



ユーザマニュアル
EWS-Series コントローラ

Version 3.45.00

Copyright Notification

Edgecore Networks Corporation

© Copyright 2019 Edgecore Networks Corporation.

The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

著作権

本書の内容は、Edgecore, INC.の書面による事前の許可なく、その一部または全部を複製、保存、情報検索システムへの転載、他言語への翻訳、機械的、磁氣的、電子的、光学的、写真複写、マニュアルなどの方法で転送することはできません。

免責条項

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適用に起因する一切の責任を負いません。また、親会社の権利に基づくライセンスも、他社の親会社の権利も伝えていません。Edgecoreは、本書に記載されている製品を予告なく変更する権利をさらに留保します。本書は、予告なしに変更されることがあります。

商標

Edgecoreは株式会社Edgecoreの登録商標です。本書に記載されているその他の商標は、識別のみを目的として使用されており、各社の所有物である場合があります。

注意事項

本ドキュメントはEdgecore社が発行した英文ドキュメントを和訳したものです。和訳内容に不明事項がある場合は、英文原文での確認をお願いします。

目次

第 1 章	序文	1
1.1	EWS WLAN 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	主な用語とコンセプト	5
1.5	推奨構成シーケンス	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 & セットアップウィザード	9
2.1	WEB マネジメントインタフェース	9
2.2	ウィザードの実行	11
第 3 章	基本的なネットワーク設定	15
3.1	ネットワーク計画	15
3.2	アップリンク(WAN 側)の構成	17
	3.2.1 WAN 設定	17
	3.2.2 デュアルアップリンク	18
	3.2.3 デュアル WAN1/WAN2 モデルの WAN ポートの選択	19
	3.2.4 WAN トラフィック制御	20
	3.2.5 アップリンクの検出とフェイルオーバー	21
3.3	ダウンリンク(LAN 側)VLAN オプション	22
	3.3.1 ポートベースサービスゾーン	23
	3.3.2 タグベースのサービスゾーン	23
第 4 章	ユーザ認証データベース	24
4.1	認証データベースの設定	24
4.2	組み込み認証データベース	25
	4.2.1 ローカルユーザデータベース	25
	4.2.2 オンデマンドユーザデータベース	28
	4.2.3 ゲスト認証オプション	33
	4.2.4 ワンタイムパスワード	37
4.3	外部認証オプション	38
	4.3.1 RADIUS	38
	4.3.2 POP3	41
	4.3.3 LDAP	42
	4.3.4 NT ドメイン	43
	4.3.5 SIP	43
	4.3.6 ソーシャルメディア	45
第 5 章	グループ属性とポリシールール	48
5.1	コンセプトの概要	48
5.2	グループとポリシーの実用的なセットアップ	51
第 6 章	サービスゾーンの基本構成	56
6.1	サービスゾーンの概念	56
6.2	サービスゾーンの設定	56
	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	56
	6.2.2 NAT モードまたはルータモード	59
	6.2.3 サービスゾーンネットワークインタフェース	59
	6.2.4 DHCP サーバオプション	60
	6.2.5 認証オプション	61
	6.2.6 キャプティブポータルのカスタマイズ	63

第 7 章	基本的な AP 管理	66
7.1	序文	66
7.2	ローカルエリア AP 管理	68
7.2.1	AP List	68
7.2.2	AP の追加と構成の適用	69
7.2.3	テンプレートの設定	71
7.2.4	AP ファームウェア管理	73
7.2.5	WDS リンク	74
7.2.6	不正なアクセスポイントスキャン	75
7.2.7	AP 負荷分散機能	76
7.3	ワイドエリア AP 管理	78
7.3.1	アクセスポイントの追加	79
7.3.2	複数のアクセスポイントを検索する AP 検出	79
7.3.3	テンプレートを使用した AP 構成	80
7.3.4	CAPWAP を使用した AP 自動検出と構成	81
7.3.5	トンネル VAP ロケーションマッピングの設定	86
7.3.6	Google マップでのアクセスポイントの監視	88
7.3.7	AP グループ化	93
7.3.8	不正なアクセスポイントスキャン	95
7.3.9	AP 負荷分散機能	96
第 8 章	ネットワーク環境の詳細設定	98
8.1	IPv4/IPv6 デュアルスタックネットワーク	98
8.2	ユーザアクセスコントロール	101
8.2.1	Black List	101
8.2.2	MAC ACL	102
8.3	証明書	103
8.3.1	システム証明書	104
8.3.2	内部ルート CA	106
8.3.3	内部的に発行された証明書	107
8.3.4	信頼できる認証局	107
8.4	管理アクセス	108
第 9 章	コントローラ管理のユーティリティ	109
9.1	EWS コントローラの管理	109
9.2	設定のバックアップとリストア	111
9.3	ファームウェアアップグレード	112
9.4	再起動	113
第 10 章	監視のためのレポートとログ	114
10.1	システム関連ステータス	114
10.1.1	ダッシュボード	114
10.1.2	システムの概要	115
10.1.3	ネットワークインタフェース	116
10.1.4	ルーティング	118
10.1.5	DHCP サーバ	118
10.2	クライアント関連ステータス	120
10.2.1	オンラインユーザ	120
10.2.2	関連する非ログインユーザ	120
10.2.3	クロスゲートウェイローミングユーザ	121
10.2.4	オンデマンドローミングアウトユーザ	121
10.2.5	MAC ログインデバイス	122
10.2.6	認証ユーザ	122
10.2.7	スマートログインユーザ	123

10.2.8	セッションリスト	123
10.3	ログとレポート	124
10.3.1	システム関連	124
10.3.2	ユーザイベント	125
10.4	レポートと通知	127
第 11 章	ホットスポットアプリケーション	129
11.1	オンデマンド課金プラン	129
11.2	オンデマンド課金プランタイプ	130
11.2.1	有効期限付き使用時間	130
11.2.2	有効期限なしの使用時間	131
11.2.3	ホテル・カットオフ時刻	133
11.2.4	ボリューム	135
11.2.5	経過時間による持続時間	136
11.2.6	カットオフ時刻による持続時間	138
11.2.7	開始/終了時間による持続時間	139
11.3	POS プリンタの設定	141
11.4	POS チケットのカスタマイズ	144
11.5	アカウントの作成	147
11.6	ユーザセルフサービス	149
第 12 章	PMS 統合	154
12.1	ホテルルームロケーションマッピング	154
12.2	PMS 構成	156
第 13 章	アカウントローミング	159
13.1	ローミング関連	159
13.2	ISP ローミング用 WISPr	159
13.3	クロスゲートウェイローミング	161
13.4	ローカル/オンデマンドアカウントローミングアウト	162
第 14 章	VPN	165
14.1	サイト間	165
14.2	リモートクライアント	166
第 15 章	スイッチ管理	168
15.1	スイッチリスト	168
15.2	PoE スケジュールテンプレート	169
15.3	バックアップ設定	170
第 16 章	プラットフォームに依存する機能	171
16.1	高可用性(HA)(EWS5203、EWS5204、EWS5207)	171
16.2	Wi-Fi モニタ(EWS5203、EWS5204、EWS5207)	173
16.2.1	フロアプランの追加	173
16.2.2	シミュレーション AP	175
16.2.3	フロアプランでの AP 監視	177
付録 A	EWS モデルとインストール	178
付録 B	外部ページ	183
付録 C	便利なマネジメント&パリュエーションツール	195
付録 D	オンデマンドアカウントタイプ	197
付録 E	UI 参照インデックス	203
I.	ダッシュボード	203
II.	セットアップウィザード	204
A.	System 205	
1)	General	205
2)	WAN 208	

3) IPv6	210
4) LAN Ports	210
5) MGMT Port	211
6) High Availability	212
7) Service Zones	213
8) Port Location Mapping	219
9) PMS Interface	223
B. Users	225
1) Groups	225
2) Internal Authentication	226
3) External Authentication	237
4) On-Demand Accounts	238
5) Schedule	239
6) Policies	239
7) Blacklists	241
8) Privilege Lists	242
5) Additional Control	242
C. Devices	245
1) Local Area AP Management	245
2) Wide Area AP Management	257
3) Switches	280
E. Network	283
1) NAT	283
2) Monitor IP	285
3) Walled Garden and Walled Garden Ad	285
4) VPN	286
5) Proxy Server	287
6) Local DNS Record	290
7) Dynamic Routing	290
8) DDNS	293
9) Client Mobility	294
F. Utilities	295
1) Administrator Account	295
2) Backup & Restore	298
3) Certificates	300
4) Network Utilities	302
5) Restart	303
6) System Upgrade	304
G. Status	305
1) System Summary	305
2) Interface	307
3) Monitor Users	309
4) WiFi Monitor	309
6) Process Monitor	311
7) Logs & Reports	311
8) Reporting	313
9) Session List	320
10) DHCP Lease	321
11) Routing Table	322

第1章 序文

1.1 EWS WLAN ゲートウェイコントローラシリーズ

Edgecore EWS WLAN ゲートウェイコントローラは、ネットワークサービスプロビジョニング、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。構築するネットワークの規模に応じて、さまざまな規模のキャパシティでネットワーク要件を満たすための Edgecore EWS WLAN ゲートウェイコントローラモデルを選択できます。

Edgecore EWS コントローラは、認証、承認、アカウンティングを表すトリプル 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 コントローラでは、さまざまなユーザがユーザロールに基づいて認証されます。そこから、ユーザのアクセス可能なネットワークセグメント、ユーザ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、使用期間、承認と総称される権限を含みます)が定義されます。最後に、クライアントがネットワークを使用している間、Edgecore EWS コントローラによってアカウンティングが定期的に実行され、内部ユーザデータベースまたは外部ユーザデータベースのいずれかにあるクライアントのアカウンティング情報が更新されます。

ワイヤレスネットワークのプロビジョニングは、スケールが複数の AP 展開に達した場合には簡単な作業ではありません。Edgecore EWS コントローラには、ローカルエリアネットワーク(LAN)にローカルに配置された 4ipnet AP デバイスだけでなく、Edgecore EWS コントローラの場所に応じてワイドエリアネットワーク(WAN)にリモートで配置された EdgecoreAP デバイスも対象とする、包括的な AP 管理機能が搭載されています。さらに、サードパーティの AP 管理インタフェースを用いて、Edgecore EWS コントローラでは、関連するオンラインユーザ監視、GUI インタフェースへのショートカット、非 EdgecoreAP の位置計画などの一般的な AP 管理機能を実行できます。

ネットワークの安全性およびトラフィックコントロールは、ネットワーク所有者、ホテル業者にとって、これらがネットワーク環境全体の品質および安定性を決定する主要な要因であるため、他の大きな関心事です。Edgecore EWS コントローラでは、これらの要求に対処するために、最適化されたパス選択のためのスタティックおよびダイナミックルーティング機能、個々のユーザへの帯域幅制御を実施するための QoS マッピング、システムアップリンク帯域幅制御、および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を備えています。

一般的なネットワーキング機能は、Edgecore EWS コントローラに収録されています。無料サイト閲覧のためのワールドガーデン、ネットワーク機器監視ツール、スタティック DNS 変換、プロキシサーバ、VPN など 3 種類の NAT 機能を提供。Edgecore EWS コントローラでは、複数のネットワーク機能を 1 つのデバイスに組み込むことで、外部 NAT サーバ、プロキシサーバ、VPN ゲートウェイなどを設定する必要がなくなり、導入の複雑さが軽減されるため、ネットワーク導入が簡素化されます。

システムトラフィック、CPU 使用率、メモリ使用率などのシステムリソース使用率、オンラインユーザレコード、DHCP リースレコードなどを表示することで、ネットワーク保守およびネットワーク監視タスクが容易になります。イベントログは、長期間のレコードの保持または詳細な解析のために外部サーバに送信できます。

1.2 EWS コントローラモデル

Edgecore EWS コントローラプロダクトラインには、さまざまなスケールのネットワーク構築を目的とした次のモデルがあります。

SMB & Enterprise WLAN Gateway-Controllers

EWS100、EWS5203

大規模エンタープライズ & キャリアグレードコントローラ

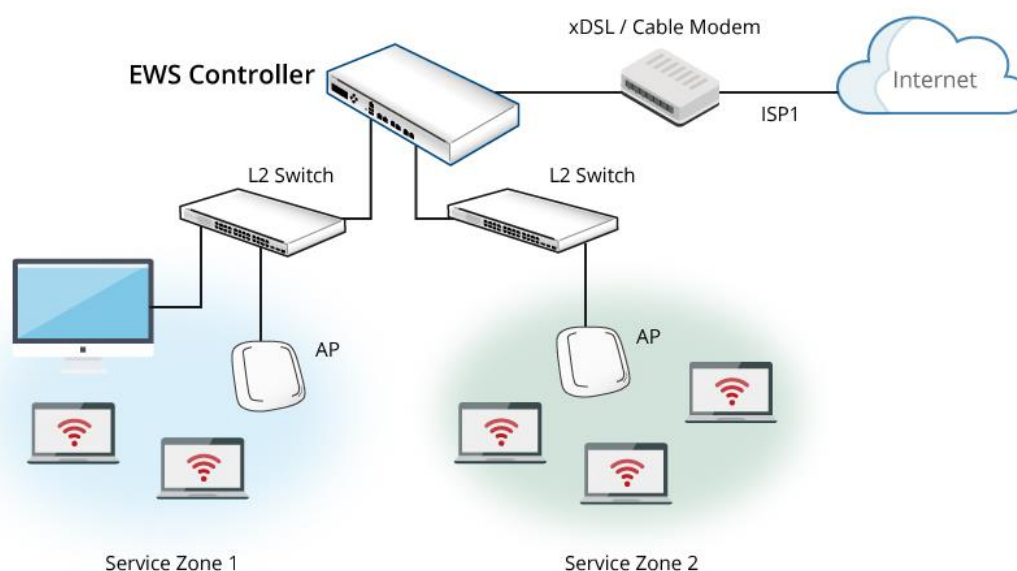
EWS5204、EWS5207

注：Edgecore は引き続き新しいプラットフォームを導入し、古いプラットフォームを廃止する可能性があります。最新の製品ラインのステータスについては、<https://wifi.edge-core.com> を参照してください。各モデルの一覧とインストール方法の詳細については、付録 A を参照してください。

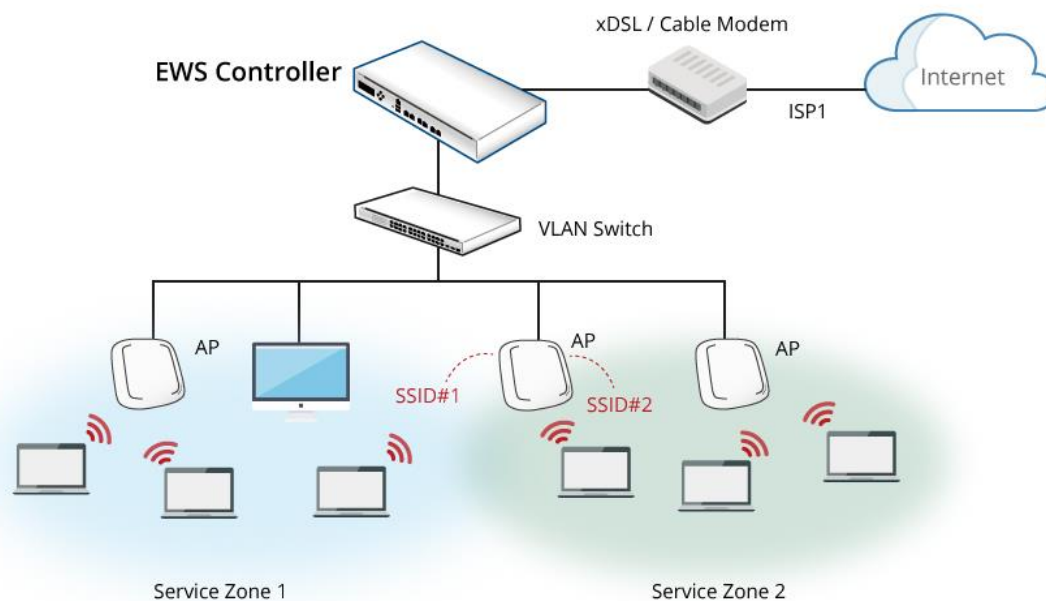
1.3 Edgecore ソリューションの概要

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)でのネットワーク管理のため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 ポートに物理的にまたがる比較的シンプルなネットワーク配置トポロジです。2 つの配置シナリオを次に示します。

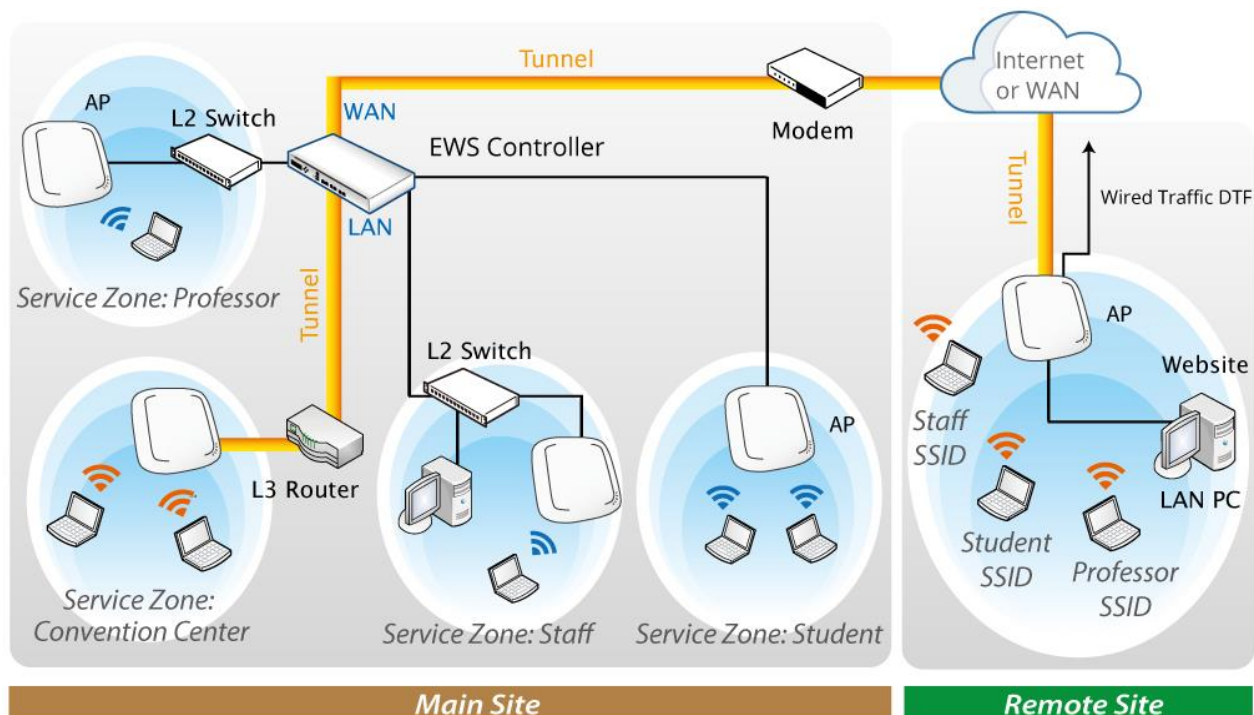


【ポートベースモードのレイヤ 2 ネットワーク】



【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、物理的に Edgecore EWS コントローラの LAN ポートにまたがっているだけでなく、さまざまな IP ネットワークを介してアクセスし、トンネルを介してルーティング可能な IP アドレスを使用してリモートサイトを管理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 主な用語とコンセプト

ゲートウェイは、小規模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、ネットワーク環境におけるゲートウェイです。従来、大規模なネットワークは WAN 側またはアップストリームネットワーク(WAN ポートを介して物理的に接続)と呼ばれ、小規模なネットワークは LAN 側と呼ばれていました。

ローカルユーザは、アカウント資格情報がローカルという名前の Edgecore EWS コントローラの組み込みデータベースに格納されているユーザの一種で、Edgecore EWS コントローラのローカルデータベースキャパシティは機種によって異なります。ローカルユーザアカウントが作成された後は、有効期限はありません。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行う必要があります。さらに、Edgecore EWS コントローラのローカルデータベースを、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設定することもできます。

On-Demand ユーザは、アカウント資格情報が Edgecore EWS コントローラの On-Demand という名前の組み込みデータベースに保存されるユーザの一種で、Edgecore EWS コントローラの On-Demand データベースの容量はモデルによって異なります。オンデマンドユーザは、短期間使用するために設計されており、時間またはボリュームの制約と有効期限があります。オンデマンドアカウントレコードの有効期限が 15 日を超えた場合、または管理者/マネージャが手動で削除した場合、そのレコードは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。さらに、Edgecore EWS コントローラの On-Demand データベースを、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設定できます。

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アカウントデータベースです。ローカルデータベースとオンデマンドデータベースのほかに、Edgecore EWS コントローラでは、RADIUS、POP3、LDAP(アクティブディレクトリを含みます)、NTDomain(Win2K の NTDS)の 4 タイプの外部認証データベースがサポートされています。外部認証データベースは、アカウントローミングと集中型アカウント管理の両方の実装に役立ちます。

サービスゾーンは、Edgecore EWS コントローラの LAN のロジックパーティションです。サービスゾーンのコンセプトは、独自のゲートウェイプロパティ(LAN IP アドレス、DHCP サーバ設定、認証オプションなど)を持つ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あるということです。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サービスを提供できます。

LAN ポートマッピングは、論理ネットワークパーティションの対応関係、すなわち、Edgecore EWS コントローラの物理 LAN ポートに対応するサービスゾーンです。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

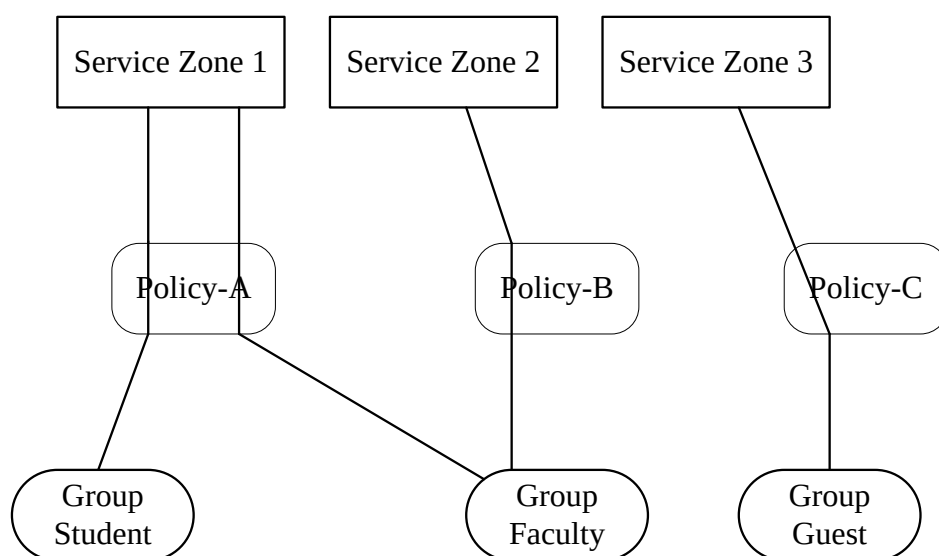
モードは、サービスゾーンを物理 LAN ポートのダウンストリームのクライアントに静的にマッピングします。このモードは、物理 LAN ポートの量に基づいてサービスゾーンの最大量のみを提供します。タグベースモードは、トラフィックパケットにタグ付けされた VLAN ID に基づいて、クライアントをサービスゾーンに動的にマッピングします。

グループは、異なるサービスゾーンへのユーザのアクセシビリティを定義し、アクセスが許可されたときに QoS プロパティとネットワークポリシーを定義するユーザロールプロファイルです。接続されているすべてのユーザは、認証に使用されるユーザアカウントの種類によって決定されるグループに属します。管理者が特定のグループに新しいアカウントを割り当てない場合、または認証が不要なユーザの場合、管理者はデフォルトで None 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、ユーザのグループプロファイルが決定された後のユーザ制御の第 2 段階です。ポリシーは、特定のグループのユーザ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は、別のポリシーによって管理できます。

None グループに属するユーザまたはネットワークポリシーが明示的に割り当てられていないユーザの場合、Global-Policy という名前のデフォルトキャッチオールポリシーによって管理されます。Global-Policy は、他のポリシーに適用されない場合、すべてのユーザに適用される基本ポリシーです。

次の図は、サービスゾーン、グループ、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 にログインする学生と教職員は、ポリシーAによって管理されます。ゲストは、サービスゾーン 3 にしかアクセスできず、ポリシーCによって制限されます。教職員は、2 つの異なるポリシーでサービスゾーン 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 推奨構成シーケンス

- システムのタイムゾーン、NTP サーバ、DNS サーバ、および WAN1 アドレスを設定します。
- 少なくとも 1 つのサービスゾーンの LAN アドレス範囲を設定し、その認証を有効にします。
- 有効なサービスゾーンの回線を介してログインページをテストするユーザアカウントを作成します。
- オンデマンドユーザを生成し、アカウントをテストします。
- サービスゾーンのワイヤレス情報を設定し、AP に追加します。
- アプリケーションに基づいて必要なサービスゾーンを設定します。
- 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みます)を設定します。
- 必要に応じて、ポータルログインページをカスタマイズし、ワールドガーデン通知リンクを追加します。
- 必要に応じて、エンドユーザのクレジットカードによるオンデマンドアカウントのセルフペイメントを許可するように決済ゲートウェイを設定します。
- Web サーバの SSL 証明書を読み込んでから運用してください。
- 生成されたステータスページとレポートを監視します。
- その他の特定のアプリケーションの詳細設定を実行します。

1.5.1 共通設定

標準ネットワークで最も一般的に展開されるシナリオについては、第 3 章から第 7 章を参照してください。

第 3 章から第 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。どのようなネットワーク構成でも第 3 章から開始し、第 7 章までお読みいただくことをお勧めします。

1.5.2 詳細設定とアプリケーション

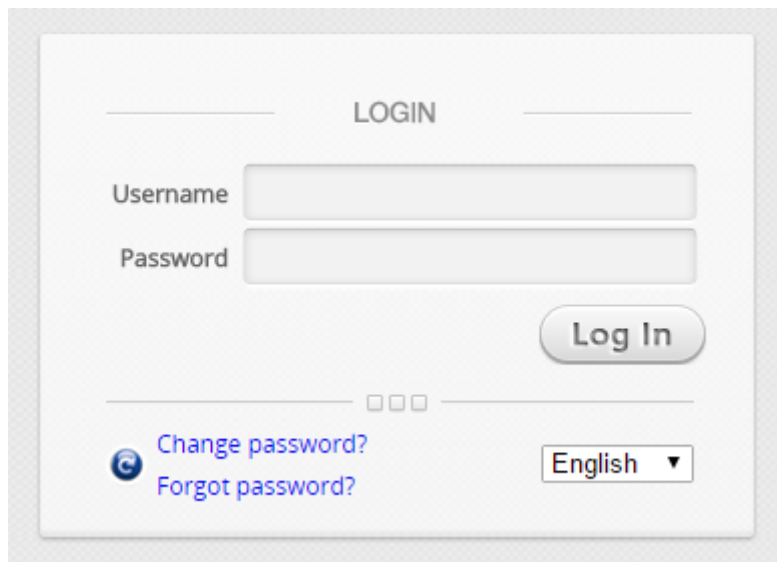
第 8 章から第 10 章では、セキュリティ、保守、監視について説明します。これらのコンテンツは、必要な機能を正常に設定し、ネットワークが起動して実行された後の運用に役立ちます。

特定のアプリケーションを満たす必要がある顧客、サードパーティ製デバイスとの統合、カスタマイズなどは、第 11 章以降の高度な機能セットアップを参照してください。

第2章 WMI & セットアップウィザード

2.1 WEB マネジメントインタフェース

EWS コントローラの Web マネジメントインタフェース(WMI)には、デフォルト IP アドレス 192.168.1.254 で LAN インタフェースに接続された任意の PC の Web ブラウザ(Firefox、Chrome、および Safari を推奨)からアクセスできます。

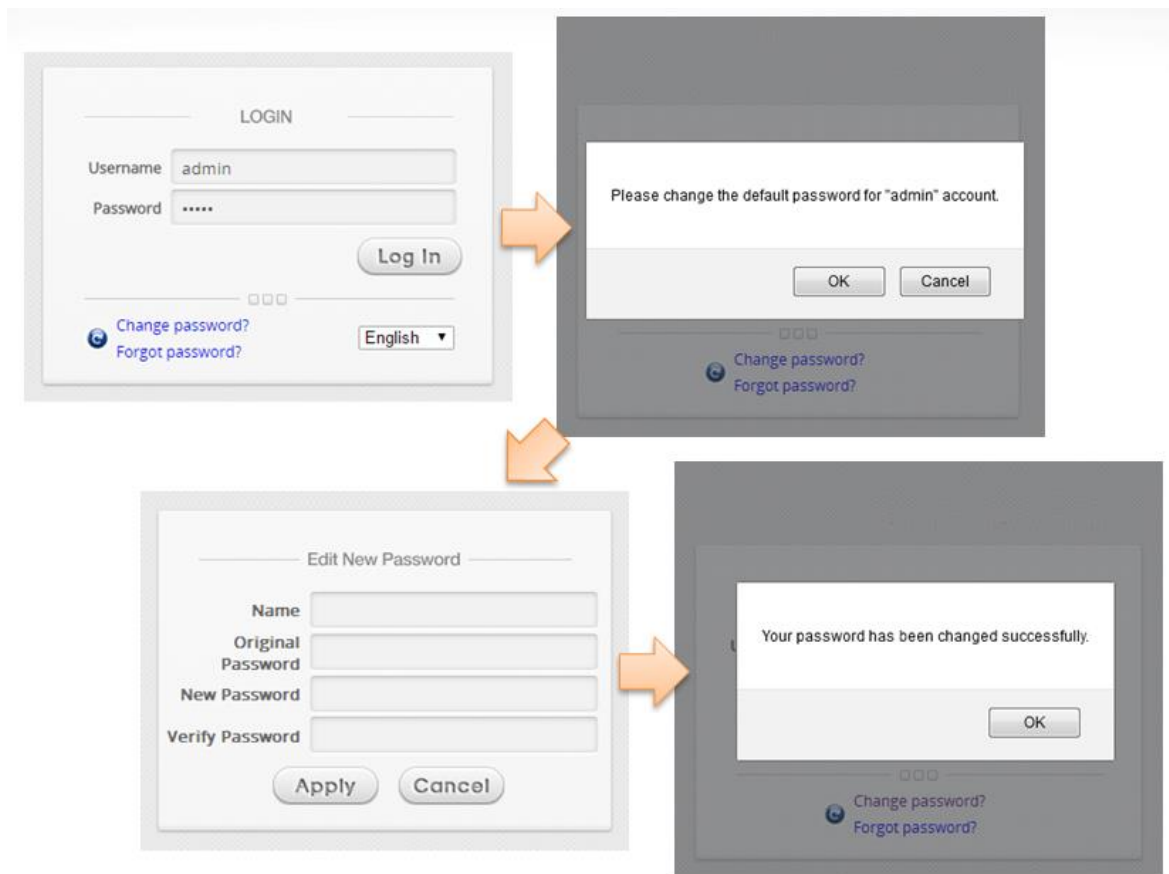


デフォルト管理者のアカウントとパスワードは、次のようになります。

- 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実施するために管理者にパスワードの変更を求めるプロンプトが表示されます。パスワードの長さは 6 文字以上で、少なくとも 1 つのアルファベットと 1 つの数字が含まれている必要があります。

管理者アカウントの設定について詳しくは、付録 F の E を参照してください。



管理者が正常にログインすると、Dashboard ページは次のようになります。



注意事項

1. ログアウトするには、インタフェースの右上隅にあるログアウト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、最小限の設定でネットワークのセットアップと動作に不可欠な設定手順のコレクション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 をすばやく設定するには、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ます。

ステップ 1. 一般

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

The screenshot shows the 'General' step of the Setup Wizard. At the top, there is a progress bar with 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 first step is highlighted. Below the progress bar, on the left, is a red vertical bar with the text: 'It is recommended to select an appropriate time zone for the system.' The main area is titled 'General' and contains a 'Time Zone' label followed by a dropdown menu showing '(GMT+08:00)Taipei'. At the bottom right, there are two buttons: 'Exit' and 'Next'.

ステップ 2. WAN1 ポートの接続タイプの選択

- ▶ WAN 接続には、Static IP Address、Dynamic IP Address と PPPoE Client の 3 種類があります。適切なインターネット接続タイプを選択します。動的 IP 接続の使用例を次に示します。
- ▶ Next をクリックして続行します。
- ▶ Static IP Address または PPPoE Client の場合は、スクリーンの指示に従います。

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. ローカルユーザアカウントの追加(オプション)

- 新しいユーザをローカルユーザデータベースに追加できます。ここにユーザを追加するには、Username(例: testuser)、Password(例: testuser)を入力し、この特定のユーザに Applied Group を割り当てます(またはデフォルト Group 1 を使用します)。
- Next をクリックして続行します。

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 4. EWS の確認と再起動

- Finish をクリックして現在の設定を保存し、システムを再起動します。
- 確認のダイアログボックスが表示されます。OK をクリックして続行します。

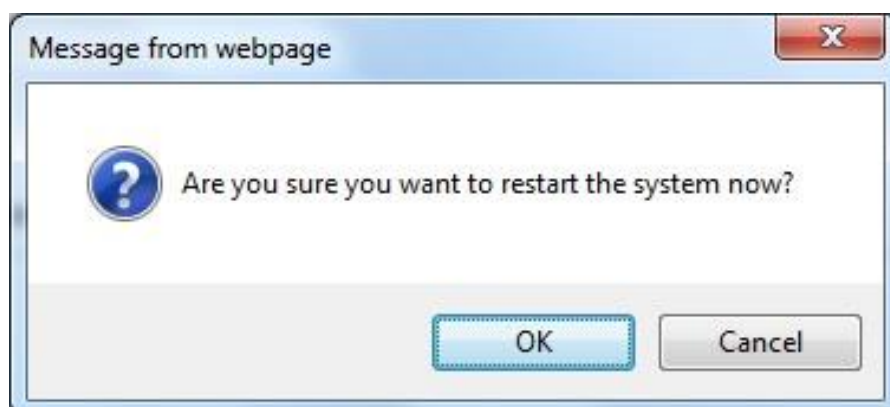
1 FIRST STEP
Set Time Zone
2 SECOND STEP
Configure WAN1
3 THIRD STEP
Create A Local User
4 YOU'RE DONE
Restart the System

Press "Finish" button to confirm the settings and restart the system.

Confirm and Restart

Please press Finish button and restart the system.

Exit
Back
Finish



- 再起動中は Confirm and Restart 画面が表示されます。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。

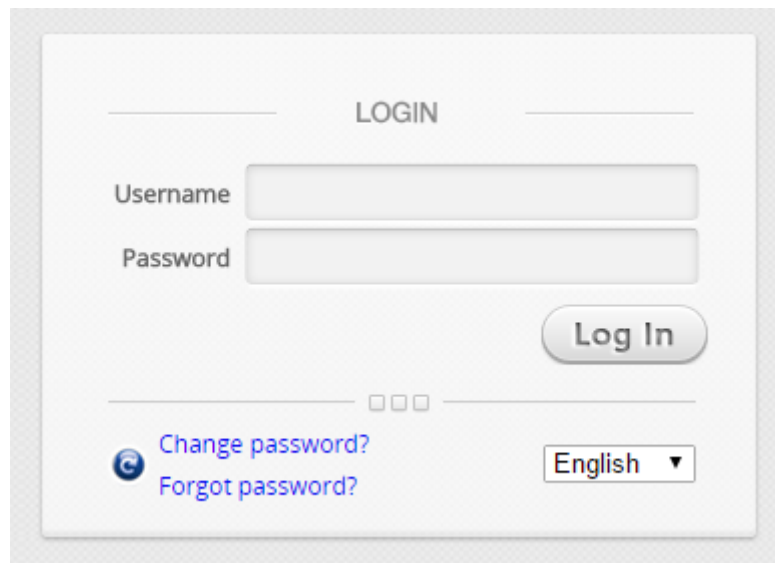
1 FIRST STEP
Set Time Zone
2 SECOND STEP
Configure WAN1
3 THIRD STEP
Create A Local User
4 YOU'RE DONE
Restart the System

Press "Finish" button to confirm the settings and restart the system.

Confirm and Restart

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表示されるまで、EWS 再起動プロセスを中断しないでください。

再起動処理が完了しました。



The image shows a web-based login interface for an administrator. At the top, the word "LOGIN" is centered. Below it are two input fields: "Username" and "Password". To the right of the "Password" field is a "Log In" button. Below the input fields, there are three small square checkboxes. At the bottom left, there are two links: "Change password?" and "Forgot password?". To the right of these links is a language selection dropdown menu currently set to "English".

