **Account Credentials** : 管理者は、RN (部屋番号)、GN (ゲスト名)、G# (ゲスト番号)、G+ (プロフィール名) の組み合わせを使用して、ユーザーアカウントの資格情報を定義し、ユーザー名とパスワード情報を伝送するための Micros プロトコルパラメータを指定できます。
 - **Case and Diacritics Insensitive for Password** : ゲスト名をパスワードとして使用する場合、大文字と小文字と発音区別記号は、PMS サーバーに保存されている情報に正確に従います。大文字と小文字と発音区別記号を無視するには、このオプションを有効にします。
- **Room Bill Description** : 入力した説明は、PMS 統合を介して部屋請求書に表示されます。
- **Login Error Message** : エラーメッセージの内容をカスタマイズできます。
- **User Account Log** : この機能に関連するバックグラウンドで発生したイベントは記録され、ここに表示されることがあります。
- **Synchronize Data with PMS** : 「Sync」をクリックして、PMS サーバーとデータを同期し、データベースが最新の状態であることを確認します。
- **PMS External Page Customization API** : PMS API は、ログイン情報、選択された請求プラン、購入単位などにアクセスプロセスを完了することができ、カスタマイズされたログインページを備えた柔軟な実装を管理者に提供します。
 - **External Page Validity Verification** : 管理者は、独自のユーザ名とパスワードを使用して、外部 Web サーバーと無線 LAN コントローラ間の API プロトコルを保護することもできます。
 - **Sample External Login Page** : 管理者が簡単に統合および変更する方法を理解できるダウンロード可能な例があります。
 - すべての req_type は、Json でファイル化された「フォーマット」を使用することができます。
 - req_type=1 (equals : bpinfo) は請求プラン情報を表示することができ、フィールド「all」を追加すると、非アクティブなものを含むすべての請求プランが表示されます
 - req_type=2 (equals : check) 利用可能な請求プラン、ユニット、および特定の請求プランを購入することが許可されているかどうかを確認し、エラーがある場合、それは管理者のためのエラーコー

ドとメッセージを返します

- req_type=3 (equals : userinfo) は、ユーザーの情報とステータスを表示することができます。フィールド「all」を追加すると、カスタマイズされた属性 A0-A9 の値が表示されます。特定のフィールド (A5、A9) を追加すると、対応する値が表示されます。
- テストする前に、それは関数 send_req で使用されている無線 LAN コントローラの管理者のパスワードであることに留意してください
- 対応するサービスゾーンについては、Use External Page (外部ページの使用) を使用してログインページをカスタマイズしてください

PMS Interface Configuration

PMS Interface Type Disable Micros Opera InnKeyPMS IDS

Query API

Post API

Shared Key

Account Credentials Username Room Number ▼
Password Guest Number ▼

Case and Diacritics Insensitive for Password Disable Enable

Login Error Message

User Account Log

Innkey PMS

- **Query API** : クエリ API の IP を入力します。
- **Post API** : ポスト API の IP を入力します。
- **Shared Key** : Innkey PMS API の共有キーを入力します。
- **Account Credential** : 部屋番号とゲスト番号は、ユーザーログイン時のユーザー名とパスワードとなります。
- **Case and Diacritics Insensitive for Password** : パスワードの確認時に大文字と小文字と発音区別記号を無視するには、このオプションを有効にします。
- **Login Error Message** : エラーメッセージの内容をカスタマイズできます。
- **User Account Log** : この機能に関連するバックグラウンドで発生したイベントは記録され、ここに表示されることがあります。

B.Users

Users : このセクションは、ユーザー認証、認可、およびアカウントに関するものです。これには、グループ設定、内部/外部認証設定、オンデマンドアカウント、ポリシー設定、権限リストの設定、追加制御が含まれます。

1) Groups

Group Overview ページには、対応するグループで使用されている認証サーバーの概要が表示されません。

This page gives a summary of which Authentication Servers are used for the corresponding Group.

Group Overview

Group Name	Authentication Type
Group 1	Local Billing Plan 1 Billing Plan 2 Billing Plan 3 Guest Social Media Login OTP POP3-Server 5 RADIUS-Server 2-Default LDAP-Server 4-Default NT Domain-Server 3 SIP
Group 2	
Group 3	
Group 4	
Group 5	
Group 6	
Group 7	
Group 8	

16セットのグループオプション（モデルの依存関係）と Zone Permission Configuration & Policy Assignment をそれぞれ定義して、異なるサービスゾーン内の異なるユーザーグループのアクセス管理を強制できます。対応は「Group Configuration」ページで設定できます。

This page gives a summary of access permissions for each Group in different Service Zones.

Group Configuration

Select Group:

Group Name:

Remark:

Number of devices which are allowed to login:
(0 to 9999 devices, 0: Unlimited)
For On-Demand accounts, number of devices is configured individually per different billing plans. The number is for the following types: LOCAL, POP3, RADIUS, LDAP, and NT Domain.

Allow to logout other devices when exceeding the maximum amount of devices: Enabled Disabled
For On -Demand accounts, allowing to logout others devices is always enabled. This setting id for the following types: LOCAL, POP3, RADIUS, LADP, and NT Domain.

Zone Permission Configuration & Policy Assignment

Enabled	Zone Name	Time Span 1	Time Span 2
		Schedule 1	Schedule 1
<input checked="" type="checkbox"/>	Service Zone : Default	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ1	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ2	Policy 1	Policy 1
<input checked="" type="checkbox"/>	Service Zone : SZ3	Policy 1	Policy 1

複数のデバイスが同じアカウント資格情報でログインできるようにするには、ここの「Number of devices which are allowed to login」で番号を定義します。オンデマンド認証オプションの複数のデバイスログインは、選択した請求プランで設定できます。

2) Internal Authentication

システムは、内部データベースと外部データベースの両方を含む複数の認証オプションをサポートしています。内部認証データベースには、「ローカル」、「オンデマンド」、「ゲスト」があります。

Authentication Option - Server 1

Server No. 1

Name: Server 1 *

User Postfix: local *

Remark:

Blacklist: None

Authentication: LOCAL

a) Local Authentication

このタイプの認証方法は、ユーザー、多くの場合、スタッフと資格情報を内部的に格納するローカルデータベースをチェックします。ローカルユーザーデータベースは、管理者が手動で実行しない限り、削除されない静的アカウントを保存するように設計されています。

「ローカル」のデフォルトの認証は、認証サーバー1に設定されています。このユーザー接尾辞は、複数のオプションが同時に使用されている場合に、特定のユーザーアカウントに対してどの認証オプションを使用するかを識別するためにシステムに使用されます。ローカルアカウントを操作するには、Local User Listの「Configure」に移動します。

Main > Users > Internal Authentication > Local Authentication

Server No. 1: Server 1

Local Authentication

Local User List: Configure

Account Roaming Out: Enable Disable

802.1X Authentication: Enable Disable

RADIUS Client Device Settings

Apply Cancel

- **Local User List** : 「Configure」をクリックして、ローカルアカウントリストを表示し、アカウントを設定します。

- **Account Roaming Out** : コントローラを外部 RADIUS 認証要求の RADIUS サーバーとして使用する場
合、ローカルアカウントデータベースを有効/無効にします。
- **802.1X Authentication** : コントローラを外部 802.1X 認証要求の RADIUS サーバーとして使用する場
合、ローカルアカウントデータベースを有効/無効にします。
 - **RADIUS Client Device Settings** : コントローラで RADIUS または 802.1X 認証を実行できるデバイ
スのクライアントリストと秘密キーを設定します。

Local User List

No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
(Total:0/10000) <input type="button" value="First"/> <input type="button" value="Prev"/> <input type="button" value="Next"/> <input type="button" value="Last"/> <input type="button" value="Go to Page"/> (Page:1/1) Row per Page: <input type="text" value="10"/>								

- **Add** : ユーザー名、パスワード、MAC アドレス、グループ、アカウントスパン、および備考などのアカ
ウント情報を持つ 1 つまたは複数のアカウントを作成します。
- **Delete** : 個別に削除でき、または「すべて選択」チェックボックスを選択することで、全部に削除するこ
ともできます。
- **Backup** : ユーザーの資格情報を CSV 形式のテキストファイルとして新しいウィンドウにエクスポートし
ます。
- **Upload** : アカウントをローカルユーザーデータベースにインポートし、大量のローカルアカウントを作成
する便利な方法です。
- **Edit Account Information** : 既存のユーザーアカウントの場合、ページ上のユーザー名のハイパーリンク
をクリックするだけで、アカウント属性を再設定し、さらに変更を加えることができます。

10000 users can be added to this local user list.

Username	Password	MAC Address	Group	Account Span	Remark
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Group 1 ▼	<input type="checkbox"/>	<input type="text"/>

- **Username** : 新しいローカルアカウントのユーザ名です。新しいアカウントを追加するときは必須です。
- **Password** : 新しいローカルアカウントのパスワードです。新しいアカウントを追加するときは必須で
す。
- **MAC Address** : 指定された MAC アドレスを持つデバイスを使用してのみアクセスを許可できるという条
件の下で、この特定のアカウントをバインドします。
- **Group** : 作成するアカウントのグループプロファイルです。
- **Account Span** : このアカウントに強制される時間制約です。
- **Remark** : 管理者が強調したい追加のメモです。これは、ユーザーリストに表示されます。

b) On-Demand Authentication

オンデマンド認証オプションは、通常、パブリックホットスポットなどの短期的な使用に使用されま
す。オンデマンド認証オプションに関連する設定は、請求プランプロファイル、POS チケットのカスタ
マイズ、ターミナルサーバーリスト、外部支払いゲートウェイの設定など、ここで設定できます。

On-Demand Authentication

User Postfix	<input type="text" value="ondemand"/>
Billing Plans	<input type="button" value="Configure"/>
Currency	<input type="radio"/> None <input type="radio"/> \$ USD <input type="radio"/> € EUR <input type="radio"/> £ GBP <input type="text" value=""/>
This is used when the currency is not defined in the Paypal account. Or input another desired monetary unit (max. 3 letters) in the blank field.	
Expired Account Cache	<input type="text" value="30"/> day(s)
Out-of-quota Account Cache	<input type="text" value="30"/> day(s)
Set Ticket's Serial Number	<input type="text" value="000001"/> <input type="button" value="Set"/>
Web Printout	<input type="button" value="Configure"/>
This will be applied to the regular printer printout when creating a single On-Demand account.	
POS Tickets	<input type="button" value="Configure"/>
Number of Tickets <input checked="" type="radio"/> 1 <input type="radio"/> 2	
This will be applied to printouts from the POS ticket printer. Templates can be edited for customization.	
Terminal Server	<input type="button" value="Configure"/>
Terminal Servers are add-on devices such as the SDS100 or SDS200W.	
Payment Gateway	<input type="button" value="Configure"/>
SMS Gateway	<input type="button" value="Configure"/>
Account Roaming Out	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

- **User Postfix** : このユーザー接尾辞は、複数のオプションが同時に使用されている場合に、特定のユーザーアカウントに対してどの認証オプションを使用するかを識別するためにシステムに使用されます。
- **Billing Plans** : 「Configure」 ボタンをクリックして、請求プランを編集します。
- **Currency** : 各オンデマンド資格情報の価格を示します。
- **Expired Account Cache** : すでに期限切れになっているため、データベースからオンデマンドアカウントを排除する日間です。
- **Out-of-quota Account Cache** : すでにクォータが不足しているため、データベースからオンデマンドアカウントを排除する日間です。
- **On-Demand Access Code** : ユーザー名とパスワード以外のアクセスコードを使用したオンデマンドユーザーのログインを許可/禁止します。
- **Smart Login** : オンデマンドユーザーのログインを特定の期間内に自動的に許可/禁止します。
- **Set Ticket's Serial Number** : 次の POS チケットの印刷のシリアル番号を設定します。
- **Web Printout** : オンデマンドアカウントを1つ作成するときにアカウント情報ページをカスタマイズするには、「Configure」 ボタンをクリックします。また、ここで結果をプレビューすることもできます。
- **POS Tickets** : POS プリンタで印刷するアカウントチケットをカスタマイズするには、「Configure」 ボタンをクリックします。
- **POS Printer** : POS プリンタを追加/削除するには、「Configure」 ボタンをクリックします。
- **Payment Gateway** : 「Configure」 ボタンをクリックして、支払いゲートウェイインターフェースを設定し、ユーザーが自分でアカウントを購入することができます。
- **SMS Gateway** : SMS ゲートウェイの統合を設定するには、「Configure」 ボタンをクリックします。オンデマンドアカウント情報は、アカウント作成時に SMS メッセージで送信できます。
- **Email Verification** : 「Configure」 ボタンをクリックして、メール認証機能を設定します。ユーザーは、電子メールで送信されたリンクを有効にすることで、アカウントの追加のクォータにアクセスできます。
- **Account Roaming Out** : コントローラを外部 RADIUS 認証要求の RADIUS サーバーとして使用する場合は、オンデマンドアカウントデータベースを有効/無効にします。
 - **RADIUS Client Device Settings** : コントローラで RADIUS または 802.1X 認証を実行できるデバイスのクライアントリストと秘密キーを設定します。

Billing Plans

No	Plan Type	Quota	Price	Active	Group	Function
1	N/A			<input type="checkbox"/>	Group 1	Reset
2	N/A			<input type="checkbox"/>	Group 1	Reset
3	N/A			<input type="checkbox"/>	Group 1	Reset
4	N/A			<input type="checkbox"/>	Group 1	Reset
5	N/A			<input type="checkbox"/>	Group 1	Reset
6	N/A			<input type="checkbox"/>	Group 1	Reset
7	N/A			<input type="checkbox"/>	Group 1	Reset
8	N/A			<input type="checkbox"/>	Group 1	Reset
9	N/A			<input type="checkbox"/>	Group 1	Reset
0	N/A			<input type="checkbox"/>	Group 1	Reset

最大 10 件の請求プランを設定できます。請求プランには、次の 4 種類があります。使用時間、ボリューム、ホテルカットオフ時間、継続時間です。請求プランタイプのご概念については、付録 D を参照してください。

Payment Gateway

External Payment Gateway

Selection

Disable Authorize.Net PayPal SecurePay WorldPay PeleCard

Number of SMS quota *(1~10) [SMS gateway configure](#)

The function to send SMS after purchasing an account is not ready. This is the given SMS quota to the client when multiple messages are required, either for multiple devices or if the SMS needs to be re-sent.

PayPal Payment Page Configuration

Business Account *

Payment Gateway URL *

Identity Token *

Instant Payment Notification (IPN) Enable Disable
 Behind NAT

Verify SSL Certificate Enable Disable
Default ▾

Currency *

- **Payment Page Configuration** : 支払いゲートウェイの種類によって、記入すべき情報が異なります。これらの情報は、支払いゲートウェイのアカウントで見つけることができます。
- **Instant Payment Notification (IPN)** : (Paypal のみ) IPN を有効にすると、Paypal は取引が発生したときにコントローラに通知を送信します。コントローラの WAN IP が NAT の下にある場合、支払いエンドユーザーが取引結果を受け取るには、IP 転送情報を設定する必要があります。
- **Choose Billing Plans for Payment Page** : ユーザーがアカウントを購入するときに利用可能な請求プラン

ンを選択します。

- **Web Page Customization** : 「Configure」をクリックして、サービス免責事項ページ、請求プラン選択ページ、およびアカウント認証ページをカスタマイズします。

SMS Gateway

- **Selection** : 統合する SMS ゲートウェイのタイプを選択します。
 - **Clickatell** : SMS メッセージを送信するために Clickatell API で接続します。
 - **SMS API** : SMS ゲートウェイの HTTP API と統合するための汎用オプションです。コントローラは、パラメータが設定された指定の API URL に HTTP リクエストを送信し、リクエストが成功したかどうかを定義されたパターンで識別します。
- **Version (Clickatell のみ)** : 旧バージョン (2016 年 11 月以前) は、REST プロトコルの Clickatell API を API ID、ユーザー名、パスワードの JSON 形式で提供しています。新バージョンは、統合のために HTTP プロトコルの API キーのみが必要となります。
- **Send SMS for** : コントローラが SMS メッセージを送信する条件を選択します。
 - **Account Registration** : ユーザーが自己登録し、SMS 経由で Wi-Fi アカウントを受信できるようにします。
 - **Account Purchases via Payment Gateway** : オンライン支払いゲートウェイ経由でオンデマンドアカウントを購入した Wi-Fi ユーザーに対して、SMS 機能を有効にします。彼らは SMS を使用して購入したアカウントを自分のモバイルデバイスに送信するオプションが与えられます。
 - **Both** : 両方のオプションを有効にします。
- **API Key (Clickatell のみ)** : 特定の統合サービスの呼び出しとロック解除に使用される Clickatell API の認証キーです。
- **API URL** : SMS リクエストを Clickatell API サーバーに送信するためのリンクです。デフォルトは <http://api.clickatell.com/http/sendmsg> です。
- **Registration before Accounts Expired** : Allow を選択すると、1 つ目のアカウントの有効期限が切れていないか、まだ使用されていない場合でも、同じ携帯電話番号で 2 つ目のオンデマンドアカウントを申請できます。Block を選択すると、1 つ目のアカウントの有効期限が切れた後に 2 つ目のオンデマンドアカウントを送信するようにユーザーを制限します。

SMS Gateway

Selection Disable Clickatell SMS API
 Version Old (Prior to November 2016) New
 Send SMS for
 API key
 API URL
 Registration before Accounts Expired Allow Block
 Billing Plans

Plan	Activation	Quota	Price	Remark
1	<input type="checkbox"/>			
2	<input type="checkbox"/>			
3	<input type="checkbox"/>			
4	<input type="checkbox"/>			
5	<input type="checkbox"/>			
6	<input type="checkbox"/>			
7	<input type="checkbox"/>			
8	<input type="checkbox"/>			
9	<input type="checkbox"/>			
10	<input type="checkbox"/>			

Account Registration Control Disable Black List White List
 Web Page Customization

- **Parameter (SMS API のみ)** : SMS リクエストを送信するための API パラメータと値です。
- **Response Format (SMS API のみ)** : JSON または HTML です。選択された選択肢は、SMS サービスによって提供される応答のタイプによって異なります。応答形式は、SMS テキストメッセージが正常に送信されたかどうかを判断するために無線 LAN コントローラによって使用されます。
- **Key of JSON Array (SMS API のみ)** : SMS リクエストの応答からの値のキーパスを JSON 形式で指定します。例 : ['data'][0]['status']
- **Return Value of Successful Request (SMS API のみ)** : 成功した応答のテキストをここに入力します。
- **Send Test Message (SMS API のみ)** : 携帯電話番号が入力され、「テスト」の SMS メッセージが送信されます。SMS メッセージの送信時に、オンデマンドアカウントは作成されません。「Test」ボタンを使用して、SMS リクエストのトラブルシューティングや、SMS プロバイダから送信された応答メッセージの表示を行うことができます。
- **Message Content (SMS API のみ)** : Message Editor ボックスで、Wi-Fi ユーザーが受信する SMS テキストメッセージをカスタマイズします。ユーザー名、接尾辞のないユーザー名、パスワード、クォータの説明など、作成したオンデマンドアカウントに関する 4 つのパラメータを入力できます。

パラメータ	定義
\$username	作成したオンデマンドアカウントのユーザー名です。
\$Username_without_postfix	\$username と同じですが、接尾辞はありません。
\$password	作成したオンデマンドアカウントのパスワードです。
\$quota	作成したオンデマンドアカウントのクォータの説明です。

SMS Gateway

Disable Clickatell SMS API

Send SMS for: Account Registration

API URL: *

Registration before Accounts Expired: Allow Block

Parameter

No.	Parameter	Parameter Value	Remark
-	<input type="text"/>	<input type="text"/>	Phone Number
-	<input type="text"/>	<input type="text"/>	SMS Content
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>

Response Format: JSON HTML

Key of JSON Array: *

Return Value of Successful Request: *

Please check the response sample code to identify the object for indicating the success of the request.

Send Test Message:

Please apply the changes in this page before sending test message.

Message Content

Message Editor

Parameter	Value
\$username	On-Demand Username
▼	<input type="button" value="Insert Parameter"/>

Billing Plans

Plan	Activation	Quota	Price	Remark
1	<input type="checkbox"/>			<input type="text"/>
2	<input type="checkbox"/>			<input type="text"/>
3	<input type="checkbox"/>			<input type="text"/>
4	<input type="checkbox"/>			<input type="text"/>
5	<input type="checkbox"/>			<input type="text"/>
6	<input type="checkbox"/>			<input type="text"/>
7	<input type="checkbox"/>			<input type="text"/>
8	<input type="checkbox"/>			<input type="text"/>
9	<input type="checkbox"/>			<input type="text"/>
10	<input type="checkbox"/>			<input type="text"/>

Account Registration Control: Disable Black List White List

Web Page Customization:

- **Billing Plans** : 作成された「アクティブ」な請求プランが表示され、SMS 経由でオンデマンドアカウントを作成するために使用されます。少なくとも 1 つの請求プランを選択する必要があります。
- **Account Registration Control** : Disable、Black List、White List を選択します。指定されている携帯電話

番号のみを制限または許可しない場合は、Disable にします。Black List は、登録から特定の携帯電話番号を拒否します。White List は、特定の携帯電話番号のみ登録できます。

- **Web Page Customization** : Default、Customize with Template（テンプレートでのカスタマイズ）、Upload Your Own（独自のアップロード）、Use External Page（外部ページの使用）オプションを使用して、サービス免責事項および請求プランの選択ページをカスタマイズします。

Email Verification

Email Verification

Selection Disable Enable

Choose Billing Plan for Redeeming Account via Email (Only Usage Time selectable)

Plan	Activation	Quota	Redeem Quota	Price	Remark
1	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
2	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
3	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
4	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
5	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
6	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
7	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
8	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
9	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		
10	<input type="checkbox"/>		<input type="text"/> D <input type="text"/> H <input type="text"/> M		

SMTP Server Settings

[Assign SMTP server](#)

SMTP server is not ready

Sender Name *(name@domain)

Activation Email Subject

Activation Email Content

Activation Link

Web Page Customization [Configure](#)

- **Selection** : この機能を有効または無効にします。
- **Choose Billing Plan for Redeeming Account via Email (only Usage Time Selectable)** : 設定済みの請求プランを選択し、使用時間タイプの請求プランのみがこの機能をサポートします。
 - **Activation** : メール検証機能を許可する請求プランを選択します。
 - **Quota** : 各請求プランの現在の概要を表示します。
 - **Redeem Quota** : 引き換え時に追加で使える使用時間です。
 - **Price** : 各請求プランの現在の価格を表示します。
 - **Remark** : ウォールド・ガーデンの各エントリーのアイデンティティを示すためのカスタムフィールドです。
- **SMTP Server Settings** : 引き換えクライアント用のメールを送信するための SMTP サーバーを割り当てます。この SMTP は、ゲスト電子メール検証と共有されます。
- **Sender Name** : クライアントのメールボックスに表示される送信者名です。

- **Activation Email Subject** : クライアントのメールボックスに表示されるカスタマイズ可能な電子メールの件名です。
- **Activation Email Content** : クライアントのメールボックスに表示されるカスタマイズ可能な電子メール内容（最大 2000 文字）です
- **Activation Link** : クライアントの電子メールでアカウントを引き換えるためのハイパーリンク付きの名前です。
- **Web Page Customization** : カスタマイズされたタイプは選択可能ですが、Edgecore Default と Customize with Template（テンプレートでのカスタマイズ）のみのサポートとなっています。

c) Guest Authentication

ゲスト認証オプションは技術的にはユーザーデータベースではなく、ユーザーがユーザーアカウントやパスワードなしでネットワークにアクセスして閲覧できるように特別に設計されたオプションです。この機能により、ユーザーは特定のサービスゾーンに関連付けて、ゲストメールや管理者が定義した社会保障番号などのゲストアンケートによって指定されたテキスト文字列を入力し、実際の認証なしでネットワークを利用することができます。

Guest Authentication

Group: Group 1

Guest Information: View

Guest Questionnaire: Configure

Guest Access Time: Unlimited 1 Day Access Multi-Day Access

Quota: 0 hour(s) 30 minute(s)
1000 MByte(s) *(Range:0~1000000, 0:Unlimited)

Reactivation: After 0 hour(s) 1 minute(s)

Access Limit: 30 per day *(0:Unlimited)

Email Verification: Disable Enable

Email Activation Time: 0 hour(s) 10 minute(s) Assign SMTP server
SMTP server is not ready

Sender Name: Internet Service *(name@domain)

Activation Email Subject: Please activate your account

Activation Email Content: Congratulations! You are eligible for free access. Please click the link below to activate your account for extended usage time.

Activation Link: Click Here!

Guest Quota List: View

E-mail Denial List: Disable Enable Configure

- **Group** : ゲストログインクライアントが属するユーザーグループです。特定のサービスゾーンにマッピングし、ユーザーポリシープロファイルの制限を適用できます。
- **Guest Information** : アカウントの一部の情報は、管理者のさらなる分析やマーケティングの目的で利用可能です。アカウントの電子メールやその他のアンケートが有効なフィールドは、管理者のデータ操作のためにダウンロードできます。エントリは自動的にクリアされませんが、残り 1000 エントリ（11000/12000、最大 12000 エントリ）のときにメールで通知するようにしています。
 - **Download** : 管理者は、収集したゲスト情報をダウンロードできます。

- **Delete All** : 管理者は、保存されたデータをすべて削除できます。管理者は、エクスポート後にすべてのエントリーを削除して、リストを最新の状態に保つことができます。
- **Questionnaire** : 管理者がゲストログイン用のログインページで追加の質問をカスタマイズできるオプションに提供します。ゲストユーザーからのアクセス情報が収集され、Guest Information リストに表示されます。
- **Guest Access Time** : MAC アドレスに基づいてユーザーの時間制約を定義します。
 - **Unlimited** : 許容の使用時間に制限はありません。
 - **1 Day Access** : クライアントは、使用時間の制約で強制されます。
 - **Multi-Day Access** : クライアントは、使用時間の制約で強制されます。
- **Quota** : 各ゲストクライアントに対して許可される期間と量です。
- **Reactivation (1 Day Access のみ)** : 時間が経過すると、新しいセッションを定義することが可能になります。
- **Access Limit (1 Day Access のみ)** : デバイスが1日に無料アカウントを要求できる回数を定義します。
- **Email Verification** : 入力された電子メールが有効な電子メールアドレスであることを確認します。クライアントはメールサーバーから送信されたメール内のリンクをクリックすることで、アクティベーション時間内にこのアカウントをアクティブにして、使用時間を延長する必要があります。アクティベーションは単なるタイマーであり、アカウントのクォータには追加されないことに注意してください。
- **SMTP Server Settings** : 引き換えクライアント用のメールを送信するための SMTP サーバーを割り当てます。この SMTP は、オンデマンド電子メール検証と共有されます。Gmail を SMTP サーバーの例とすると、設定は以下のとおりです。
 - **SMTP server address** : smtp.gmail.com
 - **SMTP port** : 465
 - **Encryption** : SSL
 - **Authentication: Login** : アカウント名 : 管理者の Gmail メールアドレス
 - **Authentication: Login** : パスワード : 管理者の Gmail メールアドレスのパスワード
 - **Sender Email Address** : 管理者の Gmail メールアドレス。
- **Sender Name** : クライアントのメールボックスに表示される送信者名です。
- **Activation Email Subject** : クライアントのメールボックスに表示されるカスタマイズ可能な電子メールの件名です。
- **Activation Email Content** : クライアントのメールボックスに表示されるカスタマイズ可能な電子メール内容 (最大 2000 文字) です。
- **Activation Link** : クライアントの電子メールでアカウントを引き換えるためのハイパーリンク付きの名前です。
- **Guest Quota List** : アクセスを制限されたゲストアカウントの残りの許容回数を MAC アドレスと電子メールアドレスで確認できます。(毎日午前 0 時に自動的に更新され、最大値に達すると最も古いエントリーは削除されます。)
- **Email Denial List** : 迷惑メールボックスの防止が必要な場合は、電子メールドメインにログイン許可を確認します。

d) One Time Password

ワンタイムパスワード (OTP) 認証オプションの場合、クライアントは自分の携帯電話番号を入力し、認証ページに入力するために必要なワンタイムパスワードを含む SMS メッセージを受信することで、インターネットにアクセスできます。その後、クライアントはインターネット閲覧を始めることができます。

One Time Password Authentication

Group	Group 1 ▾
OTP Client Information	View
Default Country Code	AF - AFGHANISTAN (+93) ▾ <input type="checkbox"/> only display default country code
Length of Mobile Number	0 *(0: Unlimited)
Quota	0 day(s) 0 hour(s) 30 minute(s) *
Questionnaire	Configure
SMS Gateway	Configure
OTP Page Customization	Configure