第3章 基本的なネットワーク設定

3.1 ネットワーク計画

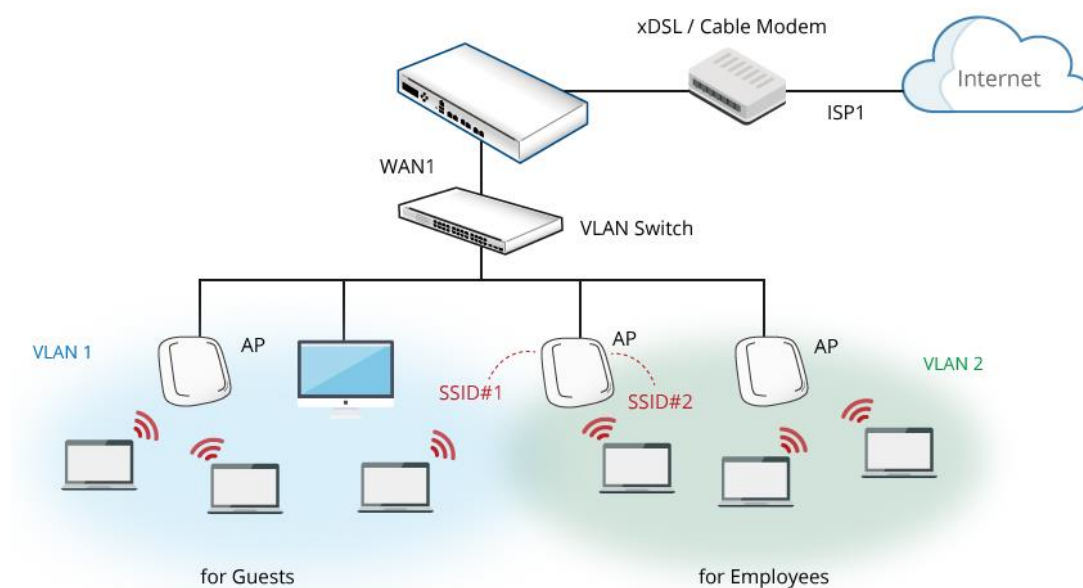
Edgecore EWS コントローラをインストールする前に、ネットワークリソースを最も効率的に使用してネットワークへのニーズを満たすために、慎重なネットワーク計画が必要です。あらゆる組織の IT スタッフは、手元にある利用可能なネットワークリソースを評価し、復元力、容量、および持続性を念頭に置いて適切なネットワークポロジを設計する必要があります。

一般的に、今日の組織ネットワークは、管理可能な有線 LAN と無線 LAN の組合せであり、時にはリモート LAN さえもある。ほとんどの配備要件を満たすように設計されているため、Edgecore EWS コントローラでサポートされるネットワークポロジの主な 2 つのカテゴリは次のとおりです。

- 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

このネットワークポロジは、オフィスビル、ホテル、校内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有線と無線の両方の機能から構成される管理された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。



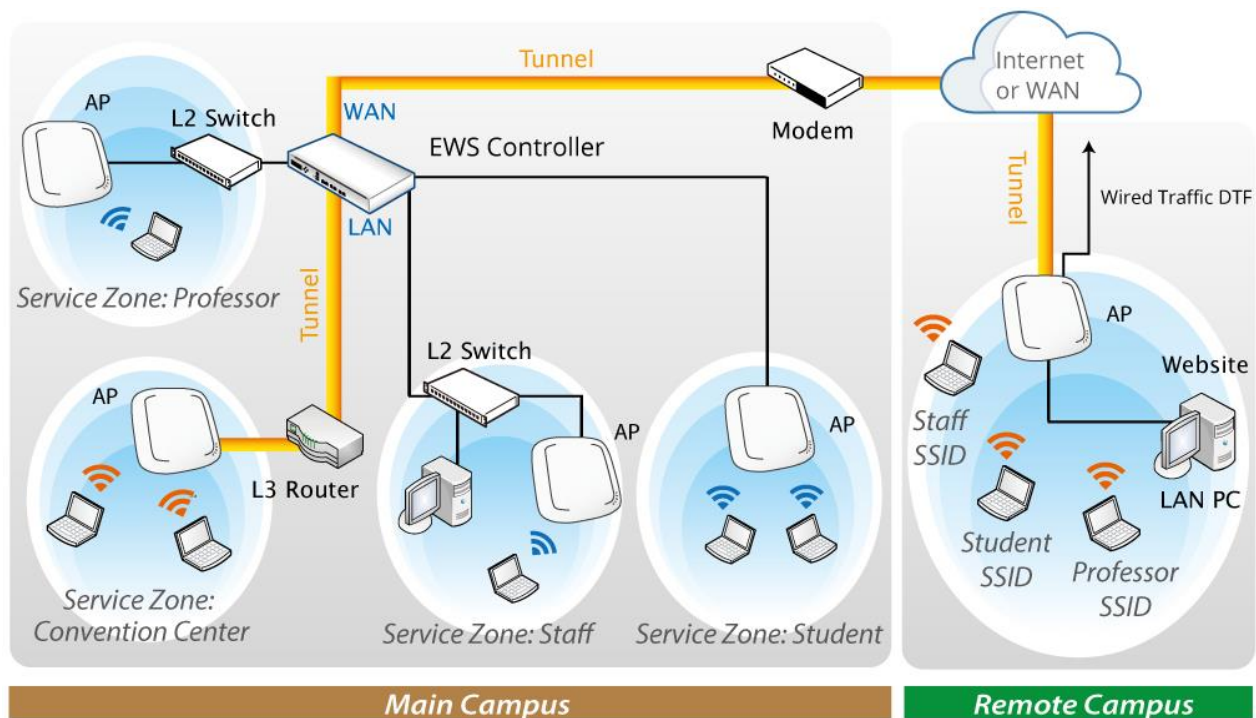
【レイヤ 2 トポロジのグラフィカルな図】

レイヤ 2 ネットワークデザインガイドライン

- 常に階層的に接続します。ビル内に複数のスイッチがある場合は、集約スイッチを使用します。
- ネットワークコア(メインフレームラックなど)に近い場所に集約スイッチを配置します。
- エッジスイッチをユーザに近い場所に配置します(フロアごとに 1 つなど)。

レイヤ 3 トポロジ

このネットワークトポロジは、エンタープライズビル、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有線および無線の両方の機能で構成される管理された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カルな図】

レイヤ 3 ネットワークデザインガイドライン

- ローカル LAN またはリモート LAN のどちらであっても、常に階層的に接続します。ビル内に複数のスイッチがある場合は、集約スイッチを使用します。
- ネットワークコア(メインフレームラックなど)に近い場所に集約スイッチを配置します。
- ユーザ(フロアごとに 1 つなど)に近いエッジスイッチを見つけます。
- 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)アップリンクは、パブリック IP アドレスまたはメイン EWS コントローラの WAN IP アドレスと同じサブネットの IP アドレスのいずれかを持つ必要があります。

3.2 アップリンク(WAN 側)の構成

3.2.1 WAN 設定

構成パス: Main Menu >> System >> WAN

WAN ポートは、4 つのコネクション構成 Static、Dynamic、PPPoE および PPTP をサポートします。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、WAN コネクションのスピードとデュプレックスを選択できます。オートネゴシエーションを ON にすると、インターフェースに接続されているデバイスとシステムがサポートする最高性能の伝送モード(速度/デュプレックス/フロー制御)を選択します。

The screenshot shows the 'WAN1 Configuration' page. On the left, there are two sections: 'Physical Mode' with a dropdown menu set to 'Auto', and 'Interface Type' with four radio button options: 'Static (Use the following IP settings)', 'Dynamic (IP settings assigned automatically)', 'PPPoE', and 'PPTP'. The 'Static' option is selected. To the right of the 'Static' option, there are five input fields with red asterisks indicating they are required: '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).

WAN ポートが接続している ISP のインターフェイスデバイスによっては、適用可能な接続タイプを選択する必要があります。たとえば、ご利用の ISP がダイナミック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: アップストリームネットワークで DHCP サーバが使用可能なネットワーク環境にのみ適用できます。Renew を選択すると、IP アドレスが自動的に表示されます。

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 にダイアルアップ接続するには、WAN 設定ページに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、ダイヤルアップ接続用の PPTP プロトコルは一部の ISP(ヨーロッパ諸国)によって採用されています。PPTP ISP は、PPTP サーバアドレスと同様に、パスワード付きのアカウントを発行します。

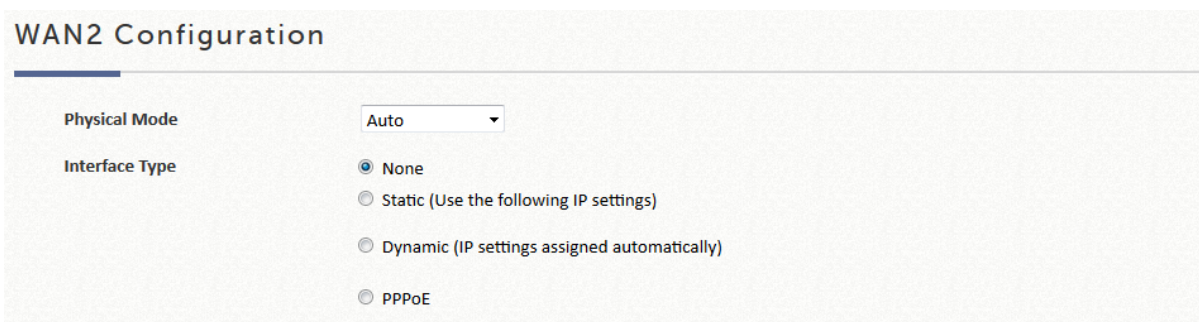
注意事項

1. お客様のアップリンクサービスの詳細については、お客様の 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およびフェイルオーバー対応のために 2 つの WAN ポートを備えて設計されています。WAN1 接続が確立されると、WAN2 をサービスに対して有効にできます。

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 (Static、Dynamic、PPPoE) のいずれかを選択します。WAN2 ポートの物理モードを選択できます。



WAN2 Configuration

Physical Mode: Auto

Interface Type:

- ☒ 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: アップストリームネットワークで DHCP サーバが使用可能なネットワーク環境にのみ適用されます。Renew を選択すると、IP アドレスが自動的に表示されます。

PPPoE: ISP が PPPoE ダイヤ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 にダイヤルアップ接続するには、WAN 設定ページにアカウント資格情報を入力する必要があります。

注意事項

1. お客様のアップリンクサービスの詳細については、お客様の 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 フェイルオーバー機能は、WAN2 が設定されている場合にのみ使用できます。

3.2.3 デュアル WAN1/WAN2 モデルの WAN ポートの選択

EWS コントローラモデル EWS5204 およびその上位モデルは、WAN1 および WAN2 用にそれぞれ SFP およびイーサネットポートを備えたキャリアグレードモデルです。管理者はさらに、物理ポートを WAN1 または WAN2、イーサネットポート、SFP ポート、イーサネットおよび SFP ポート、またはスループットを集約して使用する両方のポートとして決定できます。

構成パス: Main Menu >> System >> WAN

WAN1 Configuration

Physical Mode Auto

Interface Type

- ☐ Static (Use the following IP settings)
- ☒ Dynamic (IP settings assigned automatically) Renew
- ☐ PPPoE
- ☐ PPTP

☒ Obtain DNS server address automatically.

Preferred DNS Server: 168.95.1.1 *

Alternate DNS Server:

Transmission Option

- ☐ Ether Port
- ☐ Fiber Port
- ☒ Fiber Port and Ether Port
- ☐ Bonding

WAN2 Configuration

Physical Mode	Auto
Interface Type	☐ Static (Use the following IP settings) ☒ Dynamic (IP settings assigned automatically) Renew ☒ Obtain DNS server address automatically. Preferred DNS Server: 168.95.1.1 * Alternate DNS Server:
	☐ PPPoE ☐ PPTP
Transmission Option	☐ Ether Port ☐ Fiber Port ☒ Fiber Port and Ether Port ☐ Bonding

展開オプションは次のとおりです。

- **Ether Port:** 銅線イーサネット WAN ポートをサービス用に準備します。
- **Fiber Port:** SFP ポートをサービス用に準備します。
- **Fiber Port and Ether Port:** ブリッジファイバポートとイーサネットポート。物理的には、SFP ポートまたはイーサポートのどちらかを使い 1 つのアップリンクのみに接続します。
- **Bonding:** SFP ポートと銅線イーサネットポートの両方をサービス用に準備します。このオプションは 2 つの接続を集約し、集約されたより高いスループットを実現します。

3.2.4 WAN トラフィック制御

WAN Traffic Settings

Bandwidth Limitation	☒ Enable Bandwidth limitation on WAN
Max Uplink Bandwidth	2000000 Kbps
Max Downlink Bandwidth	2000000 Kbps

ここで設定するアップリンクとダウンリンクの帯域幅は、WAN1 と WAN2 を含む WAN インタ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ていることに注意してください。たとえば、ISP のネットワーク速度が 1Gbps に制限されている場合、コントローラに 2Gbps を設定しても、このような制約の下での合計スループットは 1Gbps を超えません。

3.2.5 アップリンクの検出とフェイルオーバー

アップリンク検出

WAN インタフェースに有効なアップリンク接続が設定されている場合、管理者は、アップリンクサービスがアクティブかダウンかを確認するための検出ターゲットとして、最大 3 つの送信側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することができます。このフィールドは、3 つのすべての検出ターゲットが応答しない場合にユーザの 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、WAN1 および WAN2 ポートにわたりシステムトラフィックを分散できます。

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 フェイルオーバー

有効にすると、WAN1 がダウンするたびに、WAN2 は最初に 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 のリンクが再びアップになると、WAN1 に戻ります。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

☒ 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

☒ Fall back when WAN1 connection is restored

注意事項

1. WAN フェイルオーバー機能は、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 Controller のダウンリンクは、基本的に、サービス用に準備された管理ネットワークです。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、ポートベースのモードとタグベースのモードの 2 種類があります。

注意事項

1. HA 機能が Enabled ステータスの場合、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。

構成パス: Main Menu >> System >> LAN Ports

3.3.1 ポートベースサービスゾーン

ポートベースモードは、それぞれの物理 LAN ポートを有効なサービスゾーンにマッピングしたり、サービスの提供を無効にしたりできるという原則で動作します。したがって、ポートベースのモードで動作は、実際にサービスを提供するために使用できるサービスゾーンの最大数が、コントローラの LAN ポートの数によって決まることを意味します。

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

Default ▼

SZ1 ▼

SZ2 ▼

Disable ▼

LAN1 LAN2 LAN3 LAN4

3.3.2 タグベースのサービスゾーン

タグベースのオペレーションモードは、異なるサービスゾーンが VLAN ID で識別されるという原則に基づいて動作します。つまり、タグベースのオペレーションでは、各物理 LAN ポートが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、VLAN ID トラフィックパケットの伝送に従っ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

Default ▼

Default ▼

Default ▼

Default ▼

LAN1 LAN2 LAN3 LAN4

第4章 ユーザ認証データベース

4.1 認証データベースの設定

認証データベースは、ユーザの資格情報を照会して有効性を確認することができる記憶装置です。ユーザがサービスゾーンで有効になっている認証に関連付けられている場合、Edgecore EWS コントローラは、送信されたユーザ ID とパスワードの組合せが存在するかどうかを確認するためにデータベースをチェックし、ユーザがネットワークアクセスできるようにします。Edgecore EWS コントローラは、組み込みおよび外部の認証データベースに対応しています。

以下に、すべての認証オプションを示します。

ビルトイン認証オプション

Local はユーザ資格情報と合わせ組み込みのローカルデータベースに保管されます。

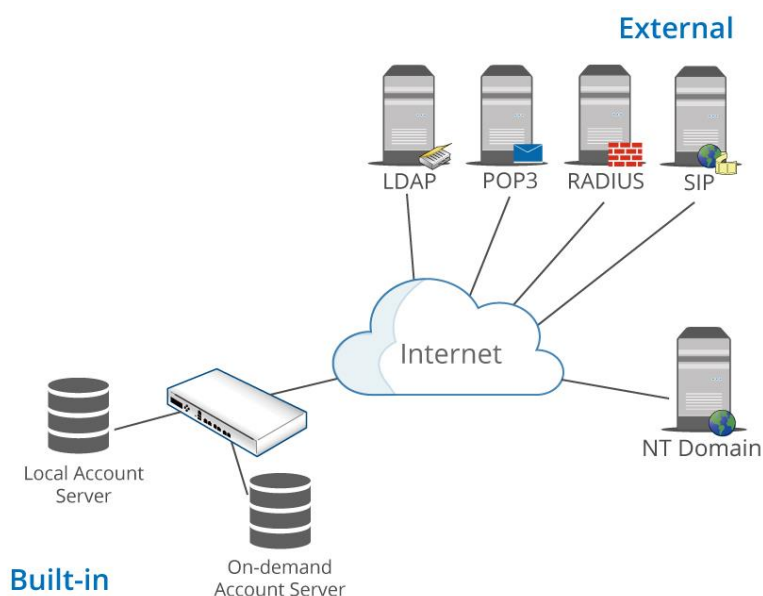
On-Demand はユーザ資格情報と合わせ組み込みのオンデマンドデータベースに保管されます。

Guest はログインページで指定された ID トークンを使用して、ユーザ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。

One Time Password は 1 つのログインセッションでのみ有効な SMS によって送信されたパスワードを使用して、ユーザ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。

外部認証オプション

これらのオプションは、外部サーバを使用して認証処理を実装します。Edgecore EWS コントローラは、RADIUS、LDAP、NT Domain、POP3、SIP、Social Media を含む、一般的な外部認証オプションに対応しています。



【EWS Controller に関する認証データベースの図解】

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

内外認証用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(RADIUS、POP3、LDAP、NTドメイン、および SIP)はカスタマイズ可能で、同時に有効にすることができます。

注意事項

1. 認証オプションは、サービスゾーンプロファイルごとのユーザを認証するために、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

構成パス: Main Menu >> Users >> Internal Authentication

4.2.1 ローカルユーザデータベース

この種の認証方式では、ユーザを格納するローカルデータベース(多くの場合は職員と資格情報)が内部でチェックされます。ローカルユーザデータベースは、管理者が手動で実行しない限り削除されないスタティックアカウントを格納するように設計されています。

構成パス: 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ます。

Local User List

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	☐	☐	
			Group 1	☐	☐	
			Group 1	☐	☐	
			Group 1	☐	☐	

注意事項

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、その他はオプションです。
2. 一度設定されると、MAC Address フィールドは、指定されたデバイスを使用してのみアクセスが許可されるという条件下で、この特定のアカウントをバインドします。
3. Group フィールドは、生成されたアカウントのグループプロファイルを指定します。
4. Remark は、管理者が強調したい任意のメモに用います。ユーザー一覧に表示されます。
5. Enable Local VPN チェックボックスをオンにすると、アカウントを使用するデバイスとコントローラ間にセキュア VPN トンネルを構築できます。
6. Expiration は、Account Span オプションがチェックされている場合に、このアカウントに適用されるオプションの時間制約です。これは、Multiple Login を使用する場合に役立ちます。たとえば、セミナーイベント中など、指定した期間、複数のグループにネットワークアクセスを提供する場合に適しています。

アカウントのインポートとエクスポート

ローカルユーザデータベースは、それぞれ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 フォーマットのテキストファイルになります。管理者は save as を実行して、今後使用するためにユーザアカウントを PC 記憶域にバックアップすることができます。アップロード処理は、バックアップされたテキストファイルを参照し、アカウントをローカルユーザデータベースにインポートすることによって実行されます。

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:

注意事項

1. 生成されたテキストファイルは、定義された CSV フォーマットがすべてのモデルで一貫しているため、すべての EWS コントローラシリーズで相互に使用できます。
2. アカウントが重複していると、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修正

既存のユーザアカウントでは、ページ上のユーザ名ハイパーリンクをクリックしてアカウント属性を再設定するだけで、さらに修正を加えることができます。

Local User List

Add... Delete Backup List Upload Search

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

Editing Existing User Data

Username

Password

MAC Address

Applied Group

Enable Local VPN ☐

Remark

Enable Expire Time ☐

Begin Date

End Date

アカウントの削除

ローカルユーザデータベース内のアカウントを個別に削除できます。また、Select All にチェックを入れると、完全に削除することもできます。アクションを実行するかどうか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

Add... Delete Backup List Upload Search

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

4.2.2 オンデマンドユーザデータベース

オンデマンドユーザデータベースは、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、エンタープライズビジターレセプションなどのネットワーク構築のニーズに最適です。オンデマンド認証オプションは、カスタマイズのために多くのオプションを提供します。POS チケットは、企業のニーズに合わせてカスタマイズすることができます。また、複数種の決済オプションを EWS Controller で利用することもできます。

構成パス: Main Menu >> Users >> Internal Authentication >> On-Demand

On-Demand Authentication

User Postfix	ondemand
Billing Plans	Configure
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	30 day(s)
Out-of-quota Account Cache	30 day(s)
Set Ticket's Serial Number	000001 Set
Web Printout	Configure This will be applied to the regular printer printout when creating a single On-Demand account.
POS Tickets	Configure Number of Tickets ☒ 1 ☐ 2 This will be applied to printouts from the POS ticket printer. Templates can be edited for customization.
Terminal Server	Configure Terminal Servers are add-on devices such as the SDS100 or SDS200W.
Payment Gateway	Configure
SMS Gateway	Configure
Account Roaming Out	☐ Enable ☒ Disable

オンデマンドアカウントの設定

1. オンデマンドアカウントデータベース全般の設定を行います。この設定には、POS/Web チケット、決済ゲートウェイオプションなどのカスタマイズが含まれます。アカウント生成のためにチケットプリンタ(EC-PP200 など)を導入する場合は、ターミナルサーバの設定で IP とポートを設定することを忘れないでください。EWS コントローラは、Clickatell SMS サーバと連携して動作し、オンデマンドアカウント資格情報を SMS メッセージを介してユーザに送信できます。

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	☐			
2	☐			
3	☐			
4	☐			
5	☐			
6	☐			
7	☐			
8	☐			
9	☐			
0	☐			

Account Registration Control

☒ Disable

☐ Black List

☐ White List

Web Page Customization

一連の Clickatell アカウント Username/Password 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 ゲートウェイを設定できます。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することができます。API ID を定義し、必要な請求計画を有効化します。必要に応じて、複数の料金プランを有効にすることができます。

アカウント生成の 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、アカウント登録制御オプションを使用できます。また、管理者は、アカウントの有効期限が切れる前に、ユーザが新しいアカウントの登録することを、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しないようにするには、オプションを Enabled に設定します。

SMS ゲートウェイを有効にすると、請求計画の選択ページが表示されます。

Plan (s)	Price (¥)	Remark
☒ 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**

Billing Plan Selection ページは、必要に応じてカスタマイズできることに注意してください。

2. Billing Plans でアカウント使用期間を定義します。管理者が、適切なアカウントの種類を選択することによって、使用期間をカスタマイズする 10 までの課金プランプロファイルが利用可能です。請求書プランごとのユーザグループプロファイルもここに割り当てられます。

Billing Plans

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

注意事項

- 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。
- 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

構成パス: Main Menu >> Users >> On-Demand Accounts

選択した料金プランを有効にすると、On-Demand Account Creation でオンデマンドアカウント生成を実行できます。オンデマンドアカウントは、個別に作成することも、バッチで作成することもできます。

The On-Demand Accounts List には、既存のすべてのオンデマンドアカウントが格納されています。それぞれのアカウントのステータス、クォータなどが参考のために表示されます。オンデマンドアカウントの読み込み、書き出し、削除、および管理者の交替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、クォータ外、および期限切れとして定義されます。

有効 = アクティブまたはクォータの残っているオンデマンドアカウント

合計 = 有効 + クォータ外 + 期限切れ

また、このリストの最後に、オンデマンドアカウントの有効件数と総件数が表示されます。

Main > Users > On-Demand Accounts > Account List

On-Demand Account List

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

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

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

4.2.3 ゲスト認証オプション

ゲスト認証オプションは、技術的にはユーザデータベースではなく、ユーザがユーザ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、サーフィンできるように特別に設計されたオプションです。

この機能を使用すると、ユーザを特定のサービスゾーンに関連付け、管理者が定義したソーシャルセキュリティ番号、電子メールなどの特定の文字列を入力し、実際の認証なしでネットワークを使用できます。

使用期間と使用制限は、ゲスト認証オプションプロファイルで設定できます。

構成パス: 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: ☐ Unlimited ☒ 1 Day Access ☐ 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: ☒ Disable ☐ Enable

Guest Quota List: View

E-mail Denial List: ☒ Disable ☐ Enable Configure

Apply Cancel

E-mail Denial List は、ジャンクメールボックスの防止が必要な場合に、ログイン許可のため電子メールアドレスをチェックします。**Guest Questionnaire** では、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するオプションが管理者に提供されます。ゲストユーザ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** を制限有りに設定すると、MAC アドレスに基づいて使用時間の制約が適用されます。**Quota** が 30 分に設定されている場合、各デバイスの使用は 30 分のみ許可され、新しいセッションは **Reactivation** 時間が経過した後にのみ許可されます。また、管理者は、**Access Limit** を設定して、デバイスが 1 日に空き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、ゲストユーザは、ポリシーアプリケーション用に選択したユーザ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、MAC アドレスと電子メールアドレスによって、アクセス制限付きのゲストアカウントに残っている許可の回数を確認できます。(毎日、深夜に自動的に更新され、最大クォータ 12000 に達すると最も古いエントリが削除されます)。

LOGIN

Username

Password

☐ Remember Me

FREE LOGIN

Email

Age

Cell Phone

Enter your Email account to login for free.

Main > Users > Internal Authentication > Guest Authentication > Guest Questionnaire

Guest Questionnaire

No.	Active	Question
1	☒	Age
2	☒	Cell Phone
3	☐	
4	☐	
5	☐	

Guest Information

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:

Email verification により、入力し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、アクティブ化時刻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、メールサーバから送付された電子メールのリンクをクリックすることにより、自分の利用時間を延長するために、有効時間内にこのアカウントを有効化しなければなりません。アクティブ化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 サーバの準備ができたらすぐにカスタマイズできます。SMTP サーバの設定は、Assign SMTP Server ボタンをクリックして行います。

Email Verification

☐ Disable ☒ Enable

SMTP server is not ready

Email activation time hour(s) minute(s)

Sender name

Activation email subject

Activation email content

Activation link

Guest Account List

アカウントの一部の情報は、管理者の詳細な解析またはマーケティング目的のために、**Guest Information** リストに収集することができます。電子メールアドレス、機器の MAC アドレス、最終ログイン時刻、および **Guest Questionnaire** の回答。

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:

管理者は、"Download"ボタンをクリックすると、収集したゲスト情報をダウンロードできます。また、"Delete All"ボタンをクリックすると、保存されているすべてのデータを削除できます。管理者は、リストを最新の状態に保つために、エクスポート後にすべてのエントリを削除できます。

注意事項

- Guest Questionnaire 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。請求とリマインダを含めるには、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にインプリメントする

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ます。Main Menu>System>Service Zone>Configure に移動します。ページを Authentication Options まで下にスクロールします。下図に示すように、ゲスト認証オプションのオプションを Enabled をチェックします。

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	☒	☒
Server 2	RADIUS	radius	☐	☒
Server 3	NTDOMAIN	ntdomain	☐	☒
Server 4	LDAP	ldap	☐	☒
Server 5	POP3	pop3	☐	☒
On-Demand	ONDEMAND	ondemand	☐	☒
SIP	SIP	N/A	☐	☐
Guest	FREE	N/A	☐	☒

ステップ 1 およびステップ 2 の設定を行った後、結果として、エンドユーザはサービスゾーンのログインページにゲストアクセスの追加セクションが表示されることを確認します。

電子メールアドレスを入力し、Login をクリックして、公開 Wi-Fi に無料でアクセスする期間と条件を承認すると、ゲストユーザはゲスト認証オプションプロファイルおよびグループプロファイルで指定された制約を使用してネットワークにアクセスできるようになります。フリー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。

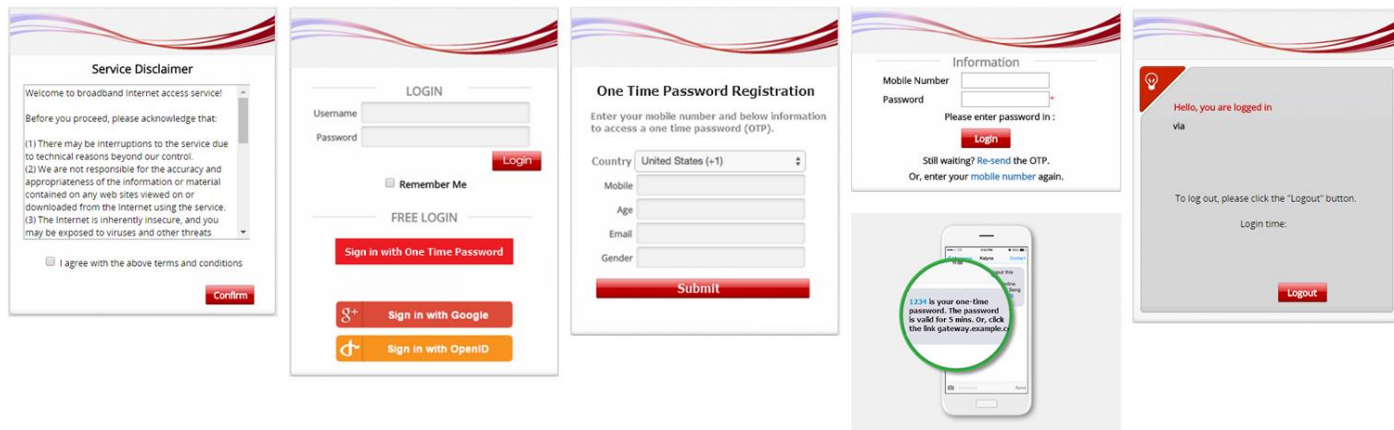
The image shows a web-based login form. At the top, there's a decorative header with blue and red wavy lines. Below this, the form is divided into two main sections. The first section is titled 'LOGIN' in bold. It contains two input fields: 'Username' and 'Password'. To the right of the 'Password' field is a red button with the text 'Login'. The second section is titled 'FREE LOGIN' in bold. It contains one input field: 'Email'. Below the 'Email' field is a line of text that says 'Enter your Email account to login for free.' To the right of this text is another red button with the text 'Login'.

4.2.4 ワンタイムパスワード

ワンタイムパスワード(OTP)認証オプションでは、クライアントは自身の携帯電話番号を入力し、認証画面に入力する必要があるワンタイムパスワードで SMS メッセージを受信することによって、インターネットにアクセスすることができます。その後、クライアントはインターネットサーフィンを開始できます。

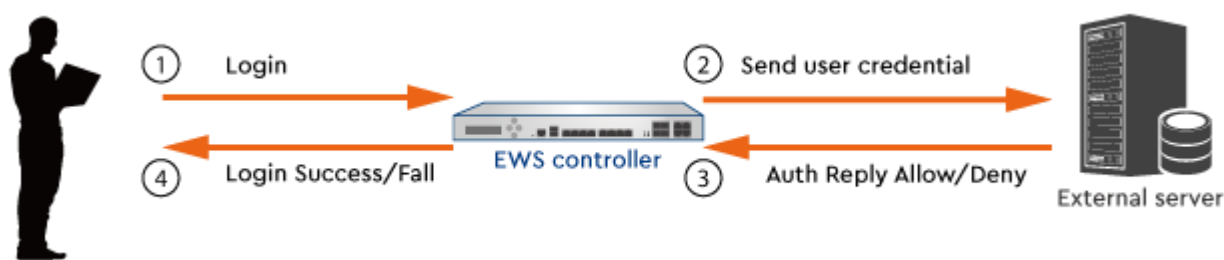
通常、ユーザログインフローには次の手順とページが含まれます。

- A. **Service Disclaimer:** (チェックした場合)ログインプロセスを続行するために条文とサービスに同意します。
- B. **General Login Page:** sign in with one time password ボタンを押します。
- C. **OTP Registration Page:** 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します。
- D. **Receive SMS with OTP:** クライアントの携帯電話はパスコードが記載されたテキストを受信します。
- E. **OTP Authentication Page:** 検証および認証のために OTP を入力します。
- F. **Login Success Page:** 素晴らしい、ネットサーフィンの時



4.3 外部認証オプション

ほとんどの組織では、すでに集中ユーザアカウントサーバが確立されています。そこで Edgcore EWS コントローラは、アカウントローミングに対応し、現行のネットワークに適応するために、様々な外部認証オプションを備えています。外部認証を使用した簡単な例を以下に示します。



注意事項

1. 組み込みデータベースまたは外部データベースを使用して認証オプションを設定した場合は、有効にするサービスゾーンごとに有効にする必要があります。

4.3.1 RADIUS

Remote Authentication Dial In User Service (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の、集中管理された認証、承認、およびアカウントティング(AAA)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最も一般的な外部認証メカニズムでもあります。

構成パス: Main Menu >> Users >> External Authentication

Server No. 2: Server 2 ▼

External RADIUS Server Settings

Group	Group 1 ▼
Local VPN	☐ Enable Local VPN
802.1X Authentication	☐ Enable ☒ Disable
Username Format	☒ Leave Unmodified ☐ Complete (e.g. user1@postfix) ☐ Only ID (e.g. user1)
NAS Identifier	
NAS Port Type	19 *(Default 19, Range: 0~35)
Accounting Delay Time	0 *(Default: 0)
Service Type	1 *(Default: 1, Range: 1~11)
Class	
Class-Group Mapping	Configure

デフォルトでは、サーバ 2 は RADIUS 認証を使用するように設定されています。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。

RADIUS 設定の詳細設定ページを以下に示します。Primary RADIUS Server および Secondary RADIUS Server の属性は、サービス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

19 *(Default 19, Range: 0~35)

Accounting Delay Time

0 *(Default: 0)

Service Type

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

Class

Class-Group Mapping

Configure

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

DM & CoA Settings

Configure

Send Acct Interim when users' IP changes

☐ Enable ☒ Disable

Failover between RADIUS Servers

☐ Enable ☒ Disable

Attributes Priority

Follow Server's Setting ▼

Standard RADIUS Attributes

Session Timeout

240 Minutes *(Range: 5-1440 mins)

Idle Timeout

10 Minutes *(Range: 1-120 mins)

Acct Interim Interval

15 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

3 *(Default: 3)

Timeout

6 *(Default: 6)

Primary RADIUS Server

Authentication Server

*(Domain Name/IP Address)

Authentication Port

*(Default: 1812)

Authentication Secret Key

*

Authentication Protocol

CHAP ▼

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

CHAP ▼

Accounting Service

☒ Enable ☐ Disable

Accounting Server

(Domain Name/IP Address)

Accounting Port

Accounting Secret Key

別の重要な設定項目として、ページ上の Class-Group Mapping があります。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プし、異なる RADIUS アカウントを異なるグループに組み込むことを可能にする変換設定です。

4.3.2 POP3

POP3 は、特定のインターネットサーバによって電子メールが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、POP3 サーバに保存されている電子メールアドレスとパスワードの入力により、ユーザにインターネットサービスを許可する認証方法を管理者に提供しています。

構成パス: Main Menu >> Users >> External Authentication

デフォルトでは、サーバ 5 は POP3 認証を使用するように設定されています。Server Name をクリックすると、POP3 サーバアドレス、セカンダリ POP3 サーバ指定など、必要な設定を問い合わせるための詳細な設定画面が表示されます。

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

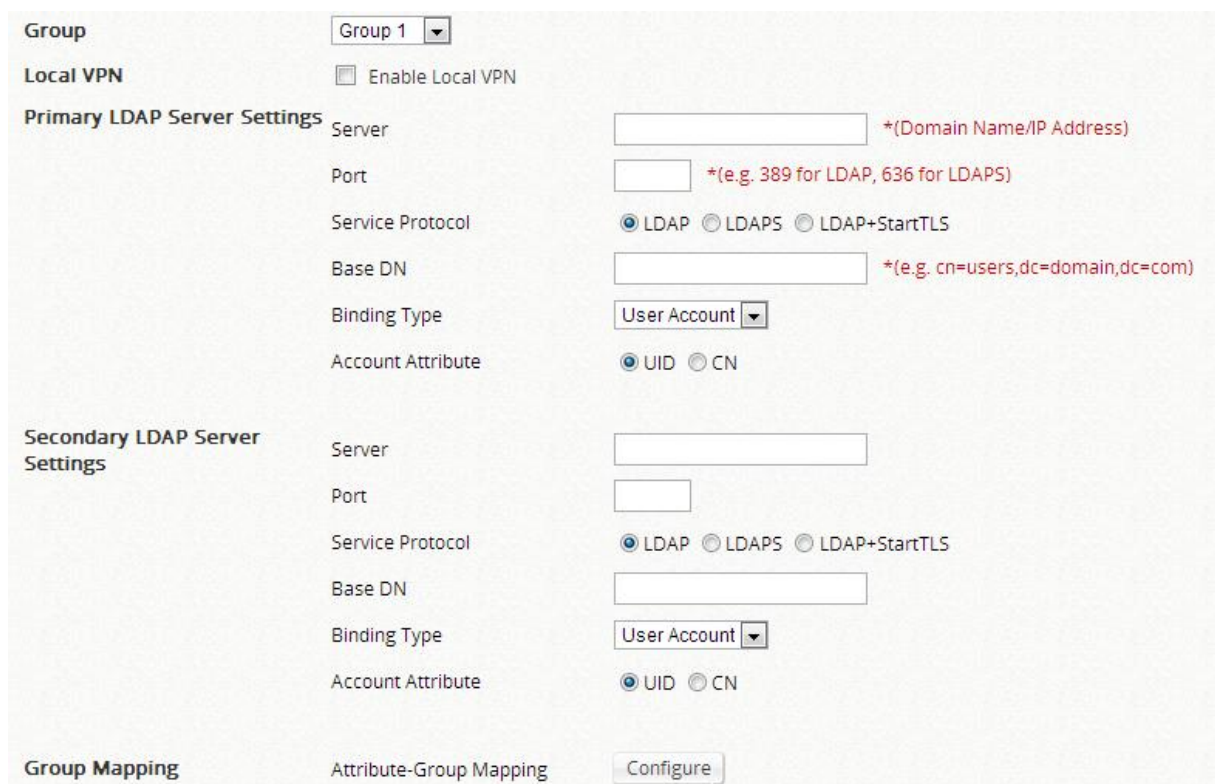
4.3.3 LDAP

Lightweight Directory Access Protocol(LDAP)は、IP ネットワークで分散ディレクトリ情報サービスにアクセスし、維持するためのアプリケーションプロトコルです。

ユーザ認証のために LDAP サーバを展開する場合は、完全な設定に進みます。

構成パス: Main Menu >> Users >> External Authentication

ユーザ認証情報の確認に LDAP データベースを使用するには、デフォルトでサーバ 4 が選択されています。Server Name を選択して、LDAP の詳細設定画面に入ります(セカンダリ LDAP サーバをバックアップサーバとして指定できます)。さらに、LDAP 設定ページには、Edgecore EWS コントローラ上の異なるグループに LDAP 属性をマッピングする Attribute-Group Mapping 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, organized into several sections:

- Group:** A dropdown menu currently set to "Group 1".
- Local VPN:** A checkbox labeled "Enable Local VPN" which is currently unchecked.
- Primary LDAP Server Settings:**
 - Server:** A text input field with a red asterisk and the note "*(Domain Name/IP Address)".
 - Port:** A text input field with a red asterisk and the note "*(e.g. 389 for LDAP, 636 for LDAPS)".
 - Service Protocol:** Three radio buttons: "LDAP" (selected), "LDAPS", and "LDAP+StartTLS".
 - Base DN:** A text input field with a red asterisk and the note "*(e.g. cn=users,dc=domain,dc=com)".
 - Binding Type:** A dropdown menu set to "User Account".
 - Account Attribute:** Two radio buttons: "UID" (selected) and "CN".
- Secondary LDAP Server Settings:**
 - Server:** A text input field.
 - Port:** A text input field.
 - Service Protocol:** Three radio buttons: "LDAP" (selected), "LDAPS", and "LDAP+StartTLS".
 - Base DN:** A text input field.
 - Binding Type:** A dropdown menu set to "User Account".
 - Account Attribute:** Two radio buttons: "UID" (selected) and "CN".
- Group Mapping:** A section with the label "Attribute-Group Mapping" 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、ユーザ資格認証を実行します。

構成パス: Main Menu >> Users >> External Authentication

Server No. 3: Server 3

NT Domain Server Settings

Group Group 1

Local VPN ☐ Enable Local VPN

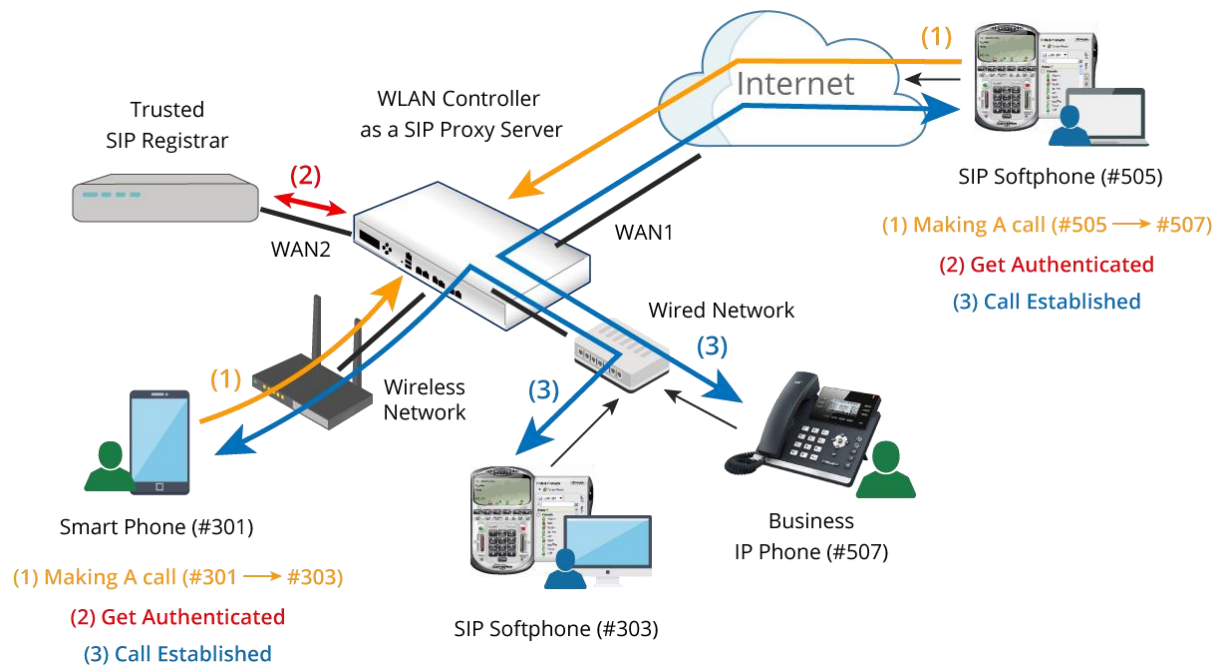
NTDomain Server Settings Server

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

デフォルトサーバでは、NTドメインを使用するには 3 が選択されています。管理者は、ユーザ資格情報が格納されているドメインコントローラ IP アドレスを入力する必要があるだけです。さらに、Windows アクティブディレクトリがデバイスアクセスのアイデンティティチェックとして準備されている場合、Transparent Login 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およびネットワークへのアクセスを許可することができます。

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 電話の使用だけでなく、SIP 認証にも対応しています。管理者は、Edgecore EWS コントローラに加えて、正常な SIP 通話を行うように他のデバイスを設定する必要があります。これには、有効な SIP レジストラ、SIP 電話機が含まれます。



- (1) ユーザは、SIPベースの電話機(#301-->#303 など)から発信しています。
- (2) ユーザがSIPレジストラに登録されている場合、ユーザは透過的に認証されます。
- (3)呼が正常に確立されました。

構成パス: 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 は選択されていません。各サービスゾーンの認証設定(Authentication Settings)から SIP を有効にします。管理者は、電話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 QoS 設定が適切に設定されている必要があることに注意してください。

Authentication Server - SIP

Trusted Registrar

IP Address	Remark

また、適切に機能させるために、SIP インタフェース設定で対応するサービスゾーンにも Enabled がチェックされていることを確認してください。

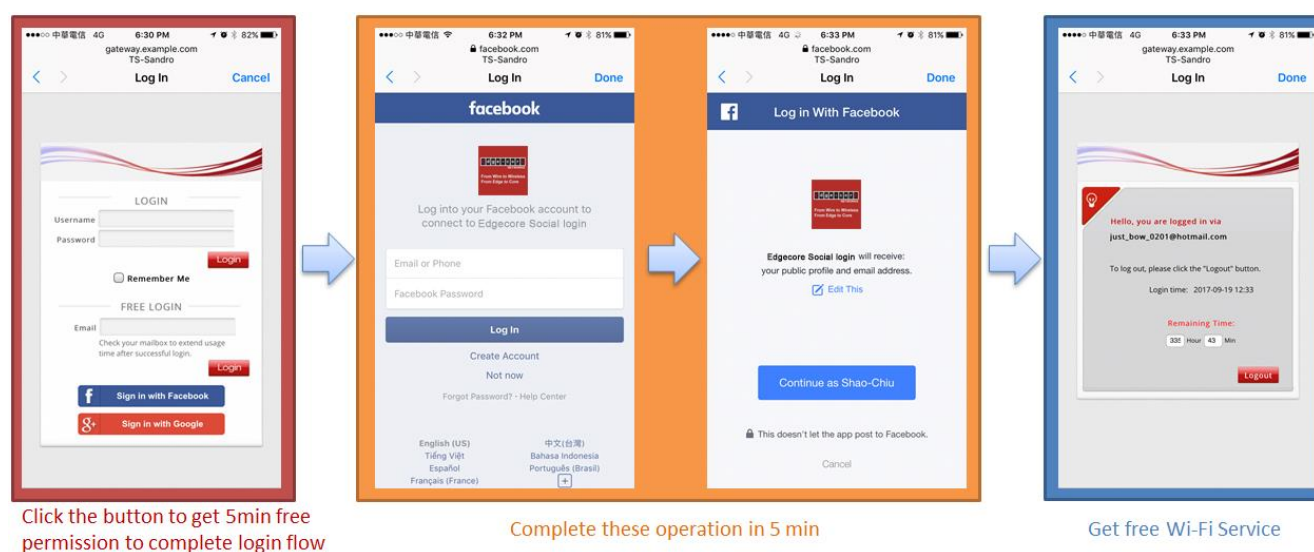
Authentication Settings

Authentication	☒ Enable ☐ Disable ☐ Suspend
When Authentication is set to Suspended, users would see a suspend message from General Settings.	
Access Permission and Authorization	<button>Configure</button>
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
WAN Interface WAN1	
WISPr Settings	<button>Configure</button>

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ユーザは面倒なアカウント登録処理を行うことなく、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、ソーシャルメディアアカウント、LINE、Facebook、Twitter、Weibo、VK、dAccount、およびOpen ID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。

ユーザがこのボタンをクリックしてソーシャルメディアアカウントでサインインすると、ログインおよび権限付与のために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を気にす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 分間無料でアクセスできます。その後、必要なソーシャルアカウントを入力して 5 分の間にログイン処理を完了する必要があります。その後、下図のようにインターネットサーフィンを開始します。



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方法について説明します。

- LINE: LINE 開発者サイト(<https://developers.line.me/console/>)の Web サイトにアクセスし、LINE Login APP を申請し、アプリの種類が WEB であるためチャンネル ID とチャンネルシークレットを取得します。
- Facebook: Facebook 開発者サイト(<https://developers.facebook.com/>)の Web サイトにアクセスし、Facebook Login APP を申請し、アプリ ID とアプリシークレットを取得します。
- Twitter: Twitter 開発者サイト(<https://developer.twitter.com/>)の Web サイトにアクセスし、Twitter API を申請して API キーと API シークレットを取得します。
- Weibo: Weibo 開発者サイト(<http://open.weibo.com/liveapi/index.php>)の Web サイトにアクセスし、LINE Login APP を申請し、アプリの種類が WEB であるためチャンネル ID とチャンネルシークレットを取得します。
- VK: VK 開発者サイト(<https://vk.com/dev>)の Web サイトにアクセスし、LINE Login APP を申請し、アプリの種類が WEB であるためチャンネル ID とチャンネルシークレットを取得します。
- dAccount: d アカウント・コネクトサイト
(https://id.smt.docomo.ne.jp/src/index_business.html?btn01)の Web サイトにアクセスし、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ます。
- OpenID: ログインパスをたどって OpenID ウォールドガーデンに追加しなければならず、リダイレクションターゲットは OpenID プロバイダに依存します。

Social API Credentials

Line Login	☐
Line App ID	
Line App Secret	
Facebook Login	☐
Facebook App ID	
Facebook App Secret	
Twitter Login	☐
Twitter API Key	
Twitter API Secret	
Weibo Login	☐
Weibo App ID	
Weibo App Secret	
VK Login	☐
VK App ID	
VK App Secret	
dAccount Login	☐
dAccount Client ID	
dAccount Client Secret	
Please use a valid and trusted HTTPS certificate when enabling dAccount login.	
OpenID Login	☐

☒ Apply

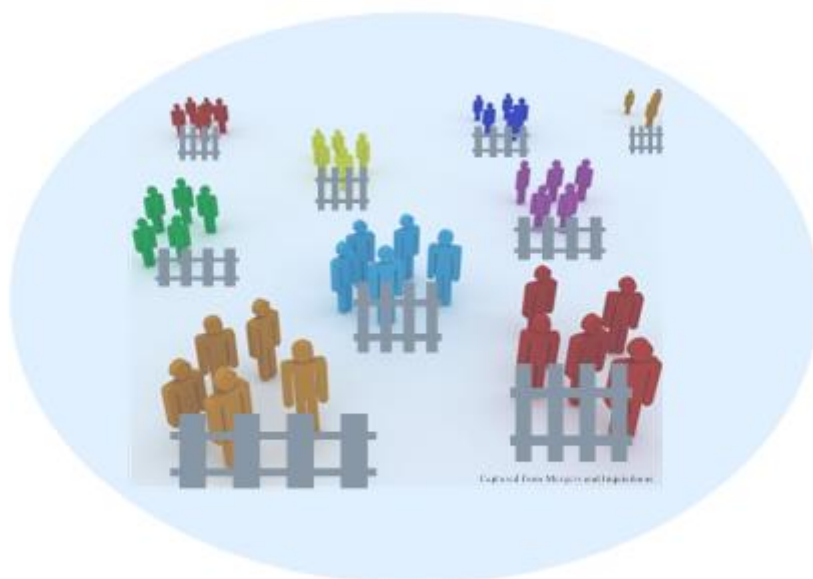
☐ Cancel

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は、グループとポリシーを利用して、ユーザのアクセシビリティとネットワーク権限を定義し、ユーザの挙動に制約を設定します。グループ化、ポリシー設定、サービスゾーンは互いに関連しているため、ここでは、グループ化、ポリシー、サービスゾーンとの関係を明確にし、次にこれら 3 つの属性について実際的なセットアップ手順を説明します。

5.1 コンセプトの概要

- グループ



グループとは、ある程度類似した特性(役割などにもとづく)を共有していると管理者が見なす一連のユーザです。たとえば、大学には、学生、教職員、およびゲストが一般的に存在します。したがって、これら 3 つのインターネット・サービス・ユーザのカテゴリを区別する 3 つのグループを、これらのグループに異なるインターネット・アクセシビリティの許可を与えることによって設定することができます。EdgecoreEWS モデルでは、モデルキャパシティに応じて、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、ローカルユーザは、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。また、外部サーバ、Edgecore EWS コントローラによって認証されたユーザについては、クラスグループマッピングおよび属性グループマッピングによって、RADIUS および LDAP オプションのアカウントごとにグループ割り当てがそれぞれ提供されます。

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. **Quality of service(QoS):**

Voice、Video、ベストエフォート、およびバックグラウンドをトラフィッククラスで選択できます。

すべてのグループメンバーが共有しているアップリンクとダウンリンクの合計レート

個々のダウンリンクおよびアップリンクの最大レート

2. **権限プロファイル:**

特定のグループの認証ユーザを有効にして、コントローラのデフォルト/テンプレートログインサksesページでオンデマンドアカウントを生成するためのオンデマンドアカウント権限。

ユーザがコントローラのデフォルト/テンプレートログインサksesページに正常にログインした後で、自分のパスワードを変更できるようにするためのパスワード変更権限。

同時セッションの最大数では、ユーザごとに許可される同時ログインの数を指定します。

3. **サービスゾーンのアクセシビリティ:**

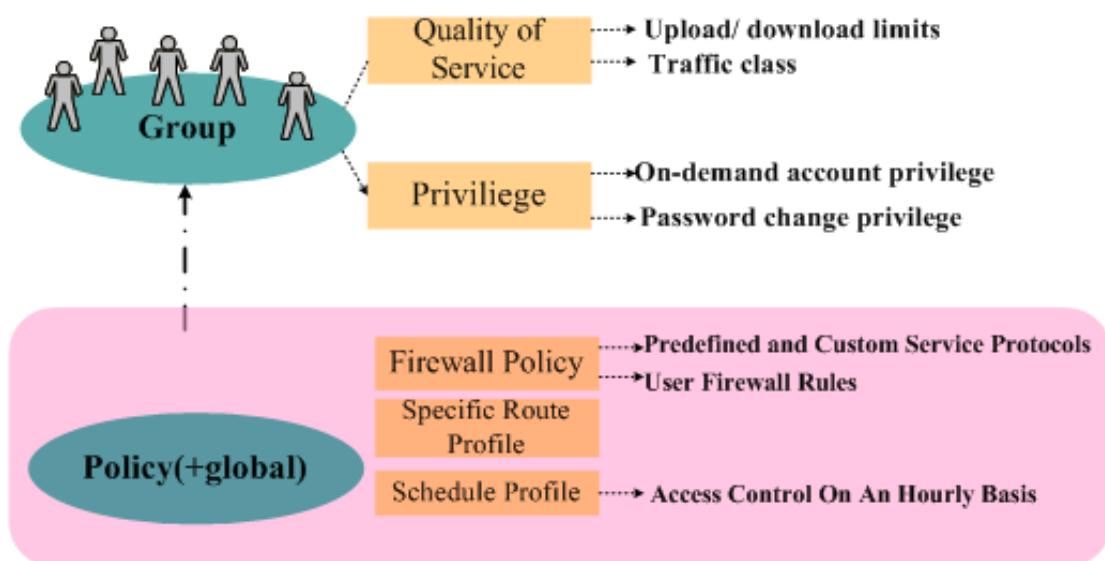
バンドルされているポリシーと同様に、特定のサービスゾーンに対して、アクセスまたはアクセス拒否の許可を設定できます。

● **ポリシー**

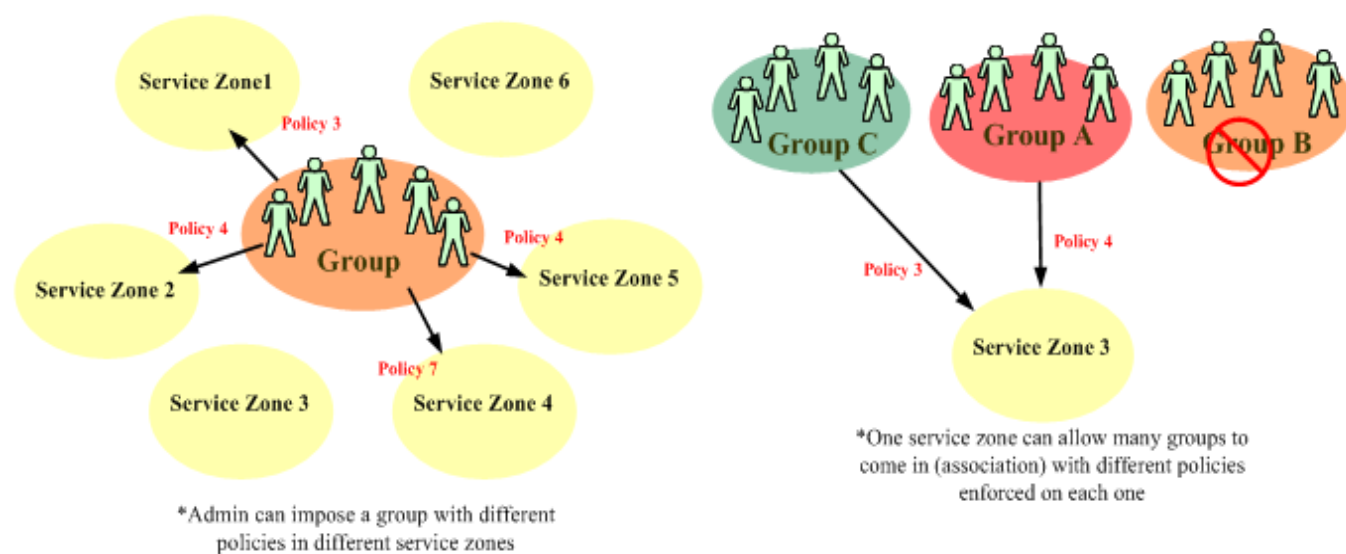
用語が示すように、ポリシーは、ファイアウォールルール、ログインスケジュール、ルーティングルール、セッション許可など、ユーザに適用される制約を制御するネットワークのプロファイルです。グローバルポリシーがあります。これは、ユーザがポリシーにバインドされていないグループに属している場合に適用されます。ポリシープロファイルの数はモデルに依存します。

グループ・プロファイルとポリシー・プロファイルは、柔軟性を高めるために分離されています。これにより、管理者が定義したグループサービスゾーンのパーミッションマッピング設定に従って、同じグループのユーザを別のポリシーでバインドできます。例えば、グループ 1 のユーザに、サービスゾーン 1 ではポリシー 1 を適用しますが、サービスゾーン 3 に移動するとポリシー 3 を適用するようなことができます。

- グループ、ポリシー、およびサービスゾーン間の関係



最初の図は、グループとポリシーの関係と、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、サービスゾーンへのグループのマッピングとそのほかの方法の 2 つの観点から定義できます。以下の図解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セットアップ

ここでは、Edgecore EWS コントローラの WMI でグループとポリシーを実際に設定する方法について、スクリーンショットを使って説明します。

- **Group Overview**

構成パス: Main Menu >> Users >> Groups >> Overview

Group Overview テーブルには、対応するグループごとにどの認証サーバが使用されるかのサマリーが表示されます。オンデマンド認証データベースの課金プランに割り当てられたユーザグループもここに表示されます。

Group Overview	
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	

- **Group Settings**

構成パス: Main Menu >> Users >> Groups >> Configuration

Group Configuration - Group x テーブルは、グループのポリシー設定を定義するためのテーブルです。複数デバイスログイン(オンデマンドを除きます)は、ここで有効にすることができます。

Zone Permission Configuration & Policy Assignment - Group x テーブルでは、管理者がグループ、ポリシー、およびサービスゾーン間の関係を決定できます。

Group Configuration

Select Group Group 1 ▼

Group Name Group 1

Remark

Number of devices which are allowed to login 1
(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 ▼
☒	Service Zone : Default	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ1	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ2	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ3	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ4	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ5	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ6	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ7	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ8	Policy 1 ▼	Policy 1 ▼
☒	Remote VPN : IKEv2	Policy 1 ▼	Policy 1 ▼

Status のチェックボックスをオンにすると、ユーザグループが対応するサービスゾーンにアクセスできるようになります。サービスゾーンの観点から設定するには、サービスゾーンの設定の Access Permission and Authorization に進んでください。

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

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

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enable
Server 1	LOCAL	local	☒	☒
Server 2	RADIUS	radius	☐	☒

Group Overview - SZ1

Name	Status	Time Span 1	Time Span 2	Time Span 3
Group 1	☒	Policy 1 ▾	Policy 1 ▾	Policy 1 ▾
Group 2	☒	Policy 2 ▾	Policy 2 ▾	Policy 2 ▾
Group 3	☒	Policy 3 ▾	Policy 3 ▾	Policy 3 ▾
Group 4	☒	Policy 4 ▾	Policy 4 ▾	Policy 4 ▾
Group 5	☒	Policy 5 ▾	Policy 5 ▾	Policy 5 ▾
Group 6	☒	Policy 6 ▾	Policy 6 ▾	Policy 6 ▾
Group 7	☒	Policy 7 ▾	Policy 7 ▾	Policy 7 ▾
Group 8	☒	Policy 8 ▾	Policy 8 ▾	Policy 8 ▾
Group 9	☒	Policy 9 ▾	Policy 9 ▾	Policy 9 ▾

● Policy Settings

構成パス: Main Menu >> Users >> Policies >> Policy Configuration

- Select Policy** を使用すると、管理者は構成するポリシープロファイルを選択できます。
- Firewall Profile** は、サービスプロトコル、ユーザ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。
- Privilege Profile** は、オンデマンドアカウントの作成、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。
- QoS Profile** を使用すると、管理者はトラフィック構成を編集できます。
- Specific Route Profile** は、管理者が特定の宛先への転送トラフィックにルーティングノードを静的に割り当てます。
- IPv6 traffic class and 802.1p mapping**(グローバルポリシーのみ) — IPv6 トラフィックが VLAN IPv4 ネットワークに転送されている場合に、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からいずれかのポリシーを選択し、**Configure** をクリックしてそれぞれの属性の設定を開始します。設定後は、必ず **Apply** をクリックして変更を保存してください。ここでも、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に適用されるポリシーであることに注意してください。

- **Schedule**

構成パス: Main Menu >> Users >> Schedule

スケジュールは、時刻から 1 時間単位で許可されるユーザログイン期間を割り当てます。チェックされていないタイムスロットは、このポリシーのもと、ユーザが、指定された期間内に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 1

Schedule Name Schedule 1

	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
☐	SUN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
☐	MON	☐	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	
☐	TUE	☐	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	
☐	WED	☐	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	
☐	THU	☐	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	
☐	FRI	☐	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	
☐	SAT	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

☐ Log off authenticated users during unauthorized periods

定義されたスケジュールは、グループ設定に適用されます。

- **Grouping Users**

グループは、認証サーバ、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)によって個別に決定されます。

一般的に、グループは認証オプションのすべてのユーザに割り当てられます。

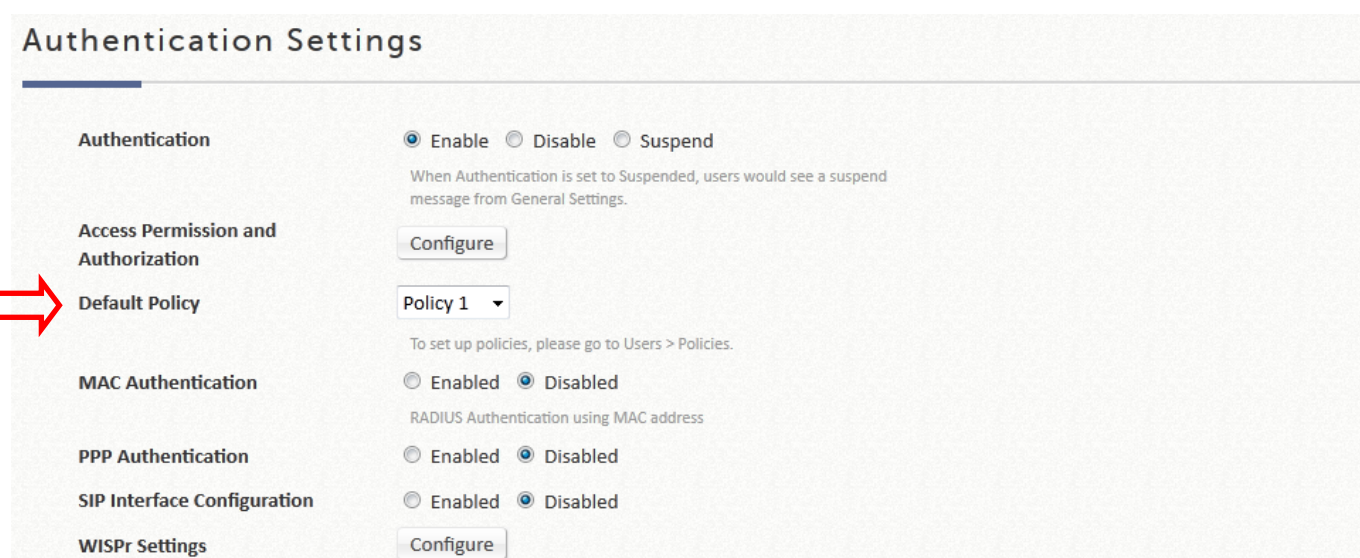
Users > Authentication > Auth Option > Group

ただし、次の柔軟性があります。

- ローカルアカウントは、作成時に、アカウントごとに個別にグループを割り当てます。または、次のパス Users>Authentication>Local>Configure>Local User List>Username から既存アカウントを割り当てます。(管理者が属性を決定するための Applied Group 行があります。)
- オンデマンドアカウントは、作成時にアカウントごとにグループを割り当てることができます。
- RADIUS ユーザは、RADIUS クラスに基づいて異なるグループにユーザを割り当てることができます。マップは Users>Authentication>RADIUS>Configure>Class-Group Mapping>Configure で設定できます。
- LDAP ユーザは、LDAP 属性に基づいてさまざまなグループにユーザを割り当てることができ、マッピングは Users>Authentication>LDAP>Configure>Map LDAP Attributes to Group で設定できます。

● ポリシー優先順位

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。



The screenshot shows the 'Authentication Settings' page. On the left, there is a list of settings: Authentication, Access Permission and Authorization, Default Policy, MAC Authentication, PPP Authentication, SIP Interface Configuration, and WISPr Settings. The 'Default Policy' setting is highlighted with a red arrow and shows a dropdown menu with 'Policy 1' selected. Below the dropdown, there is a note: 'To set up policies, please go to Users > Policies.' The other settings have radio buttons for 'Enable', 'Disable', or 'Suspend'.

ポリシーの適用優先順位は次のとおりです。

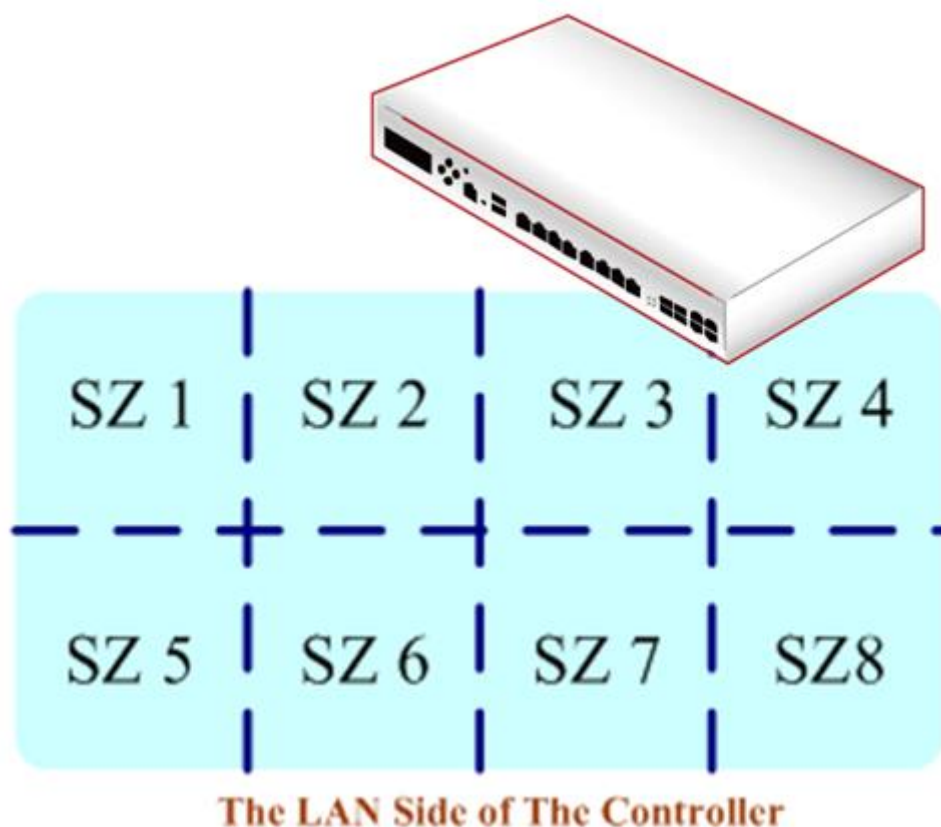
Group-Service Zone Mapping > Service Zone default Policy > Global Policy

したがって、管理者が特定のユーザの構成の階層でグループまたはポリシーを指定しない場合、システムはそれらをグローバルポリシーによって管理します。

第6章 サービスゾーンの基本構成

6.1 サービスゾーンの設定

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、独自のユーザランディングページ、ネットワークインタフェース設定、DHCP サーバ、認証オプション、ポリシーおよびセキュリティ設定などを個別に管理および定義できます。管理者は、一意の 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、有線および無線ネットワークをフレキシブルに分離できます。

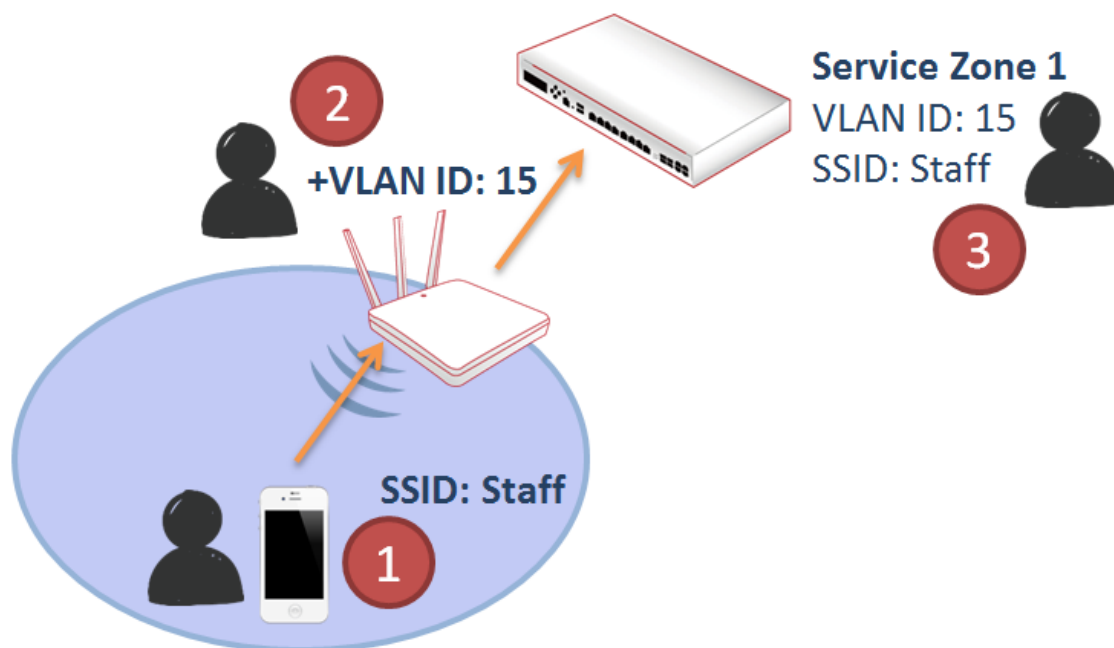


6.2 サービスゾーンの設定

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 コントローラでは、物理 LAN ポートとサービスゾーンのマッピングの 2 つのモード(ポートベースのモードとタグベースのモード)を提供しています。名前が示すとおり、直感的には、ポートベースのモードは、各 LAN ポートが 1 つのサービスゾーンを提供するか、まったくサービスゾーンを提供しないかを意味します。したがって、サービスゾーンの最大数は、Edgecore EWS コントローラの LAN ポートの数と同じになります。

逆に、タグベースのサービスゾーンはポート数に制限されません。タグベースのサービスゾーンは、LAN ポートに関わらず、管理者によって事前に定義された VLAN タグ ID によって指定されます。単純なコンセプトが下の図に表示されます。



図が示すように、企業のスタッフは、アクセスポイントによってブロードキャストされた特定の SSID に関連付けられています。この SSID は、たとえば VLAN ID15 の VAP に属しています。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構成でサービスゾーン 1 にマッピングされます。

構成マッピング

構成パス: 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。サービスゾーンが無効になっているため、一部にグレイアウトされたサービスゾーンがあります。したがって、管理者はまず System>Service Zones>Configure に移動して、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

Default SZ1 SZ2 SZ3 SZ4 SZ5 SZ6 SZ7 SZ8 Disabled

Apply Cancel

設定をタグベースに変更すると、サービスゾーンとポートの対応がグレイアウトされます。各サービスゾーンには、1～4096 の範囲から固有の 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

Default

Apply Cancel

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、タグなしトラフィックを処理するために、タグレス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

構成パス: Main Menu >> System >> Service Zones >> Configure

NAT は、ネットワークアドレス変換の頭字語で、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 に変換してからアップリンクネットワークに転送します。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表示されません。NAT が動作するコントローラのみが対応する変換を認識します。このモードは、LAN 上のユーザが外部装置から見られることを防ぐだけでなく、限られたパブリック IP アドレス問題を解決します。

名前が示すように、ルータモードは、コントローラとの間でアドレス変換を行うことなくネットワーク動作します。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します。

6.2.3 サービスゾーンネットワークインタフェース

構成パス: 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へのアクセスを許可する IP の範囲を定義します。範囲外のアドレスを使用したユーザを許可するには、Network Alias List に IP アドレスを入力し、Enable をチェックします。記入完了したら必ず Apply をクリックしてください。

タグベースモードに設定した場合、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、None です。

- Inter-VLAN Isolation: 同じ VLAN 内の 2 つのクライアントは、異なるポートからの着信時に互いを認識しません。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 を導入する場合は、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内で互いにアイソレーションが適用されます。
- Note: 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は適用されません。

なお、None を選択した場合、スイッチでループプロテクションが有効になっていて、1 つのサービスゾーンに 2 つ以上の VLAN が所属していると、EWS の LAN ポートに接続しているスイッチポートが停止することがあることに注意し

てください。

6.2.4 DHCP サーバオプション

構成パス: Main Menu >> System >> Service Zones >> Configure

DHCP(Dynamic Host Configuration Protocol)は、サーバが特定のネットワークに設定された番号(スコープ)からコンピュータに IP アドレスを自動的に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、Disable DHCP option、Enable built-in DHCP server、または DHCP Relay が含まれます。

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	☒	Scope 1	192.168.1.1	192.168.1.100	192.168.1.254		domain.com	1440		☐ Enable ☒ Disable
2	☐	Scope 2						1440		☐ Enable ☒ Disable
3	☐	Scope 3						1440		☐ Enable ☒ Disable
4	☐	Scope 4						1440		☐ Enable ☒ Disable
5	☐	Scope 5						1440		☐ Enable ☒ Disable
6	☐	Scope 6						1440		☐ Enable ☒ Disable

Reserved IP Address List Configure

DHCP Lease Protection ☐ Enable ☒ Disable

1. DHCP サーバ構成-DHCP サーバのデフォルト設定は Enable 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ます。
2. Enable built-in DHCP server を使用する場合に発行する IP 範囲を定義します。設定用の DHCP プールは合計 6 つあります。
3. 各プールの DHCP リース時間は、アイドルタイムアウト(Idle Timeout)の 2 倍の値より小さくすることはできません。
4. IP アドレスの予約-DHCP サーバ IP 範囲内の特定の IP を、特定のデバイス、(内部のファイルサーバなど)に予約するための設定リストです。
5. DHCP リースプロテクション-これは、コントローラ上のオプションのチェックメカニズムであり、有効にすると、リースの有効期限が切れた IP が現在オンラインになっているかどうかを確認します。存在する場合、ユーザセッションが終了するまで、コントローラはこの IP アドレスの発行を停止します。
6. Apply をクリックすると、変更が有効になります。

6.2.5 認証オプション

構成パス: Main Menu >> System >> Service Zones >> Configure

管理者がメインメニューで認証サーバを適切に設定すると、それぞれのサービスゾーンでは、ログイン時に、ダウンロードクライアントより優先して認証オプションを選択します。デフォルトでは、認証は必ず有効になっていることに注意してください。

1. データベース

管理者は、設定された認証サーバを使用するように指定できます。複数の認証サーバが有効になっている場合、Postfix は認証サーバの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	☒	☒
Server 2	RADIUS	radius	☐	☒
Server 3	NTDOMAIN	ntdomain	☐	☒
Server 4	LDAP	ldap	☐	☒
Server 5	POP3	pop3	☐	☒
On-Demand	ONDEMAND	ondemand	☐	☒
SIP	SIP	N/A	☐	☐
Guest	FREE	N/A	☐	☐
Social Media Login	SOCIAL	N/A	☐	☐
One Time Password	OTP	N/A	☐	☐

2. ポータル URL

ここでは、目的のランディングページの仕様を設定することができます。有効にすると、管理者はユーザの初回ログイン後に開いているブラウザの 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

Configure

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

Configure

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	☐	☒

3. MAC アドレス認証

RADIUS MAC 認証機能を有効にすると、接続された機器の MAC アドレスが設定された RADIUS サーバに入力されている場合、認証が成功すると、コントローラは自動的に認証を行い、すぐにアクセスを許可します。ユーザには透過的にログインできます。

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

Configure

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

Configure

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	☐	☒

4. PPP ダイアルアップ認証

Point-to-Point Protocol(PPP)は、2つのネットワークノード間の直接接続を確立する際に一般的に使用されるデータリンクプロトコルです。この機能を有効にすると、エンドユーザは有効なユーザ名とパスワードを使用してダイアルアップ接続設定を行うことができます(ローカルおよび RADIUS ユーザ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

Configure

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	☒
Server 2	RADIUS	radius	☐

IP アドレス範囲割り当てフィールドでは、PPP が IP アドレスをダイアルアップ仮想インタフェースに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経路情報に使用されます。

6.2.6 キャプティブポータルのカスタマイズ

構成パス: Main Menu >> System >> Service Zones >> Configure

各サービスゾーンは、一意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、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フリーアクセス用)、PMS 支払いプラン選択ページの 3 種類があります。サービスの免責事項ページは、必要に応じて有効にすることができます。これらのページは、管理者に完全なフレキシビリティを与えるために完全にカスタマイズできます。メッセージページはカスタマイズすることもでき、メッセージページには、ログイン成功ページ、オンデマンドユーザ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が含まれます。