- **Group** : OTP 認証クライアントは、各サービスゾーンで設定されたユーザーポリシーによって適用されます。
- **OTP Client Information** : ワンタイムパスワードを尋ねたクライアントの情報です。
 - **Download** : 管理者は、収集した OTP クライアントの情報をダウンロードできます。
 - **Delete All** : 管理者は、保存されたデータをすべて削除できます。管理者は、エクスポート後にすべてのエントリを削除して、リストを最新の状態に保つことができます。
- **Default Country Code** : ログインページに表示されるデフォルトの国コードを設定します。
- **Length of Mobile Number** : 携帯電話の番号形式を桁数で設定します。
- **Quota (Duration Time)** : OTP 認証クライアントの期間を指定します。最大所要時間は 364 日 23 時間 59 分です。
- **Questionnaire** : OTP 登録ページに表示された 5 つのエントリです。
- **SMS Gateway** : Clickatell (レガシー/新規)、SMS API (テキスト内容のカスタマイズを確認)、関連設定については、オンデマンドユーザーデータベースの SMS ゲートウェイ設定を参照してください
- **Web Page Customization** : カスタマイズされたタイプは選択可能ですが、*Edgecore Default* と *Customize with Template* (テンプレートでのカスタマイズ) のみのサポートとなっています。

3) External Authentication

最大 5 台の外部認証サーバーを同時に設定し、有効にすることで、ネットワーク上の既存のユーザーアカウントデータベースを容易にできます。外部認証オプションには、RADIUS、POP3、LDAP、NT ドメイン、SIP などがあります。

Authentication Options					
Auth. Option	Auth. Database	Postfix	Default	Enabled	
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	
Server 2	RADIUS	.	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 4	LDAP	ldap	<input type="radio"/>	<input checked="" type="checkbox"/>	
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>	
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>	
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>	
Guest	FREE	N/A	<input type="radio"/>	<input checked="" type="checkbox"/>	
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>	
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>	

a) Social Media Authentication

- **Group** : ソーシャルメディアログインクライアントが属するユーザーグループです。特定のサービスゾーンにマッピングし、ユーザーポリシープロファイルの制限を適用できます。
- **Social Media Account Information** : アカウントの一部の情報は、管理者のさらなる分析やマーケティングの目的で利用可能です。ソーシャルメディアアカウントリスト上のアカウント名、アカウントメール、性別、誕生日、位置情報は、管理者のデータ操作のためにダウンロードすることができます（ソーシャルメディアが提供を許可している場合）。エントリは自動的にクリアされませんが、残り 1000 エントリ（11000/12000、最大 12000 エントリ）のときにメールで通知するようにしています。
 - **Download** : 管理者は、収集したゲスト情報をダウンロードできます
 - **Delete All** : 管理者は、保存されたデータをすべて削除できます。管理者は、エクスポート後にすべてのエントリを削除して、リストを最新の状態に保つことができます。
- **Social Media Account Access Time** : 「制限付き」に設定すると、MAC アドレスに基づいて使用時間の制約が強制されます。
- **Quota** : 各ソーシャルメディアログインクライアントに対して許可される期間と量です。
- **Reactivation** : 時間が経過すると、新しいセッションを定義することが可能になります。
- **Access Limit** : デバイスが 1 日に無料アカウントを要求できる回数を定義します。

Social Media Login

Group: Group 2

Social Media Account Information: View

Social Media Account Access Time: Unlimited 1 Day Access Multi-Day Access

Quota: 0 hour(s) 30 minute(s)
0 MByte(s) *(Range:0~1000000, 0:Unlimited)

Reactivation: After 1 hour(s) 0 minute(s)

Access Limit: 5 per day *(0:Unlimited)

Social Media Account Quota List: View

Punishment: Enable Disable

Punishment List: View

Apply Cancel

- **Social Account Quota List** : アクセスを制限されたゲストアカウントの残りの許容回数を MAC アドレスと電子メールアドレスで確認できます。（毎日午前 0 時に自動的に更新され、最大値に達すると最も古いエントリは削除されます。）
- **Punishment** : 罰メカニズムを有効/無効にします。事前承認されたクライアントが 5 分以内にログインプロセスを完了していない場合、クライアントエントリがこの表に表示されます。クライアントがソーシャルログインボタンを 3 回繰り返しクリックしても失敗した場合は、罰として 15 分かかります。
- **Punishment List** : 罰せられるクライアントは、ここに記載されています。管理者は、Punishment List の制限を解除することができます。

4) On-Demand Accounts

On-Demand Account Creation

Plan	Account Type	Quota	Price	Group	Function	
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	1	Create Single	Create Batch
2	Hotel Cut-off-time	Valid until 5:01 the following day	1	1	Create Single	Create Batch
3	N/A				Create Single	Create Batch
4	N/A				Create Single	Create Batch
5	N/A				Create Single	Create Batch

- **アカウント作成**：管理者は、単一のアカウントを作成し、または「Batch Create」機能を使用して複数のアカウントを作成することもできます。アカウントを作成する前に、少なくとも1つの請求プランを設定して有効にする必要があります。アカウントは、ランダムなユーザー名とパスワードで作成することも、手動で作成することもできます（最大8文字）。ユーザー名およびパスワードは、一括作成用に手動で作成することもできます。（例：接頭辞=ABC、接尾辞=DEF、シリアル番号0001。）

On-Demand Account List

<input type="checkbox"/>	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
<input type="checkbox"/>	28v2	Until 2013/02/07-02:00	Expired	Group 1	roomN-3154-00:09:68:CD:82:47		
<input type="checkbox"/>	e69w	Until 2013/02/19-01:00	Expired	Group 1			
<input type="checkbox"/>	9u2u	Until 2013/02/19-03:03	Expired	Group 1			
<input type="checkbox"/>	ep4r	Until 2013/02/19-05:01	Expired	Group 1			

(Total:4/9000) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page 1 (Page:1/1) Row per Page: 10

- **Account List**：作成されたすべてのオンデマンドアカウントと関連情報は、このページに一覧表示されます。このリストでは、管理者は、アカウントの復元/削除や管理者の引き換えなど、オンデマンドアカウントを操作することもできます。

5) Schedule

管理者は、有効なサービスゾーンのユーザーグループに適用する別のログイン時間権限を設定できます。構成済みのスケジュールプロファイルを適用するには、Groups Configurationに進みます。

Schedule Permitted Login Hours - Profile 1

Select Schedule

Schedule Name

	Time	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<input type="checkbox"/>	SUN	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	MON	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	TUE	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	WED	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	THU	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	FRI	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	SAT	<input checked="" type="checkbox"/>																							

Log off authenticated users during unauthorized periods

6) Policies

グローバルポリシーは、**Firewall Profile**、**Specific Route Profile**、**Schedule Profile**、**Maximum Concurrent Sessions** 管理など、システムのユニバーサルポリシーであり、ユーザーが規制されて別のポリシーに適用されない限り、すべてのユーザーに適用されます。

Main > Users > Policies > Policy Configuration

A Policy is used to define a Group's authorization in a Service Zone.
The Global Policy is the general policy defined for all Groups when the Group Policy is not defined.

Select Policy

Policy Configuration

Firewall Profile	<input type="button" value="Configure"/>
Privilege Profile	<input type="button" value="Configure"/>
Specific Route Profile	<input type="button" value="Configure"/>
Specific IPv6 Route Profile	<input type="button" value="Configure"/>
IPv4 DSCP and 802.1p Mapping	<input type="button" value="Configure"/>
IPv6 Traffic Class and 802.1p Mapping	<input type="button" value="Configure"/>

各ポリシーは、**Firewall Profile**、**Specific Route Profile**、**Schedule Profile**、および **Maximum Concurrent Sessions** 管理で構成されます。ポリシーは、Policy タブで定義できます。管理者は、1つの定義済みのポリシーを選択して、特定のサービスゾーン内のグループに適用できます。異なるサービスゾーン内のユーザーのグループは、異なるポリシーを適用できます。例えば、営業部の地域や財務部の地域からアクセスしている間に、異なるネットワークアクセス権で営業を適用することができます。

- **Select Policy** : 使用可能な異なるポリシープロファイルの数は、モデルタイプによって異なります。
- **Firewall Profile** : ファイアウォールプロファイルは、このポリシーによって管理されるユーザーに適用されるプロトコルとルールを指定します。各ポリシープロファイルには、独自のパス

タマイズ可能なファイアウォールプロファイルがあります。

- **Service Protocol** : このリンクをクリックすると、ポリシーの Service List ページが表示され、管理者はプロトコル (TCP/UDP/ICMP/IP) によってサービスのリストを定義できます。ここで定義されたサービス名は、ファイアウォールルールを設定するための選択肢リストを形成します。
- **User Firewall Rules** : このリンクをクリックすると、ポリシーの Firewall Rules ページが表示されます。ルール No.1 が最も高い優先度を持ち、ルール No.2 は 2 番目の優先度を持ち、以降も順次となります。各ファイアウォールルールは、送信元、送信先、ポリシーのサービスリストからのサービス、およびパス/ブロックアクションによって定義されます。必要に応じて、ファイアウォールルールのスケジュールを設定して、ファイアウォールルールの施行時期を指定できます。このスケジュールは Always (常に)、Recurring (繰り返し)、または One Time (1 回) に設定できます。
- **DoS Protection (グローバルプロファイルのみ)** : DoS 攻撃に対する保護のオプションを設定します。
- **Privilege Profile** : ユーザー生成セッション数の制限は、ここで設定できます。ネットワークの使用状況に基づいて、この属性を慎重に調整してください
 - **Password Change (非グローバルプロファイルのみ)** : 「Allow」に設定すると、権限プロファイルを適用したユーザーがログインパスワードを柔軟に変更できます。
 - **Maximum Concurrent Sessions** : この権限プロファイルを持つユーザーがセッション制限に達すると、このユーザーは新しい接続から一定の期間中断されます。
 - **Disable timeout for this group (非グローバルプロファイルのみ)** : 「Enable」に設定すると、このポリシーによって適用されたクライアントが自動的にログアウトされないようにすることができます。このオプションを有効にすると、システムのロードが増加する可能性があることに注意してください。
- **QoS Profile (非グローバルポリシーのみ)** : トラフィックの設定を編集できます。帯域幅調整が必要な場合、管理者はチェックボックスにチェックを入れて、クライアントが認証を完了した特定の期間後に 2 番目の QoS を選択できます。
 - **Traffic Class** : 各ポリシーには独自のトラフィッククラスを設定でき、同じトラフィックプロファイル内の IPv4 と IPv6 に対して異なるトラフィッククラスリマーケティングを設定できます。
 - **Group Total Downlink** : このグループ内のクライアントが共有できる最大帯域幅を定義します。
 - **Group Total Uplink** : このグループ内のクライアントが共有できる最大帯域幅を定義します。
 - **Individual Maximum Downlink** : このグループ内の個々のクライアントに対して許可される最大帯域幅を定義します。Individual Maximum Downlink は Group Total Downlink の値を超えることはできません。
 - **Individual Maximum Uplink** : このグループ内の個々のクライアントに対して許可される最大帯域幅を定義します。Individual Maximum Uplink は Group Total Uplink の値を超えることはできません。
 - **Individual Request Downlink** : このグループ内の個々のクライアントに対して許可される保証された最小帯域幅を定義します。Individual Request Downlink は、Group Total Downlink と Individual Maximum Downlink の値を超えることはできません。
 - **Individual Request Uplink** : このグループ内の個々のクライアントに対して許可される保証された最小帯域幅を定義します。Individual Request Uplink は、Group Total Uplink および Individual Maximum Uplink の値を超えることはできません。
- **Specific Route Profile** : このポリシーでユーザーに適用するルーティングルールをここで設定できます。
- **Specific IPv6 Route Profile** : このポリシーでユーザーに適用するルーティングルールをここで設定できます。
- **IPv4 DSCP and 802.1p Mapping (グローバルポリシーのみ)** : この基準は、IPv4 DSCP タグから、管理された VLAN ネットワークで送信するために必要な 802.1p トラフィッククラスへのスタティックマッピング設定を可能にします。
- **IPv6 Traffic Class and 802.1p Mapping (グローバルポリシーのみ)** : この基準は、IPv6 トラフィックタグから、管理された VLAN ネットワークで送信するために必要な 802.1p トラフィッククラスへのスタティックマッピング設定を可能にします。

ポリシー1~x（モデル依存）は、異なるサービスゾーン内の特定のユーザーグループに適用できます。ポリシー1の優先順位が最も高く、優先度の高いポリシーが最初に適用されるポリシーとなります。

Select Policy Policy 1 ▼

Policy Configuration

Policy Name	Policy 1
Firewall Profile	Firewall 1 ▼
Privilege Profile	Privilege 1 ▼
QoS Profile	QoS 1 ▼ <input type="checkbox"/> Enable Bandwidth Throttling in 5 min(s) and change the profile to QoS 1 ▼
Specific Route Profile	Specific Route 1 ▼
Prefer DHCP Pool	None ▼

優先 DHCP プール（サービスゾーン DHCP 構成で定義）もここで選択できます。

7) Blacklists

ブラックリストプロファイルを定義できます。また、これらのブラックリストプロファイルのいずれかを使用して、アクティブ認証オプションを設定できます。ブラックリストに登録されているユーザーアカウントは、システムにログインできません。クライアントのアクセスは拒否されます。管理者は、ドロップダウンメニューからブラックリストを1つ選択すると、このブラックリストがこの特定の認証オプションに適用されます。ブラックリストの名前は、大文字と小文字を区別しないように設定できます。

Select Blacklist 1: Blacklist1 ▼

Blacklist Settings

Blacklist Name	Blacklist1
Case Insensitive with blacklist	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="button" value="Apply"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/>	

	User Name	Remark
--	-----------	--------

(Total:0/40) Go to Page (Page:1/1) Row per Page:

8) Privilege Lists

権限機能は、IP アドレス、MAC アドレス、IPv6 アドレスに基づく 3 種類の権限リストをサポートしています。リストに指定されているデバイスは、ネットワークにアクセスするための認証を必要としません。ユーザーグループは、IP Privilege List のデバイスに割り当てることができますが、MAC Privilege List には割り当てられません。

SYSTEM **USERS** ACCESS POINTS NETWORK UTILITIES STATUS

Main > Users > Privilege List > IP Address

IP Privilege List

Add... Delete Backup List Restore List Search IP

No.	IP Address	MAC Address	Group	Remark
(Total:0/200) **First ← Prev Next → Last** Go To Page <input type="text"/> (Page:1/1) Row per Page: 10				

[IP Privilege List](#)
[IPv6 Privilege List](#)
[MAC Privilege List](#)
[Additional Controls](#)

- **Privilege List** : 認証フリーリストには、管理者が認証を必要とせずに個人の特権的なアクセスを指定できる 3 つのタイプがあります。これは、IP アドレス、IPv6 アドレスまたは MAC アドレスのいずれかを介して達成することができます。

9) Additional Control

このセクションは、その他の設定に関するものです。User Session Control、Built-in RADIUS Server Settings、Customization、Remaining Time Reminder、MAC ACL が含まれます。管理者は、User Session Control でアイドルタイムアウトなどのユーザーセッションを制御できます。Built-in RADIUS Server Settings には、セッションタイムアウトなどの 3 つの機能があります。Customization では、管理者は証明書をシステムにアップロードできます。Remaining Time Reminder は、画面上のクライアントに残り時間情報を提供します。管理者は、MAC ACL (Access Control List) 内のクライアントの MAC アドレスを使用して、システムに対するアクセス制御を管理できます。

User Session Control

Idle Timeout	<input type="text" value="10"/> minute(s) *(1-5040)
Detection Interval	<input type="text" value="60"/> second(s) *(1-600)
Traffic Direction for Idle Timeout	<input type="text" value="Uplink & Downlink"/>
Timeout Threshold	<input type="text" value="0"/> byte(s) *(0-1048576, 0 is Disabled)
User Options	<input type="checkbox"/> Charge Traffic to/from Hosts in Walled Garden List
	<input type="checkbox"/> Kick user when user's IP change
	<input type="checkbox"/> Log NAT Mapped in User Session Log

Built-in RADIUS Server Settings

Session Timeout	<input type="text" value="120"/> minute(s) *(5-43200)
Idle Timeout	<input type="text" value="10"/> minute(s) *(1-5040)
Interim Update	<input type="text" value="5"/> minute(s) *(1-120)
Certificate	<input type="text" value="Default CERT"/>

Remaining Quota Reminder

Time and Cut-off Reminder	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Volume Reminder	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Reminder Refresh Time	<input checked="" type="radio"/> 10mins <input type="radio"/> 15mins <input type="radio"/> 20mins

MAC Access Control List

MAC Access Control List	<input type="button" value="Configure"/>
-------------------------	--

MAC Access Control is used to grant or deny permission to access the User Login Page.

User Session Control

- **Idle Timeout** : アクティビティなしのタイムベースをアイドルタイムアウトとみなすように設定します。
- **Idle Detect Interval** : アイドル条件に達するかどうかをチェックする時間間隔です。上記で設定したアイドル時間を超えるアイドル間隔が連続して累積されると、ユーザーがログアウトするアイドルタイムアウトアクションが発生します。
- **Traffic Direction for Idle Timeout** : ユーザーのアクティビティ検査は、アップリンクトラフィックのみまたは両方向によってチェックされます。
- **Threshold for Idle Traffic Detection** : 設定された値よりも小さいトラフィックフローがアイドルと見なされるしきい値を指定します。
- **Charge Traffic to/from Host in Walled Garden List** : オンデマンドユーザーデータベースの使用時間またはボリュームタイプのアカウントの場合、管理者は、ウォールド・ガーデンまたはウォールド・ガーデンの広告リストに記載されているウェブサイトへの訪問を請求するか、請求しないかを選択することができます。
- **Kick out user when user's IP change** : ユーザーが IP アドレスを変更したときに、システムによって強制的に切断されるかどうかを管理者が設定するオプションです。
- **Log NAT Mapped in User Session Log** : プライベート IP/ポートからパブリック IP/ポートへの各接続のマッピングを表示するには、このオプションを有効にする必要があります。

Built in RADIUS Server Settings

- **Session Timeout** : 組み込み RADIUS サーバー経由で認証されたユーザーによって生成されたセッションの場合（アカウントローミングユーザーである可能性がある）、タイムアウト範囲はここで手動で設定できます。この属性は慎重に設定してください。
- **Idle Timeout** : 組み込み RADIUS サーバー経由で認証されたユーザー（アカウントローミングユーザーなど）の場合、アイドルタイムアウト範囲はここで手動で設定できます。この属性は慎重に設定してください。
- **Interim Update** : 組み込み RADIUS サーバー経由で認証されたユーザー（アカウントローミングユーザーなど）の場合、アカウント間隔はここで手動で設定できます。この属性は慎重に設定してください。
- **Certificate** : 組み込み RADIUS サーバーの証明書が選択可能になります。

Remaining Quota Reminder

- **Time and Cut-off reminder** : このオプションは、時間ベースのアカウントクォータがなくなりそうになったことをオンデマンドユーザーに警告メッセージを表示するオプションです。
- **Volume Reminder** : このオプションは、ボリュームベースのアカウントクォータがなくなりそうになったことをオンデマンドユーザーに警告メッセージを表示するオプションです。
- **Reminder Refresh Time** : 残りのクォータ付きログイン成功ページは、10/15/20 分ごとに更新され、更新された残りのクォータが表示されるように設定できます。

MAC Access Control List

- **MAC ACL** : 管理者は、MAC 許可リストまたは拒否リストのいずれかの MAC アドレスに対して制限対策を構成できます。

C.Devices

Devices : このセクションは、AP とスイッチの管理に使用します。AP とスイッチのさまざまな属性を示すだけでなく、さまざまな設定のために提供されるさまざまな機能があります。



1) Local Area AP Management

a) 概要

各 AP タイプの基本情報をリストする概要です。AP 数、オンライン数、オフライン数、および各 AP タイプの関連クライアントの合計数が含まれます。

この表には、システムの管理下でサポートされているすべての AP が表示され、AP タイプ別に一覧表示されます。

AP Type List

AP Type	No. of AP	Online	Offline	No. of Client
ECW100	0	0	0	0
ECW5210-L	0	0	0	0
ECW5211-L	0	0	0	0
ECW5410-L	0	0	0	0
ECW05210-L	0	0	0	0
ECW05211-L	0	0	0	0
ECW05213-L	0	0	0	0
Others	0	0	0	0

チェックボックスにチェックを入れて任意の AP を選択し、必要に応じて下のボタンをクリックして、選択した AP に **Reboot**、**Enable**、**Disable**、**Delete**、**Apply Template**、**Apply Service Zone** (タグベース) を適用します。

b) List

タイプ、名前、IP アドレス、MAC アドレス、オンラインステータスなど、各管理対象 AP の情報を表示するリストです。このセクションの機能には、再起動、有効化、無効化、削除、新しいテンプレートの適用、サービスゾーンによる適用およびその他の設定などの操作も含まれます。

システム管理下のサポート対象の AP がすべてリストに表示されます。管理者は、**Discovery** タブまたは **Adding** タブからサポートされている AP を追加できます。AP が追加されると、このリストには、AP タイプ、AP 名、IP アドレス、MAC アドレス、サービスゾーン、ステータスなど、現在管理されている AP が表示されます。管理者は、個々の AP の前にあるチェックボックスにチェックを入れるか、上部のチェックボックスにチェックを入れてすべての AP をまとめて選択することで、再起動、有効化、無効化、削除、テンプレートの適用、またはサービスゾーンによる適用を実行できます。

AP List

AP Type All
 ECW100 ECW5210-L ECW5211-L ECW5410-L ECW05210-L ECW05211-L
 ECW05213-L Others Apply

Add Reboot Enable Disable Delete Refresh Interval Disable Auto Refresh Refresh

Apply Template Reset To Default Apply By Service Zone AP Name Search (Total: 0)

<input type="checkbox"/>	AP Name	Client	IP Address	Service Zone / VLAN ID / SSID	Status	MAC Address	Channel
--------------------------	---------	--------	------------	-------------------------------	--------	-------------	---------

リストのチェックボックスにチェックを入れて任意の AP を選択し、必要に応じてボタンをクリックして、選択した AP に **Reboot**、**Enable**、**Disable**、**Delete**、**Apply Template**、**Reset to Default**、**Apply Service Zone**、**Add to Floor Plan** を適用します。

c) Adding

追加機能を使用して、AP に必要な情報を入力して AP を手動で設定します。システムには、AP の設定を簡素化するために使用できるテンプレートが用意されています。

管理者は、「Add」をクリックして「Add AP」を選択すると、サポートされている AP を **List** 表に手動で追加できます。システムは、指定された値を使用して AP を設定します。処理後、AP リストに AP のステータスが「オンライン」または「オフライン」と表示されます。

Add Method Add AP

Add An AP

AP Type ECW100

AP Name

Admin Password

IP Address

MAC Address

Apply AP Template TEMPLATE1

Channel RF Card A Default RF Card B Default

- **AP Type** : リストに追加する AP のモデルタイプです。
- **AP Name** : 特定の AP のニックネームです。
- **Admin Password** : この AP に必要なパスワードです。
- **IP Address** : 指定された AP の IP アドレスです。
- **MAC Address** : 特定の AP の MAC アドレスです。

- **Apply AP Template** : 追加した AP に適用する AP テンプレートを選択します。
- **Channel** : 選択したチャンネルは、追加された AP に適用されます。

d) Discovery

この検出機能は、LAN ポートに接続されたときに、サポートされているタイプの AP を手動でまたは自動的に検出し、検出された各 AP に固有の IP アドレスを自動的に割り当てます。AP List から「Add」をクリックし、「Find Multiple APs」を選択してください。

Background AP Discovery 機能を有効にすると、システムは 10 分に 1 回、または管理者が設定した時間に従ってスキャンします。AP が検出され、**Auto Adding AP to the List** が有効になっている場合は、チェックされたサービスゾーンプロファイルで設定された開始 IP アドレスから使用可能な IP アドレスが割り当てられ、選択したテンプレートに適用されます。AP が使用するチャンネルを設定することもできます。

Add Method Find Multiple APs ▼

Find Multiple APs

AP Type ECW100 ▼

Service Zone Default ▼

VLAN for management 0 ▼

Admin Settings Used to Discover

Factory Default

IP Address: 192.168.1.10

Login ID: admin

Password: admin

Manual

Scan Now

Background AP Discovery

Status Disabled Configure

Discovery Results

Add

AP Type	IP Address	MAC Address	AP Name	Password	Template	Channel
---------	------------	-------------	---------	----------	----------	---------

(Total: 0/20) First Prev Next Last Go to Page (Page: 1/1) Row per Page: 10 ▼

- **AP Type** : 検索するシステムの AP モデル名を選択します。
- **Service Zone** : 接続されているデバイスの AP を管理するサービスゾーンを選択します。
- **VLAN for management** : 検出された AP の管理用の VLAN を設定します。
- **Admin Settings Used to Discover** : 接続されている AP のインターフェースと管理資格情報が変更されていない場合は、factory default を選択します。それ以外の場合は、manual を選択し、それに応じて IP 範囲と管理設定を指定します。管理者は、検出プロセス中いつでもコントローラのスキャンを停止できます。
- **Background AP Discovery** : 設定されると、システムは新しく接続された AP デバイスの設定済みの IP 範囲を定期的にスキャンし、検出結果を自動的に表示します。

- **Discovery Results** : 上記で設定した検出基準に一致する検出された AP デバイスを表示します。

e) Templates

AP 設定テンプレートを定義できます。最大 8 つのテンプレートを編集・保存し、「Adding」および「Discovery」セクションで使用できます。

AP モデル別のテンプレート

システムは、AP の設定を含む最大 8 つのテンプレートをサポートします。管理者は、設定を 1 つずつ設定するように AP 管理インターフェースをログに記録する代わりに、テンプレートで設定を一緒に設定できます。**AP type** を選択し、**編集**アイコンをクリックして **Template Editing** ページに入ります。

AP Template

AP Model
ECW100

Template Name	Copy Settings from	Remark	Action
<input type="text" value="TEMPLATE1"/>	<input type="text" value="NONE"/>	<input type="text" value="Template 1"/>	 

- **Template Editing** : 管理者は、テンプレート設定を手動で設定することも、**Copy Settings From** オプションを使用して、特定の既存の管理対象 AP から設定をコピーすることもできます。詳細設定を表示するには、**Configure** ボタンをクリックします。
 - ◆ **Name** : この特定のテンプレートに表示される名前です。
 - ◆ **Copy Settings From** : 事前設定された既存の AP を選択し、**Apply** をクリックして、その設定をテンプレート設定として保存します。
 - ◆ **Remark** : このテンプレートプロファイルの備考または追加情報です。
 - ◆ **Action** : 鉛筆アイコンで描かれた編集をクリックして設定を入力するか、赤い十字をクリックしてテンプレートを削除します

General

Subnet Mask	<input type="text" value="255.255.0.0"/>	*
Default Gateway	<input type="text" value="192.168.1.254"/>	*
Primary DNS	<input type="text" value="192.168.1.254"/>	*
Secondary DNS	<input type="text"/>	
NTP	Time Zone (GMT 00:00)Greenwich Mean Time:Dublin,Lisbon,London ▼	
	NTP Server 1: <input type="text" value="192.168.1.254"/>	*
	NTP Server 2: <input type="text" value="time.nist.gov"/>	
SNMP	<input type="text" value="Disabled"/>	
SYSLOG	<input type="text" value="Enabled"/>	
	SYSLOG Server IP Address: <input type="text" value="127.0.0.1"/>	*
	SYSLOG Server Port: <input type="text" value="514"/>	*
	Log Level: <input type="text" value="Debug"/>	
Port Configuration	LAN 1 <input type="text" value="Disabled"/>	
	VLAN ID <input type="text"/>	*(1 - 4094)

The 802.1p and Uplink Bandwidth settings are shared by all interfaces (LAN Ports / VAPs) that with same VLAN ID.

- **General** : このセクションでは、必要に応じて、ここで **Subnet Mask** と **Default Gateway** を修正します。**NTP Servers** と **Time Zone** を設定します。さらに、管理者は、**SYSLOG** サーバーを有効にして、AP からログを受信し、**SNMP** の読み取り/書き込み機能を有効にすることができます。また、**Port Configure** により、管理者は各 LAN ポートに VLAN タグを設定できます。

Wireless

RF Card A ▼

Band	802.11g+802.11n ▼	
Channel	Auto ▼	
Short Guard Interval	Enabled ▼	
Channel Width	20 MHz ▼	
Antenna mode	1T1R ▼	
Short Preamble	Enabled ▼	
Transmit Power	Level 1 ▼	
Beacon Interval (ms)	100	*(Default: 100; Range: 100 ~ 500)
ACK Timeout	0	*(Default: 0; Range: 0 ~ 255, 0:Auto, Unit:4 micro seconds)
Airtime Fairness	Disabled ▼	
Packet Delay Threshold	0	*(100 - 5000ms, 0:Disable)
Idle Timeout	300	*(60 - 60000)
Band Steering	Disabled ▼	
	<input type="checkbox"/> Aggressive	
Interference Detection	Utilization Threshold 0	*(60 - 99, 0:Disable)
Transmission Rate Threshold	1001 kbps	*(0:Disable)
UAPSD	Enabled ▼	
WME Configuration	AP ▼	

Access Category	Voice	Video	Background	Best Effort
CW Min	2	3	4	4
CW Max	3	4	10	6
AIFS	1	1	7	5
TXOP Limit	1504	3008	0	8192

VAP Configuration

Status	Profile Name	VLAN ID	Service Zone	SSID	WLAN Encryption	Action
	VAP-1	0	Default	Guest Network	None	

Add VAP

➤ Wireless :

- **SSID Broadcast** : AP の SSID がネットワークでブロードキャストできるようにするには、このオプションを選択します。プライベート使用を目的とした認証を無効にしたネットワークがある場合は、SSID ブロードキャスト機能を無効にすることをお勧めします。
- **Band** : 編集する AP モデルテンプレートに応じて、**802.11a**、**802.11b**、**802.11g**、**802.11a+802.11n**、**802.11b+802.11g**、**802.11g+802.11n**、**802.11ac** の各モードを選択できます。
- **Channel Width (802.11g+n, 802.11a+n, 802.11ac のみ)** : 20MHz、40MHz、または Auto のいずれかを選択します。スループットを向上させるために、チャンネル帯域幅を 40MHz に倍増することがサポートされています。80MHz は、802.11ac モードでの選択が可能です。
- **Antenna Mode (802.11g+n, 802.11a+n, 802.11ac のみ)** : MIMO で使用するストリーム番号を選

扱します。使用可能な最大ストリーム数は、モデルによって異なります。

- **Transmit Power** : 一部の AP モデルでは、システムから送信される信号強度をレベルで選択できます。各レベルは、最高電力から 1dBm の減少を示します。**Level 1** は実際の最高電力であり、**Level 2** は最高電力から 1dBm を引いた値です。
- **Beacon Interval (ms)** : 20~1000 ミリ秒の値を入力します。デフォルト値は 100 ミリ秒です。入力された時間は、アクセスポイントとワイヤレスネットワークとの間でビーコン信号が送信される頻度を意味します。
- **ACK Timeout** : 「確認応答 (ACK) フレーム」の待ち時間間隔です。ACK が間隔内に受信されない場合、パケットは再送信されます。ACK タイムアウト間隔を長くすると、パケット損失は減少しますが、スループットは低下/悪化します。
- **Airtime Fairness** : 「Fair Access」に設定すると、異なるバンドの互換性を持つすべてのデバイスのエアタイムが同じになります。「Preferred Access」に設定すると、N 個のクライアントが優先されます。この機能は、異なるバンドをサポートするデバイスを持つネットワークに最適です。
- **Packet Delay Threshold (ms)** : これは Tx キューフラッシングメカニズムで、キューが x ミリ秒以上処理されている場合にパケットをドロップし、すぐに他のキューを処理することを目的としています。これはデフォルトで無効になっています (=0)。
- **Idle Timeout (s)** : クライアントは、非アクティブ状態が設定された時間 (デフォルトは 300 秒) に達すると切断します。
- **Band Steering** : 有効にすると、5GHz 接続を持つクライアントは、2.4GHz 帯域の輻輳を軽減するために、5GHz 帯域に誘導されます。これは、2 つの RF カードで AP が 2.4GHz および 5GHz に設定されている場合にのみ適用されます。「Aggressive」にチェックを入れると、5GHz 接続を持つクライアントは、5GHz 帯に接続する必要があります。
- **Interference Detection** : 現在のチャンネルの使用率が設定されたしきい値 (%) に達すると、AP は別のチャンネルに切り替わります。
- **Transmission Rate Threshold** : 送信レートが設定されたしきい値よりも低い場合、関連付けられたクライアントはキックされます。これにより、関連付けられているすべてのクライアントに対して高い接続速度が保証されます。
- **UAPSD** : USPAD サポートを有効/無効にします。
- **WME Configuration** : アクセス優先度は、異なるパラメータを使用して設定することができます。AP 側のパラメータとクライアント側のパラメータをそれぞれ設定できます。CW Min : 競合ウィンドウの最小値、CW Max : 競合ウィンドウの最大値、AIFS : フレーム送信間隔、TXOP Limit : 送信機会の制限。
- **VAP Configuration** : 「Status」列の下の VAP を有効/無効にします。VAP の設定は、「Action」の下の編集アイコンをクリックすることによって行うことができます。

VAP Edit - ECW5211-L: TEMPLATE1

Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	<input type="text" value="VAP-1"/> *
Service Zone	<input type="text" value="Default"/> ▼
VLAN ID	<input type="text" value="0"/> ▼
SSID	<input type="text" value="Guest Network"/> *
RTS Threshold	<input type="text" value="2346"/> *(Default: 2346 ; Range: 1 ~ 2346)
DTIM Period	<input type="text" value="1"/> *(Default: 1; Range: 1 ~ 15)
Consecutive Dropped Packets	<input type="text" value="0"/> *(2 - 50, 0:Disable)
Broadcast SSID	<input type="text" value="Enable"/> ▼
Wireless Station Isolation	<input type="text" value="Enable"/> ▼
IAPP	<input type="text" value="Enable"/> ▼
Multicast-to-Unicast Conversion	<input type="text" value="Disable"/> ▼
TX STBC	<input type="text" value="Enable"/> ▼
Multicast/Broadcast Rate	<input type="text" value="5.5M"/> ▼
Management Frame Rate	<input type="text" value="5.5M"/> ▼
Receiving RSSI Threshold	<input type="text" value="-85"/> *(-95 ~ 0 dbm, 0:Disable)
Service Schedule	<input type="text" value="24/7 Service"/> ▼
Security ▼	
Authentication	<input type="text" value="Open System"/> ▼
Encryption	<input type="text" value="None"/> ▼
Access Control ▼	
Maximum Number of Clients	<input type="text" value="128"/> *(Limit per RF Card)
Access Control Type	<input type="text" value="Disable Access Control"/> ▼
Hotspot 2.0 ▶	

- **Status** : VAP はここで有効または無効にできます
- **Profile Name** : ID/管理目的で使用される特定の RF カードとその VAP のプロフィール名です。
- **Service Zone** : ドロップダウンリストから VAP のマッピングサービスゾーンを選択します。
- **VLAN ID** : この VAP の VLAN ID を選択します
- **SSID** : SSID は、クライアントが特定の VAP に関連付ける識別子として機能します。さまざまなワイヤレスセキュリティタイプのように、さまざまなサービスレベルと組み合わせることができます。
- **RTS Threshold** : 1 から 2346 までの値を入力します。RTS (送信要求) Threshold は、隠しノードの問題を防ぐために、フラグメントを送信する前にシステムが送信要求 (RTS) を発行するパケットサイズを決定します。データサイズが指定された値を超えると、RTS メカニズムが作動します。RTS Threshold を低く設定すると、多くのクライアントデバイスが AP と関連付けられているエリア

や、クライアントが遠く離れており AP だけを検出できてお互いに検出できないエリアで役立ちます。

- **DTIM Period** : 指定した周波数で周期ビーコン内に生成する DTIM 間隔を入力します。DTIM を高くすると、無線クライアントはより多くのエネルギーを節約できますが、スループットは低下します。
- **Consecutive Retries Threshold** : これは、クライアントが送信範囲外であると判断する前にパケット送信が失敗した場合に、AP が試行する最大送信リトライ回数です。設定された回数だけ送信の再試行が失敗すると、アクセスポイントはクライアントをキックして、接続されている他のクライアントのパフォーマンスを最適化します。
- **SSID Broadcast** : この機能を無効にすると、システムの SSID がブロードキャストされなくなります。SSID のブロードキャストが無効になっている場合は、正しい SSID を持つデバイスだけがシステムに接続できます。
- **Wireless Client Isolation** : この機能を有効にすると、システムに関連するすべてのステーションがアイソレーションされ、システムとしか通信できません。
- **IAPP** : IAPP (AP 間通信プロトコル) は、アクセスポイントが接続されているステーションに関する情報を共有するプロトコルです。この機能を有効にすると、システムは関連する無線ステーションの情報をピアアクセスポイントに自動的にブロードキャストします。これにより、同じ無線 LAN 内の IAPP 対応アクセスポイント間でワイヤレスステーションがスムーズにローミングできるようになります。
- **Multicast-to-Unicast Conversion** : Multicast-to-Unicast Conversion が有効な場合、マルチキャストパケットはアクセスポイントのネットワークインターフェースと IP マルチキャストホストを介して転送されます。登録情報が記録され、マルチキャストグループに分類されます。その後、内部スイッチは、マルチキャストトラフィックを要求するポートだけにトラフィックをインテリジェントに転送できます。逆に、Multicast-to-Unicast Conversion を行わないと、マルチキャストトラフィックはブロードキャストトラフィックのように扱われ、パケットがすべてのポートに転送され、ネットワークの非効率性が生じます。
- **Multicast/Broadcast Rate** : マルチキャスト/ブロードキャストパケットの帯域幅設定です。ワイヤレスクライアントがマルチキャスト/ブロードキャストパケットを送信するために帯域幅を大きくまたは小さくする必要がある場合は、管理者がアクセスポイントのマルチキャスト/ブロードキャスト帯域幅をここでカスタマイズできます。
- **Management Frame Rate** : この機能は、管理フレームの帯域幅を制御します。レートが高いほど、トランスミッションがカバーする範囲が短くなります。
- **Receiving RSSI Threshold** : 接続速度が高いステーションを維持するために、受信感度がしきい値よりも低い場合、ステーションはキックアウトされます。
- **Security** : アクセスポイントは、各 VAP プロファイルでさまざまなワイヤレス認証およびデータ暗号化方式をサポートしています。これにより、管理者はクライアントに異なるサービスレベルを提供できます。セキュリティタイプには、Open、WEP、802.1X、WPA-Personal、および WPA-Enterprise があります。
- **Access Control** : 管理者は、MAC アドレスに基づいてクライアントデバイスのワイヤレスアクセス

を制限できます。

- **Disable Access Control** : Disable を選択すると、クライアントデバイスがシステムにアクセスするための制限はありません。
- **MAC ACL Allow List** : MAC ACL Allow List を選択すると、Allow List (「許可された MAC アドレス」) にリストされているクライアントデバイス (MAC アドレスで識別される) のみが、システムへのアクセスを許可されます。管理者は、リストされた MAC を再度有効にするまで、Disable をオンにすることで、許可された MAC アドレスを一時的にブロックできます。
- **MAC ACL Deny List** : MAC ACL Deny List を選択すると、Deny List (「拒否された MAC アドレス」) にリストされているものを除き、すべてのクライアントデバイスがシステムへのアクセスを許可されます。管理者は、Disable をオンにすることで、拒否された MAC アドレスが一時的にシステムに接続することを許可できます。
- **RADIUS ACL** : クライアントが AP に関連付けようとする、AP はクライアントの MAC アドレスを指定した RADIUS 要求を、設定された RADIUS サーバーに送信します。RADIUS サーバーによって受け入れられた MAC アドレスだけが AP にアソシエートできます。ここでの RADIUS サーバー設定は、同じ VAP の WPA エンタープライズおよび 802.1X 設定と共有されることに注意してください。また、この機能はレガシー WiFi 5 AP でのみサポートされていることに注意してください。
- **Hotspot 2.0** : ホットスポット 2.0 は、公共の WiFi 加入者により良い帯域幅とサービスを提供するために WiFi Alliance によって開始された WiFi 認定パスポイントとして知られています。ホットスポット 2.0 機能は、サービスプロバイダとそのパートナー専用に設計されています。設定を完了するには、サービスプロバイダまたはサービスチームにご相談ください。

RF カード B のワイヤレス設定は、デュアル無線アクセスポイントで使用できます。一部の AP モデルでは、設定パラメータが異なる場合があります。

➤ **Layer 2 Firewall** :

Layer 2 Firewall

Enable Layer 2 Firewall

Enable Disable

Layer 2 Firewall List

No.	State	Action	Name	EtherType	Remark	Edit
1	<input checked="" type="checkbox"/>	ACCEPT	ARP	ARP	To RF Card A	Edit
2	<input type="checkbox"/>	DROP	BOOTPC	IPv4	To RF Card A	Edit
3	<input checked="" type="checkbox"/>	ACCEPT	BOOTPS	IPv4	To RF Card A	Edit
4	<input type="checkbox"/>	DROP	Broadcast	ALL	To RF Card A	Edit
5	<input type="checkbox"/>	DROP	IAPP	IPv4	To RF Card A	Edit
6	<input type="checkbox"/>	ACCEPT	IPv4 Multicast	IPv4	To RF Card A	Edit
7	<input type="checkbox"/>	ACCEPT	IPv6 Multicast	ALL	To RF Card A	Edit
8	<input checked="" type="checkbox"/>	DROP	All Multicast	ALL	To RF Card A	Edit
9	<input type="checkbox"/>					Edit
10	<input type="checkbox"/>					Edit

(Total: 50) [First](#) [Prev](#) [Next](#) [Last](#) Go to Page (Page:1/5)

Layer 2 Firewall Edit - ECW5211-L: TEMPLATE1

State Enable Disable

Rule ID 1

Rule name *

EtherType

Interface From To

Opcode

Source MAC Address: Mask:

Source ARP IP: Mask:

Source ARP MAC: Mask:

Source MAC Address: Mask:

Destination ARP IP: Mask:

Destination ARP MAC: Mask:

Action Block Pass

Remark

- **State** : それぞれのルールを有効または無効にします
- **Rule** : この特定のルールの番号付けによって、表内の使用可能なファイアウォールルールの優先順位が決定されます。
- **Rule name** : ここでルール名を指定できます。
- **EtherType** : ドロップダウンリストには、このルールが適用される使用可能なタイプのトラフィックが表示されます。
- **Interface** : これは、目的のインターフェースで着信/発信方向を示します。
- **DSAP/SSAP** (EtherType が IEEE 802.3 の場合) : この値は、802.2 LLC フレームヘッダーのフィールドに対してさらに指定できます。

- **Type** (EtherType が IEEE 802.3 の場合) : このフィールドは、カプセル化されたトラフィックのタイプを示すために使用できます。
- **Source** : MAC アドレス/マスクは送信元 MAC を示します。(EtherType が IPv4 の場合) IP アドレス/マスクは送信元 IP アドレスを示します。ARP IP/MAC & MASK は ARP ペイロードフィールドを示します。
- **Destination** : MAC アドレス/マスクは宛先 MAC を示します。(EtherType が IPv4 の場合) IP アドレス/マスクは宛先 IP アドレスを示します。ARP IP/MAC & MASK は ARP ペイロードフィールドを示します。
- **Action** : ルールは **Block** または **Pass** として選択できます
- **Remark** : このルールの注意事項はここで指定できます。

f) Firmware

ファームウェア機能は、AP ファームウェアのバージョンを確認し、新しい AP ファームウェアをシステムにアップロードするためのツールを提供します。

システムは AP のファームウェア管理をサポートし、新しいファームウェアのアップロード、既存のファームウェアの削除、および管理対象 AP へのファームウェアのダウンロードを行います。AP のファームウェアバージョンは、統合されているバージョンである必要があります。

Firmware Upload には、AP のファームウェアの現在のバージョンが表示されます。新しいファームウェアをアップロードして、現在のファームウェアを更新できます。アップロードするには、まず **Add** をクリックし、**Browse** をクリックしてファイルを選択し、**Upload** をクリックします。

AP Firmware List

Add... Delete

<input type="checkbox"/>	Filename	AP Type	Version	Size	Checksum	Actions
<input type="checkbox"/>	Edgecore_ECW5211-L_3.43.00-EN-E_1.32-1.9276.rom	ECW5211-L	3.43.00	6304078	d12806c08a4417cbae8265aedeb10571	Download

- **AP Firmware List** : アップロードされたファームウェアがここに表示されます。
- **File Name** : アップロードされた AP ファームウェアの名前です。
- **AP Type** : ファームウェアの AP タイプです
- **Version** : ファームウェアのバージョンです
- **Size** : ファームウェアのファイルサイズです
- **Checksum** : 自動的に検出されたファームウェアのセキュリティ識別情報です。
- **Download** : 選択したファームウェアをローカルディスクに保存するには、**Download** をクリックします。
- **Delete** : 選択したファームウェアをシステムから削除するには、**Delete** をクリックします。

g) Upgrade

アップグレード機能を使用すると、管理者はシステムに保存されているファームウェアファイルを使用して AP ファームウェアをアップグレードできます。

管理者は、選択列の AP のチェックボックスにチェックを入れることで、選択した AP のファームウェアを個別に、または同時にアップグレードできます。アップグレード前のバージョンと次のバージョンの両方が、システムに統合されているバージョンである必要があります。

AP Model: ECW100

List

<input type="checkbox"/>	Name	Type	Version	Next Version	Last Upgraded
--------------------------	------	------	---------	--------------	---------------

(Total:0/20) First Prev Next Last Go to Page (Page:1/1) Row per Page: 10

Apply Cancel

h) WDS Management

WDS (Wireless Distribution System) とは、AP (アクセスポイント) を無線で接続するための機能です。システムの WDS 管理機能は、管理者が WDS ネットワークの「ツリー」構造を設定するのに役立ちます。

WDS Status

Refresh Interval

WDS Tree	Security	Channel	Edit
No current WDS connection.			

WDS Update

Add WDS Connection

New Parent AP

New Child AP

Security Type

Move WDS Connection

Update Parent AP

Update Child AP

Delete WDS Link

- **WDS Status** : Status には WDS ツリーに追加された AP を、Security と Channel の設定とともに表示します。WDS は、複数のツリーに対して設定できます。関連する WDS ツリーの **WDS 接続設定** を変更するには、**Edit** をクリックします。
- **WDS Update** : 次の操作を実行して、WDS 接続を更新します。
 - **Add** : WDS がない子 AP と、AP リストから親 AP を持つ新しい WDS 接続を追加します。選択した親 AP が現在の WDS ツリーのいずれにもない場合、新しい WDS ツリーが追加されます。新しく追加された WDS ツリーの **WDS 接続設定** を変更するには、**Edit** をクリックします。
 - **Move** : WDS からの子 AP と WDS で接続可能な親 AP を使用して WDS 接続を更新すると、以前の親 AP への子 AP の以前の WDS 接続が削除されます。
 - **Delete** : 子 AP への WDS 接続を含め、選択した AP のすべての WDS 接続が削除され、有線接続のない子 AP には到達できなくなります。

i) Rogue AP Detection

配置された環境で、管理されていない AP または悪意のある AP を検出するように設計されています。非管理対象 AP が管理対象 AP と同じ SSID を使用している場合でも、管理対象 AP をセンサーとして非管理対象 AP を検出します。AP の BSSID、ESSID、タイプ、チャンネル、暗号化、およびレポート時間が表示されます。

General Configuration

Rogue AP Detection Enable Disable

Scanning Interval minutes

Sensor List 0/1

Trusted APs 0/40

Rogue AP List

ESSID

<input type="checkbox"/>	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	Report Time
(Total:0) First Prev Next Last Go to Page <input type="text"/> (Page:1/1) Row per Page: <input type="text" value="10"/>							

- **General Config** : この設定項目には、このタブページ内の機能をオンにするためのスイッチが含まれています。例えば、**Rogue AP Detection** 機能と、オプションの「Channel Switching」機能があります。
- **Sensor List Config** : この設定項目には、ワイドエリア AP 管理で現在管理されているすべての AP のリストが含まれます。管理者は、不正 AP をスキャンするセンサーとして 1 つ以上の AP を選択できます。
- **Trusted AP Config** : この設定項目を使用すると、管理者は検出された不正 AP のリストを維持し、信頼できる AP としてマークできます。
- **Rogue AP List** : このウィンドウには、検出された不正 AP がすべてリストされます。不正 AP には、BSSID、チャンネル、暗号化、レポート時間などの関連情報が示されます。ウィンドウの下部にあるオプションボタンから、このリストで選択した不正 AP を信頼できるリストに追加したり、無視できる場合は削除したりできます。

▪ General Configuration

- **Scanning Interval** : このフィールドの単位は分です。「Rogue AP Detection」を無効にするには、0 を入力します。「Rogue AP Detection」を有効にするには、検出間隔として 1~999 の範囲の整数を入力してください。

▪ Sensor List Config

- **AP Type** : ドロップダウンメニューには、選択するための管理可能なモデルタイプが含まれます。選択したモデルタイプの管理対象 AP が、下のスクロールウィンドウに表示されます。

管理者は、リストされた AP を 1 つ以上確認し、下部にある apply ボタンをクリックして、これらの AP をスキャナーとして指定することができます。

▪ Trusted AP Config

- **BSSID** : 管理者は、このリスト内の既知の信頼できる AP の BSSID を静的に割り当てることができます。このリストに入力された、まだ管理されていない AP が環境に存在する場合、不正 AP デバイスリストには表示されません。
- **Remark** : 管理者は、リスト上の信頼できる AP に関連する追加情報の文字列を入力できます。

j) AP Load Balancing

管理対象 AP が過負荷にならないようにする機能です。システムは、AP の関連クライアント数が事前に定義されたしきい値を超えていることを検出し、同じグループ内の他の AP がまだしきい値を下回っている場合、バランシング機能は、過負荷の AP の送信電力を減少させ、他の利用可能な AP の送信電力を増加させるためにアクティブにされ、これにより、他の利用可能な AP が関連付けられる可能性が高くなります。システムは、管理対象 AP をグループに分割し、グループしきい値、および AP ロードバランシングをトリガーする時間間隔を定義できます。

LAPM Load Balancing

Load Balancing Enable Disable

Balance Interval minute(s)

Cluster

Device List

Add to AP Type

	Cluster	Device Name	MAC Address	IP Address	Power Level	Clients	Log
<input type="checkbox"/>	None	123		192.168.123.123	Highest	Offline	View

- **Load Balancing** : この設定項目を使用すると、管理者は AP ロードバランシング機能を適用する基準を指定できます。
- **Balance Interval** : 管理者は、システムがクラスタ内のクライアント数を同期する時間間隔を指定します。
- **Cluster** : この項目を設定ページに入力すると、現在のすべての AP グループとそのステータス情報が表示されます。
- **Device List** : スクロール可能なウィンドウには、グループ、名前、MAC、IP、電力レベル、ローディングなどの相対情報とともに、モデル名でソートされたすべての管理対象 AP が表示されます。管理対象 AP には、AP ロードバランシング機能を適用するために属する AP グループを示す Group 列があります。

2) Wide Area AP Management

a) AP List

タイプ、名前、IP アドレス、MAC アドレス、AP オンライン/オフラインステータス、ユーザー数、トンネルのステータス、AP ファームウェアのバージョン、地理的位置など、各管理対象 AP の情報を表示するリストです。このセクションの機能には、削除、マップに追加、構成のバックアップ、バックアップ設定、復元設定、アップグレード、設定の適用、再起動などの操作も含まれます。

システム管理下のサポート対象の AP がすべてリストに表示されます。最初は、リストは空です。管理者は、Discovery タブまたは Adding タブからサポートされている AP を追加できます。AP が追加されると、このリストには、AP タイプ、AP 名、IP アドレス、MAC アドレス、ステータス、クライアント数、トンネルステータス、AP ファームウェアバージョン、地理的位置など、現在管理されている AP が表示されます。管理者は、個々の AP の前にあるチェックボックスにチェックを入れるか、上部のチェックボックスにチェックを入れてすべての AP をまとめて選択することで、削除、マップに追加、バックアップ設定、復元設定、アップグレード、設定の適用、管理対象 AP の再起動を実行できます。

AP List

Type: All
Status: All
Tunnel: None

Name: [] Search

Refresh Interval: 30 seconds Refresh

Add Delete Add to Map Backup Config Restore Config Upgrade Apply Settings Reboot Export

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
------	------	----	-----	-----	----------	--------	------------	--------	--------------	--------	---------	---------------

AP を管理対象リストに追加した後、リストされた AP の管理のためにいくつかの操作を実行できます。

- **Go** : EWS コントローラは、ワイドエリア AP の設定をリモートで直接設定することはできません。ただし、Goto ボタンは、リモート AP の WMI にアクセスするための便利なリンクです。
Goto ボタンは、表示されている AP のステータスが Online の場合にのみアクティブになります。

AP List

Type: All
 Status: All
 Tunnel: None
 Name: Search

Refresh Interval: 120 seconds Refresh

Add Delete Add to Map / Floor Plan Backup Config Restore Config Upgrade Apply Settings Reboot

Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.
ECW5211-L	ECW5211-L	10.73.7.38	00:1F:D4:06:F1:1D	Overview	1	Online	0	Edit	System Overview System Overview VAP Overview WDS Overview System Upgrade Reboot WDS Status Associated Clients Event Log	RUN	3.43.00

列ヘッダーのドロップダウンリストは、どの WMI ページに移動するかを指定するためのものです。

- **Delete** : チェックされている AP をリストから削除します。
- **Add to Map/Floor Plan** : このボタンをクリックすると、ポップアップウィンドウが開きます。管理者は、ドロップダウンリストから、マップ上またはフロアプラン上の選択した AP にマークを付けることができます。マッププロファイルまたはフロアプランが設定されていない場合、ドロップダウンリストで選択できるマップ/フロアプランはありません。
- **Backup Config**: このボタンをクリックすると、ポップアップウィンドウが開き、管理者は選択した AP の構成設定を EWS コントローラのストレージに保存された.db ファイルにバックアップできます。Backup Config タブページの下に、ダウンロードまたは削除用のバックアップファイルが一覧表示されます。
- **Restore Config** : このボタンをクリックすると、ポップアップウィンドウが開き、管理者は管理者 PC または EWS コントローラのストレージにローカルに保存された.db ファイルを使用して、選択した AP の構成設定を復元できます。
- **Upgrade** : このボタンをクリックすると、ポップアップウィンドウが開き、管理者は管理者 PC または EWS コントローラのメモリ (**Firmware** タブページの下) にローカルに保存されたファームウェアファイルを使用して、選択した AP のファームウェアをアップグレードできます。
- **Apply Settings** : すでに用意されている WAPM テンプレートを選択した AP に適用して、AP の設定を実装したり、特定の管理アプリケーションの AP 管理者のパスワードを変更したりします。
- **Reboot** : このボタンをクリックすると、選択した AP が再起動します。
- **Export** : 選択可能な列で現在の AP リストをエクスポートします。
- **Edit (AP 名)** : このボタンをクリックすると、AP の属性編集ページに入り、管理者はデバイス名と SNMP コミュニティを指定できます。AP がマップ上にマークされている場合、このページでは、管理者は地理的位置、カバレッジ、関連リンクを設定し、マップ上に表示されるマーカーまたはアイコン画像をカスタマイズすることができます。

- **Edit (トンネルステータス)** : 完全なトンネル VAP のポートロケーションマッピングパラメータを設定するには、このボタンをクリックします。管理者は、NAS 識別子を割り当て、管理対象 AP の完全トンネル化された VAP ごとにサービス用の IP プールを指定できます。

移動先 : **Main >> Devices >> Wide Area AP Management >> AP List.**

AP List

Type: All
 Status: All
 Tunnel: None
 Name: Search

Refresh Interval: Disable Auto Refresh Refresh

Add Delete Add to Map Backup Config Restore Config Upgrade Apply Settings Reboot Export

■	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
<input type="checkbox"/>	ECW5211-L	ECW05211-L	10.71.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	N/A



Enterprise_Access_Point_-_ECW5211-L: VAP Status

Profile Name	ESSID	VLAN ID	Tunnel Port Location Mapping Setup	Mapped Service Zone
VAP-1	ECW5211-L-1	1000	Configure	Default



Tunnel Port Location Mapping Setup

Service Zone / Prefer DHCP Pool: Default / None

User Limitation: (Blank is for unlimited.)