Login Page Customization

Service Disclaimer Default

General Login Page Default

PLM Open Type Login Page Default

PMS Billing Plan Selection Page Default

☒ Default ☐ Customize with Template ☐ Upload Your Own ☐ Use External Page

Enable Disclaimer ☐

Preview

Apply Cancel

Theme for Template

Button Color

Upload Logo

Browse... 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 Default ページ以外にも、Customize with Template、Upload Your Own、Use External Page、および Editor など、いくつかのカスタマイズオプションを選択できます。

Edgecore Default: ゲートウェイには、Edgecore ロゴの付いた標準の 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を選択できます。

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。全般的なレイアウトは管理者用に設定されていますが、コンテンツは自分の優先順位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でき、テンプレートプレゼンテーションレイアウト内にサービス免責事項、テキストカラーなどのコンテンツフィールドを入力できます。

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。HTML サンプルファイルのダウンロードでは、管理者は編集元のサンプル HTML コードを使用できます。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、右クリックしてページ送信元をオープンを選択します。ファイルが.html フォーマットで保存されている限り、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。このオプションには、メッセージページと連動するために、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について詳しくは、ユーザマニュアルの付録 C を参照してください。

Editor: ログインページは、What You See Is What You Get(WYSIWYG)エディタで編集できます。エディタを使用すると、管理者は簡単かつ直感的な方法でページ内のエレメントを追加、削除、または設定できます。現在、このオプションは General Login Page 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、Preview ボタンに続けて、Apply をクリックします。同様に、4 つのオプションをメッセージページで使用できます。

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

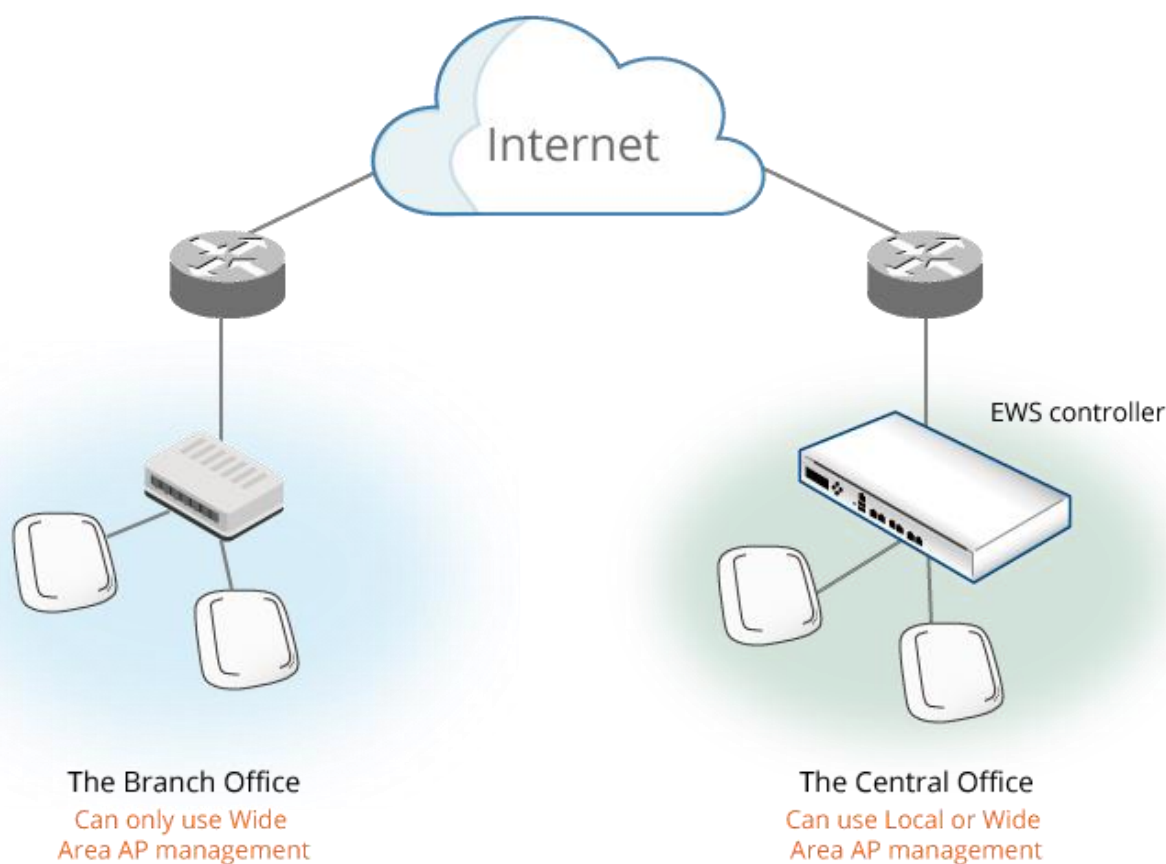
✓ Apply

✕ Cancel

第7章 基本的な AP 管理

7.1 序文

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。そのため、Edgecore では、簡単でわかりやすい一連のマネジメントツールを提供して、その実現に役立てています。一般に、WAN 側と LAN 側の両方でアクセスポイントにコントローラを置く集中型ネットワークを提案します。ここでは、WAN 側の AP 管理をワイドエリア AP 管理と呼び、インターネットやイントラネット上でのスケーラビリティと、LAN 側の AP 管理をローカルエリア AP 管理と呼びます。2 つのタイプの管理の概念を以下に図示します。



【広域およびローカル AP 管理の図】

Edgecore EWS モデルは、Edgecore のアクセスポイントとは異なる機能を備えています。つまり、管理者は、Edgecore EWS コントローラでサポートされている AP モデルを確認する必要があります。

ローカルエリア AP 管理用の管理可能な Edgecore アクセスポイントは、次の場所で確認できます。

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

AP Type List

AP Type	No. of AP	Online	Offline	No. of Client
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

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、次の場所で確認できます。

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

AP List

Type

Status

Tunnel

Name

Refresh Interval

☐	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
--------------------------	------	------	----	-----	-----	----------	--------	------------	--------	--------------	--------	---------	---------------

(Total 0) Go to Page

Row per Page

大規模な AP 展開では、個々 AP 構成に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、無線帯域、データレート、送信電力、データレートなどの設定属性を含む、各 AP モデルで使用可能な最大 8 つのテンプレートがあります。これらは、AP を自動的または手動で管理するために適用され、1 つずつ AP 構成する面倒なプロセスを避けることができます。

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。

本章では、AP 管理に関してワイヤレスネットワーク環境を設定する方法、AP 探索と追加、全般的な AP 設定などについてさらに説明します。ここでは、さまざまな共通 AP 管理設定の明確な設定手順についてのみ説明します。不正なアクセスポイント検知や AP 負荷分散など、詳細な設定については説明しません。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を紹介しています。

注意事項

1. AP を任意のサービスゾーンに追加する前に、管理者はゾーンの一般的なワイヤレス環境を事前に設定する必要があります。これはローカル管理 AP にのみ適用されます。
2. また、それぞれの AP には、管理下にある 1 つの個別の IP アドレスが割り当てられます。タグベースのモードでは、AP アドレスはデフォルトサービスゾーンの DHCP サーバによって指定されます。ポートベースのサービスゾーンでは、AP は関連サービスゾーンの DHCP サーバによって 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

構成パス: Main Menu >> Devices >> Local Area AP Management

ここでは、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。最初に、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し、その管理対象 AP にコントローラに適用できるユーティリティにアクセスポイントを追加する方法を説明します。

7.2.1 AP List

構成パス: Main Menu >> Devices >> Local Area AP Management >> AP List

システムの管理下にあるサポートされているすべての AP がリストに表示されます。目的の AP Type のチェックボックスをオンにし、Apply をクリックして AP List に表示します。ドロップダウンリストから選択して、AP Name、IP Address、MAC Address、および Channel に基づいて検索を実行できます。AP の名前はハイパーリンクとして表示されます。各管理対象 AP のハイパーリンクをクリックして、AP の詳細設定(General Setting、LAN Setting、Wireless LAN、Layer 2 Firewall)を表示します。AP の詳細なステータス情報(System Status、Service Zone Status、Wireless Status、Access Control Status、および Associated Client Status)については、表示されている各管理対象 AP の Status のハイパーリンクをクリックします。

管理者は、目的の AP モデルを選択して AP List をフィルタリングできます。AP Type の AP モデルをチェックし、Apply をクリックしてフィルターを適用します。

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ます。これは「7.2.2 節 AP の追加と構成の適用」で詳しく述べます。

APの有効化または無効化、Template および Service Zones の適用などのオプションは、AP List の左側にあるチェックボックスをオンにして、それぞれのボタンをクリックすることで実行できます。AP テンプレート構成の詳細は、「7.2.3 節 テンプレートの設定」で詳しく説明します。監視については、管理者が各管理対象 AP のステータスを正確に把握できるように、更新間隔オプションがあります。

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ないことに注意してください。Status 列で互換性を確認します。

7.2.2 AP の追加と構成の適用

構成パス: Main Menu >> Devices >> Local Area AP Management >> AP List >> Add

すべての AP が正しく接続されたら、管理者は管理リストへの追加を開始できます。これを行うには、AP List の上にある Add をクリックします。AP は、個別に追加するか、バッチで追加することができます。これは、Add Method によって決定されます。AP を個別に追加するには、ドロップダウンリストから Add AP を選択します。または、バッチで追加するには Find Multiple APs を選択します。

AP を追加するには、AP Name を指定し、その IP および MAC アドレスを入力します。赤いアスタリスクが付いたこれらの行は、入力する必要がある必須情報です。すべてのフィールドに入力したら、ページの下部にある Apply をクリックして AP を追加します (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、追加を確認します。

The screenshot shows the 'Add An AP' form with the following fields and values:

- Add Method:** Add AP (dropdown)
- AP Type:** ECW100 (dropdown)
- AP Name:** (empty text field, marked with a red asterisk)
- Admin Password:** admin (text field)
- IP Address:** (empty text field, marked with a red asterisk)
- MAC Address:** (empty text field, marked with a red asterisk)
- Apply AP Template:** TEMPLATE1 (dropdown)
- Channel:** RF Card A: Default (dropdown), RF Card B: Default (dropdown)

APを一括で追加するには、次のいずれかの方法で、管理者が 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 スキャンは、管理者が AP の設定を変更していない場合に使用されます。また、フィールドに入力する必要はありません。Scan Now をクリックするだけです。
2. AP の IP アドレスが 192.168.1.1 以外に変更された場合は、Manual スキャンを使用します。スキャンする IP アドレスの範囲を入力し、Scan Now をクリックします。

Find Multiple APs

AP Type: ECW100

Service Zone: Default

Admin Settings Used to Discover: ☐ Factory Default ☒ Manual

IP Address: 192.168.1.10 ~ 192.168.1.10

Login ID: admin

Password: admin

Scan Now

Discovery Results テーブルには、現在アクティブな AP がすべて表示されます。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ネルをさらに設定し、さらに AP を有効にした特定のサービスゾーンの下に配置できます。

注意事項

1. コントローラが AP を検出するまでに時間がかかることがあります。スキャン中の AP が Discovery Results リストに表示されるまでしばらくお待ちください。
2. 検出リストの上の Background は、管理者の設定に基づいて、一定期間ごとにワイヤレス環境を検索できるようにすることができます。Configure をクリックして機能を設定します。

以降、AP 構成の修正は、AP Name の下のハイパーリンクを使用して行うことができます。AP Name のいずれかをクリックすると、General Settings、LAN Interface Settings and Wireless Interface Settings などの設定画面が表示されます。

また、Reboot、Enable、Disable、Delete、Apply template、Apply by Service Zone、Reset to Default を示すボタン列もあります。これらは、AP List の内容を変更するため、直感的な名前になっています。1 つ以上の AP を事前に選択し、いずれかの機能を実行します。

Applying template は、管理者があらかじめ準備しておいた基本的なワイヤレスパラメータなど、AP 構成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、管理者が実際の使用後に SSID 名やワイヤレスセキュリティ事前共有キーなどの VAP 構成を変更する場合に、Applying by Service Zone 機能と呼ぶオプションを提供します。選択したサービスゾーンに VAP がマッピングされているかどうかを確認します。

The image shows two side-by-side configuration windows. The left window, titled 'Apply Template', features a dropdown menu set to 'LAPM5211-L' and 'Apply'/'Cancel' buttons. Below is a table for 'Template: LAPM5211-L' with fields for Band, Subnet Mask, and Gateway. A note at the bottom states: 'Note: If the Band of the template cannot match current Channel, the Channel will be changed to "Auto".' The right window, 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'). Below these are fields for 'Key Length' (128 bits), 'Key Format' (ASCII), 'Key Index' (Key1), and four 'Key' input fields (Key1 to Key4). 'Apply' and 'Cancel' buttons are at the bottom.

7.2.3 テンプレートの設定

構成パス: Main Menu >> Devices >> Local Area AP Management >> Templates

導入で述べたように、管理者は AP 設定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。Configure をクリックすると、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設定が表示されます。AP モデルごとに最大 8 つのテンプレートを保存できます。Add Template ボタンをクリックしてテンプレートを増やし、Action 列に表示されている Edit アイコンをクリックして設定を編集します。

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全般の設定を行います。ここでは、無線設定と適用可能なサービスゾーン/SSID も設定できます。

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
☒	VAP-1	0	Default	Default	NONE	 
☒	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。ニーズに応じて、アクセスフィルタリングが個々のサービスゾーンの管理対象 AP デバイスに適用される場合があります。VAP 構成リストの無線構成セクションでは、アクセスコントロールリストを含む無線構成を指定できます。

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。使用可能なオプションは、Open System、Share Key、WPA、WPA2 または WPA/WPA2 Mixed です。

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

WPA2: 認証が WPA の場合、WPA-Personal または WPA-Enterprise が WPA のオプションになります。WPA-Personal の場合は、事前共有キーにパスフレーズまたは HEX を選択できます。

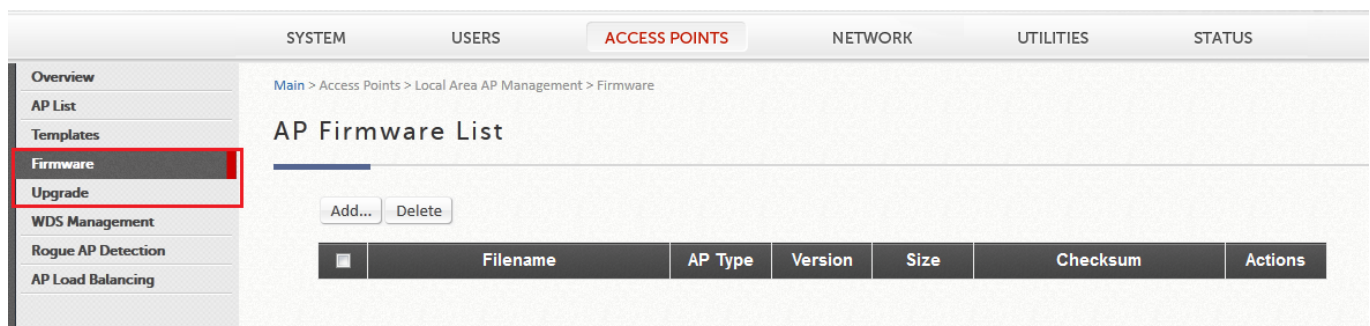
WPA/WPA2 Mixed: 認証が WPA の場合、WPA-Personal または WPA-Enterprise が WPA のオプションになります。WPA-Personal の場合は、事前共有キーにパスフレーズまたは HEX を選択できます。

MAC Address フィールドは、管理者が拒否または許可したい MAC アドレスを入力するためのものです。Denied ステータスは、ブラックリストを設定していることを意味します。Allowed は、ホワイトリストを設定することを意味します。Disabled は、以下に設定された MAC エントリに関係なく、アクセスフィルタリングが適用されないことを意味します。

ステータス	MAC アドレス	コントローラによって実行されるアクション
Disabled		コントローラは、このサービスゾーンの AP に MAC ACL を適用しません。
Allowed	Enabled	AP では、これらのアドレスを持つデバイスのみがこのサービスゾーンの AP に関連付けることができます。
Allowed	Disabled	AP では、これらのアドレスを持つデバイスをこのサービスゾーンの AP に関連付けることはできません。
Denied	Disabled	これにより、これらのアドレスを持つデバイスをこのサービスゾーンの AP に関連付けることができます。
Denied	Enabled	AP では、これらのアドレスを持つデバイスをこのサービスゾーンの AP に関連付けることはできません。

7.2.4 AP ファームウェア管理

ファームウェアのアップグレードは重要です。ソフトウェアの拡張機能の多くは、拡張された標準/機能のために定期的にリリースされているからです。Edgecore では、管理者が複数の AP デバイスを一度にアップグレードできるように、コントローラの AP 管理インタフェースから簡単にファームウェアをアップグレードできます。



- 最初に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、コントローラ内に AP ファームウェアを保存します。
- Devices >> Local Area AP Management >> Upgrade に移動して必要な AP をアップグレードし、バージョンをインポートする AP を選択します。選択が完了したら、ページ下部の Upgrade をクリックします。

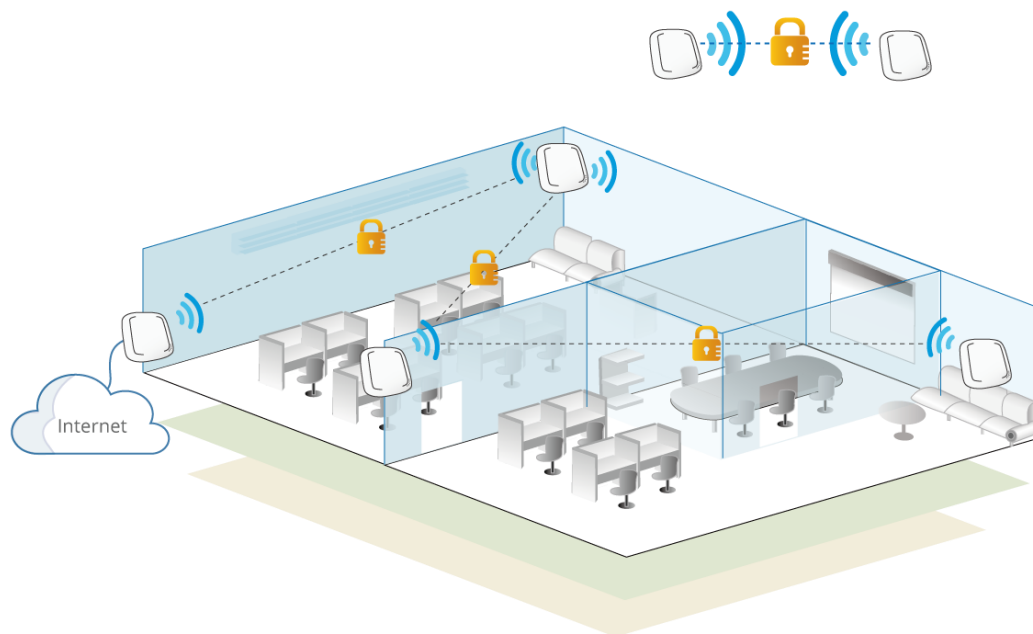
注意事項

- 予期しない結果を避けるために、それぞれの AP ファームウェアリリースについてのリリースノートをお読みください。

7.2.5 WDS リンク

構成パス: Main Menu >> Devices >> Local Area AP Management >> WDS Management

WDS は、Wireless Distribution System の略で、追加の AP を使用してネットワークのワイヤレスカバレッジを拡張する機能です。



【WDS 接続を示す単純な概念図】

WDS 管理機能は、管理者が管理対象 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設定するのに役立ちます。

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

Add

Move WDS Connection

Update Parent AP

Update Child AP

Move

Delete WDS Link

Delete

WDS Status: WDS ツリーに追加された AP のセキュリティおよびチャネル設定を表示します。ネットワークに複数の WDS ツリーを設定できます。Edit をクリックすると、関連付けられた WDS ツリーの WDS 接続設定が変更されます。このリストは、一定時間(10s、20s、30s、40s、50s、60s)ごとに自動的に更新す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 and New Child AP を選択し、Add をクリックします。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 and Update Child AP を選択し、Move をクリックします。選択した Update Child AP の元の親 AP へのリンクは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 をクリックします。選択した AP のすべての WDS 接続は、その子 AP への WDS 接続を含めて削除され、有線接続されていない子 AP は到達不能になることに注意してください。

7.2.6 不正なアクセスポイントスキャン

不正なアクセスポイント検知は、ネットワーク環境を保護するための重要な方法の一つです。ローカル AP 管理は、近隣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、ワイヤレス干渉に関する障害を引き起こす可能性があります。Main Menu >> Devices >> Enter Local Area AP Management >> Rogue AP Detection に移動して、機能を設定します。管理者は、スキャンインターバルを決定し、センサーとしてスキャンジョブの AP を選択します。さらに管理するために、安全な送信元として手動で識別できる場合は、疑わしい不正なアクセスポイントリストに表示されている AP を信頼済みリストに追加する必要があります。

75

General Configuration

Rogue AP Detection	☐ Enable ☒ Disable	Apply
Scanning Interval	0 minutes	
Sensor List	0/0	Configure
Trusted APs	0/40	Configure

Rogue AP List

Add to Trusted AP List Delete

ESSID Search

☐	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は、一時的に不正なアクセスポイント一覧に表示されます。ハイパーリンクされた 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、管理者がリスト化された AP の一部を信頼済みと認識した場合は、BSSID 列の前にあるチェックボックスをオンにしてから、Add to Trusted AP List をクリックします。この操作は、Trusted AP Configuration に記録されます。

7.2.7 AP 負荷分散機能

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。システムが、事前に定義されたしきい値を超える AP の関連クライアント数の発生を検出し、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、バランス機能がアクティブになり、過負荷 AP の送信電力が減少し、他の利用可能な AP の送信電力が増加します。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、グループしきい値と、AP 負荷分散をトリガーする時間間隔を定義できます。

また、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 間で可能な限り均等にネットワーク負荷を分散します。

管理者は、AP 負荷分散機能を適用する基準を指定できます。独自の負荷分散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、適用される時間間隔と関連付けられたクライアントしきい値が含まれます。

LAPM Load Balancing

Load Balancing

☐ Enable ☒ Disable

Apply

Balance Interval

0 minute(s)

Cluster

0/3

Configure

Device List

Add to None ▾

Apply

AP Type EAP747 ▾

List

	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 ページで実行できます。

7.3 ワイドエリア AP 管理

構成パス: 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 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 アドレスを持つことに注意してください。

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 サイトへの集中トラフィック転送。
- Graphical Map ユーティリティを使用すると、簡単な参照とネットワーク構築の計画を作成できます。
- サードパーティ AP デバイスのトラフィック送信統計。
- CAPWAP サポート、コンプリートトンネル、およびスプリットトンネル。

広域管理アクセスポイントの概要は、AP List で参照できます。

構成パス: Main Menu >> Access Points >> 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
--	------	------	----	-----	-----	----------	--------	------------	--------	--------------	--------	---------	---------------

(Total 0)

First

Prev

Next

Last

Go to Page

Row per Page

20

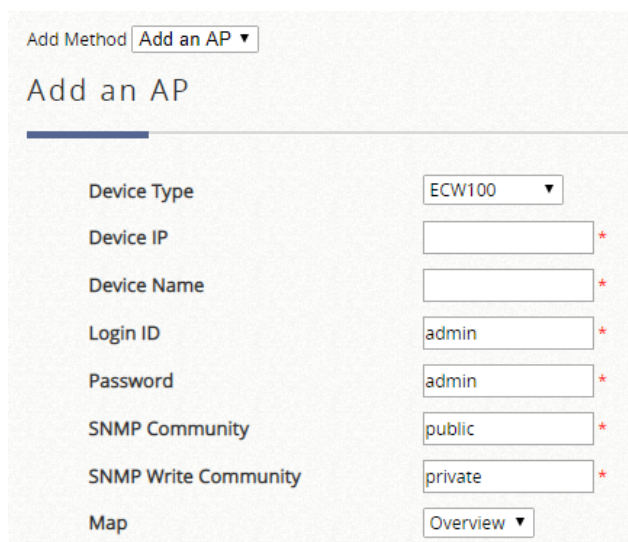
注意事項

- ワイドエリア AP 管理は、コントローラの WAN 側および LAN 側に物理的に展開された AP を管理するために使用できます。

7.3.1 アクセスポイントの追加

構成パス: Main Menu >> Access Points >> Wide Area AP Management >> AP List >> Add

追加ページでは、管理者は Status に関係なく、管理リストに 1 つのアクセスポイントを直接追加できます。装置の IP アドレス、名前、およびログイン資格情報を設定し、SNMP コミュニティストリングを設定し、Apply ボタンをクリックします。



The screenshot shows the 'Add an AP' form. At the top, there is a tab 'Add Method' with a dropdown menu 'Add an AP'. Below this is the title 'Add an AP'. The form contains several fields: 'Device Type' (dropdown menu with 'ECW100' selected), 'Device IP' (text input with a red asterisk), 'Device Name' (text input with a red asterisk), 'Login ID' (text input with 'admin' and a red asterisk), 'Password' (text input with 'admin' and a red asterisk), 'SNMP Community' (text input with 'public' and a red asterisk), 'SNMP Write Community' (text input with 'private' and a red asterisk), and 'Map' (dropdown menu with 'Overview' selected).

7.3.2 複数のアクセスポイントを検索する AP 検出

構成パス: 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、物理的位置に関係なく AP を検索できます。IP スキャン範囲を設定できます。ターゲット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 をクリックします。検出プロセスの後、新たに検出された AP は、管理者が個々の AP デバイス名および SNMP コミュニティストリングを指定することができるデバイス結果の下にリスト化されます。選択して Add ボタンをクリックすると、検出された AP がリストに追加されます。

Discovery AP

Discover

Device Type ECW5211-L▼

Admin Settings Used to Discover

Start IP Address		•
End IP Address		
Login ID	admin	•
Password	admin	•

Device Results

Add Delete

	Device Type	IP Address	Device Name	SNMP Community
--	-------------	------------	-------------	----------------

7.3.3 テンプレートを使用した AP 構成

テンプレートを使用した構成は、ワイドエリア AP 管理用のためのモデルでサポートされています。

構成パス: Main Menu >> Devices >> Wide Area AP Management >> Template

Template AP Setting

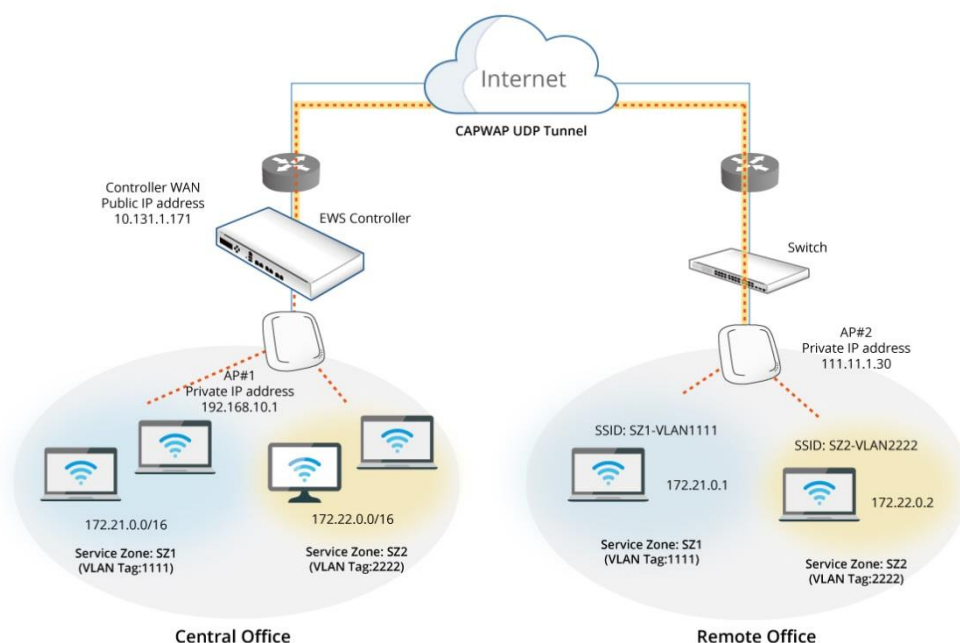
Select Template	1: Template 1 ▼	
Template Name	Template 1	Apply
General Settings	Configure	
VAP Configuration	Configure	
Security Settings	Configure	
Advanced Wireless Settings	Configure	
Hotspot 2.0 Settings	Configure	
Firewall Settings	Configure	
Linkyfi's Location Engine	Configure	
Copy Settings to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

最大 30 件のテンプレートを利用でき、テンプレートからアクセスポイント上の無線で設定可能なすべての機能を設定できます。

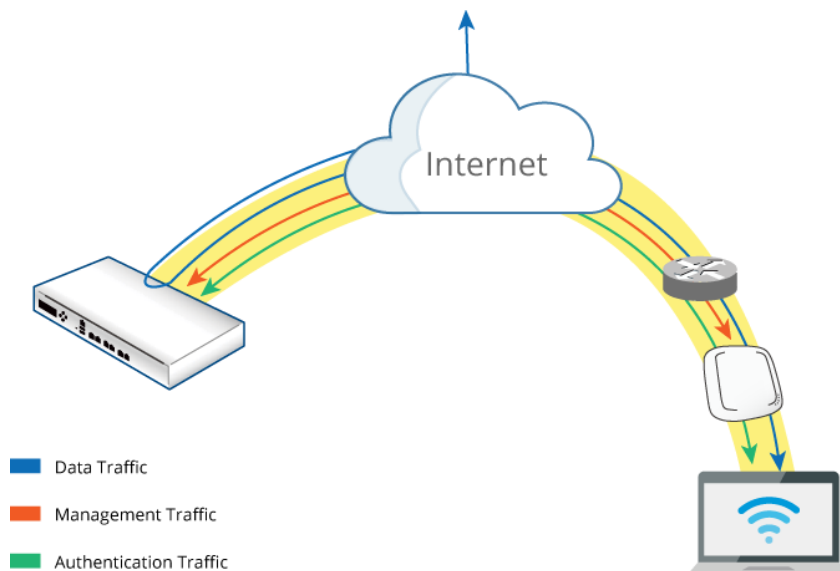
アクセスポイント一般の設定には、帯域、チャネル、送信電力、送信レートなどの基本的なワイヤレス設定が含まれます。VAP 設定を使用すると、管理者は VAP を有効/無効にしたり、ESSID を指定したり、必要に応じて対応するトンネルの有無に VLAN ID を割り当てたりできます。必要に応じて、WEP、802.1X、WPA-Personal、WPA-Enterprise などの設定セキュリティ設定。ワイヤレスの詳細設定を使用すると、管理者はアクセスポイントのパフォーマンスと効率を微調整して、関連付けられたクライアントのワイヤレス接続の品質を良好に保つことができます。Hotspot 2.0 設定は、さまざまな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。ファイアウォール設定では、プロキシ ARP 機能を有効/無効にできます。Linkyfi ロケーションエンジンについては、RTLS および DPI DNS を有効にして、ユーザ追跡のために Linkyfi ロケーションエンジンと統合することができます。

7.3.4 CAPWAP を使用した AP 自動検出と構成

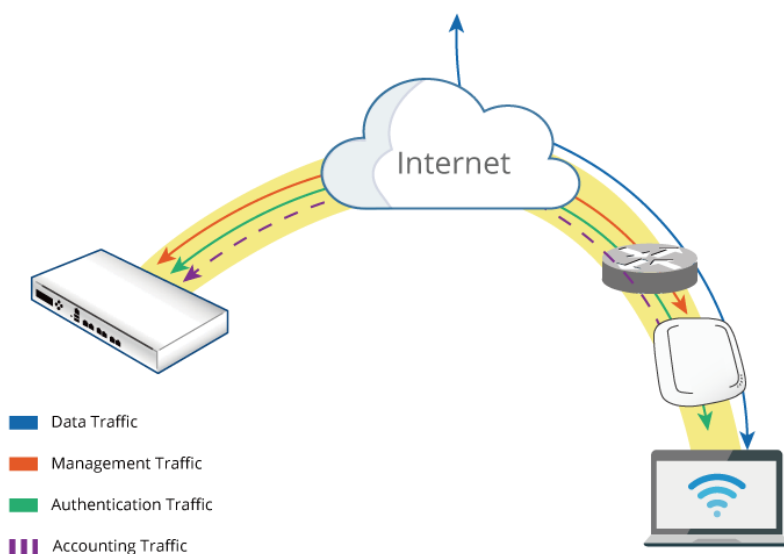
CAPWAP は、EWS コントローラがワイヤレスアクセスポイントの集合を管理できるようにする標準の相互運用可能なプロトコルです。2 つのトンネリングオプション(コンプリートンネルとスプリットトンネル)を使用できます。



コンプリートンネルは CAPWAP プロトコルを使用してアクセスポイントと通信し、提供されたサービスエリア 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コントローラに転送されてから、データトラフィックがインターネットに転送されるようにします。EWS コントローラは、リモートサイトで使用可能なユーザアクセス制御を使用して、レイヤ 3 ネットワーク上にロールベースのポリシーを実装することができます。この機能により、Edgecore EWS コントローラは集中型 AP 管理とユーザ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、ユーザ認証関連のトラフィックのみがコントローラに戻されます。認証されたユーザの場合、データトラフィックはローカルネットワークから直接インターネットに送信されます。また、ユーザデータはより短い経路で送信され、コントローラからのネットワーク負荷を低減することができます。



設定手順

1. Edgecore コントローラで 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	☒ Enable ☐ 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 の検出と参加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 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ルバックされるように選択できます。トンネルインタフェースには 3 つのタイプがあります。Disabled はトンネルを確立しません。Complete Tunnel 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 はコントローラへの管理トラフィックと認証トラフィックのみを収集します。後者の 2 つのトンネルインタフェースでのみ、管理者は VAP ごとにマッピングサービスゾーンを選択する必要があります。

VAP Configuration - 1: Template 1

Profile Name	RF Card A : VAP-1 ▼
VAP	☐ Disable ☒ 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	☐ Disable ☒ Enable
	VLAN ID 1234 *(1 - 4094)
CAPWAP Tunnel Interface	Split Tunnel ▼
Service Zone	Default ▼
Service Schedule	24/7 Service ▼
Access Control Type	☒ Disable ☐ MAC ACL Allow List ☐ MAC ACL Deny List

5. AP 側: System >> CAPWAP から CAPWAP 機能を有効にします。管理者には、以下のような複数の検出方法が表示されます。

(1) **DNS SRV Discovery**

この種の検出では、DNS サーバを使用して検出方法を完了します。AP は、取得した DNS SRV レコードを介して、CAPWAP 参加要求を送信するコントローラを認識します。

(2) **DHCP Option Discovery**

管理者は、接続しようとしている Edgecore EWS コントローラと同じサブネット内にある IP アドレスを AP が取得できるように、CAPWAP 機能とコントローラの DHCP サーバを有効にする必要があります。

(3) **Broadcast Discovery**

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 コントローラなどのゲートウェイでは、ブロードキャストがサブネットを越えるすることはほとんど許可されていません。機能を有効にするときは、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) **Multicast Discovery**

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、マルチキャスト検出パケットをネットワークに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の適切な設定に従う必要があります。関連する設定を使用して有効にしてそれらが有効になっているか確認してください。

(5) **Static Discovery**

静的検出は、あらかじめ設定を行うことなく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、この AP を参加させる Edgecore EWS コントローラの IP アドレスを入力します。

CAPWAP の参加が成功すると、以下に示すように、管理対象 AP リストに AP が表示されます。

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ルバックされるように設定されている場合は、クリック可能な Edit ボタンが黒色で表示されます。

AP List

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

Refresh Interval:

Type	Name	IP	MAC	Map	Template	Status	# of User	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、System Overview ページと同様に、VAP が有効でトンネルステータスが表示されます。

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 構成には、別の VAP で動作している CAPWAP トンネルインタフェース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

注意事項

1. APトンネルは、CAPWAP テンプレートが有効にする VAP を選択し、SZ にトンネルバックすると、自動的に確立されます。
2. CAPWAP 検出処理が失敗した場合は、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ている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 トンネル VAP ロケーションマッピングの設定

構成パス: 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ルバックされる VAP の場合。管理者は、NAS 識別子を割り当て、サービス用の IP プールを指定することを望むかもしれません。

ワイドエリア AP 管理の管理対象 AP リストで、管理者は NAS 識別子を割り当て、管理対象 AP の VAP ごとにサービスの IP プールを指定できます。これは、AP とコントローラ間のトンネルを確立するときに設定できます。

AP List

Type:
 Status:
 Tunnel:
 Name:

Refresh Interval:

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)

Row per Page:

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: /

User Limitation: (Blank is for unlimited.)