ESSID: ECW5211-L-1

Room Number / Location ID:

Room Description / Location Name:

NAS Identifier:

- **Service Zone / Prefer DHCP Pool** : このフィールドエントリには、この VAP がトンネリングされる SZ が表示されます。優先 DHCP プールを使用すると、管理者は、この VAP 内のクライアントに IP を発行に割り当てる IP プールを指定できます。
- **User Limitation** : 管理者は、この VAP からサービスの IP アドレスを割り当てることができるクライアントの数を指定できます。
- **ESSID** : この VAP の ESSID がここに表示されます。
- **Room Number / Location ID** : 管理者は、この VAP のロケーション ID を説明するテキスト文字列を入力で

きます。

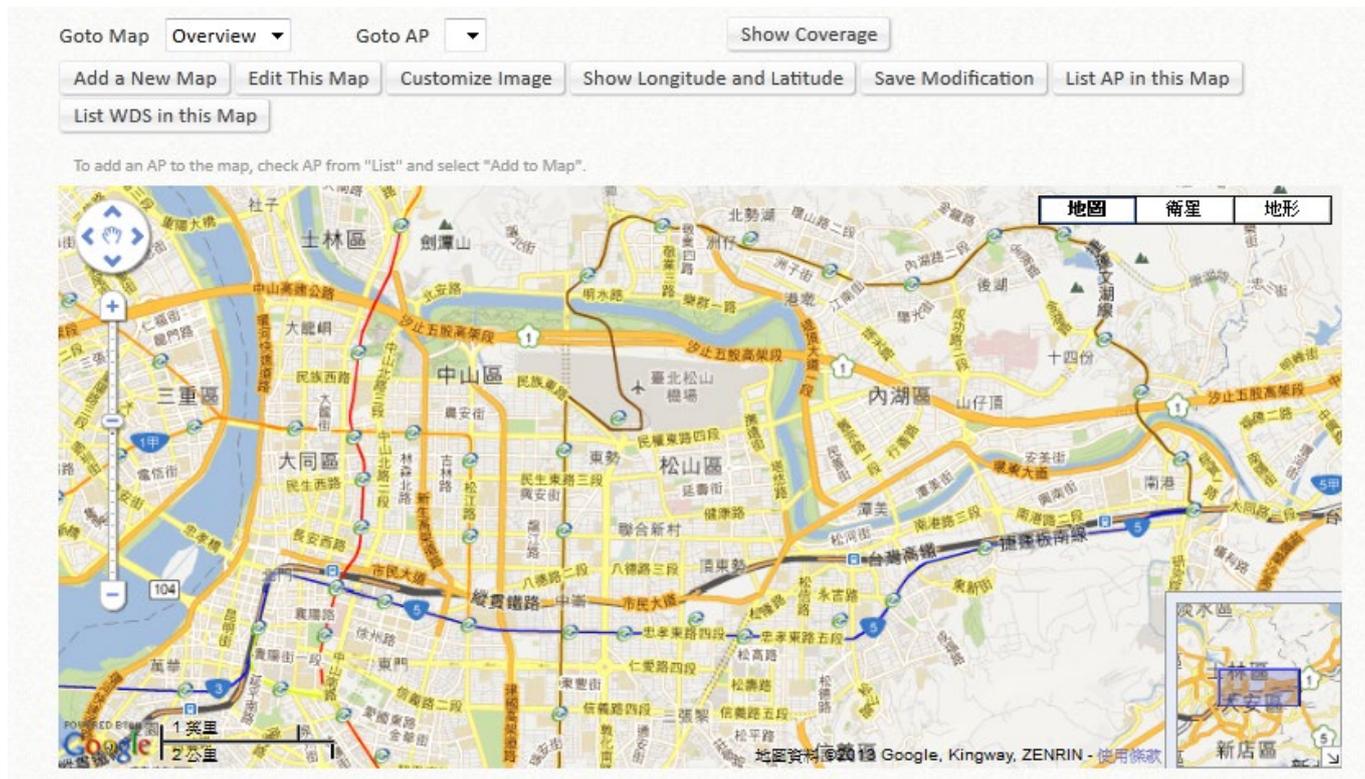
- **Room Description/ Location Name** : 管理者は、この VAP のロケーション名を説明するテキスト文字列を入力できます。
- **NAS Identifier** : 管理者は、必要に応じて、この VAP と結合する追加の NAS ID を割り当てることができます。

b) AP Grouping

Map Configuration

Map タブページは Google マップ API バージョン 3 で実装されており、管理者はワイドエリア AP 管理の下にあるすべての AP の所在を一目で確認できます。この機能は、ネットワークの計画と管理に関して役立ちます。

管理者が管理リストに AP を追加すると、以下のように Google マップ API でこれらの AP にタグを付けたり、マークを付けたりして、その地理的位置を示すことができます。



マップを作成する手順 :

ステップ 1 : ISP からパブリック IP アドレスを取得し、このアドレスを WAN インターフェースに設定します。

ステップ 2 : Google Maps Registration key (Google マップ登録キー) を申請します。

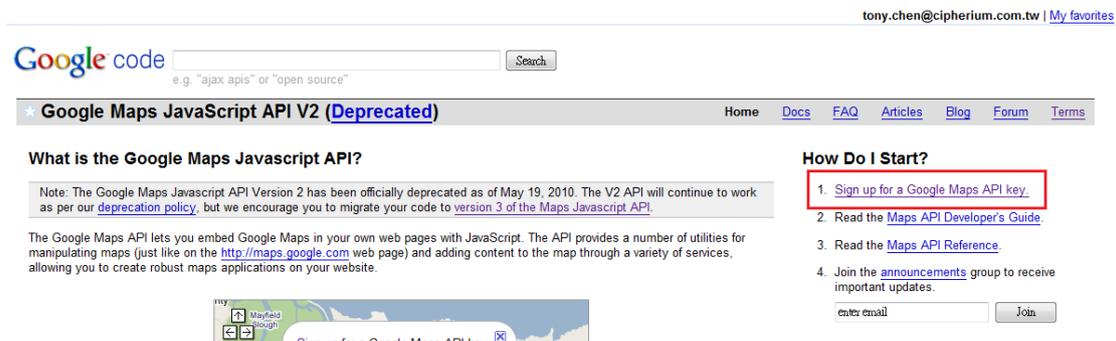
ステップ 3 : Map ページの **Add a New Map** (新しいマップを追加) ボタンをクリックします。Map Name (マップ名) と登録キーを設定します。

ステップ 4 : AP を検出し、これらの AP を管理対象リストに追加します。

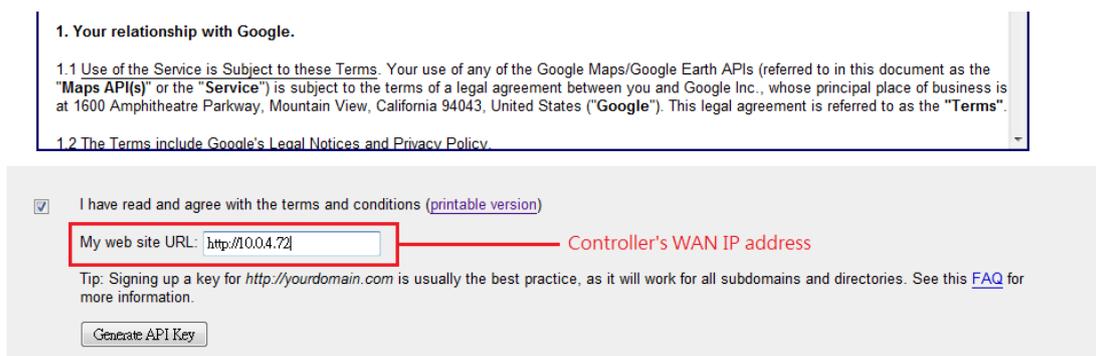
ステップ 5 : List ページで、作成したマップにいくつかの AP を追加します。

AP 情報を使用してマップを構成するために必要な手順については、以降のセクションで説明します。

ワイドエリア AP 管理で新しい地図を追加する前に、Google アカウントにサインアップする必要があります。または Google アカウントがすでに使用可能な場合は、この手順をスキップすることができます。このアカウントは、Google Maps API v3 キーの申請に使用されます。詳細については、<https://cloud.google.com/maps-platform/> の Google の指示に従って、そのような Maps API v3 キーを取得し、**Map Configuration ページ**の下の「**Google Maps Registration Key**」フィールドにキー情報を提供してください。

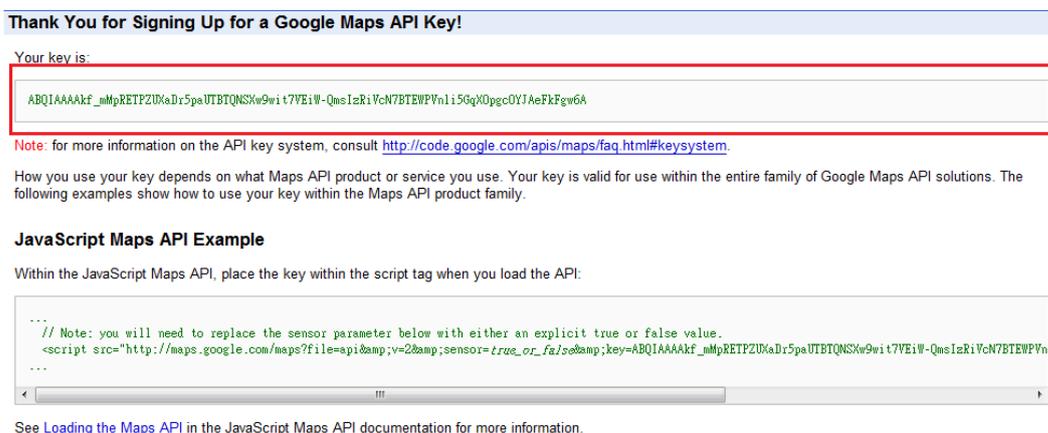


「Sign up for a Google Maps API key」をクリックします。



利用規約のチェックボックスをクリックし、EWS コントローラの WAN IP アドレスを入力します。

Google は、EWS コントローラ用の API キーを生成します。



次に、EWS コントローラの WMI の **Map** タブページに戻り、ページ一番下までスクロールし、**Add a New Map** ボタンをクリックします。

MAP Configuration

Map Name	<input type="text" value="Taipei Bridge"/>
Latitude	<input type="text" value="25"/>
Longitude	<input type="text" value="121"/>
Google Maps Registration Key	<input type="text" value="AlzaSyDzjF1tWlf6158aJw7zGAxBYscY-L8Dtd8"/>
Zoom Level	<input type="text" value="1"/>
Map Type	<input type="text" value="Normal"/>

設定のために編集ページが開きます。このマップの **Map Name**（マップ名）と、**Longitude**（経度）と **Latitude**（緯度）で定義されている地理的位置を入力してください。また、Google が発行したキーも記入してください。最後に、**Zoom Level** と **Map Type** を選択し、**Save** ボタンをクリックします。



上のスクリーンショットは、マップ名を Taipei Bridge（台北橋）、ズームレベル 14 と Normal Map Type（標準マップタイプ）として台北市を示した例です。

複数の AP を配置し、Wide Area AP Management の下の **List** に一覧表示している場合は、その地理的位置を特定のマップ上にマークできます。

まず、**List** タブページに移動し、マップ上にマークしたい AP の **Edit** ボタンをクリックします。AP 設定ページで、この AP の座標（**Latitude** と **Longitude**）と信号カバレッジの半径を設定します。

Device : ECW5211-L

Device Name	<input type="text" value="ECW5211-L"/>	*
SNMP Community	<input type="text" value="public"/>	*modify snmp setting will reboot the AP
SNMP Write Community	<input type="text" value="private"/>	*modify snmp setting will reboot the AP
Latitude	<input type="text" value="0.0"/>	*-85 ~ 85
Longitude	<input type="text" value="0.0"/>	*-180 ~ 180
Remark	<input type="text"/>	
Link 1	Name: <input type="text"/> Description: <input type="text"/> URL: <input type="text"/>	
Link 2	Name: <input type="text"/> Description: <input type="text"/> URL: <input type="text"/>	
Link 3	Name: <input type="text"/> Description: <input type="text"/> URL: <input type="text"/>	

この特定の AP をマークする座標を入力します。**Link 1~Link 3**は、マップ上のダイアログボックスに表示される HTTP リンクを設定するためのもので、この AP に接続されている IP 監視カメラの IP アドレスや、この AP が配置されている会場のウェブサイトの URL など、AP に関連する追加情報を参照することができます。

管理者は、マップ上に表示されているカスタマイズされたサムネイル画像をアップロードできます。必要な設定をすべて設定し、画像をアップロードしたら、**Apply** ボタンをクリックし、**AP List** ページに戻ります。

マップ上にマークしたい AP をチェックし、「**Add to Map/Floor Plan**」ボタンをクリックし、これらの AP をマークするマップの名前を選択して「**OK**」ボタンをクリックしてください。

AP List

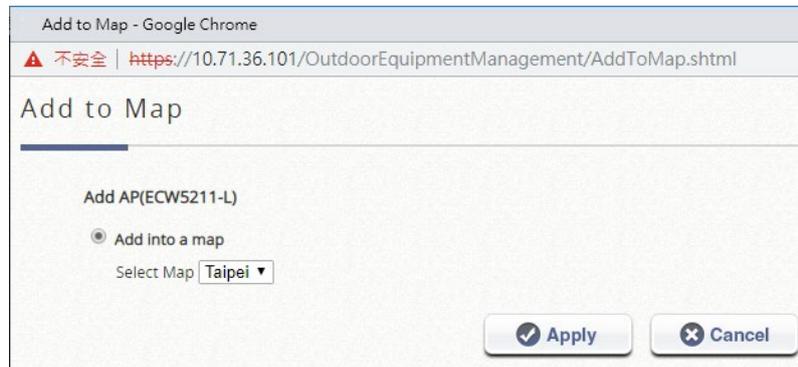
Type: Status: Tunnel:

Name: Search

Refresh Interval: Refresh

Add Delete **Add to Map** Backup Config Restore Config Upgrade Apply Settings Reboot Export

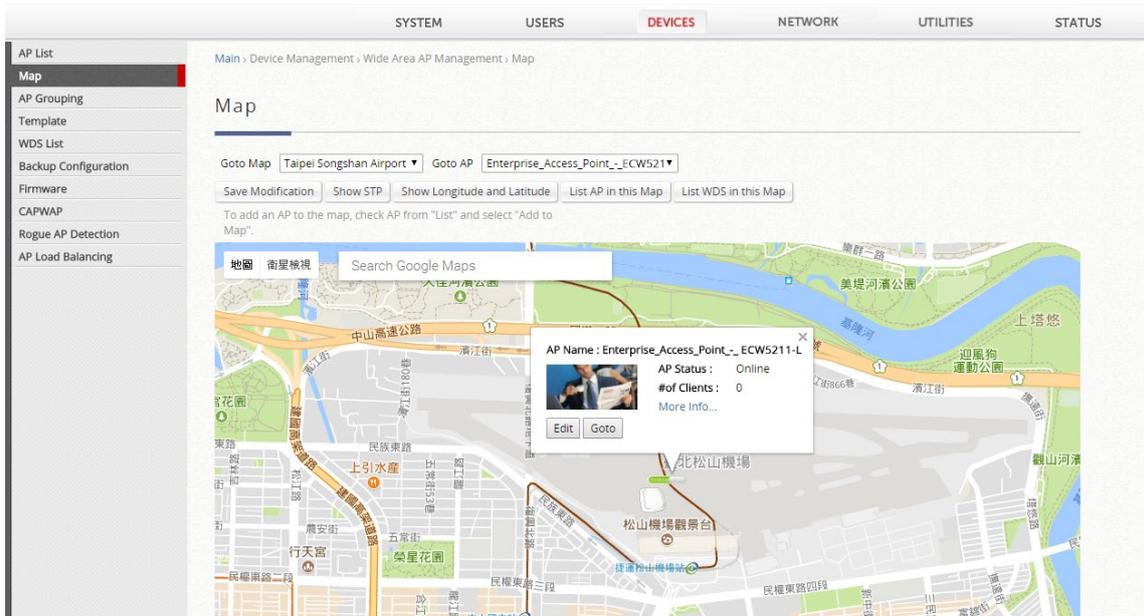
Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
ECW5211-L	ECW05211-L	10.0.36.55	00:1F:D4:07:42:CD	Overview	1	Online	0	Edit	System Overview Go	RUN	3.45.0000	N/A



選択した AP は、以下に示すように、設定された物理座標でマーカーイメージとしてマップ上に表示されます。



AP アイコンをクリックすると、設定済みの追加情報やリンクに関するダイアログボックスが表示されます。AP status、Client List、WDS List、および AP に関連する Links については、more info リンクをクリックしてください。

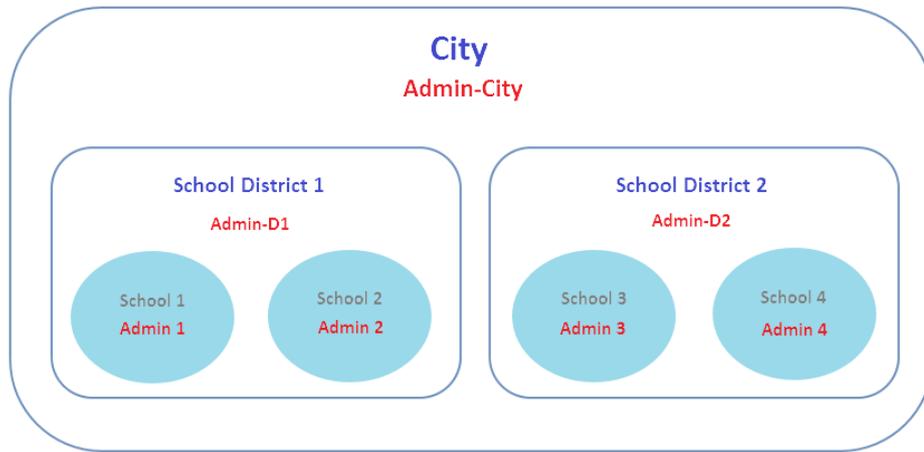


AP status、Client List、および WDS List の情報は、SNMP を介してリモート AP から収集されます。

AP Grouping

Wide Area AP Management では、すべての管理対象 AP を、マップによって AP グループに指定する必要があります。各 AP は、マップに属するように設定する必要があります。すべての AP がデフォルトマップに追加されます。または、新しい AP を追加する前に、選択用の新しいマップを作成することもできます。

AP のグループ化を使用すると、異なるレベルの管理者が異なる AP グループで AP を管理できます。AP グループには、複数のマップと AP テンプレートを含めることができます。一方、マップを異なる AP グループに含めることができます。異なる管理者グループには、AP グループごとに異なる読み取り/書き込み権限を割り当てることができます。



Edgecore コントローラは、Google マップ上の AP の追加をサポートしています。プロセスを以下に示します。

1. ページ下部の **Map List** の下にある **Add** をクリックして独自のマップを作成し、ポップアップウィンドウに表示される必要なフィールドに入力します。**Apply** をクリックします。
2. AP の属性プロファイル（経度と緯度）に AP の配置位置を追加します。 「Main Menu > Devices > Wide Area AP Management > List - AP Attribute (Edit)」
3. List ページに戻り、AP を選択し、「**Add to Map/Floor Plan**」ボタンをクリックして、目的のマップを選択します。設定後、管理者は選択したマップ上の AP のアイコンを見ることができるようになります。
4. 概要パス：「Main Menu > Devices > Wide Area AP Management > Map」
5. 「Main Menu > Devices > Wide Area AP Management > AP Grouping > AP Grouping List」の順に選択して、AP グループを追加または削除します。

AP Grouping

Add Delete

■	AP Group	Map	Template
<input type="checkbox"/>	456	123	1 3 5

6. Add をクリックして AP グループを追加してください。各 AP グループには、管理対象のマップとテンプレートを含めることができます。

AP Grouping Add

AP Group Name *

Map

Selectable	Selected
	Overview
	123

Template

Selectable	Selected
Template2	Template1
Template4	Template3
Template5	Template6
Template7	
Template8	

7. APグループを作成したら、管理者グループを Administrator Group List に追加することによって、各 AP グループにアクセス許可を割り当てることができます。

Main > Utilities > Administrator Accounts > Administrator Group List

Administrator Group List

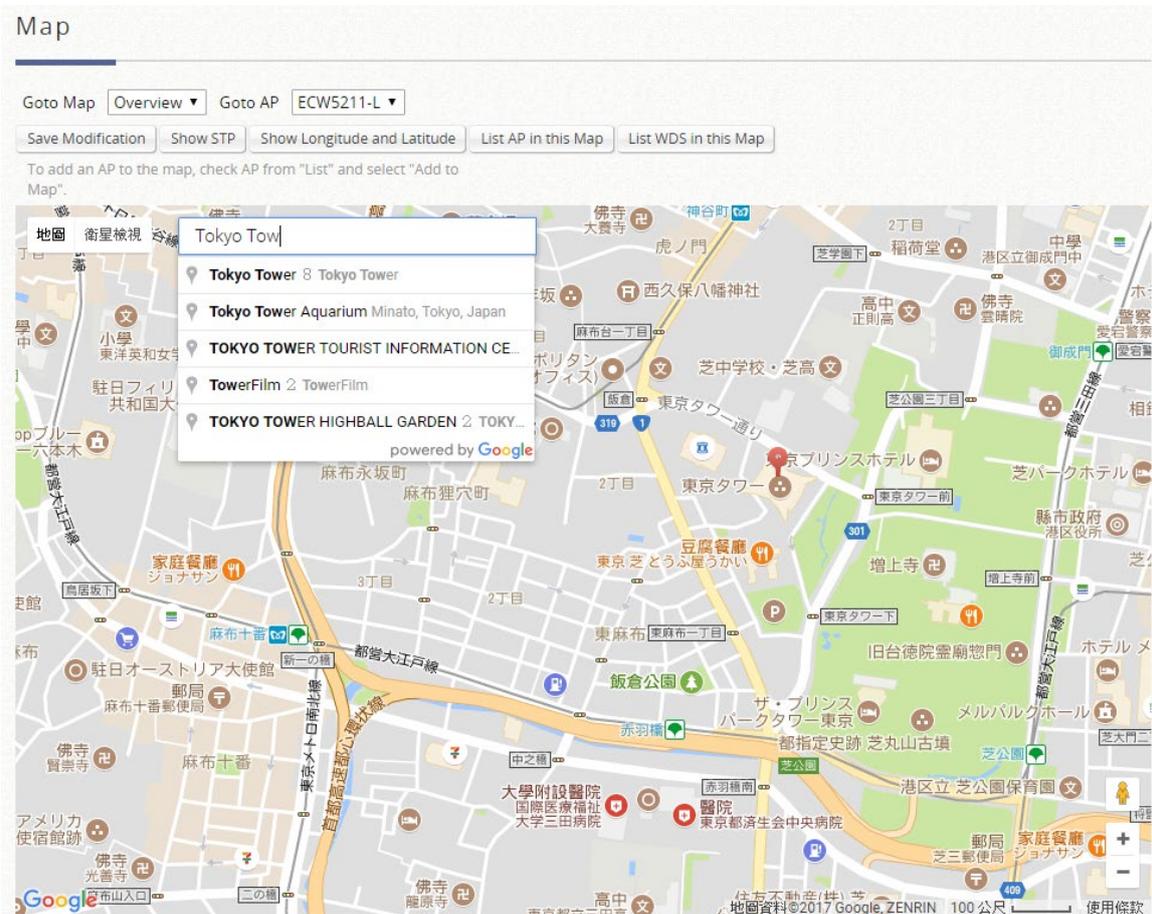
<input type="checkbox"/>	name	remark
<input type="checkbox"/>	Super Group	remark
<input type="checkbox"/>	Manager	remark
<input type="checkbox"/>	Operator	remark
<input type="checkbox"/>	On Demand	remark
<input type="checkbox"/>	Custom 1	remark
<input type="checkbox"/>	Custom 2	remark
<input type="checkbox"/>	Custom 3	remark

8. APグループへの権限の割り当ててください。

	Disabled	SZ7
	Disabled	SZ8
AP GROUP	Disabled	Select All
	Disabled	456
AP Management	Read Only	
	Read/Write	Select All
Switch Management	Disabled	Local Area AP Management
	Disabled	Wide Area AP Management
	Disabled	

c) Map

マップは、Google マップ上の管理対象 AP と WDS リンクを表示します。これは、無線ネットワークの計画と管理のためのユーティリティです。



- **Goto Map** : 複数のマッププロファイルを設定している場合、この機能では異なるマップを切り替えることができます。
- **Goto AP** : 管理者がリスト上の AP を選択し、選択した AP がマップの中央に表示されるようにマップが移動する機能です。
- **Save Modification (Overview マップを除く)** : この機能は、マップに加えられた変更を保存し、マップのプロファイル属性を上書きするためのものです。例えば、元のマップを変更または画面移動した場合、このボタンをクリックすると、変更内容が保存されます。
- **Show Longitude and Latitude** : この機能を押すと、マップの現在中心点の経度と緯度がポップアップウィンドウに表示されます。
- **List AP in this Map** : このボタンをクリックすると、ブラウザに新しいページが開き、**List** タブページにリダイレクトされ、マップ内の AP のリストが表示されます。
- **List WDS in this Map** : このボタンをクリックすると、ブラウザに新しいページが開き、**WDS List** タブページにリダイレクトされ、マップ内の WDS リンクのリストが表示されます。
- **Map/Satellite** : グラフィカルビューまたは実際の衛星画像のビューを切り替えます。

- **Search** : 管理対象 AP を検索するのではなく、Google マップから位置や場所を検索できます。
- **Distance Calculation** : 選択した 2 つの AP 間の距離を計算します。

d) Discovery

この検出機能は、インターネットまたはイントラネットを介して、サポートされているタイプの AP を検出する機能です。検出された AP は、管理されたデバイスに追加され、SNMP 読み取りコミュニティ文字列を自動的に割り当てることができます。このコミュニティ文字列は、定期的なステータス収集に使用されます。AP を検出するには、AP List から **Add** をクリックし、Add Method ドロップダウンリストから **Discovery** を選択します。

管理者が新しい AP を検出しようとしたら、Device Type を選択します。次に、AP の現在の IP 範囲、Login ID と Password を入力します。次に、Discovery ボタンをクリックします。新しい AP が検出されると、次の Discovery Results リストに表示されます。

Add Method **Discovery** ▼

Discovery AP

Device Type **ECW100** ▼

Admin Settings Used to Discover

Start IP Address

End IP Address

Login ID

Password

Device Results

■	Device Type	IP Address	Device Name	SNMP Community	SNMP Write Community	Map
---	-------------	------------	-------------	----------------	----------------------	-----

- **Start/End IP address** : 管理者は、AP 検出の IP アドレス範囲を指定する必要があります。指定した IP アドレスは、外部ネットワーク IP アドレスまたは内部ネットワーク IP アドレスです。これは、管理対象ネットワークに接続されている複数のデバイスをスキャンする場合に便利です。指定範囲外の IP アドレスを持つ AP は、検出後にリストされません。
- **Login ID/Password** : 対象 AP の管理インターフェースのログイン ID とパスワードを入力すると、管理者は AP の SNMP コミュニティをリモートで設定できます。
- **Discover** : 管理者が新しい AP を検出しようとしたら、**Device Type** を選択します。次に、AP の現在の IP 範囲、**Login ID**、**Password** を入力します。次に、**Discover** ボタンをクリックします。新しい

AP が検出されると、次の Discovery Results リストに表示されます。管理者は、検出プロセス中いつでもコントローラのスキャンを停止できます。

➤ **Device Results** : 検出プロセスが完了すると、検出された AP がここに一覧表示されます。管理者は **Add** をクリックして、AP を管理対象のリストに登録できます。

- **Device Type** : 検出された AP の AP モデルです。
- **IP Address** : 検出された AP の IP アドレスです。
- **Device Name** : 設定によってデバイスを識別するには、デバイス名を指定します。
- **SNMP Community** : ステータスアクセスに使用される SNMP 読み取りコミュニティ文字列です。
- **SNMP Write Community** : 設定の変更に使用される SNMP 書き込みコミュニティ文字列です。
- **Map** : 特定のマップで管理対象デバイスを特定の階層管理またはグラフィカルビューに指定します。

e) Adding

追加機能を使用して、AP に必要な情報を入力して AP を手動で設定します。

管理リストに追加する複数の AP を検索して一覧表示できる **Discovery** 機能に加えて、管理者は **Add an AP** を選択して、管理リストに1つのアクセスポイントを直接追加することもできます。デバイスの IP アドレス、名前、ログイン資格情報を設定し、SNMP コミュニティ文字列を設定し、**Apply** ボタンをクリックするだけです。

管理者は、ここでサポートされている AP を List 表に手動で追加できます。手動で追加した AP は、最初に AP List に「offline」の状態が表示されます。システムは、SNMP プロトコルを使用して AP への接続を試みます。SNMP 読み取りが成功すると、手動で追加した AP が online になります。

Add Method

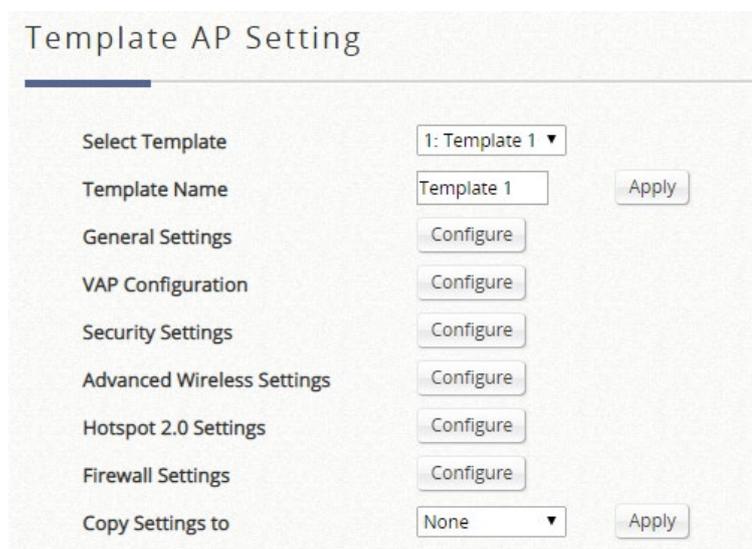
Add an AP

Device Type	<input type="text" value="ECW100"/>
Device IP	<input type="text"/>
Device Name	<input type="text"/>
Login ID	<input type="text" value="admin"/>
Password	<input type="text" value="admin"/>
SNMP Community	<input type="text" value="public"/>
SNMP Write Community	<input type="text" value="private"/>
Map	<input type="text" value="Overview"/>

➤ **Device Type** : ワイドエリア AP のデバイスタイプです。

- **Device IP** : 管理リストに追加する AP の IP アドレスです。
- **Device Name** : この AP デバイスに与えられたニック名です。
- **Login ID** : デバイスの管理インターフェースのログイン名です。
- **Password** : デバイスの管理インターフェースのログインパスワードです。
- **SNMP Community** : ステータスアクセスに使用される SNMP 読み取りコミュニティ文字列です。
- **SNMP Write Community** : 設定の変更に使用される SNMP 書き込みコミュニティ文字列です。
- **Map** : 特定のマップで管理対象デバイスを特定の階層管理またはグラフィカルビューに指定します。

f) Template



アクセスポイントのファームウェアのバージョンに応じて、国コードを選択してください。これにより、アクセスポイントで使用可能なチャンネルが動的に変更されます。

- **General Settings**

General Settings - 1: Template 1

RF Card Name	RF CARD A ▼
Band	802.11g+802.11n ▼ <input type="checkbox"/> Pure 11n
Short Preamble	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Short Guard Interval	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Channel Width	20 MHz ▼
Channel	6 ▼
Antenna Mode	Max ▼
Transmit Power	Level 1 ▼
ACK Timeout	0 <small>*(0 - 255, 0:Auto, Unit:4 micro seconds)</small>
Beacon Interval	100 millisecond(s) <small>*(100 - 500ms)</small>
Airtime Fairness	<input checked="" type="radio"/> Disable <input type="radio"/> Fair Access <input type="radio"/> Preferred Access
Packet Delay Threshold	0 millisecond(s) <small>*(100 - 5000ms, 0:Disable)</small>
Idle Timeout	300 second(s) <small>*(60 - 60000)</small>
Band Steering	<input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="checkbox"/> Aggressive
Interference Detection	Adjacent Channel Utilization Threshold 0 % <small>*(60 - 99, 0:Disable)</small> Latency 10 second(s) <small>*(10 - 999)</small> Co-Channel Utilization Threshold 0 % <small>*(60 - 99, 0:Disable)</small> Invalid Packet Rate 90 % <small>*(60 - 99)</small> Latency 10 second(s) <small>*(10 - 999)</small>
WME Configuration	<input type="button" value="Configure"/>
Transmission Rate Threshold	1001 kbps <small>*(0:Disable)</small>
CCA Minimum Power	<input checked="" type="radio"/> Auto <input type="radio"/> Dense Deployment <input type="radio"/> Sparse Deployment <input type="radio"/> Other -95 <small>*(≤ -75)</small>
UAPSD	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

- **RF Card Name** : AP の RF カードを選択します。
- **Band** : 編集する AP モデルテンプレートに応じて、**802.11a**、**802.11b**、**802.11g**、**802.11a+802.11n**、**802.11b+802.11g**、**802.11g+802.11n**、**802.11ac** の各モードを選択できます。
- **Short Preamble** : 56 ビットの同期フィールドを持つショートプリアンブルは、無線 LAN の伝送効率を向上させることができます。ショートプリアンブルを使用する場合は *Enable* を、128 ビットの同期フィールドでロングプリアンブルを使用する場合は *Disable* を選択します。
- **Short Guard Interval** (Band が **802.11g+802.11n** または **802.11a+802.11n** の場合に利用可能) : ガード間隔は、シンボル間の干渉を排除するために送信されるシンボル (文字) 間の間隔です。802.11n でスループットをさらに向上させるには、短いガード間隔が従来の半分になります。短いガード間隔を使用する場合は *Enable* を、通常のガード間隔を使用する場合は *Disable* を選択してください。

さい。

- **Channel Width (802.11g+n, 802.11a+n, 802.11ac のみ)** : 20MHz、40MHz、または Auto のいずれかを選択します。スループットを向上させるために、チャンネル帯域幅を 40MHz に倍増することがサポートされています。80MHz は、802.11ac モードでの選択が可能です。
- **Channel** : ネットワーク設定に対応する適切なチャンネルをドロップダウンメニューから選択します。「Auto」に設定され、Band が「802.11a」、「802.11a+n」、または「802.11ac」に設定されている場合、選択したチャンネルが干渉するか、DFS チャンネル信号が検出されると、チャンネルセレクト表が表示されます。
- **Antenna Mode (802.11g+n, 802.11a+n, 802.11ac のみ)** : 送受信の空間ストリームの数を設定します。
- **Transmit Power** : 一部の AP モデルでは、システムから送信される信号強度をレベルで選択できます。各レベルは、最高電力から 1dBm の減少を示します。**Level 1** は実際の最高電力であり、**Level 2** は最高電力から 1dBm を引いた値です。
- **Beacon Interval (ms)** : 20~1000 ミリ秒の値を入力します。デフォルト値は 100 ミリ秒です。入力された時間は、アクセスポイントとワイヤレスネットワークとの間でビーコン信号が送信される頻度を意味します。
- **ACK Timeout** : 「確認応答 (ACK) フレーム」の待ち時間間隔です。ACK が間隔内に受信されない場合、パケットは再送信されます。ACK タイムアウト間隔を長くすると、パケット損失は減少しますが、スループットは低下/悪化します。
- **Airtime Fairness** : 「Fair Access」に設定すると、異なるバンドの互換性を持つすべてのデバイスのエアタイムが同じになります。「Preferred Access」に設定すると、802.11n クライアントと 802.11ac クライアントが優先されます。この機能は、異なるバンドをサポートするデバイスを持つネットワークに最適です。
- **Packet Delay Threshold (ms)** : これは Tx キューフラッシングメカニズムで、キューが x ミリ秒以上処理されている場合にパケットをドロップし、すぐに他のキューを処理することを目的としています。これはデフォルトで無効になっています (=0)。
- **Idle Timeout (s)** : クライアントは、非アクティブ状態が設定された時間 (デフォルトは 300 秒) に達すると切断します。
- **Band Steering** : 有効にすると、5GHz 接続を持つクライアントは、2.4GHz 帯域の輻輳を軽減するために、5GHz 帯域に誘導されます。これは、2 つの RF カードで AP が 2.4GHz および 5GHz に設定されている場合にのみ適用されます。「Aggressive」にチェックを入れると、5GHz 接続を持つクライアントは、5GHz 帯に接続する必要があります。
- **Interference Detection** : 現在のチャンネルまたは隣接チャンネルの使用率、遅延、および無効なパケットレートが設定されたしきい値に達すると、AP は別のチャンネルに切り替わります。
- **Transmission Rate Threshold** : 送信レートが設定されたしきい値よりも低い場合、関連付けられたクライアントはキックされます。これにより、関連付けられているすべてのクライアントに対して高い接続速度が保証されます。
- **WME Configuration** : Wireless Multimedia Extensions (WME) は、Wi-Fi マルチメディア (WMM)

とも呼ばれ、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サービス品質（QoS）機能を提供します。アクセス優先度は、異なるパラメータを使用して設定することができます。CW Min：競合ウィンドウの最小値、CW Max：競合ウィンドウの最大値、AIFS：フレーム送信間隔、TXOP Limit：送信機会の制限。

- **UAPSD**：U-APSD は Unscheduled Automatic Power Save Delivery の略で、WMM で動作する 802.11 省電力機構です。クライアントデバイスが省電力モードの場合（つまり、受信機がオフになっているため、データフレームを受信できない）、AP はクライアント宛てのすべてのフレームを一時的にバッファリングします。

➤ VAP Configuration

The screenshot shows the 'VAP Configuration - 1: Template 1' interface. It contains the following fields and options:

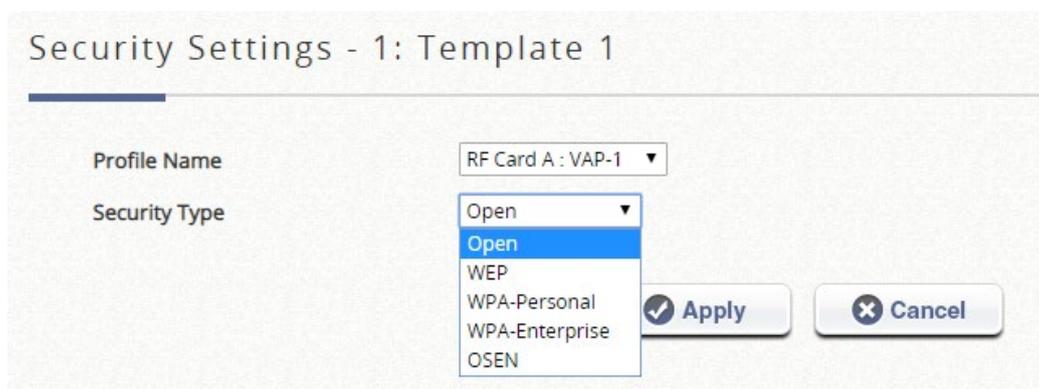
- Profile Name**: RF Card A : VAP-1 (dropdown)
- VAP**: Disable Enable
- Profile Name**: VAP-1 (text input)
- ESSID**: Guest Network (text input)
- Network Mode**: Bridge (dropdown)
- VLAN ID**: Disable Enable
- VLAN ID**: (text input) *(1 - 4094)
- CAPWAP Tunnel Interface**: Disabled (dropdown)
- Service Schedule**: 24/7 Service (dropdown)
- Access Control Type**: Disable MAC ACL Allow List MAC ACL Deny List

- **VAP**：この VAP を **有効**または**無効**にします。
- **Profile Name**：ID/管理目的で使用される特定の RF カードとその VAP のプロファイル名です。
- **ESSID**：ESSID（拡張サービスセット ID）は、クライアントが特定の VAP に関連付ける識別子として機能します。さまざまなワイヤレスセキュリティタイプのように、さまざまなサービスレベルと組み合わせることができます。
- **Network Mode**：VAP の動作モードです。
 - **Bridge Mode**：VAP は透過的に動作します（NAT なし、DHCP なし）。これにより、クライアントデバイスには LAN 側の DHCP サーバーから動的 IP アドレスが割り当てられます。アップリンクゲートウェイ/スイッチによって認識されるクライアントトラフィックの送信元 IP アドレスは、クライアントの元の IP アドレスのままになります。
 - **NAT Mode**：VAP は、この SSID に組み込み DHCP サーバーを備えたネットワークアドレス変換（NAT）デバイスのように動作します。これにより、クライアントデバイスには、この SSID で設定された DHCP プールから動的 IP アドレスが割り当てられます。NAT 変換後、アップリンクゲートウェイ/スイッチによって認識されるクライアントトラフィックの送信元 IP アドレスは

AP の IP アドレスになります。

- **Uplink Bandwidth** : アップリンク帯域幅制御は、VAP 上でキロビット/秒単位で設定できます。無制限の帯域幅制御の場合は 0 を設定します。VLAN が有効な場合にのみ設定できます。同じ VLAN ID を持つ VAP には、同じアップリンク帯域幅の制限が必要です。
- **Downlink Bandwidth** : ダウンリンク帯域幅制御は、VAP 上でキロビット/秒単位で設定できます。無制限の帯域幅制御の場合は 0 を設定します。VLAN が有効な場合にのみ設定できます。
- **VLAN ID** : Edgecore アクセスポイントは、タグ付き VLAN (仮想 LAN) をサポートします。VLAN 機能を有効にするには、各 VAP には 1 から 4094 までの有効な値を持つ固有の VLAN ID が与えられる必要があります。VLAN が有効になると、VAP で QoS がサポートされます。
- **CAPWAP Tunnel Interface** : ドロップダウンを選択して、VAP が AP とコントローラの間確立された CAPWAP トンネルを通過するトラフィックを指定します。CAPWAP トンネルインターフェースが「Complete」または「Split」トンネルである場合は、この VAP にマッピングするサービスゾーンを選択できます。
- **Service Zone** : 完全トンネル VAP またはスプリットトンネル VAP の場合は、マッピング先のサービスゾーンを選択します。
- **Service Schedule** : この VAP のサービス時間をカスタマイズします。
- **Access Control Type** : VAP に関連付けることを許可するデバイスを決定するために、デバイスのリスト (MAC アドレス) を設定します。
 - **Disable** : クライアントデバイスがアクセスするための制限はありません。
 - **MAC ACL Allow List** : リストされているクライアントデバイス (MAC アドレス) のみが、システムへのアクセスを許可されます。
 - **MAC ACL Deny List** : Deny List にリストされているものを除き、クライアントデバイス (MAC アドレス) がシステムへのアクセスを許可されます。

➤ Security Settings



ドロップダウンメニューから **Open**、**WEP**、**WPA-Personal**、**WPA-Enterprise**、および **OSEN** を含む、希望する **Security Type** を選択します。

➤ **Advanced Wireless Settings**

Advanced Wireless Settings - 1: Template 1

Profile Name	RF Card A : VAP-1
RTS Threshold	2346 *(1 - 2346)
Fragment Threshold	2346 *(256 - 2346)
DTIM period	1 *(1 - 15)
Consecutive Dropped Packets	0 *(2 - 50, 0:Disable)
Broadcast SSID	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Wireless Station Isolation	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
WMM	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IAPP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multicast-to-Unicast Conversion	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
TX STBC	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multicast/Broadcast Rate	5.5M
Management Frame Rate	5.5M
Receiving RSSI Threshold	-80 *(-95 ~ 0, 0:disable)

- **RTS Threshold** : 1 から 2346 までの値を入力します。RTS (送信要求) Threshold は、隠しノードの問題を防ぐために、フラグメントを送信する前にシステムが送信要求 (RTS) を発行するパケットサイズを決定します。データサイズが指定された値を超えると、RTS メカニズムが作動します。RTS Threshold を低く設定すると、多くのクライアントデバイスが AP と関連付けられているエリアや、クライアントが遠く離れており AP だけを検出できてお互いに検出できないエリアで役立ちます。
- **Fragmentation Threshold (802.11a、802.11b、802.11g モード)** : 256 から 2346 までの値を入力します。このしきい値より大きいパケットサイズは、送信前にフラグメント化 (1 つのチャンクではなく複数のピースで送信) されます。値が小さいほどフレームは小さくなりますが、伝送中のフレーム数は多くなります。Fragment Threshold を低く設定すると、通信が不十分なエリアや、重大な電波干渉によって妨害されるエリアに便利です。
- **DTIM Period** : 指定した周波数で周期ビーコン内に生成する DTIM 間隔を入力します。DTIM を高くすると、無線クライアントはより多くのエネルギーを節約できますが、スループットは低下します。
- **Consecutive Retries Threshold** : これは、クライアントが送信範囲外であると判断する前にパケット送信がドロップされた場合に、AP が試行する最大送信リトライ回数です。設定された回数だけ送信の再試行が失敗すると、アクセスポイントはクライアントをキックして、接続されている他のクライアントのパフォーマンスを最適化します。
- **Broadcast SSID** : この機能を無効にすると、システムの SSID がブロードキャストされなくなります。SSID のブロードキャストが無効になっている場合は、正しい SSID を持つデバイスだけがシステムに接続できます。
- **Wireless Station Isolation** : この機能を有効にすると、システムに関連するすべてのステーションがア

イソレーションされ、システムとしか通信できません。

- **IAPP** : IAPP (AP 間通信プロトコル) は、アクセスポイントが接続されているステーションに関する情報を共有するプロトコルです。この機能を有効にすると、システムは関連する無線ステーションの情報をピアアクセスポイントに自動的にブロードキャストします。これにより、同じ無線 LAN 内の IAPP 対応アクセスポイント間でワイヤレスステーションがスムーズにローミングできるようになります。
- **Multicast-to-Unicast Conversion** : Multicast-to-Unicast Conversion が有効な場合、アクセスポイントは、マルチキャストトラフィックを要求するポートだけにトラフィックをインテリジェントに転送します。逆に、無効にすると、マルチキャストトラフィックはブロードキャストトラフィックのように扱われ、パケットがすべてのポートに転送され、ネットワークの非効率性が生じます。
- **TX STBC** : STBC は、単一の RF 受信機 (非 MIMO) でも S/N 比を改善することを可能にする MIMO 送信機によって行われる事前送信エンコードです。
- **Multicast/Broadcast Rate** : マルチキャスト/ブロードキャストパケットの帯域幅設定です。ワイヤレスクライアントがマルチキャスト/ブロードキャストパケットを送信するために帯域幅を大きくまたは小さくする必要がある場合は、管理者がアクセスポイントのマルチキャスト/ブロードキャスト帯域幅をここでカスタマイズできます。
- **Management Frame Rate** : この機能は、管理フレームの帯域幅を制御します。レートが高いほど、トランスミッションがカバーする範囲が短くなります
- **Receiving RSSI Threshold** : 接続されているステーションの接続速度が高くなるように、受信感度が設定されたしきい値を満たさない限り、ステーションはネットワークに関連付けることができません。

➤ **Hotspot 2.0 Settings**

ホットスポット 2.0 は、公共の WiFi 加入者により良い帯域幅とサービスを提供するために WiFi Alliance によって開始された WiFi 認定パスポイントとして知られています。ホットスポット 2.0 機能は、サービスプロバイダとそのパートナー専用に設計されています。設定を完了するには、サービスプロバイダまたはサービスチームにご相談ください。

➤ **Firewall Settings**

- **Proxy ARP** : 有効にすると、AP はダウンリンクステーションに代わって ARP 要求に応答します。AP によって維持される ARP テーブルは、AP アップリンクから ARP 要求を受信したときにルックアップテーブルとして使用されます。逆に、Proxy ARP を使用しないと、ARP 要求が AP の無線ネットワークにブロードキャストされ、ネットワークが非効率になります。

➤ **Linkyfi's Location Engine**

Linkyfi は、公共の Wi-Fi ホットスポット用に AVSystem によって設計されたプラットフォームです。

Edgecore AP は、ロケーショントラッキングとトラフィック分析のために専用の Linkyfi サーバーと統合することができます。

- **Real Time Location System** : 屋内位置とリアルタイムナビゲーションのための Linkyfi リアルタイム位置情報システム (RTLIS) サーバーとの統合を可能にします。

- **DNS DPI** : DNS トラフィックを分析するために Linkyfi DNS DPI サーバーと統合できるようにします。

g) WDS List

このリストは、管理対象 AP に設定された各 WDS リンクの情報（Peer AP、Band、Channel、Security、TX Power、Link Speed、RSSI、TX Bytes、TX Packets、STP、Status など）を表示します。

WDS List

Peer AP	Band	Channel	Security	TX Power	Link Speed	RSSI	TX Bytes	TX Packets	STP	Status
ECW5211-L-1	ac	165	AES	Level 1	144M	-64	284378	400	Disabled	Active
ECW5211-L-2				Level 1	144M	-64	56378	78	Disabled	

List に記載された AP 間で確立された WDS リンクは、リンクのバンドとチャンネル、セキュリティ設定（ある場合）、送信電力、バイト、パケットなどの関連情報とともにここに一覧表示されます。

h) Backup Config

バックアップされた Config ファイルを使用して、AP の設定を **List** に復元できます。管理者が AP の構成設定をバックアップすると、すべてのバックアップファイルが **Backup Config** タブページに表示され、ローカルストレージデバイスにダウンロードしたり、EWS コントローラのメモリから削除したりできます。

Backup Config

Delete

<input type="checkbox"/>	Device Type	Version	Size	Backup Time	File Name	Actions
<input type="checkbox"/>	ECW5211-L	1.21.00	39947	2013/02/21 17:55:22	ECW5211-L	Download

また、自動デイリーバックアップも利用可能です。バックアップ時間を 24 時間体制で設定すると、その時間に AP のバックアップ設定が自動的に実行されます。

i) Firmware

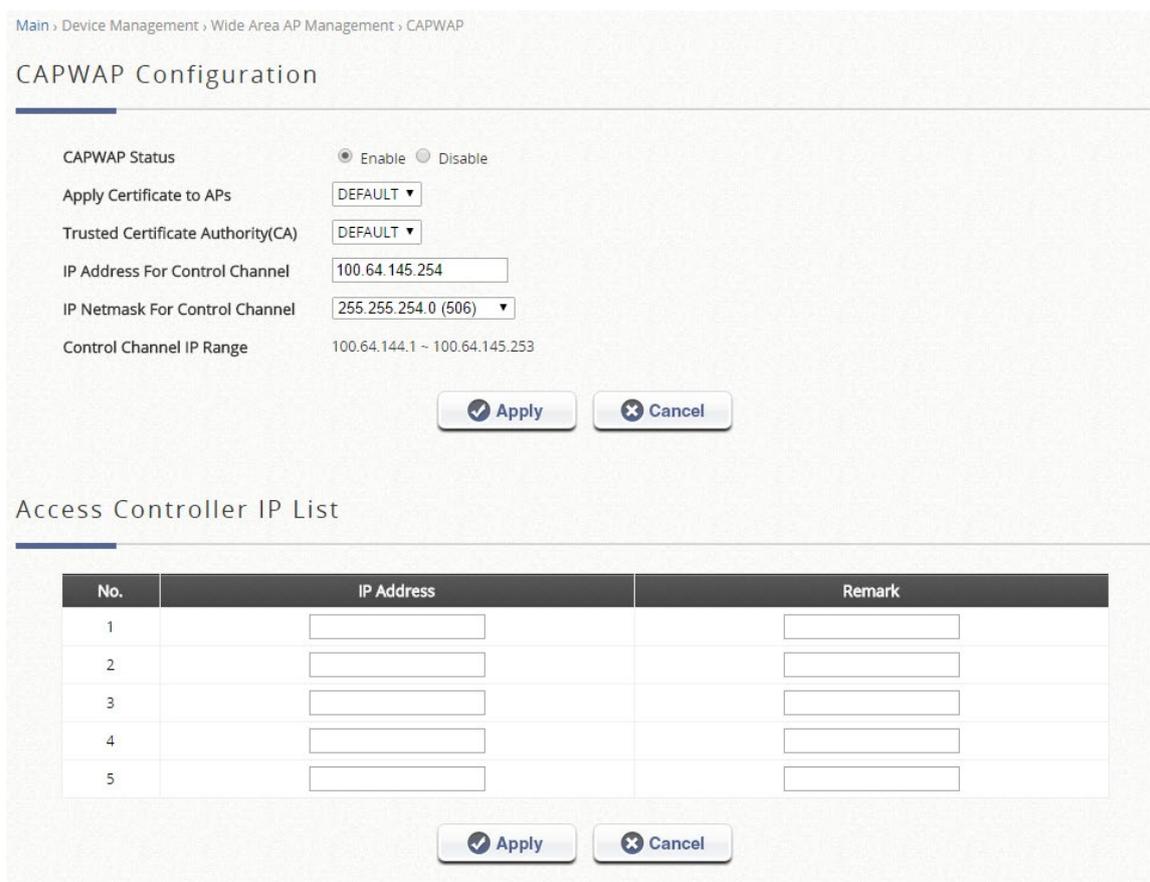
EWS コントローラは、AP のファームウェアを内蔵メモリに保存できます。**Firmware** タブページでは、管理者は新しい AP ファームウェアを EWS コントローラのメモリにアップロードできます。これによ

り、AP List ページからリモートの AP アップグレードおよび復元操作を簡単に実行できます。このページの下に表示されている AP ファームウェアは、必要に応じて EWS コントローラメモリからダウンロードまたは削除できます。



j) CAPWAP

CAPWAP は、EWS コントローラが無線アクセスポイントの集合を管理できるようにする標準の相互運用可能なプロトコルです。



- **CAPWAP Status** : CAPWAP 機能の設定状態です。**Enable** をクリックして、アクセス EWS コントローラをオンにして、CAPWAP サポート対象の AP を管理対象 AP リストに自動的に追加できるようにします。

- **Apply Certificate to APs** : この設定項目では、管理者は、AC と AP の間の CAPWAP ネゴシエーション中に使用する証明書を選択できます。選択した証明書が無効である場合、ネゴシエーションは失敗し、AP は管理対象リストに自動的に追加されません。
- **IP Address For Control Channel** : 制御チャネルの反対側で CAPWAP トンネル AP をネゴシエートする AC 側の IP アドレスです。
- **IP Netmask For Control Channel** : ネットマスクのサイズは、管理対象 AP の最大数に応じて自動/手動で設定できます。
- **Control Channel IP Range** : AP 側に割り当てる IP プールです。通信する制御チャネルを確立します。IP の数は、上記の IP アドレスと制御チャネルの IP ネットマスクによって定義されます。
- **Access Controller IP List** : AC は、サービスを提供できなくなった場合に備えて、他の CAPWAP サポート対象の AC を CAPWAP AP のバックアップ AC として静的に指定できます。番号は、これらのバックアップ AC の AP に対する優先度を指定します。元の AC がダウンした場合、AP は最初に No.1 のバックアップ AC への加入を試みます。

k) Rogue AP Detection

配置された環境で、管理されていない AP または悪意のある AP を検出するように設計されています。非管理対象 AP が管理対象 AP と同じ SSID を使用している場合でも、管理対象 AP をセンサーとして非管理対象 AP を検出します。AP の BSSID、ESSID、タイプ、チャンネル、暗号化、検出時間が表示されます。

General Configuration

Rogue AP Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Apply
Scanning Interval	<input type="text" value="0"/> minutes	
Channel Switching	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Sensor List	0/1	Configure
Trusted APs	0/40	Configure

Rogue AP List

ESSID

No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	Report Time
(Total:0) First Prev Next Last Go to Page <input type="text"/> (Page:1/1) Row per Page: <input type="text" value="10"/>						

l) AP Load Balancing

管理対象 AP が過負荷にならないようにする機能です。システムは、AP の関連クライアント数が事前に定義さ

れたしきい値を超えていることを検出し、同じグループ内の他の AP がまだしきい値を下回っている場合、バランシング機能は、過負荷の AP の送信電力を減少させ、他の利用可能な AP の送信電力を増加させるためにアクティブにされ、これにより、他の利用可能な AP が関連付けられる可能性が高くなります。システムは、管理対象 AP をグループに分割し、グループしきい値、および AP ロードバランシングをトリガーする時間間隔を定義できます。

ワイドエリア AP 管理機能は、さまざまな管理対象 AP のグループ化をサポートし、送信電力管理を実行して、同じグループの AP 間でネットワークの負荷をできるだけ均等に分散させます。

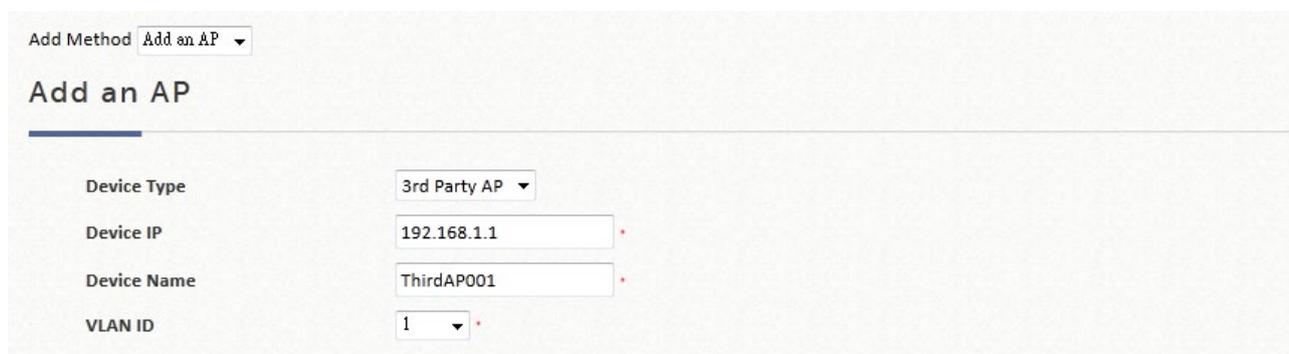
The screenshot shows two configuration sections. The first section, 'WAPM Load Balancing', includes a 'Load Balancing' toggle set to 'Disable', an 'AP Distance' input field with '100' and 'meter(s)', an 'Interval' input field with '0' and 'minute(s)', and a 'Threshold' section with radio buttons for 'Number of Clients' (selected, with '15' in the input) and 'Number of Packets'. An 'Apply' button is present. The second section, 'Map Cluster Setting', features a 'Map' dropdown menu set to 'Pick one', a 'Cluster' input field with '0', and buttons for 'Configure', 'Create', and 'Delete'. Below this is a table with columns: Cluster, Device Name, IP Address, RF, Power Level, # of Users, and Log.