ESSID:

Room Number / Location ID: *

Room Description / Location Name:

NAS Identifier:

Class:

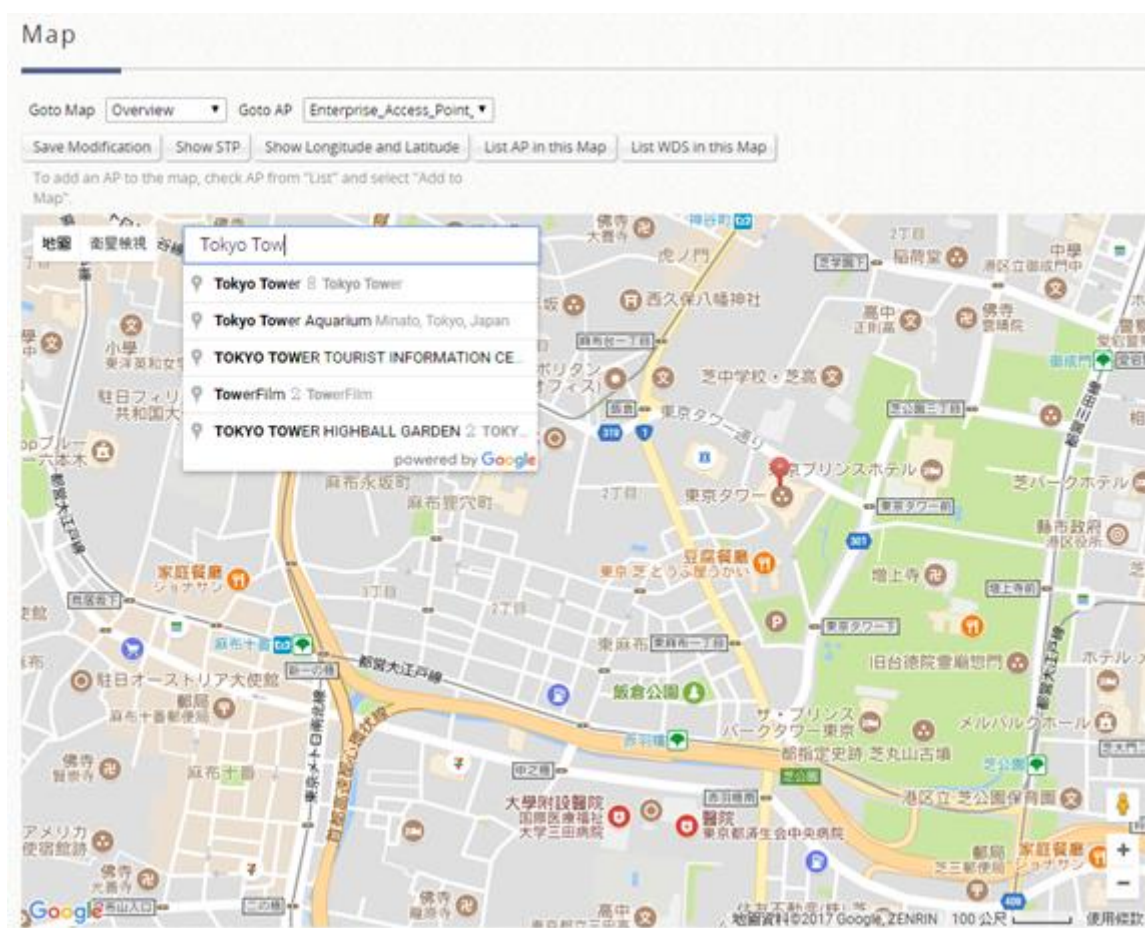
HTTP Parameter:

VAP が PLM(Port Location Mapping)を使用してトンネルバック(コンプリートンネルまたはスプリットトンネル)を設定されると、PMS システムや、ロケーションの属性や情報を必要とする他の集中管理されたホットスポット操作を使用して、リモートサイトが利点を得ることができます。

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 の場所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。

管理者が管理対象リストに AP を追加すると、次のように、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 AP の地理的な場所を表示したりできます。



マップを作成する手順は次のとおりです。

- Step 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 インタフェースに設定します。
- Step 2. Google マップ登録キーを適用します。
- Step 3. Map ページの Add a New Map ボタンをクリックします。マップ名とレジストレーションキーを設定します。
- Step 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。
- Step 5. List ページから、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設定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 管理で新しいマップを追加する前に、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 Maps API v3 鍵の適用に使用されます。詳しくは、<https://developers.google.com/maps/documentation/javascript/v2/introduction> の Google の指示に従って Maps API v3 鍵を入手してください。Map Configuration ページの Google Maps Registration Key フィールドのキー情報です。

MAP Configuration

Map Name: Overview *

Latitude: 0 *

Longitude: 0 *

Google Maps Registration Key: AlzaSyBcWmheQEdPGeKltCRWes3sA50X1Gdarfo *

Zoom Level: 1 *

Map Type: Normal *

Buttons: Apply, Cancel

この Map Configuration ページでは、このマップの Map Name と、Longitude と Latitude で定義されている地理的な場所を構成し、表示する Zoom Level と Map Type を選択することもできます。

AP をマップに追加するには、最初に AP List に移動し、AP Name 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、ターゲットマップのロケーションの周辺にある必要があります。このページでは、管理者が各 AP のマップに表示するリンクと注釈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:

Buttons: Apply, Cancel

各 AP のロケーションを定義したら、AP List ページに戻ります。マップ上でマークする AP を選択し、Add to Map 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ます。

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
☒	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

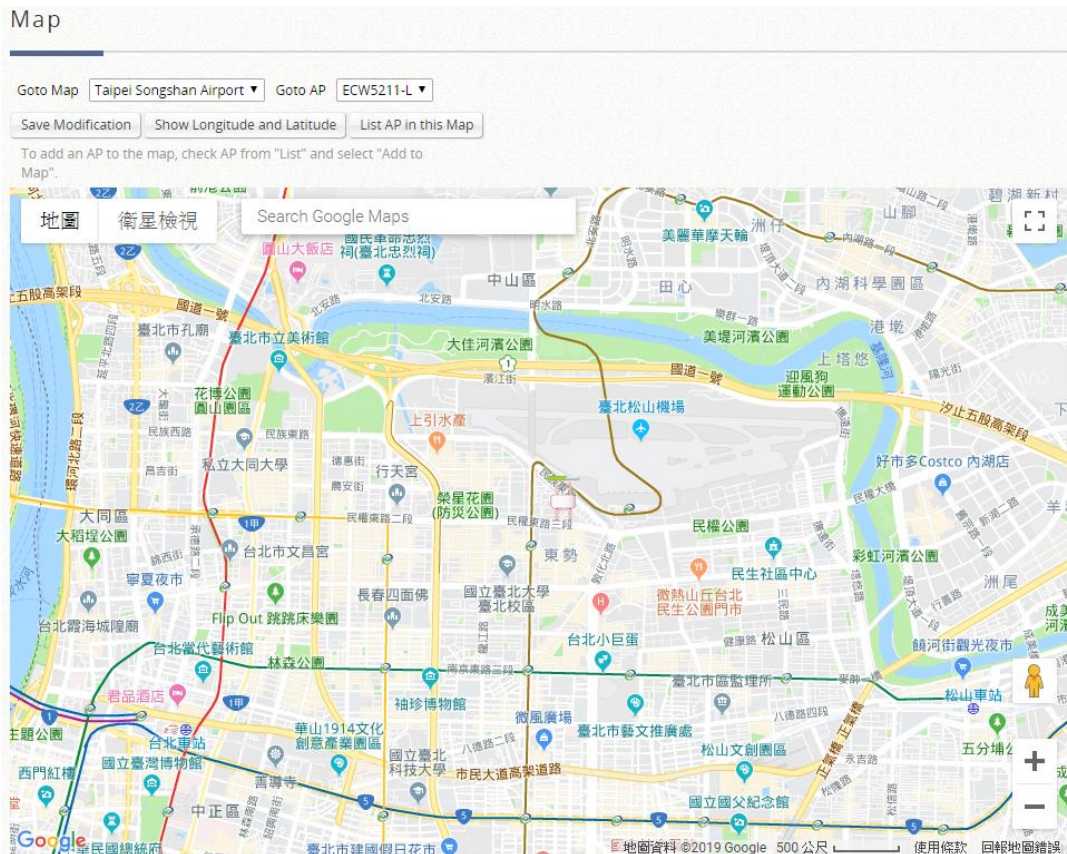
Add AP(ECW5211-L)

☒ Add into a map
Select Map: Taipei Songshan Airport

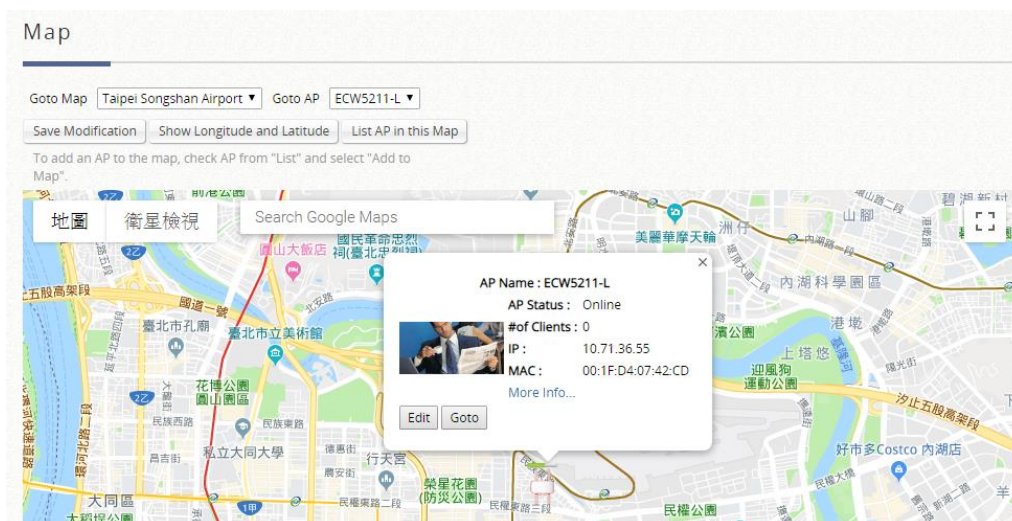
☐ Add into a floor plan
Floor Plan Name: Select an Option

Apply Cancel

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ップ上にマーカーイメージとして表示されます。



管理者は、AP アイコンをクリックして、設定した追加情報またはリンクのダイアログボックスを表示できます。また、管理者は、この AP に関連する AP リンク、AP 統計、AP ステータス、クライアントリスト、WDS リスト、およびリンクに関する情報の詳細リンクをクリックすることができます。これらの情報は、SNMP を介してリモート AP から収集されます。



Map

Goto Map Taipei Songshan Airport ▼ Goto AP ECW5211-L ▼

Save Modification Show Longitude and Latitude List AP in this Map

To add an AP to the map, check AP from "List" and select "Add to"

AP Detail Status ✕

AP Link AP Statistic **AP Status** Client List

AP Status : ECW5211-L		
General	Type	ECW5211-L
	Name	ECW5211-L
	IP Address	10.71.36.55
	MAC Address	00:1F:D4:07:42:CD
	Version	3.45.0000
System	Status	Online
	Last Report Time	2019/07/24 16:07:25
	Uptime	22:06:31
	CPU Idle	95%
	Memory Usage	49%
Network	# of Radio Card	2
	TX Byte Count	145567
	RX Byte Count	0
	TX Packet Count	395628
	RX Packet Count	0

注意事項

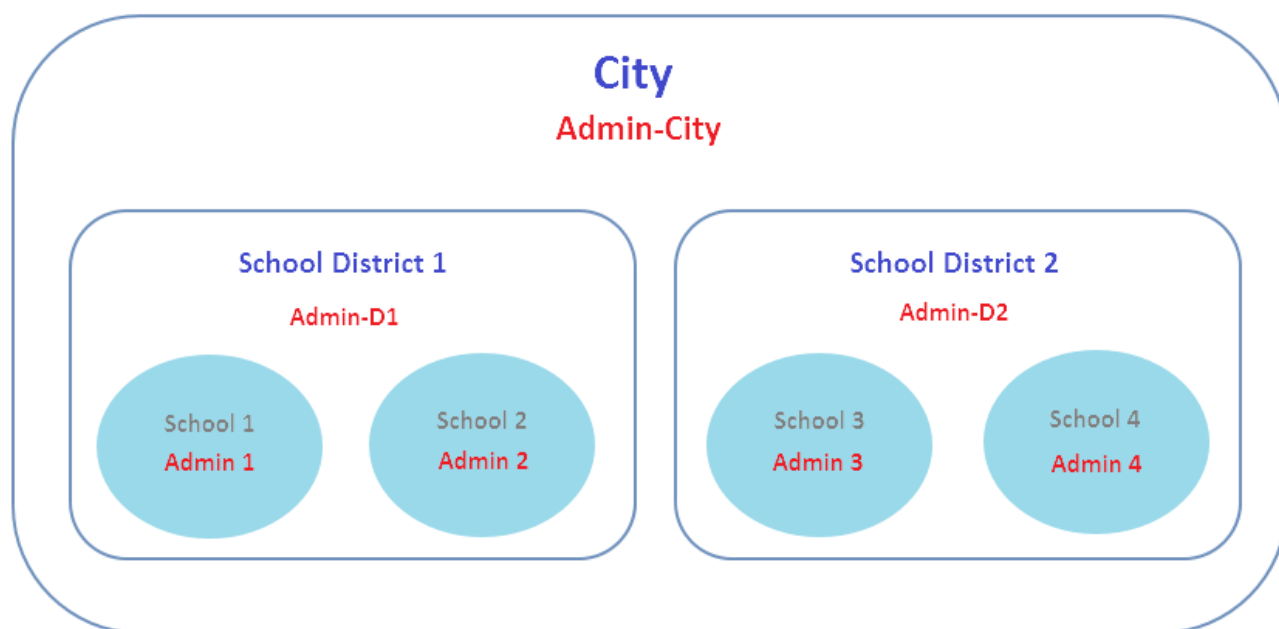
1. 概要マップは、システムのデフォルトマップです。このマップには、すべての管理対象 AP の概要が表示されます。
2. AP が管理対象リストに追加されると、概要マップに属します。
3. AP がマップに追加された後も、概要マップで監視することができます。

7.3.7 AP グループ化

構成パス: Main Menu >> Devices >> Wide Area AP Management >> AP Grouping >> Map Configuration

ワイドエリア AP 管理では、すべての管理対象 AP をマップ別 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 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、マップは、異なる AP グループによって含めることができます。AP グループごとに異なる読み取り/書き込み権限を持つ異なる管理者グループを割り当てることができます。



【AP グループ化を示す単純な概念図】

AP 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 に移動して AP グループを追加または削除します。

AP Grouping

☐	AP Group	Map	Template
☐	456	123	1 3 5

Add をクリックして AP グループを追加します。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

Selectiable

Selected

Overview
123

Template

Selectiable

Template2
Template4
Template5
Template7
Template8

Selected

Template1
Template3
Template6

AP グループが作成されたら、管理者グループを管理者グループリストに追加して、各 AP グループにアクセス権限を割り当てることができます。

[Main](#) > [Utilities](#) > [Administrator Accounts](#) > [Administrator Group List](#)

Administrator Group List

AddDel

	name	remark
☐	Super Group	remark
☐	Manager	remark
☐	Operator	remark
☐	On Demand	remark
☐	Custom 1	remark
☐	Custom 2	remark
☐	Custom 3	remark

AP グループへの権限の割り当て

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

7.3.8 不正なアクセスポイントスキャン

不正なアクセスポイント検知は、ネットワーク環境を保護するための重要な方法の一つです。ワイド AP 管理は、近隣に存在する許可されていないアクセスポイントの検知をサポートします。

許可されていないアクセスポイントは、ワイヤレス干渉に関する障害を引き起こす可能性があります。Main Menu >> Devices >> Enter Local Area AP Management >> Rogue AP Detection に移動して、機能を設定します。管理者は、スキャンインターバルを決定し、センサーとしてスキャンジョブの AP を選択します。さらに管理するために、安全な送信元として手動で識別できる場合は、疑わしい不正なアクセスポイントリストに表示されている AP を信頼済みリストに追加する必要があります。

General Configuration

Rogue AP Detection

☐ Enable ☒ Disable

Apply

Scanning Interval

minutes

Channel Switching

☐ Enable ☒ Disable

Sensor List

0/0

Configure

Trusted APs

0/40

Configure

Rogue AP List

Add to Trusted AP List

Delete

ESSID ▼

Search

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: 10 ▼							

検出されたアクセスポイントは、一時的に不正なアクセスポイント一覧に表示されます。ハイパーリンクされた 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、管理者がリスト化された AP の一部を信頼済みとして認識する場合は、BSSID 列の前にあるチェックボックスをオンにしてから、Add to Trusted AP List をクリックします。この操作は、Trusted AP Configuration に記録されます。

7.3.9 AP 負荷分散機能

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。システムが、事前に定義されたしきい値を超える AP の関連クライアント数またはネットワークトラフィックの発生を検出し、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、バランス機能がアクティブになり、過負荷 AP の送信電力が減少し、他の利用可能な AP の送信電力が増加します。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、しきい値と、AP 負荷分散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 のクラスタリングをサポートし、送信電力管理を実行して、同じクラスタの AP 間で可能な限り均等にネットワーク負荷を分散します。

管理者は、AP 負荷分散機能を適用する基準を指定できます。独自の負荷分散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、適用される時間間隔と、関連付けられた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

AP Distance

meter(s)

Interval

minute(s)

Threshold

☒ Number of Clients clients

☐ Number of Packets

Apply

Map Cluster Setting

Map

Cluster

Configure

Create

Delete

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

AP 負荷分散クラスタを作成するには、管理者が AP をマップに追加する必要があります。同じ負荷分散クラスタ内の AP は、同じマップ内に存在する必要があります。マップに AP を追加したら、Main Menu >> Devices >> Wide Area AP Management >> AP Load Balancing に移動し、Map Cluster Setting でマップを選択します。次に、Create ボタンをクリックして、AP の各ペア間の distance に基づいて、このマップ上にクラスターを自動的に生成します。クラスタが作成されたら、Configure ボタンをクリックして、クラスタごとの AP ロードバランシング機能を有効/無効にできます。

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て Save Modification ボタンをクリックした場合など)、AP は自動的に再クラスタ化されません。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、更新されたロケーション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 を変更すると、既存のクラスタは自動的に削除されます。クラスタリングの更新された基準に基づいてクラスタを生成するには、Create ボタンをクリックする必要があります。

最後に、AP 負荷分散機能がクラスタで有効になると、各 AP の送信電力管理アクションのログをチェックすることができます。

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

構成パス: 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ています。IPv6 設定オプションが有効になっている場合、管理者はネットワークインタフェースの WAN1 または WAN2 のいずれかに IPv4 IP アドレスと IPv6 アドレスを割り当てることができます。選択した WAN インタフェースに IPv6 アドレスを設定するには、スタティック、6to4、および go6 の 3 つの方法があります。ご使用の環境に適したオプションを選択してください。

The screenshot displays the 'IPv6 Setting' configuration interface. On the left, there is a sidebar with 'IPv6', 'Interface', and 'Type' sections. The main area contains the following settings:

- IPv6:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Interface:** Radio buttons for 'WAN1' (selected) and 'WAN2'.
- Type:** Radio buttons for 'Static (Use the following IPv6 settings)' and 'Use 6to4 transition' (selected).
- Mode:** Radio buttons for 'Automatic' (selected) and 'Configured'.
- IPv6 Address:** A text input field.
- Prefix Length:** A text input field.
- Preferred DNS Server:** A text input field.
- Alternate DNS Server:** A text input field.
- At the bottom, there is an option for 'Use go6 transition' which is currently unselected.

- **6to4:** 6to4は、IPv4からIPv6へ移行するためのインターネット移行メカニズムであり、明示的なトンネルを構成する必要なくIPv6パケットがIPv4ネットワーク(一般にIPv4インターネット)上を送信されることを可能にするシステムです。6to4オプションは、選択したWANインタフェースがスタティックIPv4アドレスで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します。Main Menu >> Utilities >> Network Utilities に移動します。

システムは、管理者がネットワークを簡単に管理できるように、ネットワークユーティリティを提供します。

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	▪ Ping: 管理者は、IP アドレスまたはホストドメインネームを使用してデバイスを検出し、応答しているかどうかを確認できます。 ▪ Trace Route: 管理者は、IP アドレスまたはホストドメインネームを使用して、ゲートウェイから宛先へのパケットの実際のパスを復元できます。 ▪ ARPing: 管理者は、特定の IP アドレスまたはドメイン名の ARP 要求を送信できます。 ▪ ARP Table: 管理者は、Address Resolution Protocol (ARP) で使用される IP から物理アドレスへの変換テーブルを表示できます。
IPv6	▪ Ping: 管理者は、IPv6 アドレスまたはホストドメインネームを使用してデバイスを検出し、応答しているかどうかを確認できます。 ▪ Trace Route 6: 管理者は、IPv6 アドレスまたはホストドメインネームを使用して、ゲートウェイから宛先へのパケットの実際のパスを復元できます。 ▪ Neighbor Discovery: 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ネーム上にある IPv6 ネイバーノードについて学習できます。 ▪ Neighbor Cache: ノードは、ネイバー・キャッシュ内のネイバーの情報を管理します。この機能により、管理者は、システムのネイバーキャッシュに保存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	この機能を使用すると、コントローラは同じレイヤ 2 ネットワーク内に接続されている 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の機能を実行している場合、動作のステータスがここに表示されます。
Result	操作の結果が表示されます。

8.2 ユーザアクセスコントロール

ネットワークオペレータは、時々、認証またはアソシエーションから特定のアカウントまたはデバイスへのアクセスを制限したい場合があります。ここでは、ユーザまたは装置の制限を実現する方法について説明します。

8.2.1 Black List

構成パス: Main Menu >> Users >> Black List

ブラックリストは、ユーザアクセスコントロールのためのツールです。それぞれのブラックリストには、ネットワークアクセスを拒否される固有のユーザアカウントを格納できます。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	User1	
2		
3		
4		
5		
6		
7		
8		
9		
10		

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した後(必須ではありません)、Apply をクリックしてユーザを追加します。

ブラックリストからユーザを削除するには、ユーザの Delete ハイパーリンクを選択して、そのユーザをブラックリストから削除します。

Select Blacklist 1: Blacklist1

Blacklist Settings

Blacklist Name Blacklist1 Apply

Add Delete

☐	User Name	Remark
☒	User1	

ブラックリストの設定が完了したら、目的の認証サーバでブラックリストを選択して有効にします。

Local Authentication

User Postfix local

Blacklist 1: Blacklist1 Configure

Local User List

Account Roaming Out ☐ Enable ☒ Disable

802.1X Authentication ☐ Enable ☒ Disable

8.2.2 MAC ACL

構成パス: Main Menu >> Users >> Additional Controls

MAC ACL は、MAC アドレスアクセスコントロールリストです。ここで、許可または拒否のいずれかのアクセスフィルタリングのために、特定の MAC アドレスをリスト化できます。MAC ACL 許可ユーザにはユーザ認証が必要です。Configure をクリックして MAC Address Control リストに入ります。Add MACs をクリックして希望する MAC アドレスを入力し、Allow または Deny を選択して、Apply をクリックします。

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:

注意事項

1. MAC アドレスのフォーマットは、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 証明書

構成パス: Main Menu >> Utilities >> Certificate

EWS Access Controller 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す。管理者は、システムのルート CA によって証明書発行にサインし、これらの証明書を管理対象 AP にロードできます。これらのセキュリティ証明書は、AP と AC 間の CAPWAP 検出要求の ID と認証を検証するために使用されます。また、内蔵 RADIUS サーバユーザローミングアウトの認証にも使用できます。Certificate Management には、使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	

設定を入力するには、各カテゴリの左上隅にある Edit アイコンをクリックします。

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。コントローラには組み込みのファクトリーデフォルト証明書(gateway.example.com)があり、これを削除することはできませんが、証明書をアップロードできます。Regenerate ボタンにより、管理者はゲートウェイの MAC アドレスに基づいて一意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 ボタンをクリックします。

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
Get CERT Get Key	

Get CERT および Get Key をクリックして、証明書と公開鍵をローカルディスクにダウンロードします。

証明書/秘密鍵/中間 CA をアップロードするには、Browse をクリックし、適切なファイルを選択して、Upload Files をクリックします。

Upload System Certificate

Certificate		Browse...
Private Key		Browse...
Intermediate CA		Browse...
Certification Path Verification	☐ Enable ☒ Disable	
Upload Files		

8.3.2 内部ルート CA

管理者は、内部ルート CA をアップロードするか、プライベート使用のためにルート CA を生成できます。作成されたルート CA 証明書をダウンロードし、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、1 つの内部ルート CA しか作成できないことに注意してください。

Generate Root CA

Common Name	
Email Address	
Country Name	
State or Province Name	
Locality Name	
Organization Name	
Organization Unit Name	
Key Type	RSA
Key Length	512
Generate Certificate	

内部ルート CA をアップロードするには、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鍵を選択し、Upload Files をクリックします。

内部ルート CA がアップロード/生成されると、以下のフォーマットにその詳細を示します。

Internal Root CA		
Cert Name	Common Name	Operation
Internal Root CA		
Root CA	CN=4ipnet.com	View Delete

証明書の詳細を表示するには、View ボタンをクリックします。

8.3.3 内部的に発行された証明書

このページでは、内部的に発行された証明書を生成できます。内部的に発行された証明書に署名する前に、まず内部ルート CA を作成する必要があることに注意してください。Certificate Information は、現在の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 ボタンをクリックします。

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

Email Address

Country Name

State or Province Name

Locality Name

Organization Name

Organization Unit Name

Key Type

RSA ▾

Key Length

512 ▾

Generate Certificate

8.3.4 信頼できる認証局

管理者は、自己署名証明書およびシステムのルート CA 以外に、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決済ゲートウェイまたは CAPWAP 対応 AP の証明書を認識し、信頼することを目的としています。信頼済み CA をアップロードするには、参照をクリックして証明書を選択し、Upload Files をクリックします。証明書の詳細を表示するには、対応する View ボタンをクリックします。

Trusted Certificate Authorities (CA)

Cert Name	Common Name	Operation
Certificate Authorities (CA)		
N/A	N/A	View Delete

Upload Trusted CAs

Certificate

Browse...

[Upload Files](#)

8.4 管理アクセス

構成パス: Main Menu >> System >> General >> Management IP Address

管理者は、WAN または LAN の両方から、IP アドレスまたは IP アドレスの範囲を指定して、Web 管理インタフェースへのアクセスを許可できます。たとえば、192.168.3.1 と 192.168.1.0/24 と入力すると、192.168.3.1 のデバイスと 192.168.1.0～192.168.1.255 のデバイスのみが Web マネジメントインタフェースに到達できます。

Remote Console が有効になっている場合、コンソールインタ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、悪意のあるユーザがシステムにアクセスするのを防ぐために、コンソールアクセスはデフォルトで無効になっています。

第9章 コントローラ管理のユーティリティ

9.1 EWS コントローラの管理

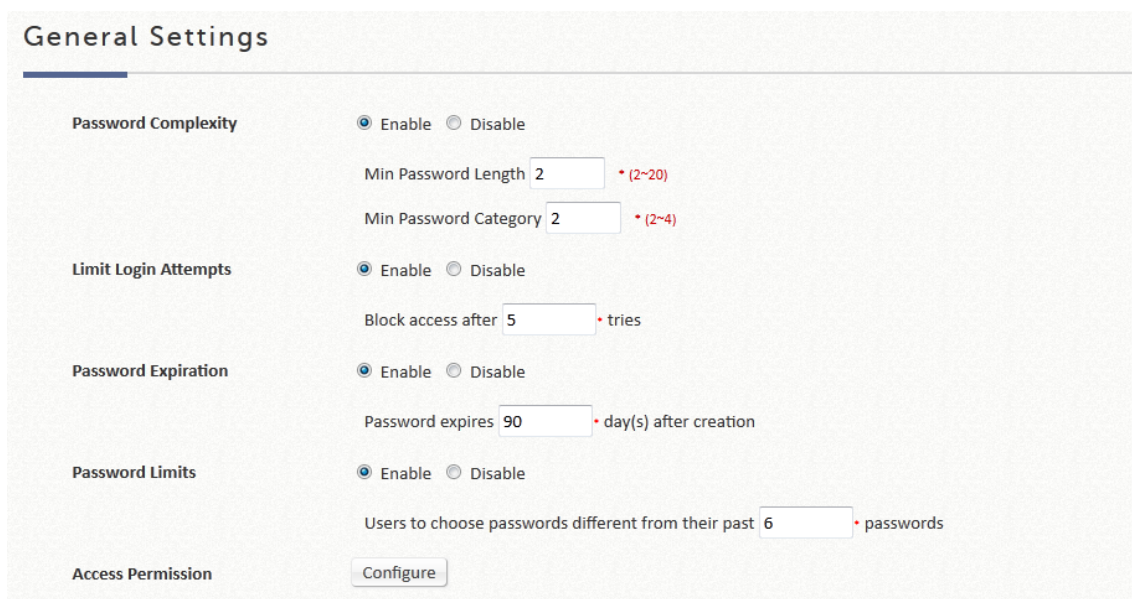
構成パス: Main Menu >> Utilities >> Administrator Account

EWS コントローラのルート管理アカウントは、完全なアクセス、修正、およびアプリケーション権限を持つ admin アカウントです。しかし、管理者が指定された権限領域にアクセスするために作成される権限が少ない第 2 位のアカウントがあります。これは、複数の管理者が必要になる大規模なネットワーク構築に必要な機能です。

この設定パスにより、権限プロパティを割り当てるページが表示され、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が生成されます。

デフォルト状態の管理アカウントは一つだけです。Group Permission Settings では、特定の管理グループのアクセス可能な WMI ページをカスタマイズし、順番に、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: パスワードの安全性の設定



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すると、権限のない人から Web マネジメントインタフェースを保護できます。これらの設定はデフォルトで無効になっていることに注意してください。

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	☐ 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、マネージャー、オンデマンドマネージャー、オペレーター)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、オンデマンドマネージャ、およびオペレータ)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/書き込みアクセスまたは読み取り専用アクセス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、管理者アカウントとそのステータスを表示できます。Add をクリックしてアカウントを作成し、任意のアカウント名、パスワード、割り当てられた承認グループを入力します。Apply をクリックすると、新しく生成されたアカウントが下の表に表示されます。

Administrator Accounts

Add ... Delete Lock Admin Unlock Backup List Restore List

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

注意事項

1. パスワードの安全性の設定には、管理アカウントの作成またはパスワードの変更時に従わなければならない制約またはルールが含まれています。
2. 管理者リストには、このアカウントが現在 WMI にアクセスしている場合、すべての管理アカウントとログインステータスが表示されます。
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リストア

構成パス: Main Menu >> Utilities >> Backup & Restore

EWS Controller の設定をバックアップ/リストアします。バックアップは、FTP により定期的に行うことができます。また、出荷時のデフォルト設定に戻すこともできます。

The screenshot displays a web-based configuration interface for system backup and restoration. It is divided into three main sections: 'Backup System', 'Restore System', and 'Reset to Default'. The 'Backup System' section includes 'General Backup' with a 'Backup' button and 'Period Backup' with a 'Configure' button. The 'Restore System' section features 'Restore System Settings' with a '選擇檔案' (Select File) button and a status indicator '未選擇任何檔案' (No file selected). Below this are several checkboxes for settings to be kept during restoration, such as 'Keep WAN1 setting' and 'Keep Management IP Address List'. A 'Restore' button is located at the bottom of this section. The 'Reset to Default' section contains a 'Reset to Factory Default' label and a 'Reset' button.

Section	Item	Action
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

注意事項

1. 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. 以前の db 構成を復元するには、WAN 設定を保持するなどのオプションを使用して、この操作がリモートで実行された場合に WMI 接続が失われないようにすることができます。
3. 出荷時のデフォルトにリセットすると、すべての構成が消去され、コントローラが出荷時の構成に復元されます。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 ファームウェアアップグレード

構成パス: Main Menu >> Utilities >> System Upgrade

管理者は、Edgecore の Web 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、アップグレードすることができます。Browse 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ます。アップグレードプロセスが完了し、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後で再起動するまで、数分かかる場合があります。FTP ファームウェアアップグレードもオプションです。FTP サーバ IP アドレス、FTP サーバポート、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 サーバに保存されている完全なファームウェアファイル名を指定します。

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て、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 has a title bar 'System Firmware Upgrade'. Below it, there are two main sections. The first section, 'Current Version', shows '3.00.00'. The second section, 'Upload New Firmware', has a text input field, a 'Browse...' button, and an 'Apply' button. The third section, 'Upgrade Firmware Via FTP', has an 'Anonymous' label with radio buttons for 'Yes' (selected) and 'No'. Below this are input fields for 'IP Address', 'Port', and 'File Name' (with a placeholder 'File Name or Dir/File Name'). There is an 'Apply' button at the bottom right of this section.

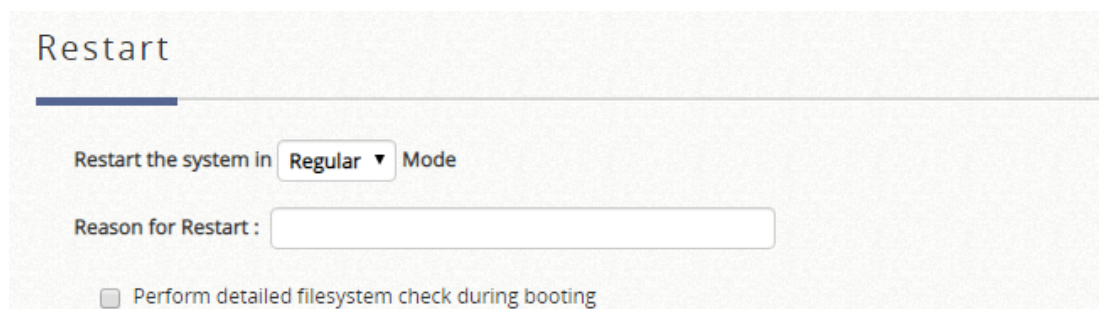
注意事項

1. ファームウェアアップグレード後、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。

9.4 再起動

構成パス: Main Menu >> Utilities >> Restart

この機能により、管理者は EWS Controller を安全に再起動でき、プロセスが完了するまでに数分かかる場合があります。Apply をクリックして、EWS コントローラを再起動します。電源を切断する必要がある場合は、最初に EWS コントローラを再起動し、再起動後に電源を切断することを強くお勧めします。管理者は、保守の目的で Reason for Restart を入力することができます。



Restart

Restart the system in Regular ▼ Mode

Reason for Restart:

☐ Perform detailed filesystem check during booting

注意事項

1. システムの再起動中は、システムのすべてのオンラインユーザの接続が切断されます。

第10章 監視のためのレポートとログ

10.1 システム関連ステータス

10.1.1 ダッシュボード

システム全般の設定、ネットワークインタフェース、オンラインユーザなど、管理者が一目で知っておく必要があるシステム関連の重要な情報を表示します。このページのインフォメーション更新率を選択するためのドロップダウンメニューがあります。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。

管理者は、右上隅の Display Mode ボタンを使用して、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。



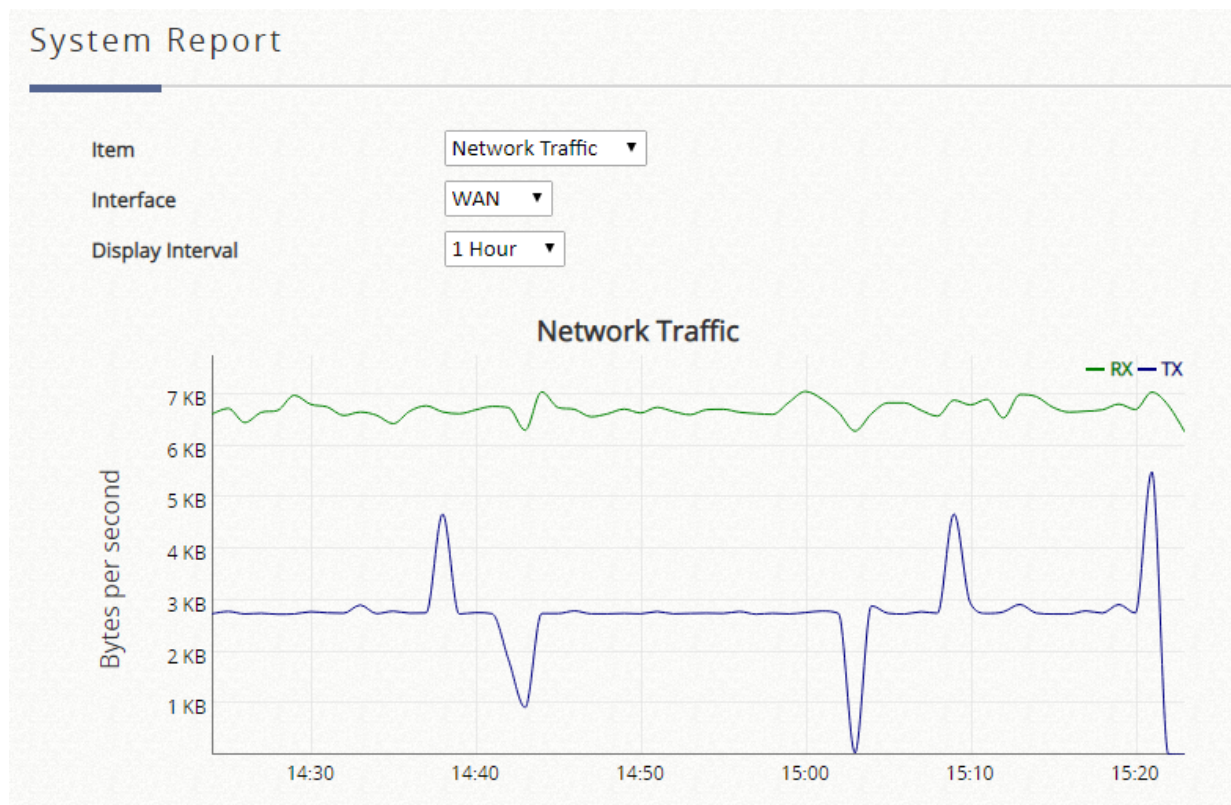
10.1.2 システムの概要

構成パス: 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、レポートサーバの設定、WAN オプション設定、ユーザログプロファイル、システム時刻、セッション制御設定などのコンテンツ一覧が表示されます。この概要は、主な構成アイテム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。