- **WAPM Load Balancing** : この設定項目を使用すると、管理者は AP ロードバランシング機能を適用する基準を指定できます。
- **AP Distance** : このパラメータを使用すると、管理者は管理対象 AP をグループ化するための手段として使用される距離を指定できます。単位はメートルで、管理者は 0~999 の範囲の整数を設定できます。0 は機能が無効であることを示します。設定された距離内で互いに距離を置いた AP は、同じグループと見なされます。
- **Interval** : このパラメータにより、管理者は、コントローラが同じグループ内の各 AP のロードをチェックし、必要に応じてロードバランシングを開始する時間間隔を指定できます。
- **Threshold** : 管理者はこのパラメータを使用して、AP のシステム負荷の測定値として、**Number of Client** または **Number of Packets** のどちらかを選択できます。管理者は、ロードバランシングメカニズムを開始するシステムしきい値を指定できます。
- **Map** : マップを選択して、このマップ上のクラスタと AP を表示します。
- **Cluster** : このマップ上のクラスタ数を表示します。
 - **Configure** : 各クラスタの AP ロードバランシング機能を有効/無効にするページに入ります。

- **Create** : AP の距離に従って、現在のマップ上にクラスタを作成します。
 - **Delete** : 現在のマップ上のクラスタを削除します。
- **Cluster and Device List** : スクロール可能なウィンドウには、グループ、名前、IP、電力レベル、ローディングなどの相対情報とともに、モデル名でソートされたすべての管理対象 AP が表示されます。管理対象 AP には、AP ロードバランシング機能を適用するために属する AP クラスタを示す Group 列があります。View ボタンをクリアする、各 AP の AP ロードバランシングのログが表示されます。

m) Third Party AP Management

Device Type から THIRDPARTY を選択して、サードパーティの AP を追加します。サードパーティの AP の IP アドレス、名前、VLAN ID を指定して、AP リストに手動で追加します。**Add** をクリックしてすると、リストアイコンへの追加とチェックリストの追加が完了します。



サードパーティの AP のリストを確認および管理するには、次のページに移動します。 **Access Points >> Enter**

Wide Area AP Management >> List

タイプリストからこのサードパーティの AP を管理します。列から AP 属性と管理を編集します。

Map アイコンに移動します。追加されたサードパーティの AP は、Google マップの機能やすべてのマップ機能にも配置できます。

3) Switches

Switches : このセクションは、スイッチ管理に関連するすべての設定を設定するために使用します。

a) Switch List

EWS コントローラは、Edgecore スイッチを管理することができます。システム管理下のスイッチがこのリストに表示されます。



Switch List

Status

<input type="checkbox"/>	Name	Type	Status	IP address	MAC address	Total allocated/Used/Max supply power [W]	Switch UI
--------------------------	------	------	--------	------------	-------------	---	-----------

スイッチの名前がハイパーリンクとして表示されます。各管理対象スイッチのハイパーリンクをクリックすると、スイッチのその他の設定（一般設定、PoE 設定、VLAN メンバーシップ設定、ポート設定、PoE スケジュール）ができます。

AP の詳細ステータス情報（一般設定、PoE 設定、VLAN メンバーシップ設定、ポート設定、PoE スケジュール）を表示するには、各管理対象 AP のステータスを示すハイパーリンクをクリックします。

- **Add** : 「追加」機能は、必要な情報を入力してスイッチを設定するために使用されます。スイッチをリストに追加すると、スイッチのステータスが「online」または「offline」と表示されます。
- **Delete** : 対応するチェックボックスにチェックを入れてリストから削除したいスイッチを選択し、Delete ボタンをクリックします。
- **Restart** : 対応するチェックボックスにチェックを入れてリストから再起動したいスイッチを選択し、Restart ボタンをクリックします。
- **Backup** : 「Backup」ボタンは、コントローラ上のスイッチの設定.db ファイルを保存します。このファイルは、スイッチの設定を復元するために使用できます。
- **Restore** : バックアップ設定ファイルがコントローラに保存されている場合、スイッチのチェックボックスにチェックを入れ、Restore ボタンをクリックしてスイッチの設定を復元します。

b) PoE Schedule Template

システムは、EWS モデルに応じて、最大数の PoE スケジュールテンプレートをサポートします。

PoE Schedule Template

Add template

Template Name	Copy Settings From	Remark	Action
Default	NONE		

Apply

Cancel

最初のテンプレートは既定のテンプレートであり、削除できません。テンプレート名は簡単に参照できるようにカスタマイズできます（例：Switch-Core1）。

鉛筆アイコンで示された「設定」をクリックして、テンプレートの設定を入力します。PoE スケジュールテンプレートでは、次の項目を設定できます。

- Power Supply Schedule

Template Edit - Power supply schedule : Template_2

	Day	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
<input type="checkbox"/>	Sun	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Mon	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Tue	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Wed	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Thu	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Fri	<input checked="" type="checkbox"/>																							
<input type="checkbox"/>	Sat	<input checked="" type="checkbox"/>																							

- Apply to : バンド、チャンネル幅、送信電力など

Apply to

Refresh

Switch Name ▼

<input type="checkbox"/>	Port	PoE Mode	Connected Device	<input type="checkbox"/>	Port	PoE Mode	Connected Device
<input type="checkbox"/>	1			<input type="checkbox"/>	13		
<input type="checkbox"/>	2			<input type="checkbox"/>	14		
<input type="checkbox"/>	3			<input type="checkbox"/>	15		
<input type="checkbox"/>	4			<input type="checkbox"/>	16		
<input type="checkbox"/>	5			<input type="checkbox"/>	17		
<input type="checkbox"/>	6			<input type="checkbox"/>	18		
<input type="checkbox"/>	7			<input type="checkbox"/>	19		
<input type="checkbox"/>	8			<input type="checkbox"/>	20		
<input type="checkbox"/>	9			<input type="checkbox"/>	21		
<input type="checkbox"/>	10			<input type="checkbox"/>	22		
<input type="checkbox"/>	11			<input type="checkbox"/>	23		
<input type="checkbox"/>	12			<input type="checkbox"/>	24		

既存の管理対象スイッチがオンラインで、新しく追加したスイッチに同じ設定を適用する場合は、Copy Settings From のドロップダウンリストから選択し、Apply をクリックします。

管理者が参照できるように、Remark セクションに追加の備考を追加できます。

c) Backup Configuration

このリストには、バックアップされた設定の概要が表示されます。管理者は、復元用に設定ファイルをダウンロードできます。または、チェックボックスにチェックを入れて、選択した設定ファイルを削除します。

Backup Configuration

Delete

<input type="checkbox"/>	Device Type	Size	Backup time	File Name	Action
--------------------------	-------------	------	-------------	-----------	--------

E.Network

Network : このセクションは、すべてのネットワーク設定を設定するために使用されます。

1) NAT

NAT 機能は、次の 3 種類のネットワークアドレス変換をサポートします。DMZ (Demilitarized Zone)、Public Accessible Server、IP/Port Forwarding です。

Demilitarized Zone

DMZ (Demilitarized Zone)

WAN Assignment
Select this function to assign the WAN1 IP of the system as the External IP Address. This feature is designed for PPPoE or Dynamic WAN when the External IP Address changes as the WAN1 IP Address changes.

Assign WAN IP automatically

External Interface: WAN1
External IP Address: 10.30.40.45
Internal IP Address:
Remark:

Static Assignments

No.	External IP Address	External Interface	Internal IP Address	Remark
1	<input type="text"/>	WAN1 ▼	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	WAN1 ▼	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	WAN1 ▼	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	WAN1 ▼	<input type="text"/>	<input type="text"/>

システムは、静的割り当てで、内部 IP アドレス (LAN) から外部 IP アドレス (WAN) へのマッピングの特定のセットをサポートします。WAN IP 自動割り当ての外部 IP アドレスは、WAN1 インターフェースが動的である場合に動的に変更される外部インターフェース (WAN1) の IP アドレスです。**Assign WAN IP Automatically** (WAN IP を自動的に割り当てる) をオンにすると、入力した内部 IP アドレスが WAN1 インターフェースにバインドされます。各 **Static Assignment** (静的割り当て) は、選択した外部インターフェース (WAN1 または WAN2) にバインドできます。使用できる静的 **Internal IP Address** (内部 IP アドレス) と **External IP Address** (外部 IP アドレス) のセットがあります。**Internal IP Address** (内部 IP アドレス) と **External IP Address** (外部 IP アドレス) はセットとして入力されます。セットアップ後、WAN へのアクセスは、内部 IP アドレスにアクセスするためにマッピングされます。これらの設定は、**Apply** ボタンをクリックするとすぐに有効になります。

Public Accessible Servers

Public Accessible Server

Enable	No.	External Port	Local Server IP Address	Local Server Port	Type	Remark
<input type="checkbox"/>	1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
<input type="checkbox"/>	10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>

Public Accessible Servers を使用すると、管理者は仮想サーバーを設定できます。これにより、管理対象ネットワーク外のクライアントデバイスが、管理対象ネットワーク内のこれらのサーバーにアクセスできるようになります。一般に、TCP サービスや UDP サービスなど、物理サービスの異なるセットに対して、異なる仮想サーバーを構成できます。「**External Service Port**」(外部サービスポート)、「**Local Server IP Address**」、「**Local Server Port**」を入力してください。サービスの種類として「**TCP**」または「**UDP**」を選択します。**Enable** 列で、有効にするサーバーをチェックします。これらの設定は、**Apply** ボタンをクリックするとすぐに有効になります。

Port & IP Forwarding

Port and IP Forwarding

No.	Destination		Translated to Destination		Type	Remark
	IP Address	Port	IP Address	Port		
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>

この機能により、管理者はリダイレクトの目的で IP アドレスの特定のセットを設定できます。ユーザーがここに記載されている宛先 IP アドレスに接続しようとする、接続パケットが変換され、対応する宛先にリダイレクトされます。**Destination** (宛先) の「**IP Address**」と「**Port**」、**Translated to Destination** (変換先) の「**IP Address**」と「**Port**」を入力してください。サービスの種類として「**TCP**」または「**UDP**」を選択します。これらの設定は、**Apply** をクリックするとすぐに有効になります。

2) Monitor IP

監視 IP 機能では、複数の IP アドレスを定義できます。システムは、これらの IP ベースのネットワークデバイスを監視し、設定可能な間隔に基づいて電子メールを介して定期的にオンラインステータスを報告することができます。これらの監視対象デバイスには、HTTP または HTTPS 接続を介してアクセスできます。監視対象デバイスの管理インターフェースは、システムが NAT モードで動作しているときに、デバイスの IP アドレスのハイパーリンクを介してアクセスできます。

Monitor IP List

Monitor Now

No.	Protocol	IP Address	Hyperlink	Remark
1	http ▾	192.168.1.1	Delete	<input type="text"/>
2	http ▾	<input type="text"/>	Create	<input type="text"/>
3	http ▾	<input type="text"/>	Create	<input type="text"/>

3) Walled Garden and Walled Garden Ad

この機能は、ユーザーがログインと認証の前にここにリストされているウェブサイトアクセスするための特定の無料サービスを提供します。このリストでは、ウェブサイトの特定のアドレスまたはドメイン名を定義できます。ネットワークアクセス権を持たないユーザーは、実際のネットワークサービスを無料で体験することができます。リストにウェブサイトの **IP アドレス** または **ドメイン名** を入力し、**Apply** をクリックして設定を保存します。ウォールド・ガーデンリストは、バックアップまたは復元できます。

Walled Garden List

200 entries can be added to the Walled Garden List.
40 advertisement entries can be displayed on the user login page.

<input type="checkbox"/>	No.	Domain Name/IP Address/URL	Walled Garden / Advertisement
(Total:0/200) First Prev Next Last Go to Page <input type="text" value=""/> (Page:1/1) Row per Page: <input type="text" value="50"/>			

Walled Garden Advertisements は、クライアントがシステムによって認証される前にアクセスするための広告リンクです。例えば、ホテルにネットワークアクセス権がないゲストは、これらのサイトを無料で訪問することができます。

システムは、最大 200 個のウォールド・ガーデンエントリをサポートし、200 個のうち 40 個をウォールド・ガーデンの広告として選択することができます。

Add Walled Garden List

Domain Name/IP Address/URL: <input type="text"/>	
Walled Garden	Advertisement
Active: <input type="checkbox"/>	Display: <input type="checkbox"/>
Service Zone: All <input type="text"/>	Protocol: http <input type="text"/>
Remark: <input type="text"/>	Topic: <input type="text"/>
	Description: <input type="text"/>

- **Add** をクリックして、新しいエントリを追加します。Domain Name/IP Address/URL（ドメイン名/IP アドレス/URL）を入力し、「Active」チェックボックスを選択します。**Apply** をクリックすると、項目が追加され、リストに表示されます。
- **Display** : **Display** を選択すると、サービスゾーン設定に対応するログインページに広告リンクが表示されます。

ウォールド・ガーデンの広告として選択したエントリは URL である必要があります。また、接頭辞を持つ IP アドレスにすることはできません。

ウォールド・ガーデンの広告機能を有効にするには、ウォールド・ガーデンと広告チェックの両方のチェックボックスにチェックを入れる必要があります。

4) VPN

このタブでは、システム上で2種類のVPNを使用できます。Remote VPN（リモートVPN）、およびSite-to-Site VPN（サイト間VPN）です。Remote VPN（リモートVPN）の場合、システムは、リモートクライアントとシステム間のVPNトンネルで、IKEv2を介したデータ転送を暗号化できるようにします。Site-to-Site VPN（サイト間VPN）の場合、IPSecトンネルを使用して、インターネット経由で他のIPSec対応デバイスに接続できます。

Remote VPN IKEv2

Function

Enable Disable

Allocate IP Address from

IP Address * Subnet Mask

Certificate

Default CERT ▼

WISPr

Authentication Options

Auth Option	Auth Database	Postfix	Enable
Server 1	LOCAL	local	<input type="checkbox"/>
Server 2	RADIUS	.	<input type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="checkbox"/>
Server 4	LDAP	ldap	<input type="checkbox"/>
Server 5	POP3	pop3	<input type="checkbox"/>

Site-to-Site VPN

Local Sites

<input type="checkbox"/>	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
--------------------------	-----	-------------------	-----------------	--------------------	--------------------	---------------

Remote Sites

<input type="checkbox"/>	No.	Name	IP Address	Pre-shared Key
--------------------------	-----	------	------------	----------------

5) Proxy Server

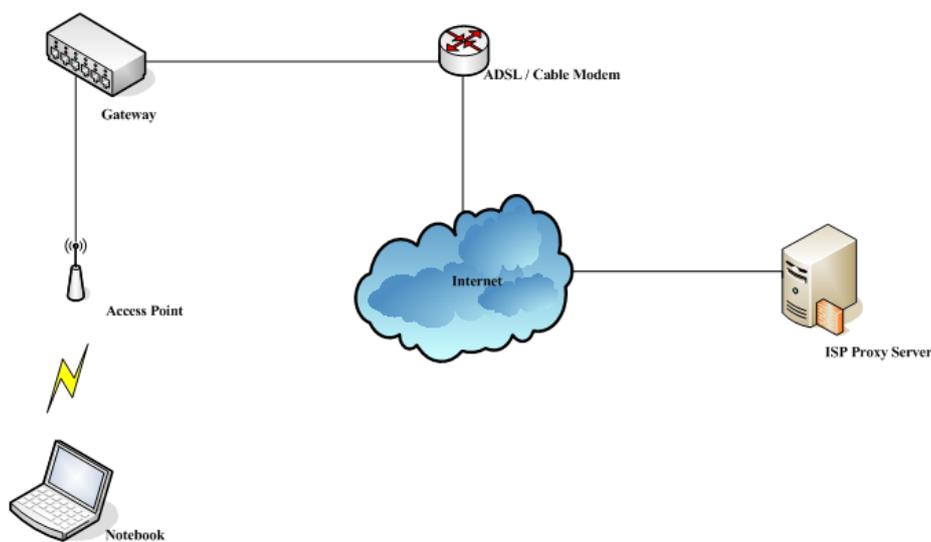
システムは、組み込みプロキシサーバーと外部プロキシサーバー機能を提供します。認証が成功すると、クライアントは目的のプロキシサーバーに戻ります。

基本的に、プロキシサーバーは、クライアントがネットワークリソースにすばやくアクセスするのに役立ちます。このセクションでは、EWS コントローラのプロキシサーバー設定を設定する基本的な例を示します。



■ インターネットプロキシサーバーの使用

コントローラに内蔵されたプロキシサーバーは、LAN 環境の外側またはインターネットに配置されたプロキシサーバーであっても、有効にすることができます。例えば、次の図は、ISP のプロキシサーバーの使用方法を示しています。



次の手順に従って、プロキシ設定を完了してください。

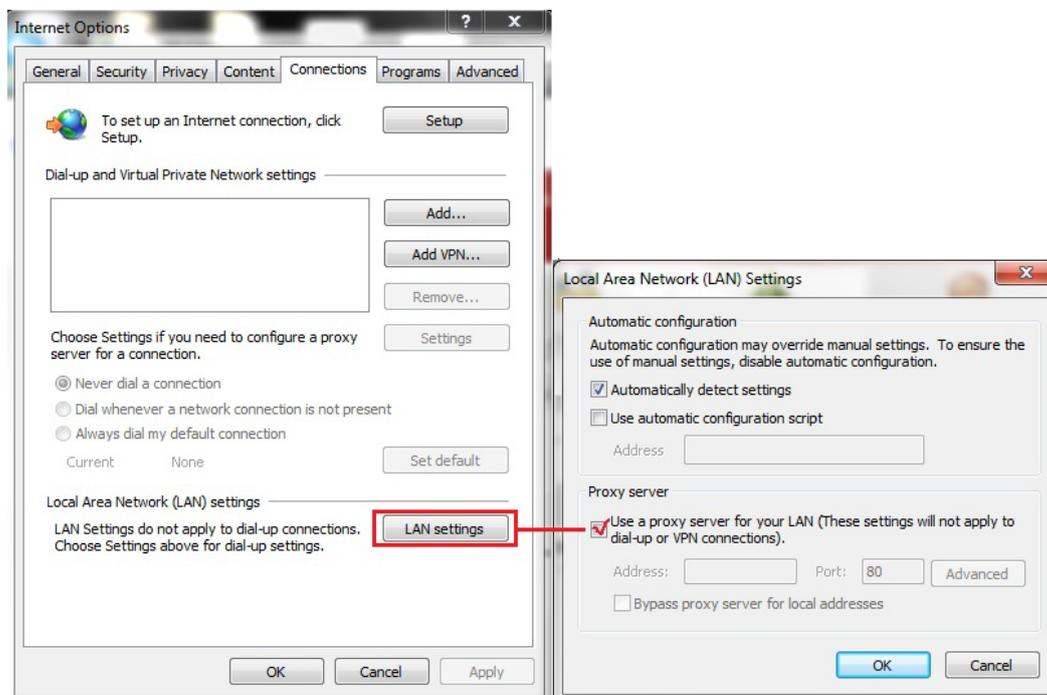
ステップ1 *admin* アカウントを使用してシステムにログインします。

ステップ2 *Network >> Proxy Server >> Web Proxy Settings* ページの順に選択します。

Built-in Proxy Server (組み込みプロキシサーバー) を有効にします。 **Apply** をクリックして設定を保存します。



ステップ3 クライアントステーションの Internet Options でプロキシサーバー設定を有効にします。



組み込みプロキシサーバーを有効にすると、すべてのトラフィックがコントローラ上のローカルのプロキシサーバーに転送されます。

外部プロキシサーバーの使用

外部プロキシサーバーを指定するには、「External」オプションを選択し、プロキシサーバーの適切な IP アドレスと使用ポートを入力します。

次の手順に従って、プロキシ設定を完了してください。

ステップ1 *admin* アカウントを使用してシステムにログインします。

ステップ2 **Network >> Proxy Server >> Web Proxy Settings** の順に選択します。Proxy Server で **External** (外部) を選択します。

プロキシサーバーの IP アドレスとポート番号を External Proxy Servers (外部プロキシサーバー) 設定に追加します。**Apply** をクリックして設定を保存します。

Web Proxy Settings

Proxy Server Enable Built-in Disable Built-in External

External Proxy Server External Proxy

External Proxy Port

ステップ3 クライアントステーションの Internet Options でプロキシサーバー設定を有効にします。

メモ

プロキシサーバーを有効にすると、クライアントはクライアントステーションの Internet Options でプロキシサーバー設定を手動で確認する必要があります。透過プロキシを適用するには、IP/Port Forwarding を使用してください。

6) Local DNS Record

管理者は、EWS コントローラの LAN ネットワークに接続されているすべてのクライアントに対して、IP マッピングにドメイン名を静的に割り当てることができます。この機能を使用すると、特定のドメイン名の優先 IP アドレスにクライアントをディスパッチできます。

Local DNS Records Configuration

DNS time-to-live seconds *(1~604800, i.e. up to 7 days)
The entered time span is the limit for lifetime of data in the network.

Local DNS Record List (Total: 100)

No.	IP Address	Domain Name
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>

7) Dynamic Routing

この機能は、次の3つの動的ルーティングプロトコルをサポートします。RIP、OSPF、およびIS-ISです。

- ISIS 設定**：これは、コンピュータネットワーク、物理的に接続されたコンピュータまたは類似のデバイスのグループ内で効率的に情報を移動するように設計されたルーティングプロトコルです。各インターフェースの回線タイプは、レベル1またはレベル2に設定できます。

Function

 Enable Disable

Setup Table

Configuration

Net ID

Router Level

Level 1 ▾

Interface	Status	Circuit Type
WAN1	Enabled	Level 1 ▾
WAN2	Disabled	Level 1 ▾
Default	Enabled	Level 1 ▾
SZ1	Disabled	Level 1 ▾
SZ2	Disabled	Level 1 ▾
SZ3	Disabled	Level 1 ▾
SZ4	Disabled	Level 1 ▾
SZ5	Disabled	Level 1 ▾
SZ6	Disabled	Level 1 ▾
SZ7	Disabled	Level 1 ▾
SZ8	Disabled	Level 1 ▾

- Net ID : これは、ISO アドレスのネットワークエンティティタイトル (NET) です。NET は IP アドレスと同じように、インターネットワーク上のルータを一意に識別するために使用されます。
- Route Level : Level 1 のシステムは、エリア内でルーティングされます。目的地がエリア外にある場合、Level 2 のシステムに向かってルーティングされます。Level 2 の中間システムは、エリア間や他のルーティングドメインに向かってルーティングします。各ネットワークインターフェースのレベルタイプを割り当てることができます。
- **OSPF 設定** : これは、インターネットプロトコル (IP) ネットワークのための適応型ルーティングプロトコルです。各インターフェースのエリア、スタブと認証を設定することができます。

OSPF

Function Enable Disable

Setup Table

Interface	Status	Area	Stub	Authentication
WAN1	Enabled	<input type="text"/>	<input type="checkbox"/>	None ▾
WAN2	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
Default	Enabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ1	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ2	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ3	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ4	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ5	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ6	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ7	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾
SZ8	Disabled	<input type="text"/>	<input type="checkbox"/>	None ▾

Advertise as default gateway
 Advertise Global Policy Route
 Re-distribute RIP

- Area : エリアとは、管理上グループ化されたルーティングドメイン内のネットワークとホストのセットです。Area 0 は、バックボーンエリアと呼ばれ、階層の最上位レベルにあり、非バックボーンエリア（番号 1、2）への接続を提供します。
- Stub : AS 外部広告がフラッディングされないエリアです。
- Authentication : OSPF ネイバーの認証を許可します。認証方式の「none」は、OSPF に認証が使用されないことを意味し、これがデフォルトの方式です。MD5 認証では、MD5 パスワードを入力します。パスワードはネットワークを通過しません。
- Advertise as Default Gateway : このコントローラがデフォルトゲートウェイであることを近隣ノードに通知します。
- Advertise Global Policy Route : このコントローラのグローバルポリシールート在近隣ノードに通知します。
- Redistribute RIP : このオプションをオンにすると、OSPF を使用して RIP 経由で取得したルーティング情報を配信できるようになります。

- **OSPF v3 設定 : IPv6 dynamic routing configuration**

OSPF v3

Function Enable Disable

Setup Table

Interface	Status	Area
WAN	Disabled	<input type="text"/>
Default	Enabled	<input type="text"/>
SZ1	Disabled	<input type="text"/>
SZ2	Disabled	<input type="text"/>
SZ3	Disabled	<input type="text"/>
SZ4	Disabled	<input type="text"/>
SZ5	Disabled	<input type="text"/>
SZ6	Disabled	<input type="text"/>
SZ7	Disabled	<input type="text"/>
SZ8	Disabled	<input type="text"/>

Advertise Global Policy Route

- RIP 設定** : これは、ローカルおよびワイドエリアネットワークで使用される動的ルーティングプロトコルです。各インターフェースをパッシブバージョンまたはサポートバージョン、および認証に設定できます。

RIP

Function Enable Disable

Setup Table

Status	Passive	Version	Authentication
WAN1 Enabled	<input type="checkbox"/>	Both ▾	None ▾
WAN2 Disabled	<input type="checkbox"/>	Both ▾	None ▾
Default Enabled	<input type="checkbox"/>	Both ▾	None ▾
SZ1 Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ2 Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ3 Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ4 Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ5 Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ6 Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ7 Disabled	<input type="checkbox"/>	Both ▾	None ▾
SZ8 Disabled	<input type="checkbox"/>	Both ▾	None ▾

Advertise as default gateway
 Advertise Global Policy Route
 Re-distribute OSPF

RIP Timer

Update timer: * (30~600 seconds)

Timeout timer: * (30~600 seconds)

Garbage collect timer: * (30~600 seconds)

- **Passive** : RIP パケットは、パッシブとしてチェックされている場合、ネットワークインターフェースから送信されません。
- **Version** : このインターフェースの RIP バージョンを選択します。RIPv1 はブロードキャストを使用して RIP パケットを配信し、RIPv2 はマルチキャストを使用して RIP パケットを配信します。どちらもブロードキャストとマルチキャストを使用します。
- **Authentication** : RIP ネイバーの認証を許可します。認証方式の「none」は、RIP に認証が使用されないことを意味し、これがデフォルトの方式です。RIP 認証が有効になっているインターフェースでの認証には、プレーンテキスト認証と MD5 認証の 2 つのモードがあります。
- **Advertise as Default Gateway** : このコントローラがデフォルトゲートウェイであることを近隣ノードに通知します。
- **Advertise Global Policy Route** : このコントローラのグローバルポリシールートを実近隣ノードに通知します。
- **Redistribute OSPF** : このオプションをオンにすると、RIP を使用して OSPF 経由で取得したルーティング情報を配信できるようになります。
- **RIP Timer** :
 - ◆ **Update timer** : システムがルーティング情報の即時更新を要求する時間を秒単位で指定します。
 - ◆ **Timeout Timer** : ルートは、限られた時間だけルーティングテーブルに保持されます。ルーティングテーブルにルートがインストールされるたびに、特別なタイムアウトタイマーが開始されます。ルータが、そのルートに関する情報を含む別の *RIP* 応答を受信すると、そのルートは「リフレッシュ」と見なされ、タイムアウトタイマーがリセットされます。このタイマーが期限切れになると、ルートは無効としてマークされます。
 - ◆ **Garbage Collection Timer** : ルーティングテーブルから無効なルートを消去するまでの時間を秒単位で指定します。

8) DDNS

この機能を有効にする前に、動的 DNS ホスト名を動的 DNS プロバイダに登録しておく必要があります。EWS コントローラは、WAN ポートの動的 IP アドレスから静的ドメイン名へのエイリアスを作成する DNS 機能をサポートしており、管理者は EWS コントローラの WAN に簡単にアクセスできます。動的 DHCP が WAN ポートでアクティブ化されると、DNS サーバーの IP アドレスが定期的に更新されます。これらの設定は、**Apply** をクリックするとすぐに有効になります。

Dynamic DNS

DDNS Enable Disable

Provider DynDNS.org(Dynamic) ▼

Host Name

Username/E-mail admin

Password/Key ●●●●

- **DDNS** : この機能を有効または無効にします。
- **Provider** : DNS プロバイダを選択します。
- **Host name** : WAN ポートの IP アドレス/ドメイン名です。
- **Username/E-mail** : DNS プロバイダの登録 ID (ユーザー名または電子メール) です。
- **Password/Key** : DNS プロバイダの登録パスワードです。

9) Client Mobility

- **IP PNP** : この機能を有効にすると、静的/DHCP IP、DNS、ゲートウェイを持つデバイスがコントローラからインターネットにアクセスできるようになります。
- **Cross Gateway Roaming** : このゲートウェイを **Master** または **Slave** に設定します。 **Master** モードでは、 **Slave IP** と **Secret Key** (秘密キー) も入力する必要があります。 **Slave** モードでは、 **Master IP** と **Key** を入力します。
 - **Master Node** : マスターノードの設定では、1つのマスターが最大 15 個のスレーブノードの設定を有効にすることができます。

Cross Gateway Roaming

Mode Disable Master Mode Slave Mode

Status

Slave Nodes Setting	No.	Active	Remote IP Address*	Secret Key*	Remark
	1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

- **Slave Node** : スレーブノードの設定では、マスターノードの設定を入力します。

Cross Gateway Roaming

Mode

Disable Master Mode Slave Mode

Status

[Node List](#)

Master Node Setting

Remote IP Address

*

Secret Key

*

Remark

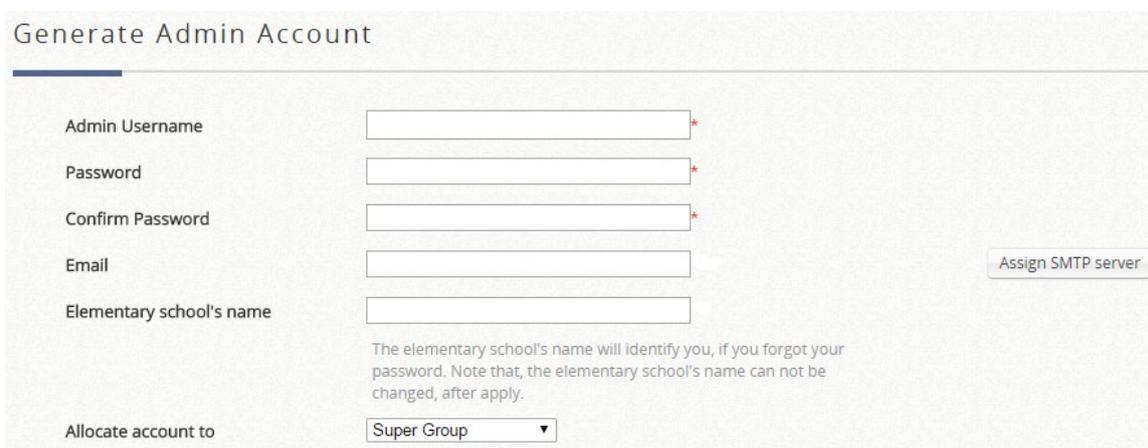
F.Utilities

Utilities : このセクションでは、アカウントの変更、システムのバックアップ/復元、ファームウェアのアップグレード、サービスの再始動、ネットワークユーティリティ、および証明書の機能を提供します。

1) Administrator Account

これは、管理者アカウントの作成、編集、削除、および確認に使用できます。

管理者のログインアカウントは「admin」です。システムの管理者パスワードは、管理者名をクリックし、元のパスワードと新しいパスワードを入力することで変更できます。システムのデフォルトの管理者パスワードは「admin」です。Elementary School's Name（小学校名）フィールドは、管理者のユーザー名またはパスワードを忘れた場合に備えて、セキュリティのために入力することもできます。Email と Elementary School's Name（小学校名）は両方とも空欄にするか、または両方とも記入する必要があります。ことに注意してください。



Generate Admin Account

Admin Username

Password

Confirm Password

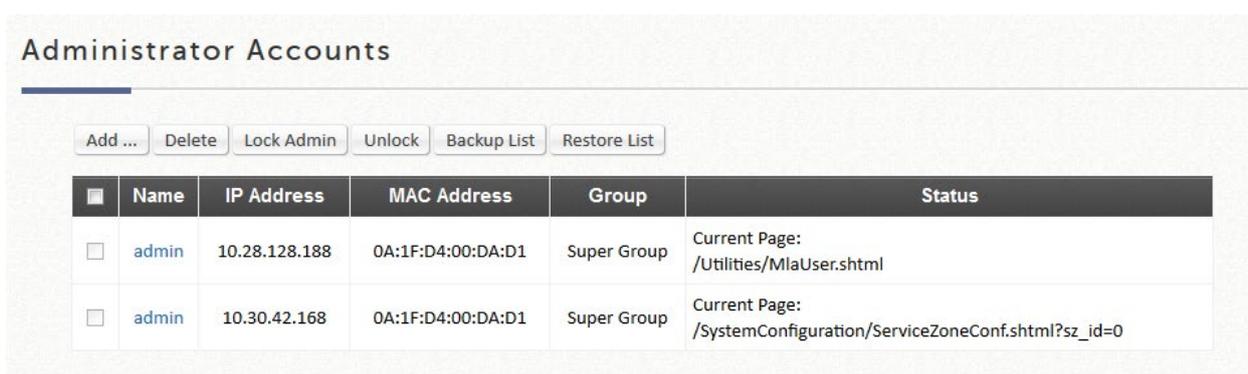
Email

Elementary school's name

The elementary school's name will identify you, if you forgot your password. Note that, the elementary school's name can not be changed, after apply.