See Reports ボタンをクリックすると、選択したレポートを使用できます。これらのレポートは、インタフェースと時間間隔に基づいて並べ替えることができます。

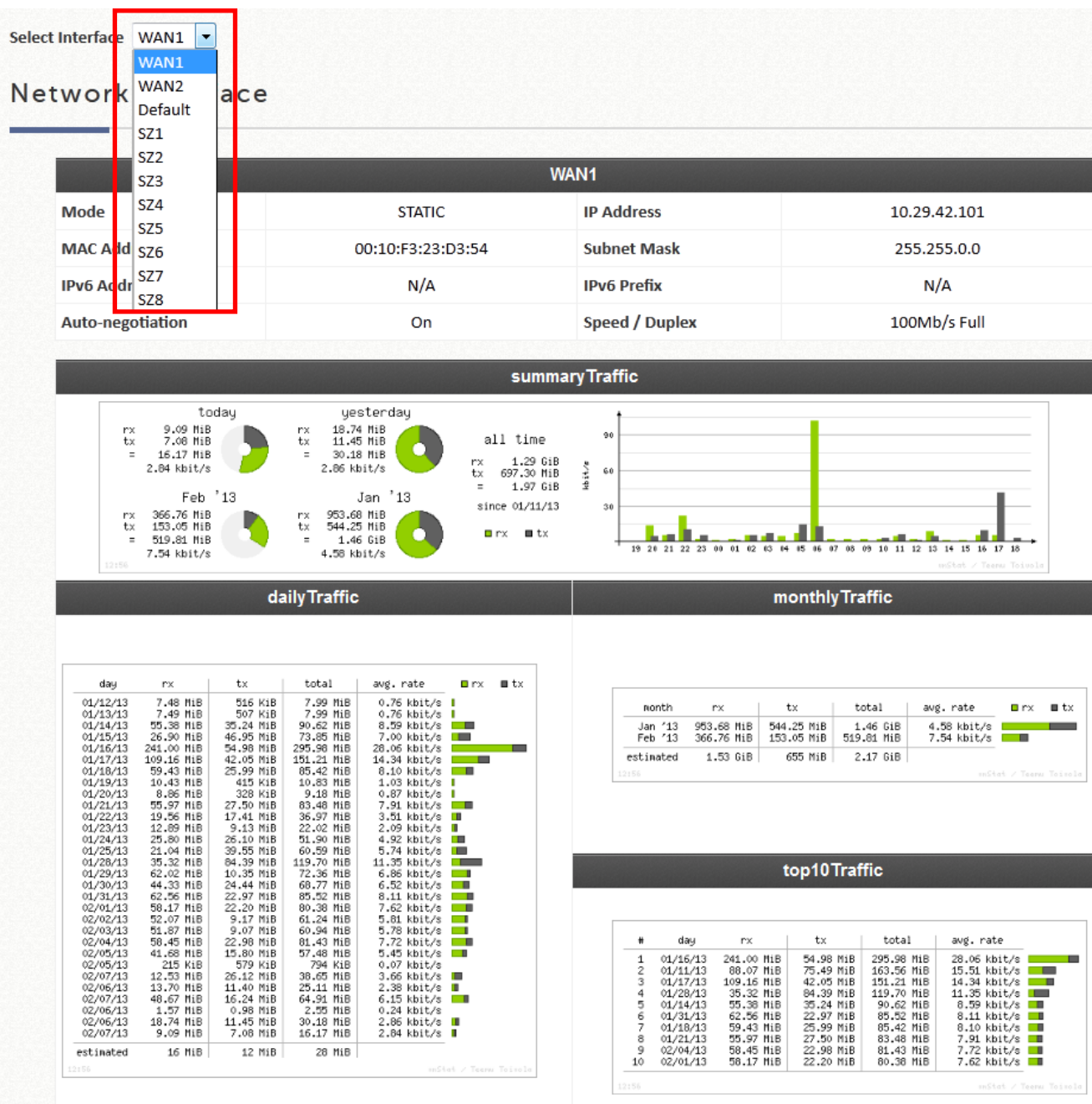


10.1.3 ネットワークインタフェース

構成パス: Main Menu >> Status >> Interface

ここでは、管理者が検査するネットワークインタフェース(WAN1、WAN2、SZ Default、SZ1～SZ8を含みます)について説明します。

表示したいネットワークインタフェースを選択します。選択したインタ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。ページを下にスクロールすると、トラフィックサマリー、当日のトラフィック、当月のトラフィック、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。



注意事項

1. 長期間の統計を保存する必要がある場合、外部サーバでネットワークトラフィックを送信および保存する手順については、「レポートと通知」節を参照してください。

10.1.4 ルーティング

構成パス: Main Menu >> Status >> Routing Tables >> IPv4/IPv6

このステータスページには、すべてのポリシー経路情報ルールが表示され、グローバルポリシー経路情報ルールがここに表示されます。これにより、管理者はウィンドウを参照してすばやく、別のポリシーに属するユーザのルーティングルール適用を確認できます。また、インタフェースごとに指定されたシステム経路情報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、そこで設定されたルールは、IPv6 トラフィックのシステムインタ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

構成パス: Main Menu >> Status >> DHCP Leases

DHCP IP リース統計は、このページの Show Statistics List をクリックすると表示されます。

- **Statistics of offered list**

Last 10 Minutes、Hours と Days の有効なリース数がここに表示されます。ヘッダー1～10 は乗数です。たとえば、列 2 の下の数字は過去 20 分/時/日のリースカウントを示し、列 3 の下の数字は過去 30 分/時/日のリースカウントを示します。

- **Statistics of expired list**

Last 10 Minutes、Hours と Days で期限切れになったクライアントにリースされた IP がここに表示されます。ヘッダー1～10 は乗数です。たとえば、列 2 の下の数字は過去 20 分/時/日の期限切れカウントを示し、列 3 の下の数字は過去 30 分/時/日の期限切れカウントを示します。

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 Lease List

DHCP サーバから発行された有効な IP アドレスと、この IP アドレスを使用しているクライアントの関連情報が表示されます。

DHCP Leases

Statistics List Show

DHCP Lease Log Show

DHCP Lease List

Refresh Delete

Refresh Disable ▾

☐	No.	IP Address	MAC Address	Host Name	VLAN	Lease Expires
☐	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 クライアント関連ステータス

10.2.1 オンラインユーザ

ページパス: Main Menu >> Status >> Monitor Users >> Online Users

この画面に表示されるユーザは、LAN またはリモートトンネルサイトのいずれか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ものです。

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

2つのモードから選択できます。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を強制終了し、Access FromのAP NameのハイパーリンクをクリックしてユーザアクセスAPのステータスを確認できます。特定のオンラインユーザのIPまたはMACアドレスを検索するための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一覧を更新するか、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します。

10.2.2 関連する非ログインユーザ

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サーバからIPアドレスを取得しましたが、LANまたはリモートトンネルサイトで認証されていないユーザが表示されます。この機能は、システムのリソースが使い果たされないように管理者が追跡できるように設計されています。このリストには、クライアントのMAC Address、IP Addressと関連付けられたVLAN ID、Service Zone、および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

ページパス: Main Menu >> Status >> Monitor Users >> Roaming In Users

このページには、このコントローラの物理的な配下にあります、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が表示されます。ここにリスト化されているユーザのトラフィックは、ホームコントローラにトンネルバックされて、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

ページパス: Main Menu >> Status >> Monitor Users >> Roaming Out Users

このページには、他の Controller がこの Controller 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認証したユーザが表示されます。

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:

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、単独で 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 ボタンをクリックすることで、デバイスの認証を手動で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 認証ユーザ

ページパス: Main Menu >> Status >> Monitor Users >> Authenticated Users

コントローラに IP 情報が認識されていない認証完了ユーザを表示します。いくつかのタイプの認証(802.1X、MAC 認証、PPP 認証、CoA ログイン)の場合、ユーザは、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しなければなりません。したがって、ユーザは、認証が完了した後にのみ、DHCP を介した IP アドレスをリクエストできます。認証されたユーザは、IP アドレスを取得し、ネットワークの使用を開始すると、認証済みユーザリストからオンラインユーザリストに移動します。

管理者は、ユーザを選択して Logout ボタンをクリックすることで、認証されたユーザをログアウトすることができます。

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

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に適した機能です。スマートログインを有効にした状態で、オンデマンドユーザが正常にログインすると、デバイスは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します。

スマートログイン期間内のオンデマンドユーザが表示されます。このリストのユーザは、次回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リストのユーザを削除できます。削除されたユーザは、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

構成パス: 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間で現在確立されているセッションを検査できます。それぞれの結果には、送信元および宛先の IP およびポートの値が表示されます。フィルタ条件を定義し、必要な結果のみを表示することができます。

Session List

Filter					
Address Family	Protocol	Source IP	Port	Destination IP	Port
IPv4 ▾	All ▾				

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

構成パス: Main Menu >> Status >> Logs and Reports

このページには、システム起動後の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保存されるため、再起動/リブート時に失われます。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:** コントローラと AP が有効化された CAPWAP 間で通信された 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 構成を変更したユーザのアカウントと IP が表示されます。
- **Local Monthly Usage:** このページには、ローカルユーザの集計された統計が表示され、その月の送信トラフィックが表示されます。
- **Local Web Log:** このページは、コントローラ組み込み Web サーバのどの Web ページがアクセスされたかを示します。
- **On-Demand User Billing Report Log:** オンデマンドアカウントトランザクションの概要が表示されます。
- **RADIUS Server Log:** 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、起動時刻、発信者、着信者、接続時間(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:** イベントトレースのシステム関連ログを表示します。
- **UAMD Log:** UAM デーモンから出力された 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。アラームメッセージは、障害が解決されるまでアラームリストに残ります。アラーム項目は、Alarms & Event Settings ページで設定できます。
- **Management Event:** 選択したマネジメントイベントのログを表示します。管理イベントは、Alarms & Event Settings で設定できます。

10.3.2 ユーザイベント

構成パス: Main Menu >> Status >> Logs and Reports >> User Events

このページには、すべてのユーザログとイベントが含まれています。ユーザログとイベントは、最大 40 日間保存できます。管理者の好みによりカスタマイズ可能なすべてのユーザ関連の情報を表示します。管理者は、ページごとに表示する行数(20、40、60、80、および 100)を選択できます。カレンダーから開始日と終了日を選択して、不要なユーザイベントをフィルタリングします。開始日と終了日を選択した後、Display をクリックすると、選択した日付内のすべてのユーザイベントが表示されます。

Download ボタンで、表示されているユーザイベントがカンマ区切りのテキストファイルにダウンロードされます。ダウンロードしたデータを拡張子.csv の新しいファイルとして保存して、セルに並べ替えます。Clear ボタンで、ユーザインタフェースに表示されている現在のユーザイベントが削除されます。

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 User Events に表示される列を変更できます。

なお、User Type によってユーザ情報が異なることに注意してください。User Type に該当しない場合は、カテゴリは空白のままになります。

ローカルユーザに適用可能なユーザイベントカテゴリ:

Date、Type、Name、IP、IPv6、MAC、Pkts In、Bytes In、Pkts Out、Bytes Out、VLAN ID、Group、Policy、MaxDnLoad、MaxUpload、ReqDnLoad、および ReqUpload

オンデマンドユーザに適用可能なユーザイベントカテゴリ:

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、および ReqUpload

ローミングアウトユーザに適用可能なユーザイベントカテゴリ:

Date、Type、Name、NSID、NASIP、NASPort、UserMAC、SessionID、SessionTime、Bytes In、Bytes Out、Pkts In、Pkts Out と Message

ローミングインユーザに適用可能なユーザイベントカテゴリ:

Date、Type、Name、NSID、NASIP、NASPort、UserMAC、UserIP、SessionID、SessionTime、Bytes In、Bytes Out、Pkts In、Pkts Out と Message

10.4 レポートと通知

構成パス: Main Menu >> Status >> Reporting

EWS コントローラは、設定された E-mail アドレス、SYSLOG サーバ、または FTP サーバに、さまざまな種類のユーザおよび/またはシステム関連の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	☐	☐	☐	☐	☐		N/A	N/A	1 Hour ▼
Local Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼
On-Demand Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼
Guest Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼
Roaming Out Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼
Roaming In Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼
External Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼
Session Log	☐	☐	☐	☐	☐		☐		1 Hour ▼
Firewall Log	☐	☐	☐	☐	☐		☐	N/A	1 Hour ▼
High Availability Mode Change	☐	☐	☐	☐	☐		N/A	N/A	N/A
Local Area AP Status Change	☐	☐	☐	☐	☐		N/A	N/A	2 Mins ▼
On-Demand User Billing Report	☐	☐	☐	☐	☐		N/A	☐	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report
Wide Area AP Status Change	☐	☐	☐	☐	☐		N/A	N/A	2 Mins ▼
Wide Area AP Report ☐ CPU Loading ☐ Memory Usage ☐ Network Delay ☐ Network Traffic ☐ Associated Clients ☐ VAP Traffic ☐ WDS Traffic							N/A	☐	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Switch Status	☐	☐	☐	☐	☐		N/A	N/A	2 Mins ▼
Switch Report ☐ PoE overview	☐	☐	☐	☐	☐		N/A	N/A	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Local HTTP Web Log							☐		1 Hour ▼
HTTP Web Log							☐		1 Hour ▼
Configuration Change Log	☐	☐	☐	☐	☐		N/A	☐	1 Hour ▼
DHCP Server Log							☐	N/A	N/A
DHCP Lease Log							N/A	☐	1 Hour ▼
System Report ☐ CPU Loading ☐ CPU Temperature ☐ Memory Usage ☐ Storage Usage ☐ Network Traffic ☐ Online User ☐ Successful Login ☐ Session ☐ DHCP Lease ☐ DNS Query							N/A	☐	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Traffic Report (Text) ☐ Service Zone ☐ VLAN							N/A	☐	1 Hour ▼

- **SMTP Settings:** 5つの受信者電子メールアドレスと、さまざまなユーザ関連のログが送信されるメールサーバに必要な設定を構成できます。
- **SYSLOG Settings:** 選択したユーザログとシステムログの送信先となる2つの外部SYSLOGサーバを設定できます。
- **FTP Settings:** 選択したユーザログとシステムログを送信する外部FTPサーバの設定できます。
- **Notification Settings:** 使用可能なすべてのユーザ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、およびFTP)に送信できます。
- **Alarms & Events Settings:** 選択可能な管理イベントの一覧が表示されます。管理イベントとして項目を選択すると、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。アラームを選択した場合、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ますが、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 オンデマンド課金プラン

構成パス: Main Menu >> Users >> Internal Authentication >> On-Demand >> Billing Plans

請求プランプロファイルは、ゲストインターネットアクセスの期間と条件を定義します。Billing Plan Number をクリックすると、選択した請求書プランプロファイルの設定画面が表示されます。課金プランプロファイルの設定が完了したら、Billing Plans の画面に戻り、Active チェックボックスをオンにして、Apply をクリックして有効にします。

Billing Plans						
No	Plan Type	Quota	Price	Active	Group	Function
1	Usage-time	2 hr(s) of connection time quota with expiration	1.99	☒	Group 1	<button>Reset</button>
2	N/A			☐	Group 1	<button>Reset</button>
3	N/A			☐	Group 1	<button>Reset</button>
4	N/A			☐	Group 1	<button>Reset</button>
5	N/A			☐	Group 1	<button>Reset</button>

- **Plan:** 選択した請求書プランプロファイルの数。
- **Plan Type:** このプランで選択されたアカウントタイプ。アカウントタイプによって、プロパティが異なります。最適なアカウントの種類を選択することで、お客様の使用要件を満たすことができます。
- **Quota:** オンデマンドユーザがネットワークへのアクセスを許可される量または期間に関する使用条件。
- **Price:** それぞれの請求書プランの単価。
- **Active:** チェックボックスをオンにして、課金プランを有効にします。無効化された請求計画を使用してオンデマンドゲストアカウントを生成することはできません。
- **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のグループ割り当て。
- **Function:** Reset をクリックすると、選択した請求書プランプロファイルの設定がクリアされます。

11.2 オンデマンド課金プランタイプ

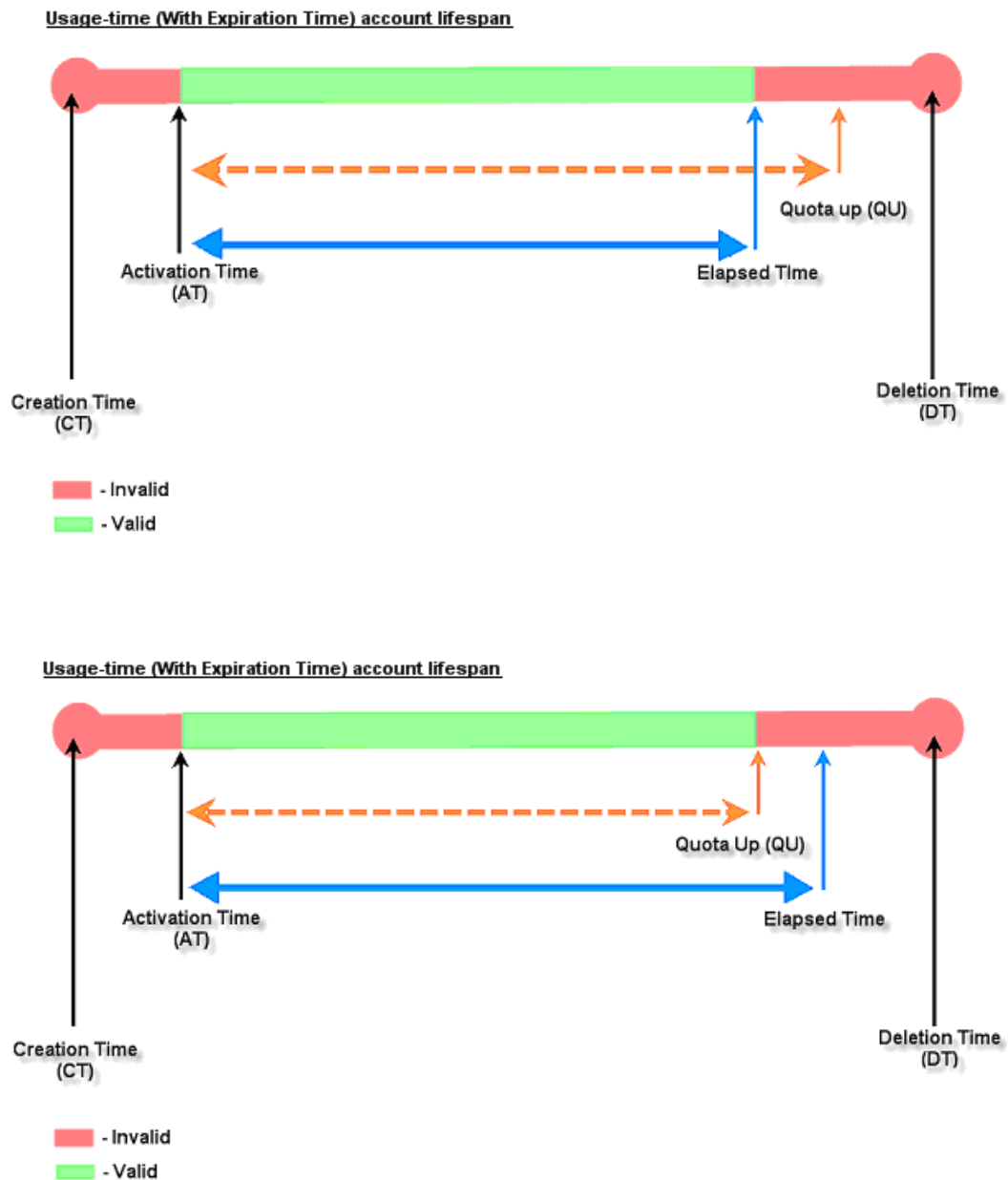
11.2.1 有効期限付き使用時間

ユーザは、アカウントが有効で、残りのクォータ(使用可能時間)がある限り、インターネットにアクセスできます。ユーザは、ログインして、一定期間内に購入したアカウントを有効化する必要があります。コーヒーショップ、空港ターミナルなど、短期間のご利用に適しています。クォータは使用中にのみ減算されますが、ログインまたはログアウトに関係なく、有効期限までのカウントダウンは継続されます。アカウントは、Valid Period が使い尽くされたとき、または割り当てが枯渇したときに期限切れになります。

- **Quota** は、オンデマンドユーザがネットワークへのアクセスを許可される総期間(xx 日 yy 時 zz 分)です。合計最大クォータは、引き換え後「364 日 23 時間 59 分 59 秒」です。
- **Account Activation** は、ユーザが最初のログインを実行する必要がある期間です。Account Activation で設定した時間内にこれを行わないと、アカウントの有効期限が切れます。
- **Valid Period** は、使用できる有効期限です。この期間を過ぎると、クォータが残っていても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に適用されます。
- **Reference** フィールドには、管理者が追加情報を入力することができます。

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	



11.2.2 有効期限なしの使用時間

ユーザは、アカウントが残りのクォータ(使用可能時間)を持っている限り、インターネットにアクセスできます。ユーザは、ログインして、一定期間内に購入したアカウントを有効化する必要があります。コーヒーショップ、空港ターミナルなど、短期間のご利用に適しています。クォータは使用中にのみ差し引かれ、クォータが使い果たされた場合にのみアカウントが期限切れになります。

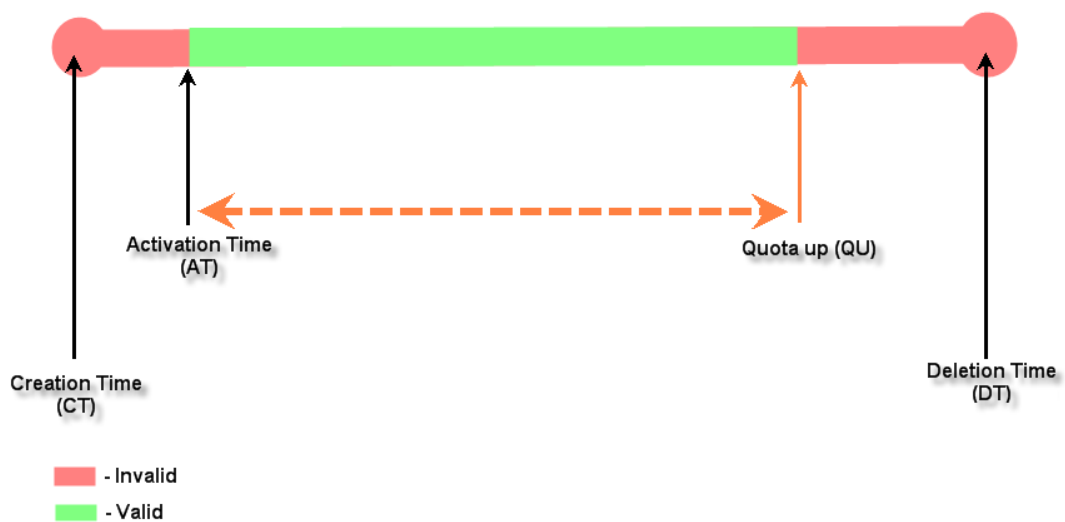
- **Quota** は、オンデマンドユーザがネットワークへのアクセスを許可される総期間(xx 日 yy 時 zz 分)です。合計最大クォータは、引き換え後「364 日 23 時間 59 分 59 秒」です。
- **Account Activation** は、ユーザが最初のログインを実行する必要がある期間です。Account Activation で設定した時間内にこれを行わないと、アカウントの有効期限が切れます。

- **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に適用されます。
- **Reference** フィールドには、管理者が追加情報を入力することができます。

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
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 (No Expiration) account lifespan



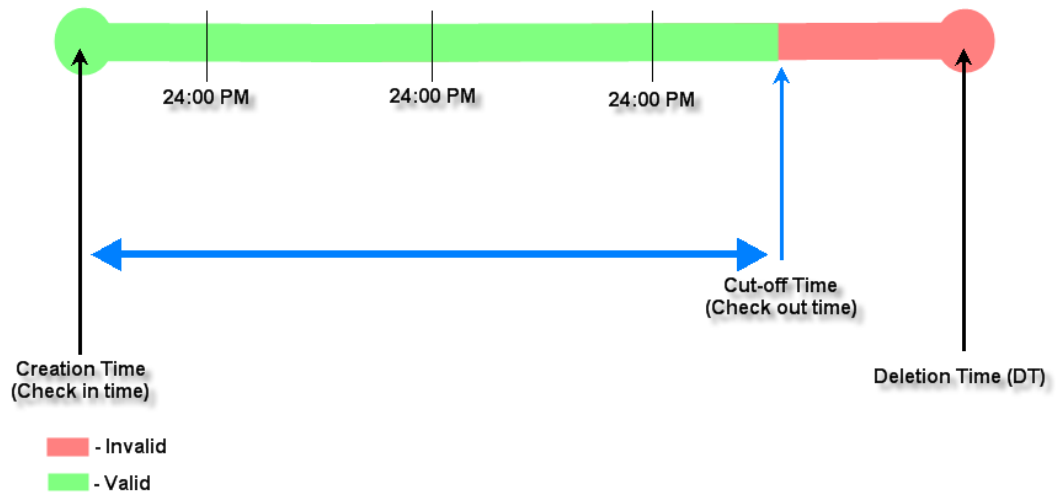
11.2.3 ホテル・カットオフ時刻

Hotel Cut-off-time 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切断(期限切れ)される時刻(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、カットオフ時刻までの日数である Unit 値を入力できます。たとえば、Unit=2days、Cut-off Time=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 は、アカウントが切断された後、短期間の猶予時間であり、ユーザ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い続けることができます。Number of Devices では、アカウントごとに許可される同時ログインデバイス数を定義します。Unit Price は、この請求プランの日額です。主に、ゲストの滞在時間に応じたインターネットサービスを提供するホテルの会場で使用されます。Group は、このプランから作成されたユーザに適用されます。Reference フィールドには、管理者が追加情報を入力することができます。

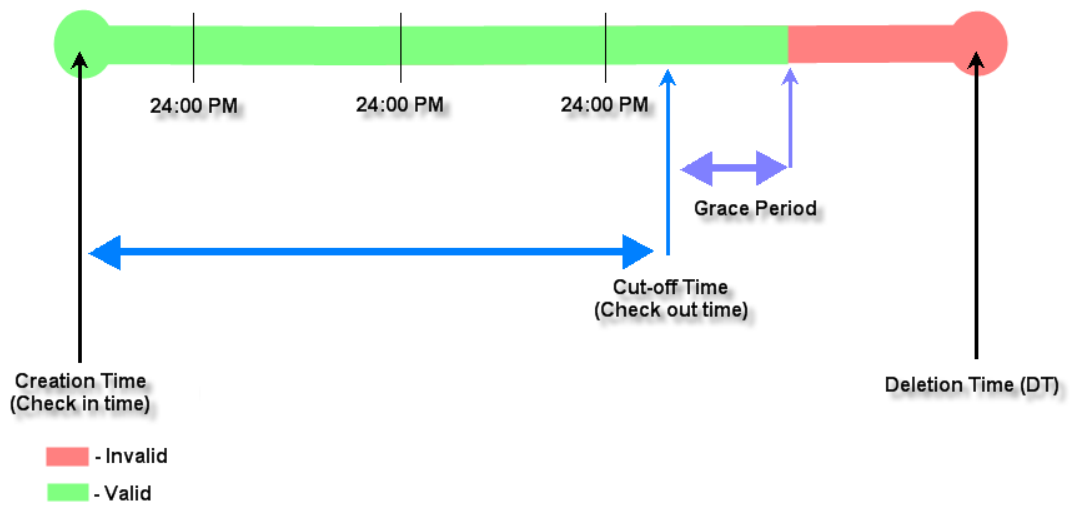
Billing Plan Configuration

Plan Number	1
Plan Type	Hotel Cut-off time ▼
Cut-off Time	: The cut-off time has to be between 00:00~23:59 in the form of hh:mm.
Grace Period	0 ▼ hour(s) after Cut-off
Number of devices	1 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	11 per day The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1 ▼
Reference	

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



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



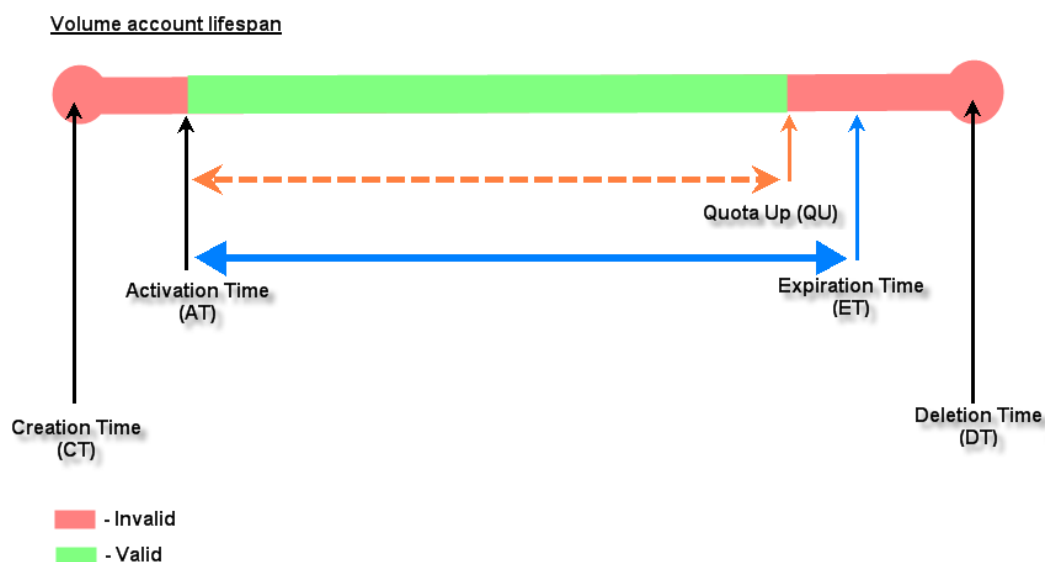
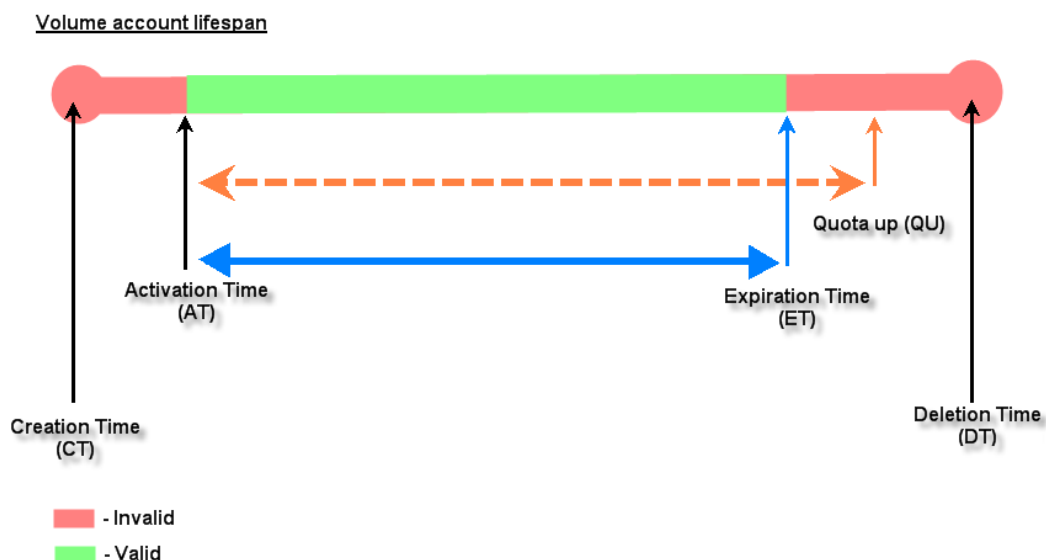
11.2.4 ボリューム

ユーザは、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る限り、インターネットにアクセスできます。有効期限が切れるのは、有効期限が使用されているか、クォータが使い果たされた場合です。メールの送受信、ファイルの転送など、少量のアプリケーションに適しています。ログイン/ログアウトにかかわらず、有効期間のカウントダウンは継続されます。

- **Account Activation** は、ユーザが最初のログインを実行する必要がある期間です。Account Activation で設定した時間内にこれを行わないと、アカウントの有効期限が切れます。
- **Expiration** は、使用できる有効期限です。この期間が経過すると、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がネットワークにアクセスできる合計 M バイト(1~1000000)です。
- **Number of Devices** では、アカウントごとに許可される同時ログインデバイス数を定義します。(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に適用されます。
- **Reference** フィールドには、管理者が追加情報を入力することができます。

Billing Plan Configuration

Plan Number	1
Plan Type	Volume ▼
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	Account will expire in 7 day(s) after activation
Quota	100 MByte(s) *(Range : 1 ~ 1000000)
Number of devices	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	2 The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1 ▼
Reference	



11.2.5 経過時間による持続時間

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、アカウントの有効期限が切れます。これは、一定期間の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最適です。

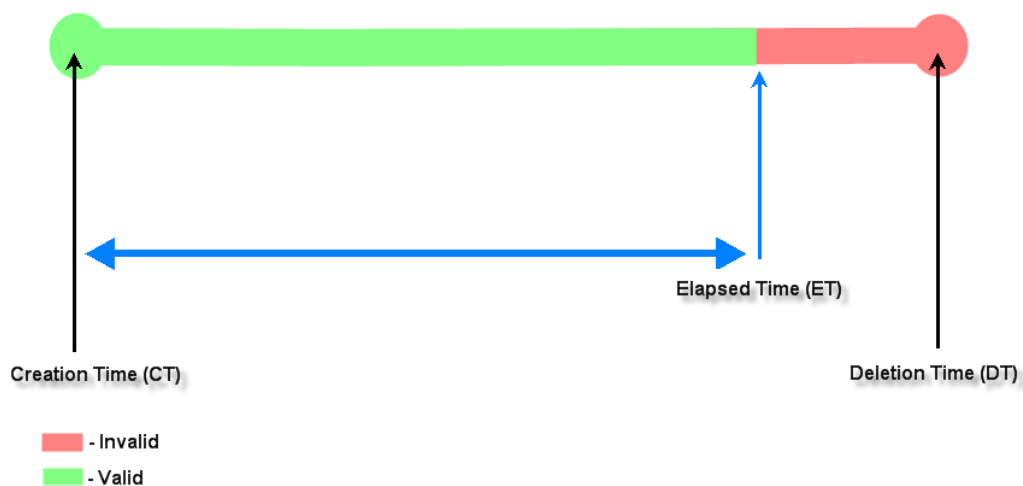
- **Begin Time** は、アカウントが使用のためにアクティブ化される時刻です。アカウント作成時間に設定されます。
- **Elapsed Time** は、アカウントがインターネットアクセスに対して有効な期間(xx 時間 yy 分)です。
- **Number of Devices** では、アカウントごとに許可される同時ログインデバイス数を定義します。
- **Price** は、このプランの単価です。

- **Group** は、このプランから作成されたユーザに適用されます。
- **Reference** フィールドには、管理者が追加情報を入力することができます。

Billing Plan Configuration

Plan Number	1
Plan Type	Duration-time ▼
Duration Type	☒ Elapsed Time ☐ Begin-and-End Time ☐ Cut-off Time
Begin Time	☒ Upon Account Creation ☐ Upon First Login
Quota	day(s) hr(s) 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.
Number of devices	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	11 The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1 ▼
Reference	

Duration-time (Elapsed Time) account lifespan



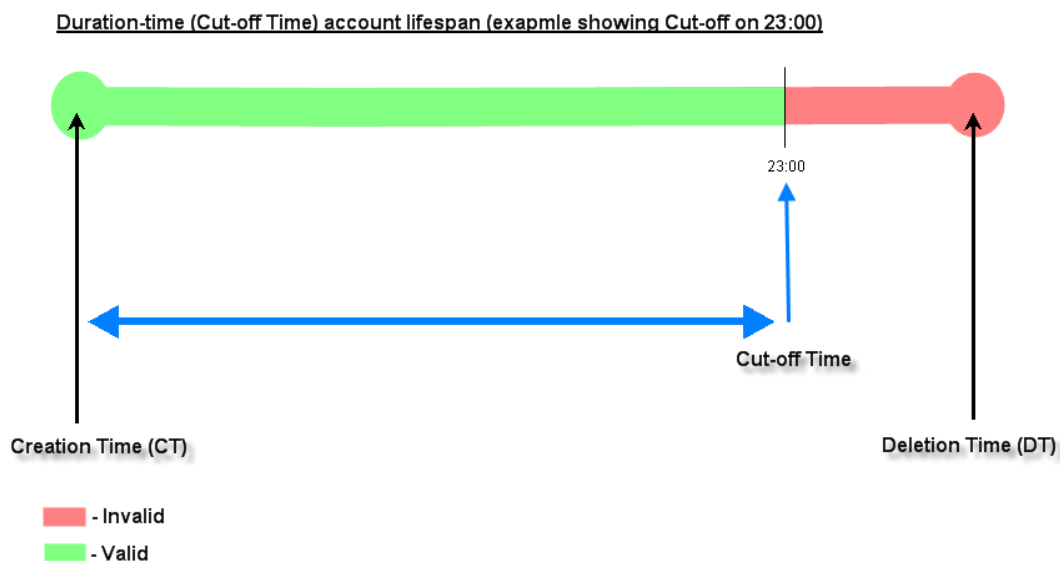
11.2.6 カットオフ時刻による持続時間

Cut-off Time は、その日にシステムによってオンデマンドアカウントが切断(期限切れ)される時刻です。たとえば、ショッピングモールが 23:00 にクローズす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オペレータは、このプランを使用して、23:00 にカットオフに設定されたチケットを作成できます。この種のアカウントがカットオフ時刻後に作成されると、アカウントは自動的に期限切れになります。

- **Begin Time** は、アカウントが使用のためにアクティブ化される時刻です。アカウント作成時間に設定されます。
- **Cut-off Time** は、アカウントの有効期限が切れる時刻です。
- **Number of Devices** では、アカウントごとに許可される同時ログインデバイス数を定義します。
- **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に適用されます。
- **Reference** フィールドには、管理者が追加情報を入力することができます。

Billing Plan Configuration

Plan Number	1
Plan Type	Duration-time ▼
Duration Type	☐ Elapsed Time ☐ Begin-and-End Time ☒ Cut-off Time
Begin Time	Upon Account Creation
Cut-off Time	: The cut-off time has to be between 00:00~23:59 in the form of hh:mm.
Number of devices	1 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	11 The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1 ▼
Reference	



11.2.7 開始/終了時間による持続時間

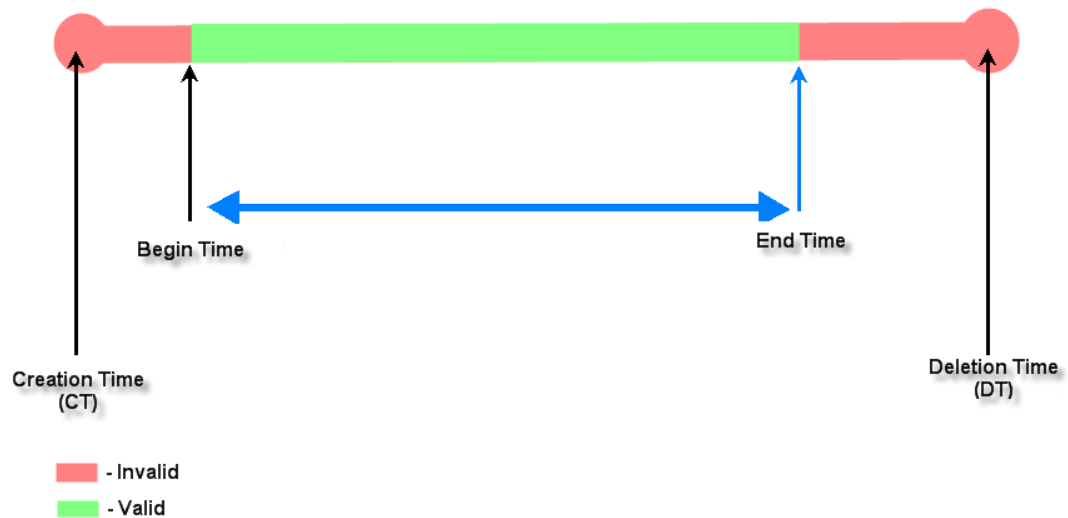
アカウントの開始時間と終了時間は明示的に定義されます。カウントダウンは、アカウントがアクティブ化された直後に開始され、終了時刻に達すると期限切れになります。これは、特定の期間にわたってインターネットサービスを提供するのに理想的です。例えば、Computex のような展示会イベントや大規模な大会の期間中、登録された各参加者は 6 月 1 日午前 8:00 から 6 月 5 日午後 5 時まで有効な、クーポンのようにバッチ生成されたインターネットアカウントを取得します。

- **Begin Time** は、アカウントが使用のためにアクティブ化される時刻で、オペレータによって明示的に定義されます。
- **End Time** は、アカウントがオペレータによって明示的に定義された期限切れになる時刻です。
- **Number of Devices** では、アカウントごとに許可される同時ログインデバイス数を定義します。
- **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に適用されます。
- **Reference** フィールドには、管理者が追加情報を入力することができます。

Billing Plan Configuration

Plan Number	1
Plan Type	Duration-time ▾
Duration Type	☐ Elapsed Time ☒ Begin-and-End Time ☐ Cut-off Time
Begin Time	-- ▾ : -- ▾ , -- ▾ -- ▾ ---- ▾
End Time	-- ▾ : -- ▾ , -- ▾ -- ▾ ---- ▾
Number of devices	1 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	11 The unit price cannot exceed 100000, and can take values up to two decimal places.
Group	Group 1 ▾
Reference	

Duration-time (Begin-and-end Time) account lifespan



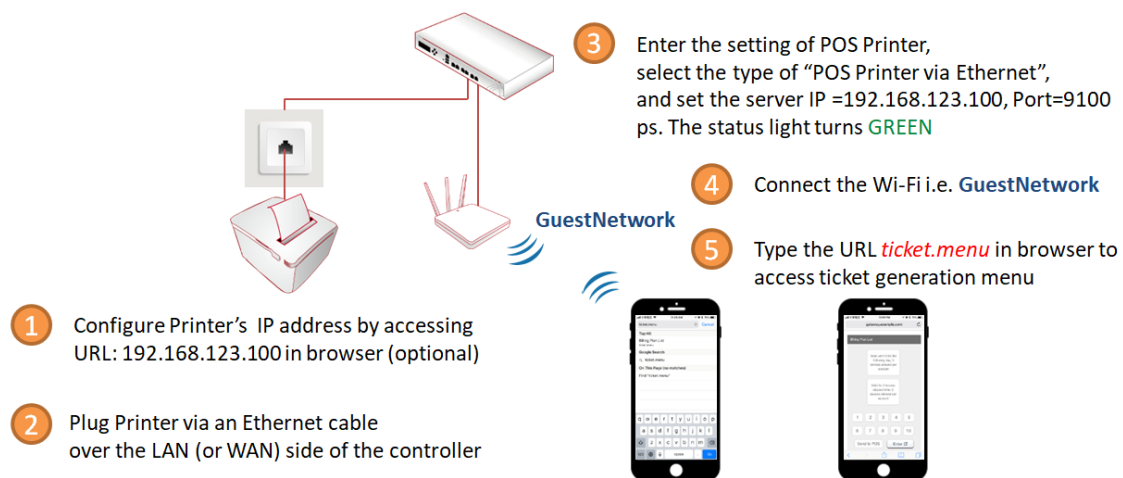
11.3 POS プリンタの設定

ネットワークチケットジェネレータの概要

オンデマンドアカウント生成に対応した EC-PP200 は、Edgecore Wireless LAN Controller 内蔵のオンデマンド課金プラン機能を使用してチケットを印刷することができます。注目すべきは、EC-PP200 は、追加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。

EC-PP200 をネットワークに組み込む

次の概略図は、ネットワークで EC-PP200 を使用するための簡単なユースケースとクイック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. EC-PP200 とコントローラをイーサネットで接続します。
3. EC-PP200 の IP アドレスとポートは、コントローラのターミナルサーバ画面で入力します。
4. Wi-Fi またはイーサネットを介してネットワークに接続します。
5. コントローラの Web マネジメントインタ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。

マネジメントインタフェースで EC-PP200 を管理する

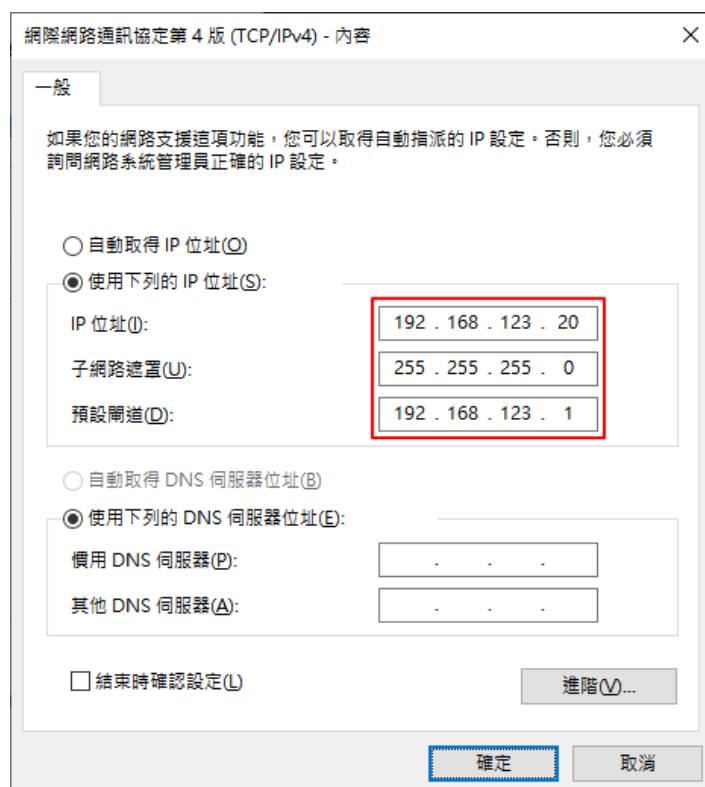
EC-PP200 は、すべての Edgecore Gateway/Controller と連携して動作するように特別に設計されています。EC-PP200 を Edgecore Gateway/Controller に接続する前に、いくつかの設定手順が必要です。

EC-PP200 の関連する構成については、Web マネジメントインタフェース(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

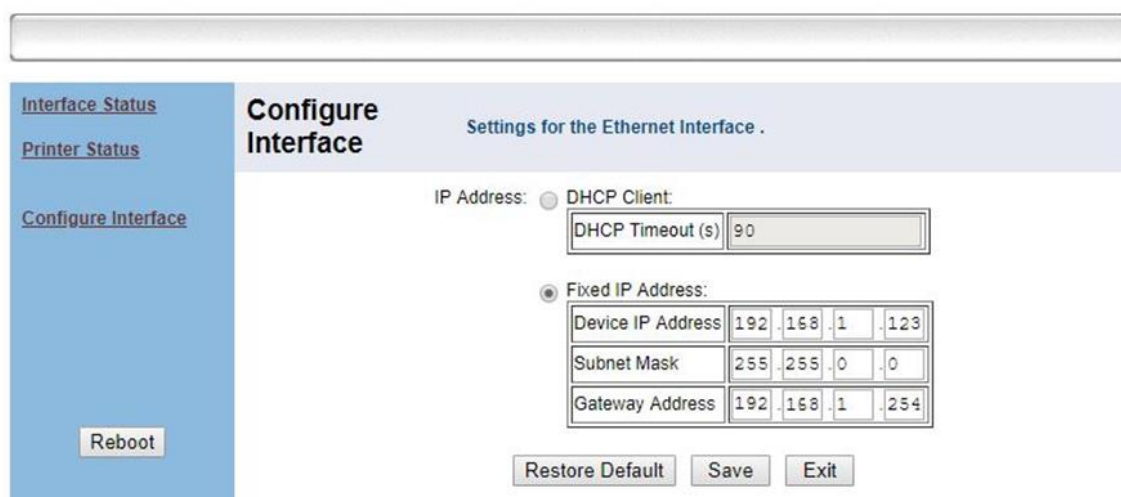
サブネットマスク: 255.255.255.0

使用するコンピュータの TCP/IP 設定は、EC-PP200 と同じサブネットにあるスタティック IP アドレスで設定してください。例：192.168.123.20



EC-PP200 の WMI では、Configure Interface 画面で IP 設定を変更し、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



EC-PP200 を再起動後、新しい IP アドレスで WMI に接続し、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	
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

Edgecore Gateway/Controller を使用した EC-PP200 のセットアップ

構成パス: Main Menu >> Users >> Internal Authentication >> On-Demand Authentication >>
POS Printer Configuration

Edgecore Gateway/Controller は、複数の POS プリンタの管理をサポートしています。EC-PP200 を使用してアカウントチケットを印刷するには、管理者はプリンタの IP アドレスをコントローラの一覧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. 請求計画を作成して有効にします。(11.1、11.2 参照)
2. POS チケットテンプレートを設定します。(11.4 参照)
3. 「POS Printer via Ethernet」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、有効にする請求予定を確認します。

注意事項

1. POS プリンタリストに EC-PP200 を追加する場合、ポートは 9100 にする必要があります。

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 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐

(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 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐
	2				Template 1 ▼	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐
	3				Template 1 ▼	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐

11.4 POS チケットのカスタマイズ

構成パス: Main Menu >> Users >> Internal Authentication >> On-Demand >> POS Tickets

ホットスポットでの展開の柔軟性のために、テンプレートを使用した POS チケットのカスタマイズが EWS コントローラでサポートされています。チケットテンプレートは 5 件まで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

☒ 4 characters
 ☐ 8 characters

Ticket Type

Type 1 ▼

Restore

For Usage-Time with expiration time & Volume

- 必要に応じて、TMB フォーマットにイメージ(会社のロゴなど)をアップロードできます。
- 幅タイプは 2 種類あり、EC-PP200 は 3" を推奨します。
- 設定したチケットテンプレートの言語を選択します。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するオプションがあります。

- 設定した請求計画に応じて、適切なチケットタイプを選択します。

The screenshot shows a configuration window titled "Type I". On the left, under "Parameters", there is a list of variables: Username: \$username, Password: \$password, Quota: \$quota, Price: \$price, ESSID: \$qr, Activation: \$duration, and Expiration: \$duration days after activation. A dropdown menu is open, showing a list of parameters including \$remain, \$username, \$username_without_postfix, \$password, \$usage, \$price, \$extid, \$activationtime, \$expiretime, \$expire_time, \$duration, \$remark, \$image, \$unit, \$date, \$quota, \$sprice, \$qr, and \$max_user. The \$remain parameter is selected. To the right of the dropdown is an "Insert Parameters" button. Below the dropdown, the text "SN:\$remain" is displayed. At the bottom of the window is a "Preview" button.

POS チケットのカスタマイズは、以下の画面から手動で入力するか、上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することで開始できます。

これが完了したら、端末サーバに課金プランとチケットテンプレートを割り当てることができます。

Terminal Server Configuration

Status	Item	Server IP	Port	Remark	Ticket template	Billing plan
●	1				Template 1 ▼	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐
●	2				Template 1 ▼	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐
●	3				Template 1 ▼	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐
●	4				Template 1 ▼	1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 0 ☐

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の希望する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 コードログインのアプリケーション

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では非常に一般的な配置です。アカウントのユーザ名とパスワードを手動で入力するのが面倒なのは、とくに小さなキーボードで入力する必要があり、見えにくい携帯端末の場合です。

ユーザ名、パスワード、使用クォータ、価格などの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 コードを読み取るだけで、インターネットサーフィンの準備が整います。

QR コードをサポートするように Web チケットを設定する

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る必要があります。

Main Menu >> Users >> Authentications で、チケットテンプレートをカスタマイズするために On-Demand User と Configure をクリックします。

POS Tickets

Templates

Image

Width

Languages

length of password

Ticket Type

Template 1 ▼

Upload

3" ▼

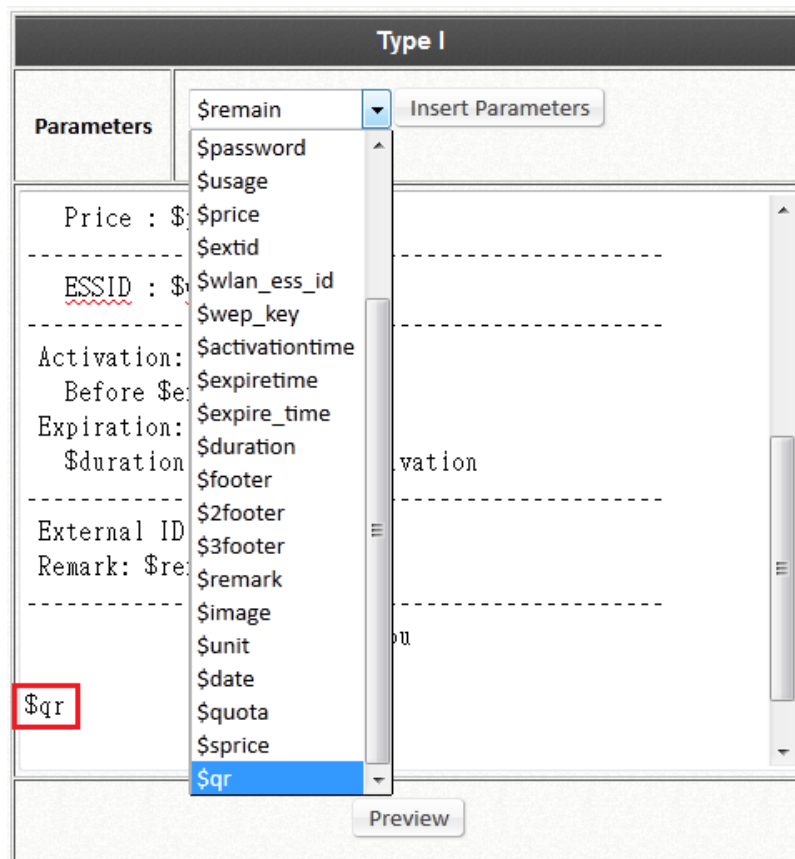
English ▼

☒ 4 characters ☐ 8 characters

Type I ▼

Restore

For Usage-Time with expiration time & Volume



利用する課金プランの場合、対応するチケットテンプレートをカスタマイズして QR コードをサポートする必要があります。

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

11.5 アカウントの作成

構成パス: Main Menu >> Users >> On-Demand Accounts >> Accounts Creation

管理者は、単一アカウントまたは一括アカウントを作成するオプションがあります。オンデマンド機能には、ゲストアカウントを事前に作成して販売するホットスポットオペレータ向けに、管理者またはオペレータがオンデマンドページにアクセスできるようにするバッチ作成機能があります。この機能を使用すると、管理者またはオペレータは、有効になっている請求プランの複数のアカウントを一括で作成し、POS プリンタに送信して、販売用の物理チケットプリントアウトを生成できます。

On-Demand Account Creation

Plan	Account Type	Quota	Price ()	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、ランダムに生成されたユーザ名とパスワードを使用するか、バッチオンデマンドアカウントを作成するときにユーザ名とパスワードを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、短い(4 文字)または長い(8 文字)のいずれかになります。

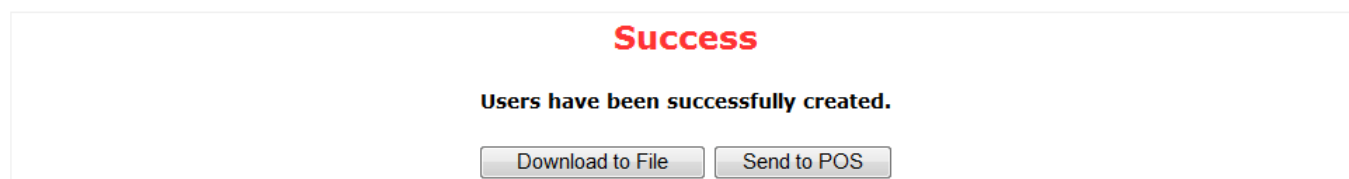
Creating Batch On-Demand Accounts

Plan : Account Type	1 : Usage-time
Quota	2 hr(s) of connection time quota with expiration
Numbers	1 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 4ipnet
Valid Period	After activation, the account will be expired in 7 day(s)
Total Price	1.99
Unit	1 Number of units per ticket
Group	Group 1

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

カスタムユーザ名を作成する場合、アカウントのシリアル番号は 1 つずつ増加しますが、プレフィックスとポストフィックス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、または一括印刷のためにプリンタに送ることができます。



11.6 ユーザセルフサービス

外部決済ゲートウェイ経由のクレジットカード

構成パス: Main Menu >> Users >> Authentication >> On-Demand User >> External Payment Gateway

EWS コントローラは、Authorize.net、PayPal、SecurePay、WorldPay、PeleCard など、オペレーターが所有するアカウントタイプに応じて、異なるタイプの決済ゲートウェイオプションをサポートします。

最も一般的に使用される PayPal は、以下の例として使用されます。

PayPal を設定するには、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いた後、ホットスポット所有者は、PayPal 支払いページ構成を継続するために、この PayPal アカウントの ID トークンを見つけるべきです。

決済ページ設定で、必要な商業アカウントの資格情報を入力します。コントローラの WAN IP が NAT に設定されている場合は、決済側ユーザがトランザクション結果を受信するために、Instant Payment Notification(IPN)項目で IP 転送情報を設定する必要があることに注意してください。

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 ▼

エンドユーザが決済ゲートウェイを介して自己購入することを許可されている有効な請求計画を選択します。

Choose Billing Plan for PayPal Payment Page

Plan	Activation	Quota	Price	Remark
1	☒	2 hr(s) of connection time quota with expiration	1.99	
2	☒	Valid until 5:01 the following day	1	
3	☐			
4	☐			
5	☐			
6	☐			
7	☐			
8	☐			
9	☐			
0	☐			

サービス免責事項は、Web ページカスタマイズを設定することによってカスタマイズできます。

その後、外部決済ゲートウェイを構成すると、ログインページにハイパーリンクが表示され、有効なクレジットカードを使用してアカウントを購入するために、エンドユーザが段階的に案内されます。

新しいアカウントを購入した後、ユーザが SMS でアカウント情報を入手し、次回ログイン時にユーザ名とパスワードを忘れる危険性を排除するために、管理者は SMS ゲートウェイを決済ゲートウェイに統合することを選択できます。

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

設定が正常に完了すると、Number of SMS Quota 項目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、アカウントのオンライン料金を支払った後、携帯電話番号を入力します。アカウント購入者は、設定された回数を超えない範囲で SMS を再送信できます。

外部決済ポータルをプレビューするには、画面下部の Web Page Customization の Configure をクリックします。システム内のカスタマイズ可能なすべての Web ページと同様に、このページもテンプレートを使用したカスタマイズ、html のアップロード、または外部ページの使用をサポートしています。External Payment Gateway を SMS Gateway と併用した場合の表示例を以下に示します。

Account Credentials	
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

You have to login before 2014/04/15 15:33
The account will be expired in 2 days after account activation.

****Please remember your login credentials before closing the window**

Cellphone number (with country code)

You can send the account info to your cellphone

Login Now

PMS セルフサービス

VLAN ネットワークを計画し、Port Location Mapping 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。「ポートタイプ」の設定に従い、ユーザが 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。

ユーザが部屋からインターネットにアクセスしようとする、利用可能なプランとサービス契約の一覧を含むログインページが表示されます。サービス契約の本文は、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。ユーザが請求書発行プランを選択し、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。すでにユーザアカウントがある場合は、here リンクをクリックすると、所有しているユーザアカウントでログインできます。

Welcome to Broadband Internet Service

Please choose from the following service selection

Plan (s)	Price ()	Unit
☒ 2 hr(s) of usage time and expired in 10 day(s)	0.99	
☐ Valid until 23:00 the following day; 40 devices allowed per account	1.49	
☐ Valid for 3 day(s) elapsed time; 40 devices allowed per account	1.99	

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

このセクションでは、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(別々の LAN ポートであるかのように)を作成し、これらの VLAN を別々の場所に個別にマッピングするために設計されています。この機能を使用すると、VLAN スイッチがゲートウェイの下に配置され、個々のルームに VLAN 接続を提供する MTU/MDU 展開で個別のクライアントに個別の VLAN を提供できます。

ポートロケーションマッピング機能は、ゲストルームおよびパブリックエリアのインターネットサービスを管理するホスピタリティ会場でも一般的に使用されます。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、ゲートウェイと人気の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)ソフトウェアとの間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 タグに対応する場所です。有料(単一または複数のユーザ)、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。有料サービスを利用するには、少なくとも 1 つ以上のオンデマンド料金プランが作成されている必要があります。これにより、ユーザは、希望するプランを選択してインターネットアクセス料金を支払うことができます。

注意事項

1. EWS コントローラは、Micros PMS、InnKey PMS、および IDS インタフェースにデフォルト対応しています。独自のインタ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 の営業担当者にお問い合わせください。

12.1 ホテルルームロケーションマッピング

構成パス: Main Menu >> System >> Port Location Mapping

ポートロケーションマッピング機能により、各サービスゾーンは(各 VLAN がポートであるかのように)複数の VLAN を所有し、クライアントがどこから来ているかを識別することができます。

PMS ミドルウェアの設定や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。

Create

Status

☒ Enable ☐ Disable

Apply

Mapping

Create

Subinterface

Use LAN Port

LAN1

Subinterface ID

Enter a Number Here

Remark

Optional

AddCancel

Lists

PLM List

Show

Subinterface List

Show

Tunnel PLM List

Show

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、場所(ホテルルームなど)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、各部屋を別々のサービスゾーンに割り当てて、別々のポリシーを取得することもできます。さらに、アプリケーションに応じて、さまざまな部屋をさまざまなポートタイプ(Open、Block、または Auth. Required)に設定できます。

- Open、このポートタイプは、ユーザがこの部屋のインターネットに無料でアクセスできることを意味します。
- 部屋にインターネットアクセス権を付与しない場合は、部屋のポートを Block に変更できます。ユーザがブラウザを開き、インターネットにアクセスしようすると、ユーザに通知するブロックメッセージがポップアップ表示されます。
- Auth. Required ポートタイプは、主にユーザに請求するホスピタリティアプリケーションに使用されます。ユーザがブラウザを開き、インターネットにアクセスしようすると、免責事項と課金プランのオプションが記載されたページが表示されます。ユーザは希望するプランを選択し、確認ボタンを押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 に送られ、構成されたミドルウェアを介してホテル請求書に追加されます。

注意事項

1. 音声 VLAN ポート作成することも、一括作成することもできます。Change Port Type 設定ボックスで、以降の変更を行うことができます。
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た VLAN タグと競合しないようにする必要があります。

155

Port Location Mapping List には、すべてのプロフィールエントリと、その VLAN ID、部屋番号/ロケーション ID、ポートタイプ、サービスゾーンなどの情報が表示されます。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ィールが消去されます。Delete All 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ィー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

	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
	100	1000		Single User	LAN1	Default	
	101	1001		Single User	LAN1	Default	
	102	1002		Single User	LAN1	Default	
	103	1003		Single User	LAN1	Default	
	104	1004		Single User	LAN1	Default	
	105	1005		Single User	LAN1	Default	
	106	1006		Single User	LAN1	Default	
	107	1007		Single User	LAN1	Default	
	108	1008		Single User	LAN1	Default	
	109	1009		Single User	LAN1	Default	
	110	1010		Single User	LAN1	Default	

12.2 PMS 構成

構成パス: Main Menu >> System >> PMS Interface

PMS Interface Configuration ページでは、管理者は、サイトのホスピタリティマネジメントシステムまたは PMS システムと互換性のあるインタフェースの種類を選択することができます。

PMS Interface Configuration

PMS Interface Type	☐ Disable ☒ Micros Opera ☐ InnKeyPMS ☐ IDS		
PMS IP Address	10.29.42.101		
PMS Port	5010		
Account Credentials	Username	RN ▼	
	Password	RN ▼	
Room Bill Description	Wireless Access		
Login Error Message	An error has occurred during login. Please contact the front desk for assistance.		
User Account Log	View		
Synchronize Data with PMS	Sync		
PMS External Page Customization API	☐ Disable ☒ Enable		
External Page Validity Verification	Username	adminkey	
	Password	adminkey	
Sample External Login Page	Download		

Micros Opera/IDS

インタフェースの種類が Micros Opera または IDS の場合は、PMS システムエンドで設定されている PMS IP およびポートを入力します。管理者は、RN(部屋番号)、GN(ゲスト名)、G#(ゲスト番号)、または G+(プロフィール名)の組合せを使用して、ユーザ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して、ユーザアカウント資格情報を定義できます。Micros Opera ユーザの詳細は、オンデマンドアカウント一覧からも監視できます。

On-Demand Account List

Delete Restore List Backup List Delete Expired Delete Out of Quota PMS Micros Opera Search							
☐	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
☐	1	16 hr(s) 9 min(s) 8 sec(s)	Expired	Group 1			
☐	pf3k	Until 2013/10/29-12:30	Expired	Group 1	roomN-100-9C:E8:E8:0B:76:8B		
☐	8krm	Until 2013/10/29-22:11	Expired	Group 1	122		
☐	gtum	Until 2013/10/29-22:11	Expired	Group 1	aaaa		
☐	6uw5	Until 2013/10/29-22:11	Expired	Group 1	111		
☐	42s7	Until 2013/10/29-22:11	Expired	Group 1	xx		
☐	qr6e	Until 2013/10/29-22:11	Expired	Group 1	aqg		

Micros Opera User List

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

インタフェース種別が Innkey PMS の場合、PMS の Query API、Post API、PMS システムの共有鍵が統合に必要です。部屋番号とゲスト番号がユーザアカウント資格情報になります。

外部ログインページの PMS API

PMS API では、管理者はカスタマイズされたログインページを使用して柔軟に実装できます。このページでは、ログイン情報、選択された請求計画、購入ユニットなどがアクセスプロセスを完了できます。また、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の PMS API は、Micros Opera および IDS インタフェースでのみ使用できます。

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、より多くの利益送信元を生み出すために、他の ISP 加入者にネットワークアクセスを提供しようとするオペレータにとって大規模な配備または提携協力のための必須の機能要件です。

EWS コントローラは、Boingo、iPass Connect など、市場の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 属性をサポートしています。

通信事業者の互換性および技術的な評価に関する詳細なサポートについては、サポート部門にお問い合わせください。

13.2 ISP ローミング用 WISPr

構成パス: Main Menu >> System >> Service Zones >> Service Zone Configuration

WISPr またはワイヤレスインターネットサービスプロバイダローミング-「Whisper」と呼ばれる、ユーザがワイヤレス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ために、携帯電話ユーザがキャリア間でローミングできるようにするのと同様の方法で Wi-Fi Alliance に提出されたプロトコルの草案です。RADIUS サーバは、サブスクライバの資格情報を認証するために使用されます。

RADIUS サーバが設定されている場合は、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	☒ Enabled ☐ Disabled		
Smart Client Black List	☐ Enabled ☒ Disabled (Separate by comma)		
WISPr Location ID	ISO Country Code		(e.g. US)
	E.164 Country Code		(e.g. 1)
	E.164 Area Code		(e.g. 408)
	Network (SSID/ZONE)		(e.g. MYWIFI)
WISPr Location Name	Hotspot Operator		(e.g. MYISP)
	Location		(e.g. Lobby_of_Airport)
WISPr Billing Time	0 : 0 (HH:MM)		

WISPr Smart Client: WISPr エージェント(iPass、Wi-Fi Skype、Boingo など)からローミングアカウントを使用する顧客にインターネットアクセスを許可する場合は、Enabled を選択します。クライアント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ように、System >> General の HTTPS で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 WISPr ローミングエージェントからのユーザを遮断してインターネットにアクセスできるようにします。たとえば、「ipassconnect」と入力すると、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: ワイヤレス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これらの属性は、クライアントデバイスの場所に基づいており、RADIUS ベンダー固有の属性(VSA)です。

WISPr Location Name: ワイヤレス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これらの属性は、クライアントデバイスの場所に基づいており、RADIUS ベンダー固有の属性(VSA)です。

WISPr Billing Time: RADIUS アカウントの課金時刻を設定します。

13.3 クロスゲートウェイローミング

構成パス: Main Menu >> Network >> Client Mobility

クロスゲートウェイローミング機能により、エンドユーザは、多数のコントローラが稼働している大規模なネットワーク構成内をシームレスに移動できます。通常、ユーザが Edge AP から別のコントローラによって管理されている別の Edge AP に移動すると、ユーザはネットワークの切断を経験し、ネットサーフィンを継続するために再ログイン手順を必要とします。

クロスゲートウェイローミングを有効にすると、エンドユーザでネットワークが中断されることはありません。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。

採用されている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 つのマスタノードが最大 15 のスレーブノードピアを持つスター型トポロジ設計です。マスタノードという用語は、単に、このノードがスター型トポロジの中心に位置することを意味します。

ロールの決定は、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ノードに設定し、別のコントローラをスレーブノードに設定します。シークレットキーと両方のコントローラの WAN インタフェースがルーティング可能であることを確認します。

スレーブノードの IP アドレスとシークレットキーを設定します。

Cross Gateway Roaming

Mode ☐ Disable ☒ Master Mode ☐ Slave Mode

Status [Node List](#)

Slave Nodes Setting	No.	Active	Remote IP Address*	Secret Key*	Remark
	1	☐			
	2	☐			
	3	☐			
	4	☐			
	5	☐			

スレーブノードのマスタノードとシークレットキーを設定します。

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両方の組み込みユーザ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、認証プロセス中に単一の中央コントローラを参照してアカウント資格情報を検索する機能を提供し、複数の支社を持つ企業に最適です。

ローカルユーザ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、次の画面で設定します。

構成パス: 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、次の画面で設定します。

構成パス: Main Menu >> Users >> Internal Authentication >> On-Demand

On-Demand Authentication

User Postfix	ondemand
Billing Plans	Configure
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	30 day(s)
Out-of-quota Account Cache	30 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 10 Days
Set Ticket's Serial Number	000020 Set
Web Printout	Configure
This will be applied to the regular printer printout when creating a single On-Demand account.	
POS Tickets	Configure
Number of Tickets ☒ 1 ☐ 2	
This will be applied to printouts from the POS ticket printer. Templates can be edited for customization.	
POS Printer	Configure
Payment Gateway	Configure
SMS Gateway	Configure
Email Verification	Configure
Account Roaming Out	☒ Enable ☐ Disable
Blacklist	None
RADIUS Client Device Settings	

RADIUS Client Device Settings

No.	Type	IP Address	Subnet Mask	Secret Key	SNMP Community
1	Roaming Out	10.30.40.45	255.255.255.255 (/32)		
2	Disable		255.255.255.255 (/32)		
3	Roaming Out		255.255.255.255 (/32)		
4	802.1X DM & CoA		255.255.255.255 (/32)		
5	Disable		255.255.255.255 (/32)		
6	Disable		255.255.255.255 (/32)		
7	Disable		255.255.255.255 (/32)		
8	Disable		255.255.255.255 (/32)		

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後、RADIUS Client Device Settings ハイパーリンクをクリックします。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。

注意事項

1. ユーザーデータベースポストフィックスが 2 つのコントローラで互いに競合しないように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

構成パス: Main Menu >> Network >> VPN

EWS コントローラは、2 つ以上の EWS コントローラが WAN ネットワークを介して互いに VPN トンネルを生成するための Site-to-Site VPN をサポートします。たとえば、2 つの EWS コントローラがある場合、VPN トンネルを作成して、1 つの EWS コントローラのサブネットに別の EWS コントローラのサブネットにアクセスさせることができます。

Site-to-Site VPN

Local Sites

Add...

Delete

☐	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Test Tunnel to Remote IP
--------------------------	-----	-------------------	-----------------	--------------------	--------------------	--------------------------

Remote Sites

Add...

Delete

☐	No.	Name	IP Address	Pre-shared Key
--------------------------	-----	------	------------	----------------

✓ Apply

✕ Cancel

最初に、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

IP Address

Authentication Method

Pre-shared Key

Phase1 Proposal

Diffie-Hellman Group

IKE Life Time

Dead Peer Detection

Remote Subnet

Pre-shared Key ▼

Encryption

AES256 ▼

Authentication

SHA-1 ▼

☐ Group 1 ☐ Group 2 ☐ Group 5

8

h ▼

(The time is a 5-digit number; e.g. 36h stands for 1 day and 12 hours)

DPD Delay

10

(second)

DPD Timeout

15

(second)

No.	Network	Mask
1		255.255.255.255 (/32) ▼
2		255.255.255.255 (/32) ▼

注意事項

1. 両方のサイトの IPsec 設定が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。EWS Controller_A の「192.168.11.0/24」>EWS Controller_B の「192.168.111.0/24」のように、トンネルが作成された後、これら 2 つのサブネット内のユーザは相互に通信できます。

The screenshot shows the 'Local Site Configuration' page. It includes the following fields and options:

- Local Interface:** WAN1 (dropdown)
- Remote VPN Gateway:** (dropdown) with buttons 'Edit Host' and 'Add a New Host'
- Local Host/Subnet:** Host (selected radio button), Subnet (radio button)
- Remote Host/Subnet:** (dropdown)
- Phase2 Proposal:**
 - Encryption:** AES256 (dropdown)
 - Authentication:** SHA-1 (dropdown)
- Key Life Time:** 24 (input) h (dropdown) (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
- Rekey:**
 - ☐ Enable Rekey
 - Rekey Margin:** 9 (input) m (dropdown) (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
- Perfect Forward Secrecy:**
 - ☒ Enable PFS
 - PFS Group:** Group 2 (dropdown)

注意事項

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することはできないため、IP セグメントマッピングを重複させることはできません。

14.2 リモートクライアント

構成パス: Main Menu >> Network >> VPN

EWS コントローラは、リモート領域からのユーザログインのためのリモート VPN をサポートします。ユーザが 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に属していることがユーザに表示されます。リモートユーザとコントローラ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、ポリシーを適用し、ユーザを制御してネットワークにアクセスすることもできます。

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	☐
Server 2	RADIUS	.	☐
Server 3	NTDOMAIN	ntdomain	☐
Server 4	LDAP	ldap	☐
Server 5	POP3	pop3	☐

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、専用の subnet、Certificate、WISPr 構成と Authentication Options を使用して構成することもできます。

リモート VPN を有効にすると、ユーザはクライアントデバイスの VPN ツールを使用して、有効な認証オプションのユーザ名とパスワードを使用して VPN リンクを設定できます。

注意事項

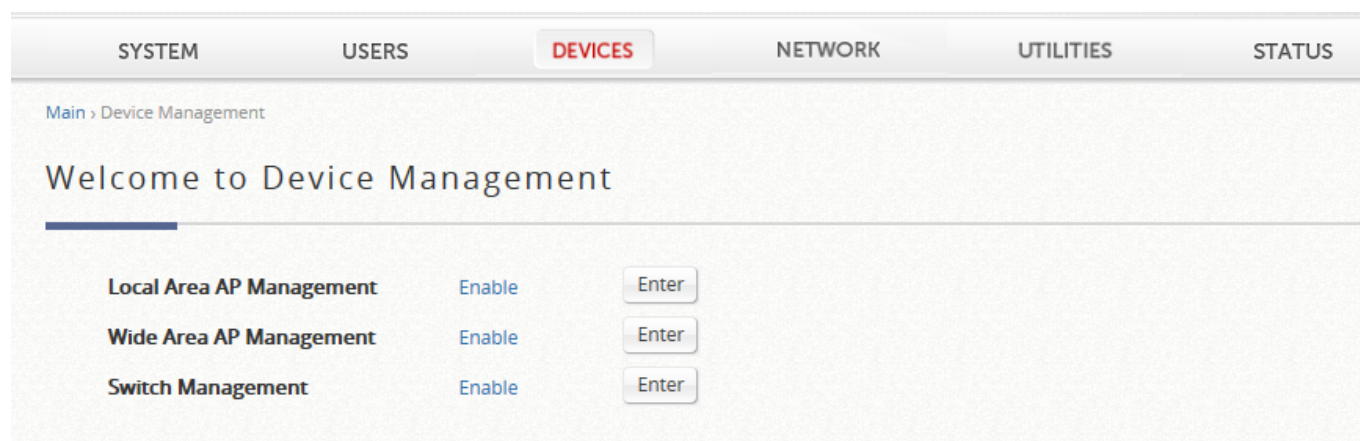
1. リモート VPN クライアントは、Main Menu >> Users >> Groups >> Configuration のページで別のユーザポリシーで適用できます。

第15章 スイッチ管理

管理者には、スイッチを管理するための包括的なインタフェースが 1 つ提供されます。

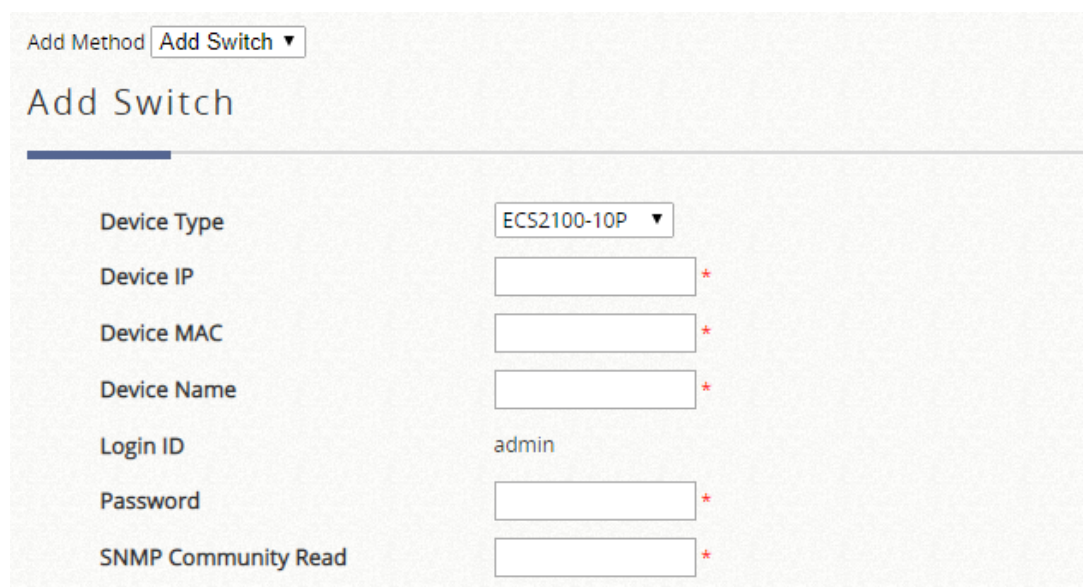
15.1 スイッチリスト

構成パス: Main Menu >> Devices >> Switch Management >> Switch List



SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Main > Device Management					
Welcome to Device Management					
Local Area AP Management		Enable	Enter		
Wide Area AP Management		Enable	Enter		
Switch Management		Enable	Enter		