Allocate account to

また、管理者は、異なる権限を持つ他の管理者アカウントを作成することもできます。



Administrator Accounts

	Name	IP Address	MAC Address	Group	Status
<input type="checkbox"/>	admin	10.28.128.188	0A:1F:D4:00:DA:D1	Super Group	Current Page: /Utilities/MlaUser.shtml
<input type="checkbox"/>	admin	10.30.42.168	0A:1F:D4:00:DA:D1	Super Group	Current Page: /SystemConfiguration/ServiceZoneConf.shtml?sz_id=0

管理者は、自分のパスワードを変更したり、管理責任を取るために管理者リストにアカウントを追加したりする権限を持っています。

General Settings

Password Complexity	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Min Password Length <input type="text" value="2"/> * (2~20)
	Min Password Category <input type="text" value="2"/> * (2~4)
Limit Login Attempts	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Block access after <input type="text" value="5"/> * tries
Password Expiration	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Password expires <input type="text" value="90"/> * day(s) after creation
Password Limits	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
	Users to choose passwords different from their past <input type="text" value="6"/> * passwords
Access Permission	<input type="button" value="Configure"/>

- **Password Complexity** により、管理者は、サブ管理者が使用するパスワードをどのように形成するかを制限できます。

Min password Length は、パスワード文字列の最小長に制限を設定します。

Min password Category を使用すると、管理者はサブ管理者のパスワードが必要とされる複雑さを定義できます。以下は、それぞれの数字が何を表しているかを示しています。

数字	定義
0	パスワードはチェックされません
1	パスワードには、少なくとも 1 つの形式（大文字/小文字/数字/特殊文字）を含める必要があります
2	パスワードには少なくとも 2 つの形式を含める必要があります
3	パスワードには、少なくとも 3 つの形式を含める必要があります
4	パスワードには少なくとも 4 つの形式を含める必要があります

- **Limit Login Attempts (有効な場合)** : サブ管理者がパスワードを再試行できる回数を入力します。この数以上を試行した場合、サブ管理者は再度文字列を入力することができません。
- **Password expiration (有効な場合)** : 管理者がパスワードの有効期限日数を決定する機能です。最初のログインから数えて、各パスワードに対して有効な期間を定義できます。パスワードの有効期限が切れると、オペレータは将来の使用のために新しいパスワードを設定する必要があります。期限切れのパスワードは再利用できません。
- **Password Limits (有効な場合)** : 過去に使用されたパスワードを確認する数を決定します。例えば、管理者が「5」を入力した場合、システムは新しく追加されたパスワードが最新の 5 つのパスワードとどうかをチェックします。もし同じであれば、サーバーは管理者に新しいパスワード文字列を再度選択するように要求します。

■ サブ管理者の作成

Generate Admin Account

Admin Username	<input type="text"/>	*
Password	<input type="password"/>	*
Confirm Password	<input type="password"/>	*
Email	<input type="text"/>	*
Elementary school's name	<input type="text"/>	*

The elementary school's name will identify you, if you forgot your password. Note that, the elementary school's name can not be changed, after apply.

Allocate account to

Generate 表に移動して、サブ管理者を作成し、権限制限を定義します。管理者がパスワードを忘れた場合、Email と Elementary School Name（小学校名）の両方を入力することで、アカウント資格情報が割り当てられたメールアドレス宛てにメールされます。システムが電子メールリマインダーを送信するには、SMTP サーバーを設定する必要があります。

Send Password

Username	<input type="text"/>
Elementary school's name	<input type="text"/>

サブ管理者は、Super Group、Manager、Operator、On-Demand Manager、Custom1、Custom2、Custom3 の6つのカテゴリに分類できます。ドロップダウンリストの右側にある configure をクリックして、相違点を表示および変更します。「Super Group」の権限制限は変更できないことに注意してください。設定が完了したら、Apply ボタンを押して、リストにアカウントを作成します。

Select Group

Note: Left checkbox means Read-Write, right checkbox means Read-Only.

Permission Settings

Service Zone	<input type="checkbox"/> <input type="checkbox"/> Select All <input type="checkbox"/> <input type="checkbox"/> Default <input type="checkbox"/> <input type="checkbox"/> SZ1 <input type="checkbox"/> <input type="checkbox"/> SZ2 <input type="checkbox"/> <input type="checkbox"/> SZ3 <input type="checkbox"/> <input type="checkbox"/> SZ4 <input type="checkbox"/> <input type="checkbox"/> SZ5 <input type="checkbox"/> <input type="checkbox"/> SZ6 <input type="checkbox"/> <input type="checkbox"/> SZ7 <input type="checkbox"/> <input type="checkbox"/> SZ8
Map	<input type="checkbox"/> <input type="checkbox"/> Select All <input type="checkbox"/> <input type="checkbox"/> Overview <input type="checkbox"/> <input type="checkbox"/> EL
AP Management	<input type="checkbox"/> <input type="checkbox"/> Select All <input type="checkbox"/> <input type="checkbox"/> Local Area AP Management <input type="checkbox"/> <input type="checkbox"/> Wide Area AP Management

- **The admin list** は、管理者がオンライン管理者の数と各サブ管理者の状態など、各管理アカウントの活動状態を追跡するためのリストとして機能します。

Administrator Accounts

<input type="checkbox"/>	Name	IP Address	MAC Address	Group	Status
<input type="checkbox"/>	admin	10.28.128.188	0A:1F:D4:00:DA:D1	Super Group	Current Page: /Utilities/MlaUser.shtml
<input type="checkbox"/>	admin	10.30.42.168	0A:1F:D4:00:DA:D1	Super Group	Current Page: /SystemConfiguration/ServiceZoneConf.shtml?sz_id=0

削除できるのは作成されたサブ管理者のみであることに注意してください。チェックボックスにチェックを入れて、特定のサブ管理者が管理ページにアクセスすることを禁止することに対して「Lock」または「Unlock」（ロック解除）します。また、管理者は、「name」列のハイパーリンクをクリックして、管理者/サブ管理者の関連設定を編集することもできます。

2) Backup & Restore

これは、システム設定のバックアップと復元に使用されます。システムの工場出荷時のデフォルトに戻すこともできます。

Backup System

General Backup Backup

Period Backup Configure

Restore System

Restore System Settings 選擇檔案 未選擇任何檔案

- Keep WAN1 setting.
- Keep Management IP Address List.
- Keep LAN, Alias, DHCP setting and Management Service Zone List.
- Keep Certificates.
- Keep Local Area AP Management setting.
- Keep Wide Area AP Management setting.
- Keep Internal Authentication Server accounts.

Restore

Reset to Default

Reset to Factory Default Reset

General Backup の下の **Backup** ボタンをクリックして、現在のシステム構成を管理コンソールのローカルディスク上のバックアップファイルに保存します。バックアップファイルは、現在のシステム設定とローカルユーザーアカウントを保持します。

バックアップファイルをシステムに復元するには、**Browse** ボタンをクリックしてバックアップファイルを選択し、**Restore** ボタンをクリックしてプロセスを実行します。

バックアップは FTP 経由で定期的に行うことができます。この機能を有効にするには、Period Backup の下の **Configure** ボタンをクリックします。

Period Backup System Settings

Primary FTP Status Enable Disable

Primary FTP Folder

Secondary FTP Status Enable Disable

Secondary FTP Folder

Period :

- **Restore System Settings** : **Browse** をクリックして、コントローラによって作成された.db データベースバックアップファイルを検索し、**Restore** をクリックして、バックアップファイルを保存した時点と同じ設定に復元します。「Keep WAN1 setting and Management IP Address List」オプションを選択すると、リモートアクセス用の WAN1 設定を保持できます。
- **Reset to Factory Default** : **Reset** をクリックして、コントローラの工場出荷時のデフォルト設定を読み込みます。

3) Certificates

このタブでは、管理者は、システム証明書の管理、ルート CA の作成、ルート CA からの証明書の署名、および証明書のアップロードを行うことができます。「Used By」列には、現在使用中の証明書とそれに対応するアプリケーションが表示されます。さまざまな種類の証明書をさらに構成するには、「鉛筆」アイコンをクリックします。

Certificate Management

Cert Name	Common Name	Used by
System Certificate 		
Default Certificate	CN=mknhhi.example.com	WEB Server, Built-in RADIUS, CAPWAP
Internal Root CA 		
Internal Root CA	N/A	
Internally Issued Certificate 		
N/A	N/A	
Trusted Certificate Authorities (CA) 		
N/A	N/A	

- **System Certificate**

これは、システムを識別する証明書です。これらの証明書は、HTTPS ログイン、CAPWAP などのアプリケーションに使用できます。コントローラには、削除できない出荷時デフォルト証明書 (gateway.example.com) が組み込まれていますが、証明書のアップロードは許可されています。「Regenerate」(再生成) ボタンをクリックすると、固有の CN を持つ新しいデフォルト証明書が作成されます。証明書の詳細を表示するには、対応する View (表示) ボタンをクリックしてください。証明書と公開キーをローカルディスクにダウンロードするには、「Get CERT」(証明書を取得する) と「Get Key」(キーを取得する) をクリックしてください。

System Certificate

Cert Name	Common Name	Operation
Factory Default Certificate		
Factory Default Certificate	CN=gateway.example.com	<input type="button" value="View"/> <input type="button" value="Regenerate"/>
Internally Issued Certificate		
N/A	N/A	<input type="button" value="View"/> <input type="button" value="Delete"/>
Uploaded Certificate		
N/A	N/A	<input type="button" value="View"/> <input type="button" value="Delete"/> <input type="button" value="Upload Intermediate/Root CA"/> <input type="button" value="Verify"/>

Upload System Certificate

Certificate 未選擇任何檔案
 Private Key 未選擇任何檔案
 Intermediate CA 未選擇任何檔案

■ Internal Root CA

管理者は、プライベート用にルート CA を生成することができます。作成されたルート CA 証明書をダウンロードして、システムによって生成された証明書に署名するために使用できます。システムでは、内部ルート CA を 1 つしか作成できないことに注意してください。

Internal Root CA

Cert Name	Common Name	Operation
Internal Root CA		
N/A	N/A	<input type="button" value="View"/> <input type="button" value="Delete"/>

Generate Root CA

Common Name
 Email Address
 Country Name
 State or Province Name
 Locality Name
 Organization Name
 Organization Unit Name
 Key Type
 Key Length

Upload Root CA

Certificate
 Private Key

ルート CA 証明書は、一致する秘密キーを使用してアップロードすることもできます。

- **Internally Issued Certificates**

内部ルート CA を作成する必要がある場合は、内部発行の証明書に署名できます。



Cert Name	Common Name	Operation
Internally Issued Certificate		
N/A	N/A	View Delete

Use Internal Root CA to generate certificate

You must Create Root CA First.

生成された証明書が一覧表示され、証明書/キーのペアは、**View** の **Get Cert**、**Get key** でダウンロードできます。

- **Trusted Certificate Authorities**

自己署名証明書とシステムのルート CA とは別に、管理者は、他の CA エンティティまたは信頼できる CA によって署名された他の証明書をシステムにアップロードすることもできます。これらの信頼できるルート CA 証明書は、コントローラが外部支払いゲートウェイおよび/または CAPWAP 対応 AP の証明書を認識し、信頼するためのものです。

信頼できる CA をアップロードするには、**browse** をクリックして、信頼できる CA 証明書をローカルディスクからシステムにアップロードしてください。



Cert Name	Common Name	Operation
Certificate Authorities (CA)		
N/A	N/A	View Delete

Upload Trusted CAs

Certificate [Browse...](#)

[Upload Files](#)

4) Network Utilities

Web ベースの Ping、トレースルート、ARP テーブルなどの一部のネットワークユーティリティは、システムでサポートされています。

Network Utilities

Type IPv4 IPv6 Sniff IP Discovery

Ping

Trace Route

ARPing Interface

VLAN ID

ARP Table

Status

Result

項目	説明
IPv4	<ul style="list-style-type: none">▪ Ping : 管理者が IP アドレスやホストドメイン名を使用してデバイスを検出し、それが生きているかどうかを確認することができます。▪ Trace Route : 管理者は、IP アドレスまたはホストドメイン名を使用して、ゲートウェイから宛先へのパケットの実際のパスを回復することができます。▪ ARPing : 管理者が特定の IP アドレスまたはドメイン名に対する ARP 要求を送信できるようにします。▪ ARP Table : 管理者は、アドレス解決プロトコル (ARP) で使用される、IP から物理アドレスへの変換表を表示できます。
IPv6	<ul style="list-style-type: none">▪ Ping : 管理者が IPv6 アドレスやホストドメイン名を使用してデバイスを検出し、それが生きているかどうかを確認することができます。▪ Trace Route 6 : 管理者は、IPv6 アドレスまたはホストドメイン名を使用して、ゲートウェイから宛先へのパケットの実際のパスを回復することができます。▪ Neighbor Discovery (近隣検出) : 管理者は、この機能を使用して、同じ IP セグメン

	トまたはドメイン名にある IPv6 近隣ノードを知ることができます。 <ul style="list-style-type: none"> ▪ Neighbor Cache (近隣キャッシュ) : 近隣キャッシュ内の近隣の情報を管理するノードです。この機能により、管理者はシステムの近隣キャッシュに格納されている情報を表示できます。
Sniff	この機能を使用すると、管理者は選択したインターフェースからのパケットをリッスンできます。管理者は、 Expression フィールドの tcpdump コマンドを使用して、キャプチャするパケットのタイプをさらにフィルタリングできます。
IP Discovery (IP 検出)	この機能を使用すると、コントローラは同じレイヤ 2 ネットワーク内で接続されている AP の IP アドレスを検出できます。管理者は、検出された AP の IP 設定を変更することもできます。
Status	管理者がネットワークユーティリティ機能を実行している場合、操作の状態がここに表示されます。
Result (結果)	操作結果が表示されます。

5) [Restart](#)

Restart ボタンをクリックして、システムを再始動します。システム Web 管理インターフェースに再度アクセスする前に、点滅タイマーが終了するまでお待ちください。

Restart

Restart the system in Mode

Reason for Restart :

6) [System Upgrade](#)

管理者は、ウェブサイトから最新のファームウェアをダウンロードし、ここでシステムをアップグレードすることができます。**Browse** をクリックしてファームウェアファイルを検索し、**Apply** をクリックしてファームウェアアップグレードを実行します。アップグレードプロセスが完了するまでに数分かかる場合があります。その後、新しいファームウェアをアクティブ化するためにシステムを再起動する必要があります。

FTP ファームウェアのアップグレードもオプションです。FTP サーバーの IP アドレス、FTP サーバーポート、および FTP アカウント名とパスワードを入力し、最後に、システムのアップグレードに使用する FTP サーバーに格納されている完全なファームウェアファイル名を指定してください。

システムファームウェアをアップグレードするには、**Browse** ボタンをクリックして新しいファームウェアファイルを選択し、**Apply** ボタンをクリックしてプロセスを実行します。ファームウェアのアップグレードが正常に完了した後、システムを再起動するよう管理者に通知する確認メッセージが表示されます。
(**ファームウェアのアップグレードには数分かかる場合がありますので、確認メッセージをお待ちください)

ファームウェアのアップグレード後に工場出荷時のデフォルトにリセットする前に、システムを再起動する必要があります。

Note: For better maintenance, we strongly recommend you backup system settings before upgrading firmware.

System Firmware Upgrade

Current Version	3.00.00		
Upload New Firmware	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Apply"/>
Upgrade Firmware Via FTP	Anonymous	<input checked="" type="radio"/> Yes <input type="radio"/> No	
	IP Address	<input type="text"/>	Port <input type="text"/>
	File Name	<input type="text" value="File Name or Dir/File Name"/>	
			<input type="button" value="Apply"/>

G.Status

Status : システムステータス、インターフェースステータス、ハードウェアステータス、ルーティングテーブル、オンラインユーザー、セッションリスト、ユーザーログ、および通知構成の設定に関する情報を提供します。

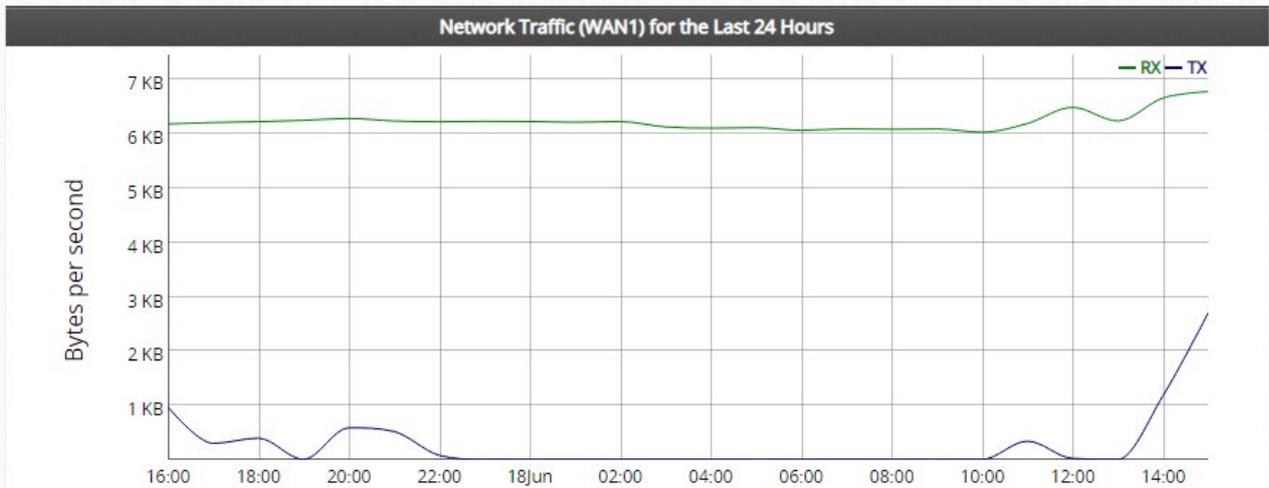
1) [System Summary](#)

システム上の現在の設定を表示します。

システムの概要は、管理者の参考のためにここに記載されています。

System Summary

[See Reports](#)



General			
System Name	EWS101	Firmware Version	3.45.0000
System Up Time	14 days, 23 hours, 27 min	Build Number	1.36-1.9737
System Time	2019/06/18 15:20:58 +0800	NTP Server	ntp1.pads.ufrj.br
Preferred DNS Server	8.8.8.8	Alternate DNS Server	N/A
Proxy Server	Disabled	APM Version	3.45.0000
SNMP	Enabled	Warning of Internet Disconnection	Disabled
Idle Timeout	10min	Traffic Direction for Idle Timeout	Uplink & Downlink
Num of Current Users	0	Num of Maximum Users	400

Report			
SYSLOG server 1		N/A:N/A	
SYSLOG server 2		N/A:N/A	
User Logs	Retained Days	30 days	
	Receiver E-mail Address(es)	N/A	
		N/A	

General			
System Name	システム名です。デフォルト名はモデル番号です。	Firmware Version	EWS コントローラの現在のファームウェアバージョンです
System Up Time	システムの動作時間を表示します。	Build Number	現在のビルド番号です。
System Time	ローカル時間はシステム時間として表示されます。	NTP Server	システムが整列するように設定されているネットワークタイムサーバーです。
Preferred DNS	優先 DNS サーバーの IP アドレス	Alternate DNS	代替 DNS サーバーの IP アドレス

Server	です。	Server	です。
Proxy Server	有効/無効/外部	APM Version	AP 管理モジュールのバージョンです。
WAN Failover	有効/無効	Load Balancing	有効/無効
SNMP	有効/無効	Warning of Internet Disconnection	有効/無効
Idle Timeout	アカウントが自動的に失効する前に、ユーザーがアクティブでないことを許可した分です。	Traffic Direction for Idle Timeout	アップリンク/アップリンク & ダウンリンク ユーザーのアクティビティ検査は、アップリンクトラフィックのみまたは両方向によってチェックされます。
Num of Current Users	現在のオンラインユーザー数です。	Num of Maximum Users	オンラインユーザーの最大数です。
Report			
Syslog server 1		外部 Syslog サーバーの IP アドレスとポート番号です。N/A は、設定されていないことを意味します。	
Syslog server 2		外部 Syslog サーバーの IP アドレスとポート番号です。N/A は、設定されていないことを意味します。	
User Logs	Retained Days	システムがユーザーの情報を保持する最大日数です。	
	Receiver Email Address (es)	トラフィック履歴またはユーザーのトラフィック履歴情報の送信先となる電子メールアドレスです。	

「See Reports」をクリックすると、インターフェース別にソートされた次のレポートが表示されます。ネットワークトラフィック、CPU 負荷、CPU 温度、メモリ使用量、ストレージ使用量、オンラインユーザー、ログイン成功、セッション、DHCP リース、DNS クエリが含まれます。また、時間範囲と間隔を選択することで、レポートを好みに合わせてカスタマイズすることもできます。これらのレポートは、電子メール、syslog、または FTP 経由で送信できます。

2) Interface

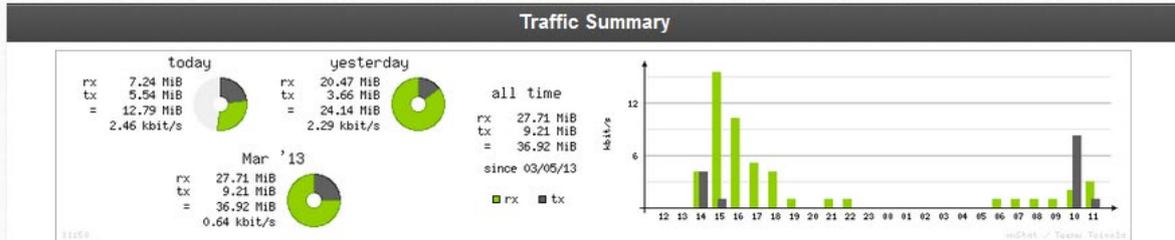
すべてのネットワークインターフェースの現在の設定を表示します。ドロップダウンメニューから Interface を選択してください。

各サービスゾーンは仮想システムを表します。したがって、システムのネットワークインターフェースの情報はサービスゾーン別にグループ化されます。

Select Interface **WAN1**

Network Interface

WAN1			
Mode	STATIC	IP Address	10.29.42.101
MAC Address	00:10:F3:23:D3:54	Subnet Mask	255.255.0.0
IPv6 Address	N/A	IPv6 Prefix	N/A
Auto-Negotiation	On	Speed / Duplex	100Mb/s Full



Daily Traffic

day	rx	tx	total	avg. rate
03/05/13	20.47 MiB	3.66 MiB	24.14 MiB	2.29 kbit/s
03/06/13	7.24 MiB	5.54 MiB	12.79 MiB	2.46 kbit/s
estimated	14 MiB	10 MiB	24 MiB	

Monthly Traffic

month	rx	tx	total	avg. rate
Mar '13	27.71 MiB	9.21 MiB	36.92 MiB	0.64 kbit/s
estimated	152 MiB	50 MiB	202 MiB	

Top 10 Traffic

#	day	rx	tx	total	avg. rate
1	03/05/13	20.47 MiB	3.66 MiB	24.14 MiB	2.29 kbit/s

項目	説明	
インターフェース (WAN1/WAN2)	Mode	このインターフェースの動作モードです。
	MAC Address	WAN ポートの MAC アドレスです。
	IP Address	WAN ポートの IPv4 アドレスです。
	Subnet Mask	WAN ポートのサブネットマスクです。
	IPv6 Address	選択したインターフェースの IPv6 アドレスです
	IPv6 Prefix	IPv6 アドレスの接頭辞です
	Auto-Negotiation	自動ネゴシエーションがオンの場合、システムはインターフェースに接続されたシステムとデバイスの両方がサポートする最高性能の伝送モード(速度/二重/フロー制御)を選択します。
	Speed/Duplex	選択したインターフェースの現在の速度と二重を表示します。
Traffic Summary	このインターフェースの TX レートと Rx レートの毎日、毎月、およびすべての時間のグラフィカルな概要を表示します。	
Daily Traffic	その日のトラフィック情報を表で表示します。	

Monthly Traffic		トラフィック情報を表で表示します。
Top 10 Traffic		その日のトラフィックのトップ 10 の記録を表示します。
サービスゾーン — Default、SZ1～SZ8	Mode	SZ の操作モードです。
	MAC Address	SZ の MAC アドレスです。
	IP Address	SZ の IP アドレスです。
	Subnet Mask	SZ のサブネットマスクです。
	IPv6 Address	SZ の IPv6 アドレスです
サービスゾーン — DHCP Scope (Default、SZ1～SZ8)	Status	有効/無効は、デフォルトのサービスゾーン内の DHCP サーバーのステータスを表します
	WINS IP Address	DHCP サーバー上の WINS サーバーの IP です。N/A は、設定されていないことを意味します。
	Start IP Address	DHCP IP 範囲の開始 IP アドレスです。
	End IP address	DHCP IP 範囲の終了 IP アドレスです。
	Lease Time	IP アドレスのリース時間の分です。

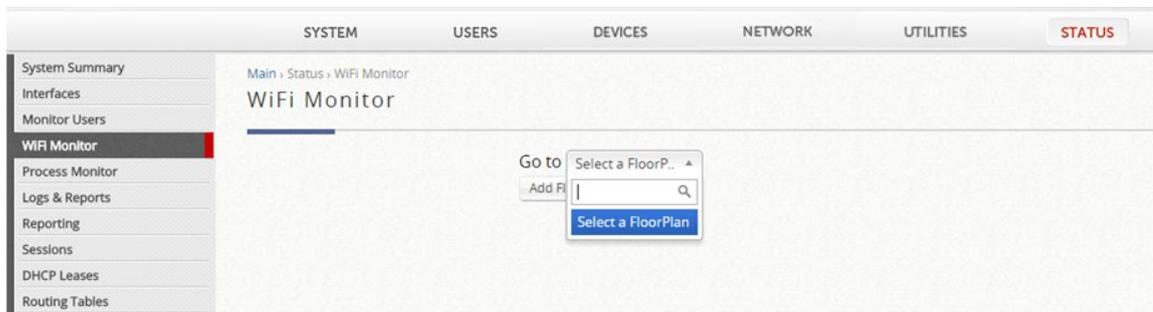
3) Monitor Users

すべてのオンラインユーザー/デバイスがここに表示されます。管理者は、**Kick Out** ボタンをクリックして、任意のユーザーセッションを終了できます。非ログインユーザーもここに表示されます。

- **Online Users** : 認証に成功したローカルユーザーです。
- **Roaming In User** : ローミングピアコントローラで認証されたローミングユーザーです (クロスゲートウェイローミングの場合)。
- **Roaming Out User** : RADIUS プロトコルを介して外部コントローラで認証されたオンデマンドユーザーです。
- **Non-Login Local User** : IP アドレスを取得しましたが、ローカルユーザーの認証はまだされていません。
- **MAC Login Devices** : 切断された MAC 認証デバイスは、物理的に再接続する必要がなく、MAC ログインデバイスリストで MAC 認証が可能です
- **Authenticated Users** : コントローラに対して不明な IP 情報を持つ認証完了ユーザーです (802.1X、MAC 認証、PPP 認証、または CoA ログイン経由)。
- **Smart Login Users** : スマートログイン期間内のオンデマンドユーザーです。このリストのユーザーは、次回ネットワークにアクセスするときに自動的にログインされます。

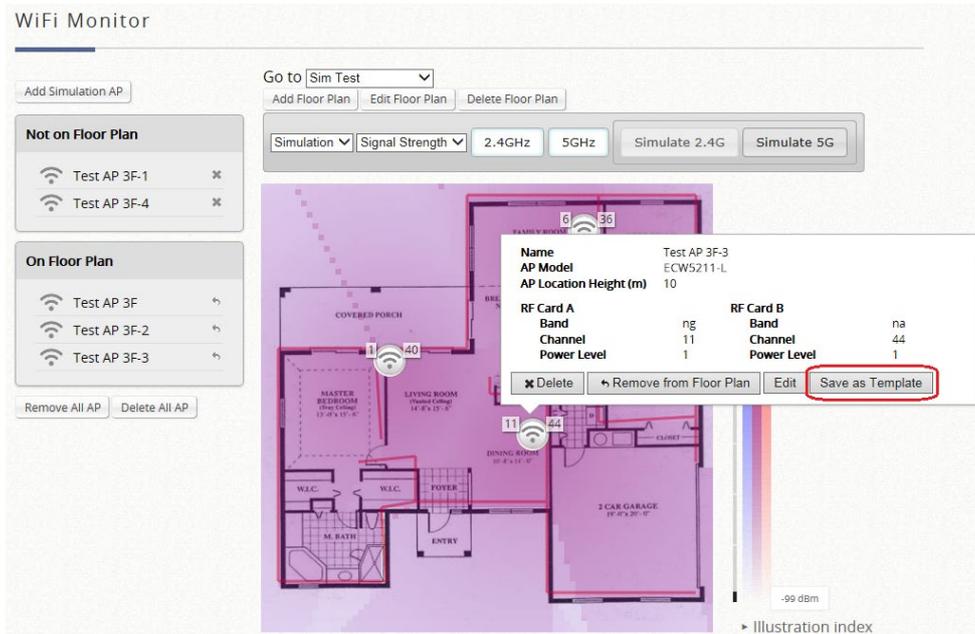
4) WiFi Monitor

WiFi モニターを実行するには、まずフロアプランを作成して管理対象 AP 監視またはシミュレーションを開始してから、2-D フロアプランを EWS コントローラにアップロードする必要があります。**Add Floor Plan** ボタンをクリックして、フロアプランを追加してください。

The screenshot shows the 'Add Floor Plan' form. It contains the following fields:

- Floor Plan Type: Local (dropdown)
- Floor Plan Name: (text input, required)
- Floor Plan (.jpg): (file selection, required, under 256k, JPG)
- Wall (.xml / .osm): (file selection, required)
- Map Width (m): (text input, required, 1~200)
- Map Length (m): (text input, required, 1~200)
- Country Code: EUROPE (dropdown)
- Height of Receiving Device (m): (text input, required, 1~10)

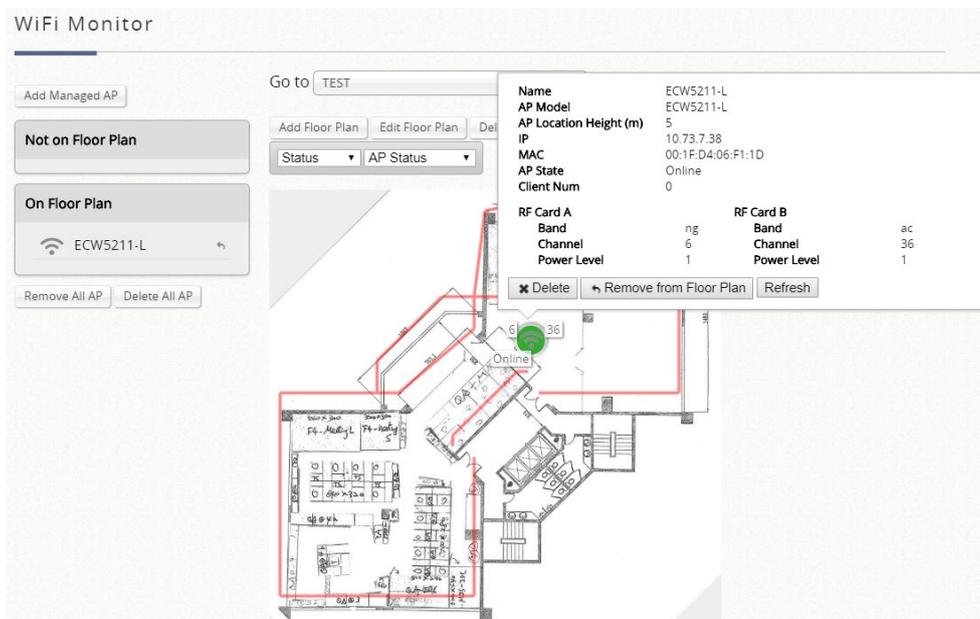
- **Floor Plan Type** : フロアプランのタイプです。ローカルエリア AP 管理またはワイドエリア AP 管理から管理対象 AP を監視する場合は、「Local」または「Wide」を選択します。AP シミュレーションの場合は「Virtual」を選択します。
- **Floor Plan Name** : 管理者の参照用の自己定義名です。
- **Floor Plan** : フロアプランのファイル (.jpg 形式) を選択します。
- **Wall** : ウォールのファイル (.xml または .osm 形式) を選択します。
- **Map Width** : フロアプランの実際の幅です。
- **Map Length** : フロアプランの実際の長さです。
- **Country Code** : 国コード (EU/US) を選択します。これにより、アクセスポイントの最大出力電力が決まります
- **Height of Receiving Device (m)** : 想定される受信クライアントデバイスの平均高さです。



Virtual Type

シミュレーションは、**Simulate 2.4G** または **Simulate 5G** ボタンをクリックして実行できます。満足のいく結果が得られれば、各 AP の設定をテンプレートとして保存して、AP 管理で AP に適用できます。

- **Signal Strength** : 色が濃いほど、信号強度は強くなります。
- **Coverage** : 各 AP のカバレッジエリアは、異なる色によって表されます。
- **Distribution** : 信号の強さを示すために、さまざまな色を使用します。



Local & Wide Type

- **AP Status** : オンライン/オフラインの状態、CPU 使用率（ワイドタイプのみ）、メモリ使用率（ワイドタイプのみ）を視覚化します。

- **Statistics** : 各 AP のデバイス密度と平均トラフィックレート（ワイドタイプのみ）を表示します。
- **Coverage** : 仮想タイプと同様に、各 AP のカバレッジをさまざまな方法で表示します。

6) Process Monitor

プロセスモニターは、ゲートウェイ上のプロセスデーモンのアクティブなステータスを表示するネットワークユーティリティです。管理者は、ラジオボタンをクリックすることで、プロセスモニタの **Enable** または **Disable** を選択することができます。

Process Monitor

Process Monitor		
Enable Monitor	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Process Name	Status	ID
apache		11140
proxy		10069
proxy_logout		10085
proxy_fake		10098
cipgwsrv		9271
cipgwlnsrv		9272
dnsmasq		9435
dnsmasq_fake		9176
radiusd	N/A	
snmpd	N/A	
cipgrd	N/A	

7) Logs & Reports

このページは、CAPWAP ログ、設定変更ログ、ローカル Web ログ、RADIUS サーバーログ、システムログ、UAMD ログなどのログを含むシステムのトラフィック履歴を確認するために使用されます。ユーザーログはユーザーイベントにまとめられ、各ユーザーによって生成されたトラフィックデータの累積記録も最新の暦月に保持されます。ただし、これらの情報はすべて揮発性メモリに格納されるため、再起動/再始動操作中に失われます。したがって、ログ情報を文書化する必要がある場合は、管理者が手動でバックアップを作成する必要があります。

- **CAPWAP Log** : このページには、コントローラと CAPWAP 対応の AP 間で通信される CAPWAP メッセージが表示されます。
- **Configuration Change Log** : このページには、コントローラの WMI 設定を変更したユーザーのアカウントと IP が表示されます。
- **Local Monthly Usage** : システムは、各ローカルユーザーによって生成されたトラフィックデータの累積記録を、最新 2 カ月の間に保持します。ローカルユーザー一月間ネットワーク使用量記録の各行は、システム名、接

続時間使用量、Packets In、Bytes In、Packets Out、Bytes Out の 6 フィールドで構成されています。

- **Local Web Log** : このページには、コントローラ組み込み Web サーバー上でアクセスされた Web ページが表示されます。
- **On-Demand Billing Report** : このページは、オンデマンドアカウントの取引概要です。
- **RADIUS Server Log** : このページには、コントローラを通過する RADIUS メッセージが表示されます。
- **SIP Call Usage** : ログには、開始時刻、発信者、着信者、期間 (秒) などの SIP クライアント (デバイスおよびソフトクライアント) のログインおよびログアウトアクティビティが表示されます。
- **System Log** : このページには、イベントトレース用のシステム関連のログが表示されます。
- **UAMD Log** : UAM デモンから出力される UAM 関連情報を表示します。
- **User Events** : 管理者の好みに合わせてカスタマイズ可能なすべてのユーザー関連情報を表示します。

「Download」ボタンでは、表示されたユーザーイベントをカンマ区切りの.txt ファイルにダウンロードできます。このファイルは、セル (MS Excel) にインポートできます。

ユーザータイプが異なると、ユーザー情報が異なることに注意してください。ユーザータイプに適用できない場合、カテゴリは空白のままになります。

ローカルユーザーに適用可能なユーザーイベントカテゴリ :

Date、Type、Name、IP、IPv6、MAC、Pkts In、Bytes In、Pkts Out、Bytes Out、VLAN ID、Group、Policy、MaxDnLoad、MaxUpload、ReqDnLoad、ReqUpload。

オンデマンドユーザーに適用可能なユーザーイベントカテゴリ :

Date、System Name、Type、Name、Unit、Price、Total Price、IP、IPv6、MAC、Pkts In、Bytes In、Pkts Out、Bytes Out、Activation Time、1st Login Expiration Time、Account Valid Through、Remark、VLAN ID、Group、Policy、MaxDnLoad、MaxUpload、ReqDnLoad、ReqUpload。

ローミングアウトユーザーの適用可能なユーザーイベントカテゴリ :

Date、Type、Name、NSID、NASIP、NASPort、UserMAC、SessionID、SessionTime、Bytes in、Bytes

Out、Pkts In、Pkts Out、Message。

ローミングインユーザーに適用可能なユーザーイベントカテゴリ：

Date、Type、Name、NSID、NASIP、NASPort、UserMAC、UserIP、SessionID、SessionTime、Bytes in、Bytes Out、Pkts In、Pkts Out、Message。

- **Alarm**：選択した項目のエラーまたは警告メッセージです。障害が解決されるまで、アラームはアラームリストに残ります。
- **Management Events**：選択した項目の管理関連のログです。

8) Reporting

EWS コントローラは、設定された電子メールアドレス、SYSLOG サーバー、または FTP サーバーに、ユーザーおよび/またはシステム関連のさまざまなレポートを自動的に送信できます。

Notification Settings ページ：

この設定ページでは、選択した時間間隔に基づいて、事前設定された電子メール、SYSLOG サーバー、または FTP サーバーに送信するログの種類を選択できます。

■ ログを電子メールに送信する

「SMTP Settings」で設定した電子メールアドレスには、以下のログの種類を送信できます。監視 IP のレポート、ユーザーログ、オンデマンドユーザーログ、トライアルユーザーログ、ローミングアウトユーザーログ、ローミングインユーザーログ、外部ユーザーログ、セッションログ、ファイアウォールログ、ローカルエリア AP ステータス変更、オンデマンドユーザー請求レポート、ワイドエリア AP ステータス変更、および設定変更ログです。1~5 の数字は、「SMTP Settings」で設定された対応する電子メールアドレスを表します。必要な電子メールアドレスプロファイル（1~5）をクリックし、レポートまたはログを送信する時間間隔を選択してください。

Notification Settings

	Receiver E-mail Address(es)						SYSLOG	Primary FTP	Interval		
	1	2	3	4	5	Detail / Test					
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	N/A	1 Hour ▼	
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
One Time Password Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	1 Hour ▼	
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	N/A	1 Hour ▼	
Online User Limit Notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	N/A	N/A	
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	N/A	2 Mins ▼	
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	<input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	N/A	2 Mins ▼	
Wide Area AP Report											
<input type="checkbox"/> CPU Loading										<input type="checkbox"/> Daily Report	
<input type="checkbox"/> Memory Usage										<input type="checkbox"/> Weekly Report	
<input type="checkbox"/> Network Delay										<input type="checkbox"/> Monthly Report	
<input type="checkbox"/> Network Traffic							N/A	<input type="checkbox"/>			
<input type="checkbox"/> Associated Clients											
<input type="checkbox"/> VAP Traffic											
<input type="checkbox"/> WDS Traffic											
Guest Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Social Account Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report	
Guest/Social Account Info Full	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	N/A	2 Mins ▼	
Local HTTP Web Log							<input type="checkbox"/>	<input type="checkbox"/>			1 Hour ▼
HTTP Web Log							<input type="checkbox"/>	<input type="checkbox"/>			1 Hour ▼
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			N/A	<input type="checkbox"/>	1 Hour ▼	

- ▶ **Detail** : このオプションボタンをクリックすると、対応するログの電子メールの件名を設定できます。
- ▶ **Send** : このラジオボタンをクリックすると、選択した電子メールアドレスにテストログが送信されます。

■ ログを SYSLOG に送信する

「SYSLOG Settings」で設定した外部 SYSLOG サーバーには、以下のログの種類を送信できます。ローカルユーザーログ、オンデマンドユーザーログ、トライアルユーザーログ、ローミングアウトユーザーログ、ロー

ミングインユーザーログ、外部ユーザーログ、セッションログ、ファイアウォールログ、ローカル HTTP Web ログ、HTTP Web ログ、DHCP サーバーログです。必要なログの種類をクリックし、ログを送信する時間間隔を選択してください。

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval	
	1	2	3	4	5				Detail / Test
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	1 Hour ▼
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
One Time Password Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>		1 Hour ▼
Online User Limit Notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	N/A
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼
Wide Area AP Report							N/A	<input type="checkbox"/>	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report
<input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associated Clients <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic	N/A						N/A	<input type="checkbox"/>	
Guest Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Social Account Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Guest/Social Account Info Full	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A	2 Mins ▼
Local HTTP Web Log	N/A						<input type="checkbox"/>		1 Hour ▼
HTTP Web Log	N/A						<input type="checkbox"/>		1 Hour ▼
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A		1 Hour ▼
DHCP Server Log	N/A						<input type="checkbox"/>		N/A

- ▶ **Detail** : このボタンをクリックすると、SYSLOG サーバー上のフィルタリング要件を満たすために、対応するログに割り当てられるタグ、重大度、ファシリティなどの SYSLOG 属性を設定できます。

注： 選択したログを設定済みの SYSLOG サーバーに送信するには、SYSLOG Settings で「System Log」オプションを有効にする必要があります。

■ ログを FTP に送信する

「FTP Settings」で設定した外部 FTP サーバーには、以下のログの種類を送信できます。ローカルユーザーログ、オンデマンドユーザーログ、トライアルユーザーログ、ローミングアウトユーザーログ、ローミングインユーザーログ、外部ユーザーログ、セッションログ、オンデマンド請求レポートログ、ワイドエリア AP レポート、ローカル HTTP Web ログ、HTTP Web ログ、設定変更ログ、DHCP リースログ、システムレポート、トラフィックレポートです。必要なログの種類をクリックし、ログを送信する時間間隔を選択してください。

Notification Settings

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval							
	1	2	3	4	5				Detail / Test						
Monitor IP Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	1 Hour ▼							
Local Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
On-Demand Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
Guest Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
Roaming Out Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
Roaming In Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
External Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
Social Media Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
One Time Password Users Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
Session Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
Firewall Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	1 Hour ▼							
Online User Limit Notification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	N/A							
Local Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	2 Mins ▼							
On-Demand User Billing Report	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report							
Wide Area AP Status Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	2 Mins ▼							
Wide Area AP Report	N/A						<input type="checkbox"/>	<input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Network Delay <input type="checkbox"/> Network Traffic <input type="checkbox"/> Associated Clients <input type="checkbox"/> VAP Traffic <input type="checkbox"/> WDS Traffic	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report						
Guest Information								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Social Account Information								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	<input type="checkbox"/> 0 ▼ Daily Report <input type="checkbox"/> Sun ▼ Weekly Report <input type="checkbox"/> 1 ▼ Monthly Report
Guest/Social Account Info Full								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	2 Mins ▼
Local HTTP Web Log								N/A						<input type="checkbox"/>	1 Hour ▼
HTTP Web Log								N/A						<input type="checkbox"/>	1 Hour ▼
Configuration Change Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		N/A	1 Hour ▼							
DHCP Server Log	N/A						<input type="checkbox"/>	N/A							
DHCP Lease Log	N/A						<input type="checkbox"/>	1 Hour ▼							
System Report	N/A						<input type="checkbox"/>	<input type="checkbox"/> CPU Loading <input type="checkbox"/> Memory Usage <input type="checkbox"/> Storage Usage <input type="checkbox"/> Network Traffic <input type="checkbox"/> Online User <input type="checkbox"/> Successful Login <input type="checkbox"/> Session <input type="checkbox"/> DHCP Lease <input type="checkbox"/> DNS Query	<input type="checkbox"/> Daily Report <input type="checkbox"/> Weekly Report <input type="checkbox"/> Monthly Report						
Traffic Report (Text)								<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		1 Hour ▼	
Service Zone								N/A						<input type="checkbox"/>	1 Hour ▼
VLAN								N/A						<input type="checkbox"/>	1 Hour ▼

Detail : このボタンをクリックすると、送信されたログがFTPサーバーに格納されるFTPサーバーフォルダを指定することができます。

注：FTP サーバーに出力されるログファイルは、\$トピック_追加の説明_\$システム名_\$日付_時間.txt の形式に従って名前が付けられます。例えば、次のようになります。HTTPWebLog_GW1_2010-10-15_0800.txt

- ▶ **FTP Settings**： 選択したユーザーログとシステムログが送信される外部 FTP サーバーの設定を許可できます。

FTP Settings ページ：

FTP Settings

Primary FTP Server

IP Address

Port

Login

Anonymous Normal

Username

Password

Send Test File

Secondary FTP Server

IP Address

Port

Login

Anonymous Normal

Send Test File

- ▶ **FTP Destination**： FTP サーバーの IP アドレスとポート番号を指定します。FTP で認証が必要な場合は、ユーザー名とパスワードを入力します。「Send Test File」ボタンを使用すると、現在の FTP 送信先の設定をテストするためのテストログを送信できます。

- ▶ **SMTP Settings**： 5つの受信者の電子メールアドレスと、さまざまなユーザー関連のログを送信する必要なメールサーバー設定を設定できます。

SMTP Settings

SMTP Server

Server Address *

Port *

Encryption

Disable TLS SSL

Authentication

None ▼

Sender E-mail Address *

Receiver E-mail Address

Receiver 1

Receiver 2

Receiver 3

Receiver 4

Receiver 5

Send Test E-mail

- **SMTP Server** : 送信者の SMTP サーバーの IP アドレスを入力します。
 - **SMTP Port** : デフォルトでは、ポート番号は 25 です。SMTP サーバーが SSL 経由の SMTP を実行している場合、管理者は他のポートを指定できます。
 - **Encryption** : SMTP サーバーが TLS または SSL 経由で SMTP を実行する場合は、このオプションを有効にしてください。
 - **SMTP Authentication** : システムには、**Plain**、**Login**、**CRAM-MD5**、**NTLMv1**、または「**None**」の 4 つの認証方法が用意されています。選択した認証方法に応じて、**アカウント名**、**パスワード**、**ドメイン**を入力します。
 - **NTLMv1** は現在一般に使用できません。
 - **Plain** と **CRAM-MD5** は標準化された認証メカニズムであり、**Login** と **NTLMv1** は Microsoft 独自のメカニズムです。UNIX のログインとパスワードを使用できるのは、**Plain** と **Login** のみです。Netscape は **Plain** を使用しています。Outlook と Outlook Express は、**NTLMv1** を使用するよう設定できますが、デフォルトでは **Login** を使用します。
 - Pegasus は **CRAM-MD5** または **Login** を使用していますが、どの方法を使用するかを設定できません。
 - **Sender E-mail Address** : 監視を担当する管理者の電子メールアドレスです。これは、送信者の電子メールとして表示されます。
 - **Receiver E-mail Address (1~5)** : 最大 5 件の電子メールアドレスを設定して、通知を受信できます。
- **SYSLOG Settings** : 選択したユーザーログとシステムログが送信される 2 つの外部 SYSLOG サーバーの設定を許可できます。

SYSLOG settings ページ :

The screenshot shows the 'SYSLOG Settings' configuration page. At the top, there is a section for 'SYSLOG' with radio buttons for 'Enabled' (selected) and 'Disabled'. Below this, there are two sections for 'SYSLOG Server', labeled 'Server 1' and 'Server 2'. Each server section has input fields for 'IP Address' and 'Port'. At the bottom, there is a 'Severity Level' dropdown menu currently set to 'emergency'.

- **SYSLOG Destinations** : 最大 2 つの外部 SYSLOG サーバーを設定できます。外部 SYSLOG サーバーの IP アドレスとポート番号を入力してください。
- **Severity Level** : このレベルよりも深刻なログは、外部 SYSLOG サーバーに送信されます。

- ▶ **Alarms & Events Settings** : アラームまたは管理イベントとして監視する項目を設定します。アラームは、選択した項目のエラーメッセージまたは警告メッセージで、Alarms ページおよび Dashboard に表示されます。障害が解決されるまで、アラームはアラームリストに残ります。管理イベントは、Management Events ページに表示される、選択した項目のログです。最新のいくつかのイベントも Dashboard に表示されます。

Alarms & Events Settings

Alarms are error or warning messages for the selected items to be displayed on the Alarms page and Dashboard. An alarm remains on the alarm list until the fault is resolved.
Management Events are logs for the selected items to be displayed on the Management Events page. The latest few events will also be listed in Dashboard.

	Alarms	Management Events	Threshold
AP Online/Offline	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Backup Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Restore Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Firmware Upgrade	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP Template Applying	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
AP High CPU Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
AP High Memory Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
AP High Airtime Utilization	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
Controller High CPU Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
Controller High Memory Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼
Controller High Storage Usage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	70% ▼

9) Session List

このページでは、管理者はクライアントとシステムの間で現在確立されているセッションを検査できます。各結果には、送信元と宛先の IP とポートの値が表示されます。フィルタ条件を定義し、希望する結果のみを表示できます。

Session List

Filter					
Address Family	Protocol	Source IP	Port	Destination IP	Port
IPv4 ▼	All ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Filter

Display Mode: ALL ▼

No	Protocol	Source IP	Port	Destination IP	Port	State	Timeout
1	udp	10.29.129.131	137	10.29.255.255	137	UNREPLIED	3
2	udp	10.29.129.87	138	10.29.255.255	138	UNREPLIED	29
3	udp	10.29.129.87	137	10.29.255.255	137	UNREPLIED	23
4	udp	10.29.129.110	17500	255.255.255.255	17500	UNREPLIED	21
5	tcp	10.28.128.188	55026	10.29.42.101	80	TIME_WAIT	119
6	udp	10.29.129.79	137	10.29.255.255	137	UNREPLIED	27

10) DHCP Lease

DHCP IP リース情報は、このページで確認できます。

- **Statistics of IP Offered**

ここには、**Last 10 Minutes**（分）、**Hours**（時間）、および**Days**（日間）の有効なリース数が表示されます。ヘッダー1~10は単位乗数です。例えば、列2の下の数字は過去20分/時間/日間のリース数を示し、列3の下の数字は過去30分/時間/日間のリース数を示します。

- **Statistics of IP Expired**

ここには、**Last 10 Minutes**（分）、**Hours**（時間）、および**Days**（日間）に期限切れになったクライアントへのIPリースが表示されます。ヘッダー1~10は単位乗数です。例えば、列2の下の数字は過去20分/時間/日間の期限切れ数を示し、列3の下の数字は過去30分/時間/日間の期限切れ数を示します。

The screenshot shows a web interface for DHCP lease statistics. At the top left is a 'Refresh' button, and at the top right is a 'Refresh' button with a 'Disable' dropdown menu. Below this is the 'IPs Offered' section, which contains a table with 11 columns (headers 1-10) and 3 rows (Last 10 Minutes, Last 10 Hours, Last 10 Days). All values in this table are 0. Below that is the 'IPs Expired' section, which also contains a table with 11 columns (headers 1-10) and 3 rows (Last 10 Minutes, Last 10 Hours, Last 10 Days). All values in this table are 0.

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	1	0	0	0	0	0	0	0	0	0
Last 10 Hours	1	0	0	0	0	0	0	0	0	0
Last 10 Days	1	0	0	0	0	0	0	0	0	0

	1	2	3	4	5	6	7	8	9	10
Last 10 Minutes	0	0	0	0	0	0	0	0	0	0
Last 10 Hours	0	0	0	0	0	0	0	0	0	0
Last 10 Days	0	0	0	0	0	0	0	0	0	0

- **DHCP Lease Log**

DHCP リースログがここに表示され、IP アドレス、MAC アドレス、またはサービスゾーンでの検索が可能です。

DHCP Lease Log								
Date	Type	IP Address	MAC Address	Host Name	Service Zone	Lease Expires	Client ID	Vendor Class
2013-03-06 11:50:37	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 11:50:33	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 11:57:35	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 11:57:35	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 14:03:29	Update	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 14:03:29	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 14:07:38	Update	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 14:07:38	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 14:56:23	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 14:56:23	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 15:05:51	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:05:49	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 15:14:08	Load	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:05:49	01:00:09:6b:cd:82:47	*
2013-03-06 15:15:10	Add	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:15:09	01:00:09:6b:cd:82:47	MSFT 5.0
2013-03-06 15:23:00	Update	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	Default	2013-03-07 15:23:00	01:00:09:6b:cd:82:47	MSFT 5.0

- **DHCP Lease List**

DHCP サーバーから発行された有効な IP アドレスと、この IP アドレスを使用するクライアントの関連情報がここに表示されます。

DHCP Lease List						
No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires	
1	192.168.1.47	00:09:6b:cd:82:47	Support_IBM_X30	3202	2013/03/07 15:23:00	

(Total:1) [First](#) [Previous](#) [Next](#) [Last](#) Go to Page (Page:1/1) Row per Page:

11) Routing Table

ルーティングテーブルには、すべての IPv6 および IPv4 ルートルールがあります。システムルートルールもここに示されています。ポリシールートルールの優先度はグローバルポリシールートルールよりも高く、システムルートルールの優先度は最も低いです。

Global Policy			
Destination	Subnet Mask	Gateway	Interface
169.254.0.0	255.255.0.0	0.0.0.0	Default
192.168.0.0	255.255.0.0	0.0.0.0	Default
10.29.0.0	255.255.0.0	0.0.0.0	WAN1

Interface			
Destination	Subnet Mask	Gateway	Interface
169.254.0.0	255.255.0.0	0.0.0.0	Default
192.168.0.0	255.255.0.0	0.0.0.0	Default
10.29.0.0	255.255.0.0	0.0.0.0	WAN1

System			
Destination	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	10.29.0.1	WAN1

Policy 1			
Destination	Subnet Mask	Gateway	Interface

Policy 2			
Destination	Subnet Mask	Gateway	Interface

IPv4 または IPv6 をクリックすると、各ポリシーまたはインターフェースのルーティングルールが表示されます。

- **Policy 1~n** : 1 から n までの個々のポリシーの情報を表示します。
- **Global Policy** : グローバルポリシーの情報を表示します。
- **System** : システム管理に関する情報を表示します。
 - **Destination** : デバイスの宛先 IP アドレスです。
 - **Subnet Mask** : ポートのサブネットマスクの IP アドレスです。
 - **Gateway** : ポートのゲートウェイ IP アドレスです。
 - **Interface** : **WAN1**、**WAN2**、**デフォルト**、またはトラフィックインターフェースに適用する名前付きサービスゾーンを含むインターフェースネットワークの選択です。

AP の WAPM 機能に関するキャパシティー表

AP の種類	AP リス ト	MAP/AP グルー ピング	テンプレ ートコン フィグ	WDS リス ト	バック アップ コンフ ィグ	ファーム ウェアア ップロー ド	CAPWAP トンネル	不正 AP の探知	AP ロー ドバラン シング	対応バージ ョン
OAP100	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
OAP100e	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
EAP100	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
ECW100	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
ECW5210-L	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
ECW5211-L	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
ECW5410-L	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
ECWO5210-L	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
ECWO5211-L	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
ECWO5213-L	V	V	V (Legacy)	V	V	V	V	V	V	3.45.0000 or newer
OAP103-BR	V	V	V (Legacy)		V	V	V		V	11.6.4 or newer
EAP101	V	V	V (New Generati on)		V	V	V		V	11.2.0- 795 or newer
EAP102	V	V	V (New Generati on)		V	V	V		V	11.2.0- 796 or newer
EAP104	V	V	V (New Generati on)		V	V	V		V	12.0.0 or newer
SP-W2M- AC1200	V	V	V (New Generati on)		V	V	V		V	7.0.0-2987 or newer
サードパー ティー	V	V								