EWS コントローラの WAN ポートまたは LAN ポートのいずれかに接続されているスイッチは、手動で追加することも、検出によって追加することもできます。



Add Method: Add Switch ▼

Add Switch

Device Type	ECS2100-10P ▼
Device IP	*
Device MAC	*
Device Name	*
Login ID	admin
Password	*
SNMP Community Read	*

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るようになります。

Switch List

Status

All ▼

Add

Delete

Restart

Backup

Restore

☐	Name	Type	Status	IP address	MAC address	Total allocated/Used/Max supply power [W]	Switch UI
☐	TestSW	ECS2100-10P	Offline	10.73.36.210	AA:BB:CC:DD:EE:FF	Switch Offline	Go to

スイッチリストには、スイッチ名、スイッチの種類、状態、IP アドレス、MAC アドレス、電力バジェット、およびスイッチの管理 Web インタ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

構成パス: 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源を供給するスケジュールを設定できます。この機能を使用して、AP が管理対象スイッチから PoE によって電源供給されときの AP スケジュールを制御できます。

Main > Switches > PoE Template

PoE Schedule Template

[Add template](#)

Template Name	Copy Settings From	Remark	Action
Default	NONE		

☒ Apply

☐ Cancel

テンプレートは、鉛筆アイコンをクリックして追加したり、カスタマイズしたりできます。

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
☐	Sun	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Mon	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Tue	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Wed	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Thu	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Fri	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Sat	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Apply to

Refresh Switch Name ▼

■	Port	PoE Mode	Connected Device	■	Port	PoE Mode	Connected Device
☐	1			☐	13		
☐	2			☐	14		
☐	3			☐	15		
☐	4			☐	16		
☐	5			☐	17		
☐	6			☐	18		
☐	7			☐	19		
☐	8			☐	20		
☐	9			☐	21		
☐	10			☐	22		
☐	11			☐	23		
☐	12			☐	24		

15.3 バックアップ設定

構成パス: Main Menu >> Devices >> Switch Management >> Backup Configuration

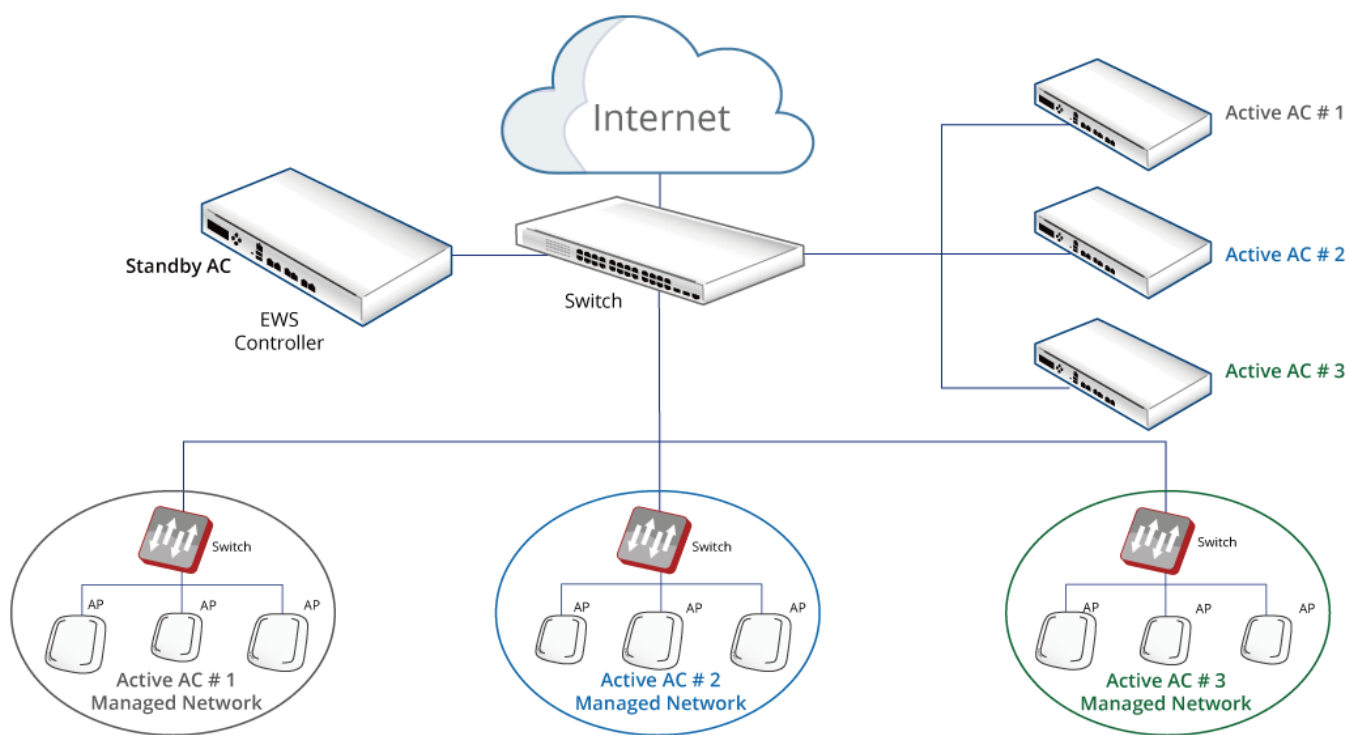
Backup Configuration には、管理対象スイッチからバックアップされた構成のリストが表示されます。スイッチを選択して Backup をクリックすると、このリストに設定を保存できます。

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)

HA の原則は、冗長性を使用して、サービス移行時の影響を最小限に抑えながら高可用性を実現することです。HA 方式では、 $N \leq 3$ の $N+1$ 冗長システムを作成するために、AC(アクセスコントローラ)間に専用のメッセージリンクが実装されます。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を処理し、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ネットワークサービスを引き継ぐ準備が整います。

構成パス: Main Menu >> System >> High Availability



機能説明

1. HA 機能はソフトウェアによって決定される機能であり、有効または無効にできます。
ソフトウェア決定イーサネットロール
 - 有効にした場合、LAN1 ポートが専用 HA ポートになります。
 - 無効にした場合、LAN1 は LAN ポートとして通常の機能を維持します。
2. Web UI は、HA 機能が有効になっているときに、この AC を Active または Standby のいずれかに指定するための構成アイテムを有します。
3. すべての HA 構成が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 ロールと、AC がダウンした後の HA ペアの復元が含まれます。

Configuration

Status	☒ Enabled ☐ Disabled
Number of Active(s)	2 ▼
Mode	☒ Active ☐ 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	☒ Enabled ☐ Disabled
Number of Active(s)	2 ▼
Mode	☐ Active ☒ 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	☐ Enabled ☒ Disabled

- HA リンクが確立されると、すべてのシステム設定、ユーザデータベース、ユーザ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 プロファイルがアクティブ AC からスタンバイ AC に同期されます。
- HA リンクが確立されたとき、スタンバイ AC によって HA リンク監視メカニズムがあります。このリンクモジュールは、アクティブの AC のステータスをチェックします。アクティブ AC が応答していない場合、このモジュールはこの AC がサービスを提供していないと見なし、ネットワークサービスを引き継ぎます。
- 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。ローカル管理 AP に関連付けられたクライアントは、サービスの切り替え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はほとんどまたはまったく発生しません)になります。
- トンネルが確立された L3 デバイス上のワイドエリアネットワーク管理対象 AP(手動または CAPWAP 経由)は、完全な AP 管理容量でのサービス切り替え後、最大 5 分(概算)以内にサービスを再開できます。
- HA ステータス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、電子メールは、サービスを提供するために置き換えられたときに新しいアクティブ AC によって送信されます。また、HA がすでに有効になっているときにスタンバイ AC が検出されないと、アクティブ AC からスタンバイ AC がダウンしたという内容の電子メールが送信されます。
- HA 機能は、同じブランドと同じ 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。

16.2 Wi-Fi モニタ(EWS5203、EWS5204、EWS5207)

Wi-Fi モニタを使用すると、管理者は、仮想領域または実際の管理対象 AP の信号カバレッジであるアクセスポイントの Wi-Fi 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 ステータスと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、初期インストール段階での計画、パフォーマンスの向上、および既存の展開での管理対象 AP の監視を行えるように設計されています。

フロアプランには、仮想、ローカル、およびワイドの 3 種類があります。

16.2.1 フロアプランの追加

Wi-Fi モニタは、管理者が AP を配置する場所を決定し、最初のインストール時に AP の数がスループット要件を満たすかどうかを判断できるように設計されています。まず、.jpg 形式の地図またはフロアプランと、.xml または.osm 形式で描画されたパーティションが必要です。

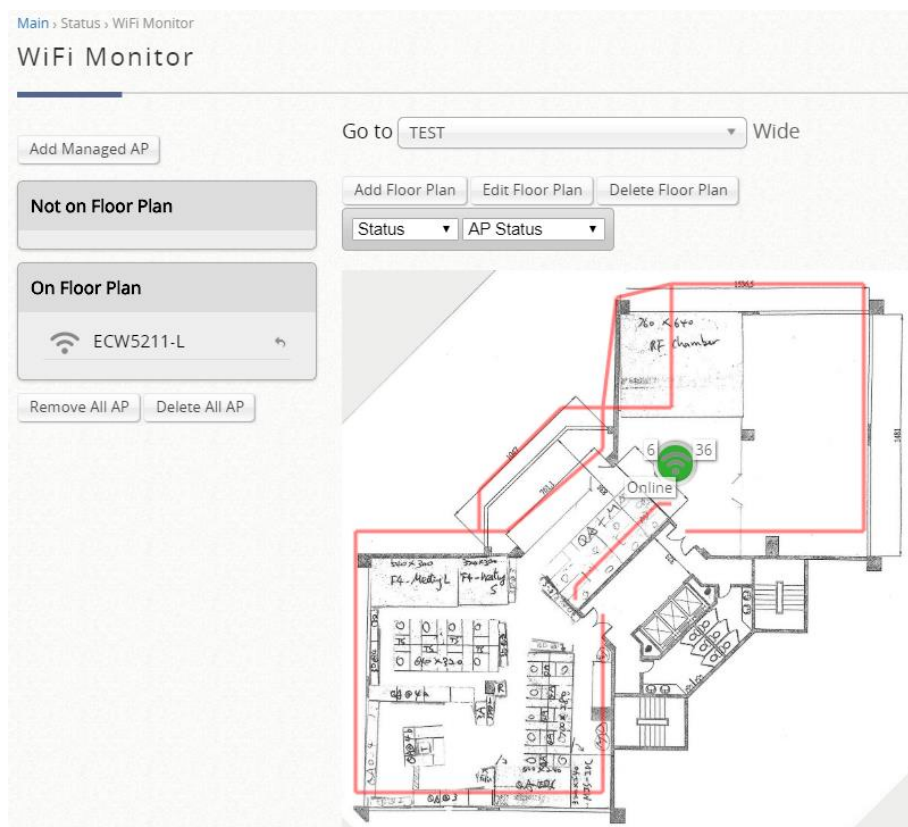
The screenshot displays the 'WiFi Monitor' section of a web application. The top navigation bar includes 'SYSTEM', 'USERS', 'DEVICES', 'NETWORK', 'UTILITIES', and 'STATUS'. The left sidebar lists various monitoring tools, with 'WiFi Monitor' currently selected. The main content area shows the 'Add Floor Plan' form, which includes fields for 'Floor Plan Type' (set to 'Local'), 'Floor Plan Name' ('WiFi Monitor Testing'), 'Floor Plan (.jpg)' (selected file: 'House-Design...lans-011.jpg'), 'Wall (.xml)' (selected file: 'floor.xml'), 'Map Width (m)' (79), 'Map Length (m)' (79), 'Country Code' (USA), and 'Height of Receiving Device (m)' (1). A preview of a floor plan is shown on the right, with a note indicating the original size is twice the displayed sample. The form has 'Apply' and 'Cancel' buttons at the bottom.

Managed AP Simulation は、場所に基づいたアクセスポイントの監視に使用されます。管理対象 AP シミュレーションフロアプランの 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)。

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、IP アドレス、MAC アドレス、関連するクライアント番号などの実際の AP 情報が表示されます。これにより、管理者は AP のロケーションに関する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アンドドロップします。信号強度は 2.4GHz が青色、5GHz が赤色(両帯域が重なっている場合は紫色)で表示されます。



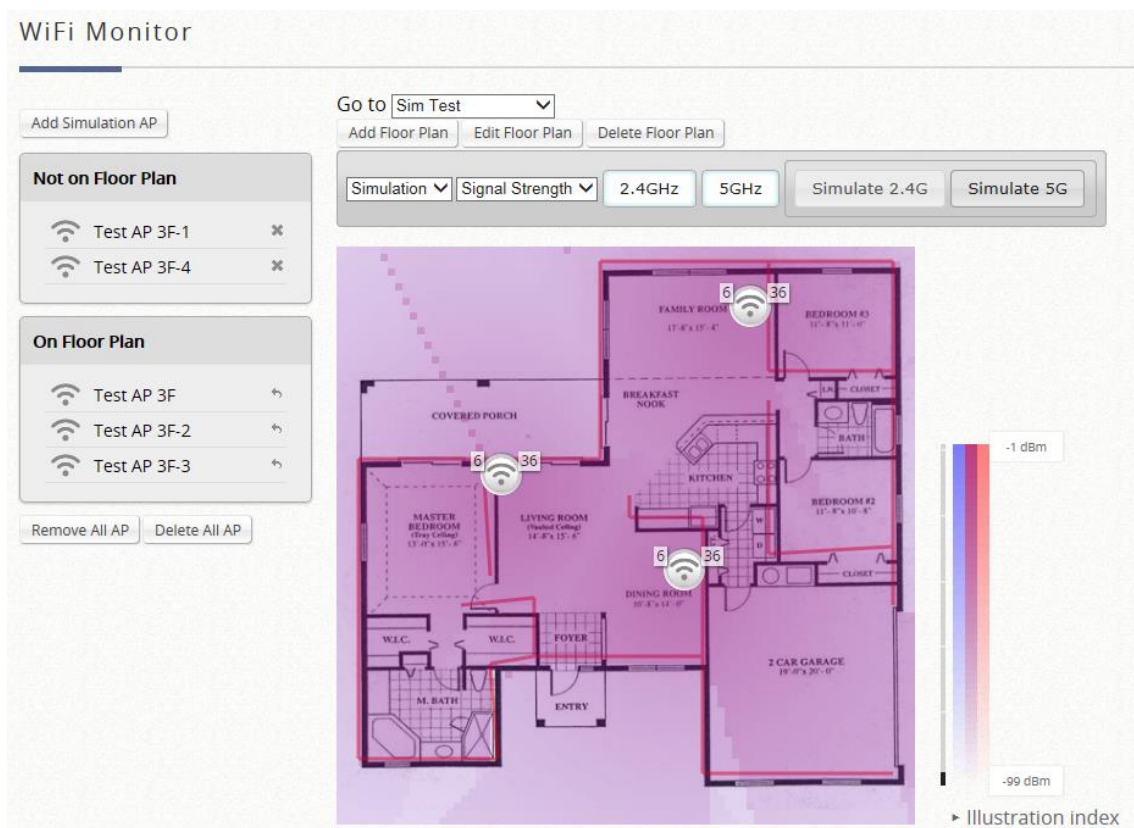
管理対象 AP の信号強度とカバレージは、AP モデル、送信電力、AP の高さなどの要因に依存します。



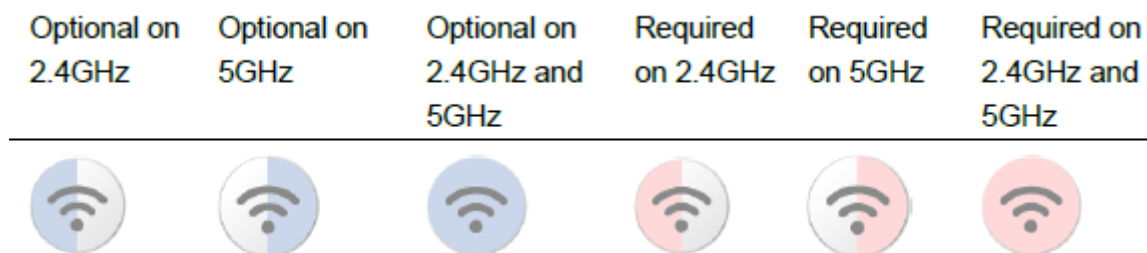
16.2.2 シミュレーション AP

Wi-Fi モニタは、AP をシミュレートし、フロアプランに配置して、最適化で関連付けられた設定を確認できます。一方、シミュレーション AP の信号強度とカバレージは、AP モデル、送信電力、AP の高さなどの要因に依存します。

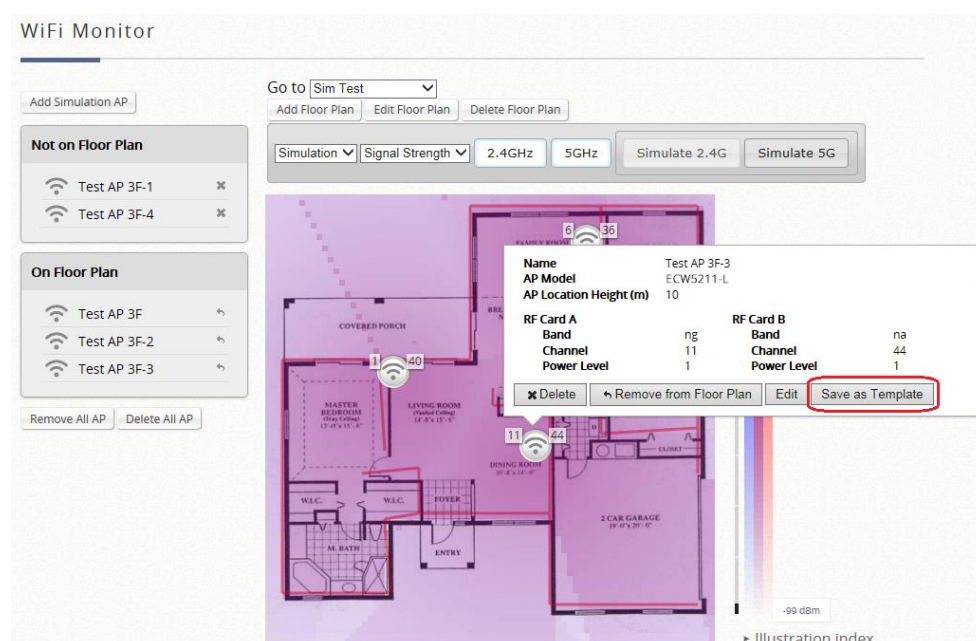
フロアプランとパーティションを配置した状態で、シミュレーション用のフロアプランにシミュレーション AP を追加できます。



Simulate 2.4G または Simulate 5G を選択して、構成された AP が必要に応じて適切かどうかを確認します。



シミュレーションが正常に終了すると、推奨される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。



構成は、AP 管理に使用するテンプレートに簡単に保存できます。

16.2.3 フloorプランでの AP 監視

運用 AP があるエリアでは、管理者は作成されたフロアプランから AP ステータスを表示できます。

AP ステータスには、オンライン、オフライン、または無効が表示されます。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 アイドルおよびメモリ使用量を取得できます。

WiFi Monitor

Go to: TEST

Add Managed AP

Not on Floor Plan

On Floor Plan

ECW5211-L

Remove All AP Delete All AP

Add Floor Plan Edit Floor Plan

Status AP Status

Name ECW5211-L
AP Model ECW5211-L
AP Location Height (m) 5
IP 10.73.7.38
MAC 00:1F:D4:06:F1:1D
AP State Online
Client Num 0

RF Card A
Band ng
Channel 6
Power Level 1

RF Card B
Band ac
Channel 36
Power Level 1

Delete Remove from Floor Plan Refresh

AP 密度や AP 平均トラフィックなどの AP 統計情報、および AP 平均トラフィックも、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にサポートされます。

WiFi Monitor

Go to: TEST

Add Managed AP

Not on Floor Plan

On Floor Plan

ECW5211-L

Remove All AP Delete All AP

Add Floor Plan Edit Floor Plan

Statistics Device Density

Name ECW5211-L
AP Model ECW5211-L
AP Location Height (m) 5
IP 10.73.7.38
MAC 00:1F:D4:06:F1:1D
AP State Online
Client Num 0

RF Card A
Band ng
Channel 6
Power Level 1

RF Card B
Band ac
Channel 36
Power Level 1

Delete Remove from Floor Plan Refresh

付録A EWS モデルとインストール

EWS コントローラのキャパシティテーブル

容量	EWS100	EWS101	EWS5203	EWS5204	EWS5207
フォームファクタ	7.5" デスクトップ	7.5" デスクトップ	19"(1U)	19"(1U)	19"(2U)
WAN	(1 または 2)*1 × GbE	1 × GbE	2 × GbE または 2 × 1G SFP	2 × GbE 2 × 1G SFP	2 × GbE、 2 × 10Gb SFP+
LAN	(4 または 3)*1 × GbE	4 × GbE	8 × GbE	6 × GbE 2 × 1G SFP	6 × GbE、 2x10Gb SFP+
ローカルアカウント	2000	2000	10000	30000	50000
オンデマンド アカウント	2000	2000	10000	30000	50000
管理対象 AP キャパシティ (ローカルとワイドの 組み合わせ)	10	50	300	1000	3000
最大同時ユーザ	100	400	3000	10000	30000
管理可能な AP モデル	OAP100 EAP100 ECW100 ECW5210-L ECW5211-L ECW5410-L ECWO5210-L ECWO5211-L ECWO5212-L ECWO5213-L				
監視対象 AP	100	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+8	デフォルト+32	デフォルト+64
ユーザグループ	8	8	16	24	24
ユーザポリシー	グローバル+12	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: さまざまな設置シナリオのためのイーサネットポート割り当てオプション

*テーブルの内容は、予告なしに変更されることがあります。

ハードウェアの概要

EWS100 ハードウェア

1	ボタン	リセット: 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 のステータスが点滅を始め、この段階でボタンを放してシステムを再起動します。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 のステータスが点滅から消灯に変わります。この段階で解放すると、システムが初期設定にリセットされます。 電源: このボタンはシステムの主電源のオン/オフです。
2	LED ディスプレイ	電源: 電源がオンになると、電源 LED が緑色に点灯します。 ステータス: 点滅は、システム OS が起動中であることを示します。システムが動作可能な状態になると、LED が常時点灯します。
3	WAN1 (オプションの WAN2)	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(10/100/1000Base-T RJ45)。構成可能な WAN2 オプション。
4	LAN1~LAN4	クライアントマシンまたはスイッチは、LAN ポート(10/100/1000Base-T RJ45)を介して EWS コントローラに接続します。
5	USB	将来の使用のために予約されています。

EWS101 ハードウェア

1	リセット/再起動 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 のステータスが点滅を始め、この段階でボタンを放してシステムを再起動します。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 のステータスが点滅から消灯に変わります。この段階で解放すると、システムが初期設定にリセットされます。
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 のハイパーターミナルなどのターミナル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フェースにログインし、管理者パスワードの変更やシステムステータスの監視などを行うことができます。
3	LAN1~LAN4	クライアントマシンまたはスイッチは、LAN ポート(10/100/1000Base-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(10/100/1000Base-T RJ45)。
5	USB	将来の使用のために予約されています。
6	LED ディスプレイ	電源: 電源がオンになると、電源 LED が緑色に点灯します。 ステータス: 点滅は、システム OS が起動中であることを示します。システムが動作可能な状態になると、LED が常時点灯します。

EWS5203 ハードウェア

1	リセット/再起動ボタン	リセットボタンを約 5 秒間押し続けると、システムを再起動する前にフロントパネルの LED のステータスが点滅を始めます。 リセットボタンを 10 秒以上長押しすると、前面パネルの LED のステータスが点滅を速め、システムがデフォルト設定にリセットされます。
2	USB	将来の使用のために予約されています。
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(10/100/1000Base-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 のハイパーターミナルなどのターミナル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フェースにログインし、管理者パスワードの変更やシステムステータスの監視などを行うことができます。
6	LED インジケータ	電源: 電源がオンになると、電源 LED が緑色に点灯します。 ステータス: 点滅は、システム OS が起動中であることを示します。システムが動作可能な状態になると、LED が常時点灯します。
7	LAN1～LAN8	LANトラフィックをサービスするための 8 つのギガビット LAN ポート(10/100/1000Base-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フェース、SZ 構成などの重要な設定を確認できます。左から右へのナビゲーションボタンは、それぞれ「Esc」、「Up」、「Down」、および「Enter」です。
2	LED インジケータ	システムのステータスを示すために、電源と HDD(ハードディスク)の 2 つの LED インジケータがあります。
3	再起動ボタン	再起動ボタンを約 5 秒間押し続けると、システムが再起動します。
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 のハイパーターミナルなどのターミナル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フェースにログインし、管理者パスワードの変更やシステムステータスの監視などを行うことができます。
5	USB	将来の使用のために予約されています。
6	WAN1/WAN2 (RJ45)	2 つの WAN ポート(10/100/1000Base-T RJ45)が、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(10/100/1000Base-T RJ45)を介して EWS コントローラに接続します。
8	WAN1/WAN2 (SFP)	2 つのコンボ WAN ポート(SFP)が、ISP(インターネットサービスプロバイダ)からの 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	ERR(Power Error): PSU ステータスが正常の場合はオフ、いずれかの電源に障害が発生した場合はオレンジ色に点灯します。 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、オレンジ色のライトが常に点灯します。 HDD(Hard Disk): データ転送中でない場合は消灯、HDD の読み取り/書き込み中は緑色に点滅します。 PWR(Power): 電源オン時に緑色のライトが点灯します。
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フェース、SZ 構成などの重要な設定を確認できます。左から右へのナビゲーションボタンは、それぞれ「Esc」、「Up」、「Down」、および「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 のハイパーターミナルなどのターミナル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フェースにログインし、管理者パスワードの変更やシステムステータスの監視などを行うことができます。
4	USB	将来の使用のために予約されています。
5	MGMT ポート	管理者が EWS コントローラを管理する場合。
6	再起動ボタン	再起動ボタンを約 5 秒間押し続けると、システムが再起動します。
7	WAN1/WAN2 (SFP+)	2 つの WAN ポート(10G SFP+)が、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(10/100/1000Base-T RJ45)が、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(10/100/1000Base-T RJ45)を介して EWS コントローラに接続します。

インストール手順

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. フロントパネルと背面パネルを確認し、「ハードウェアと仕様」の項に記載されている各コントロールとネットワークインタフェースを確認します。
3. RJ-45 コネクタを備えたイーサネットケーブルを用意します。
4. Web Management インタ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、CABLE 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。プロバイダから提供された DNS サーバアドレスを収集します。

設置

- 1) 電源アダプターまたは電源コードを背面パネルの電源ソケットに接続します。正常に接続されていることを示すために、電源 LED が点灯している必要があります。
- 2) フロントパネルの 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他端を、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。適切な接続を示すために、このポートの LED が点灯している必要があります。
- 3) フロントパネルの LAN 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他端を管理者用パソコンに接続し、システムを構成します。本機の LAN ポートに複数の機器を接続するために LAN スイッチを使っても構いません。

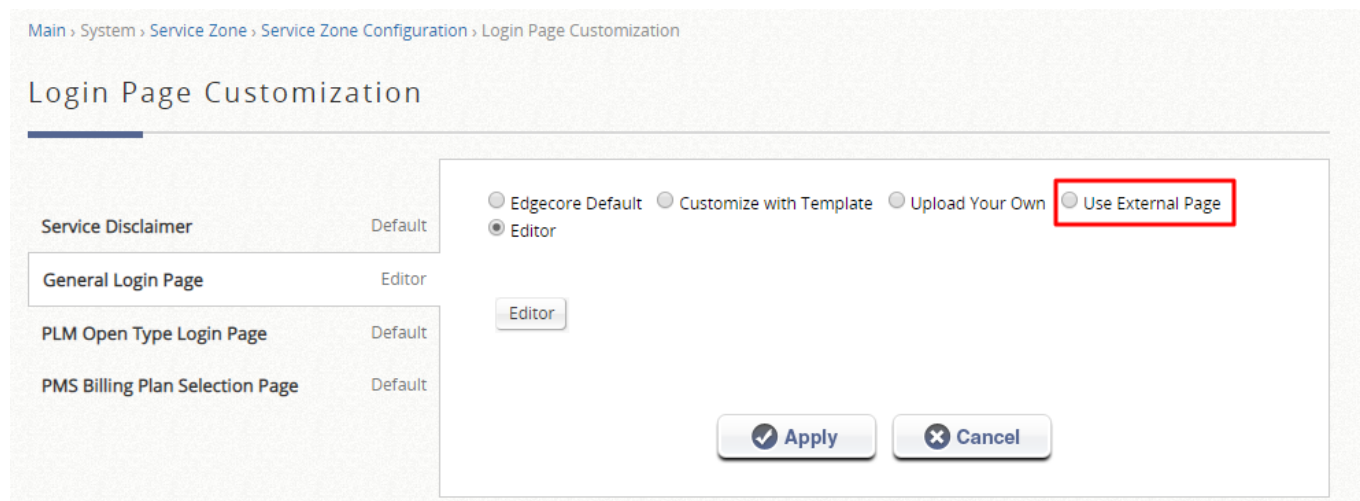
注意事項

1. 最高のパフォーマンスを保証するために、他のサプライヤの部品を使わず、パッケージ内のすべてのサプライ品を使用することを強くお勧めします。
-

付録B 外部ページ

外部ページ概念

カスタムページに外部Webページを使用する場合は、External Pageを選択します。外部WebページのURLを入力し、Previewボタンをクリックして、外部Webページが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確認してから、Applyボタンをクリックします。



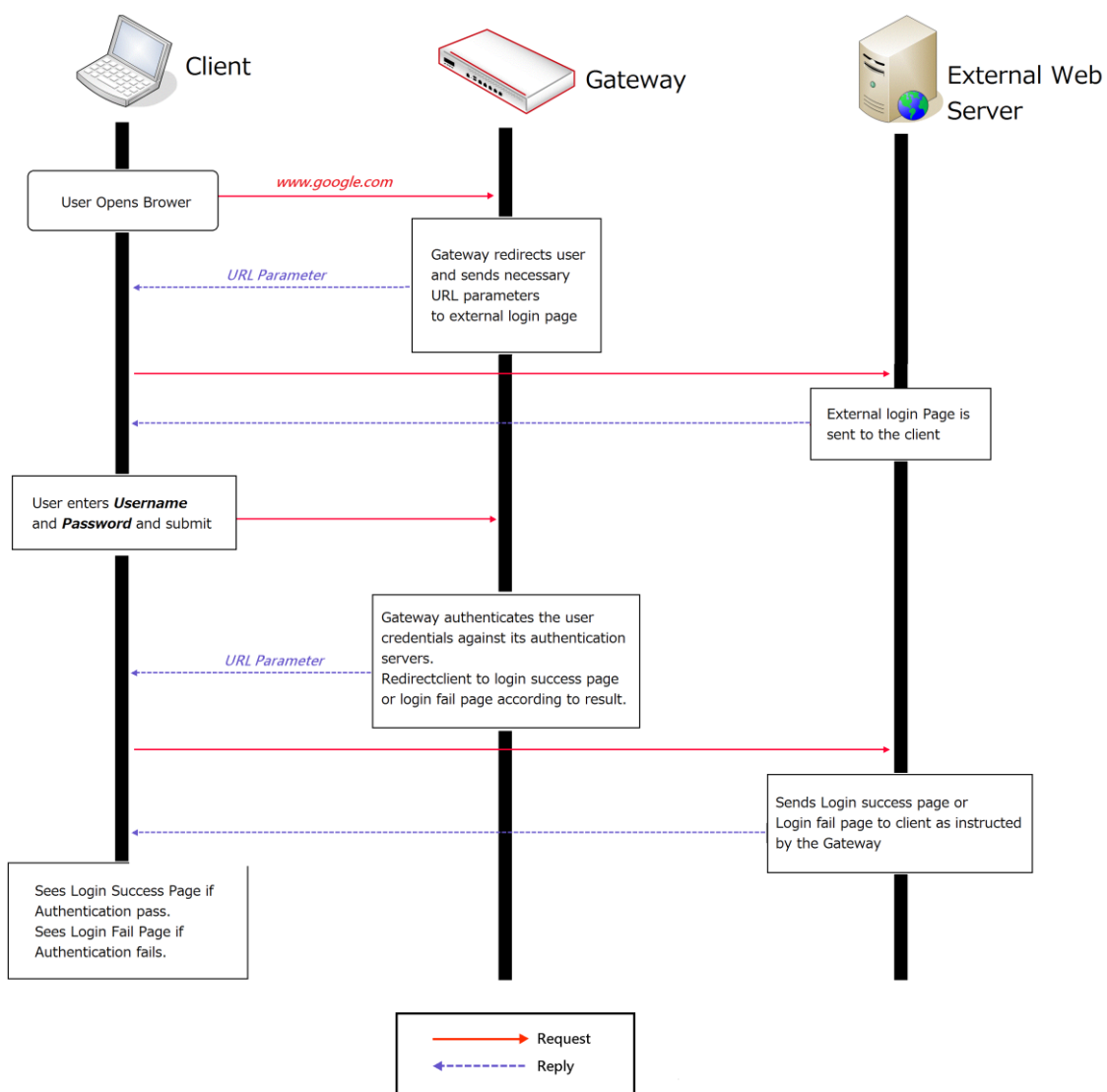
Main Menu>System>Service Zone>Service Zone Configuration>Login Page

ユーザがこのサービスゾーンに接続し、Webブラウザを開き、インターネットアクセスを試みると、設定された外部ログインページへのユーザに対処します。ゲートウェイは、外部Webページへのユーザをアドレッシングしながら、ユーザ認証など、動作に必要なURLパラメータも送信します。したがって、各自己定義の外部ページ(ログイン、ログアウト、ログイン成功、ログアウト成功など)では、ゲートウェイとの間で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次に示します。Login Success Page...など、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。

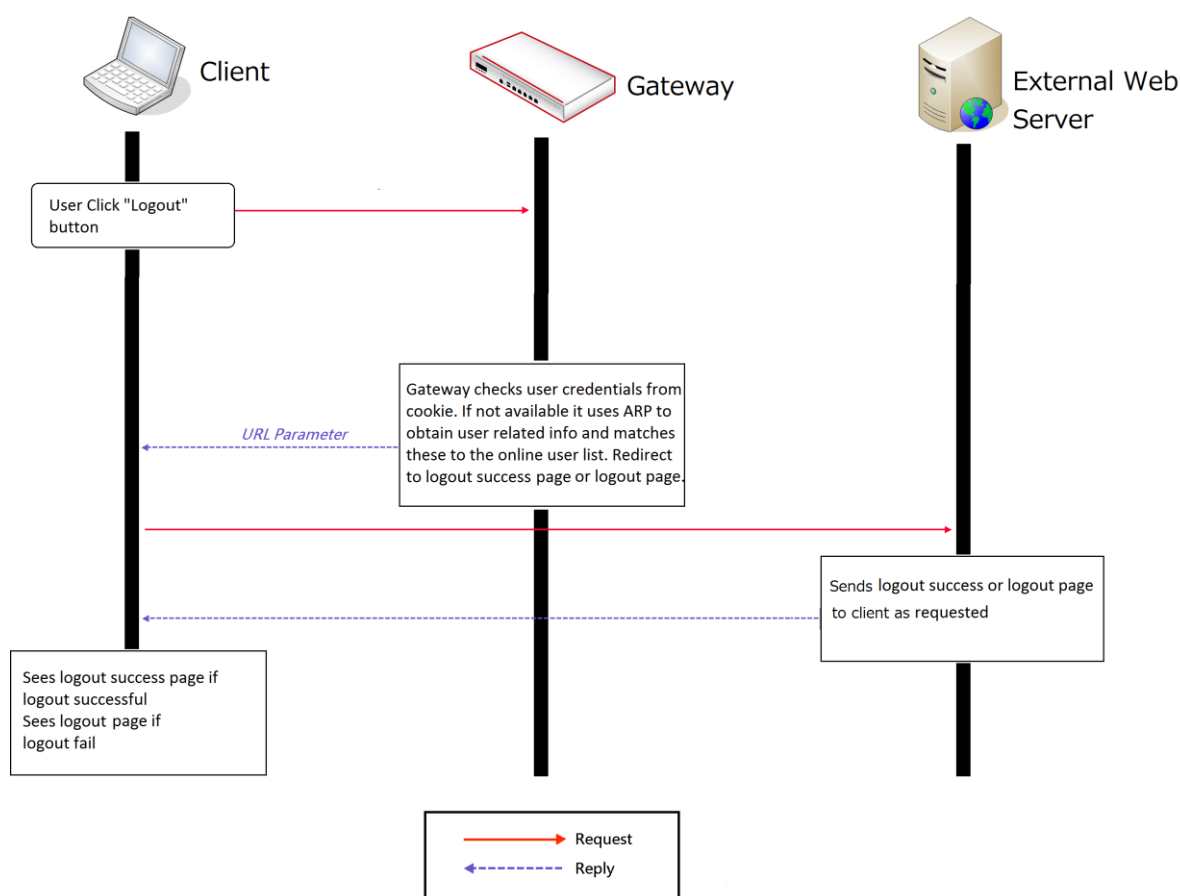
したがって、外部ページは、URLパラメータの利用について十分な知識を持つユーザが設計することが重要です。

次の概略図は、ユーザログイン/ログアウトフローを使用した外部ページの動作を示しています。

ログイン:



ログアウト:



ゲートウェイによって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	ストリング(URL エンコード)	ユーザがログインしたときに送信される URL
remainingurl	ストリング(URL エンコード)	ユーザが残りのクォータを取得する場合に送信される URL
vlanid	整数(1~4094)	VLAN ID
iface	整数(0~8)	サービスゾーン ID、デフォルトサービスゾーンの場合は 0
gwip	IP フォーマット	ゲートウェイがアクティブ化された WAN IP アドレス
gwmac	MAC フォーマット(“:”で区切る)	ゲートウェイがアクティブ化された WAN MAC アドレス
client_ip	IP フォーマット	クライアント IP アドレス
ipv6_addr	IPv6 フォーマット	クライアント IPv6 アドレス
umac	MAC フォーマット(“:”で区切る)	クライアント MAC アドレス
session	ストリング	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、URL が含まれます。

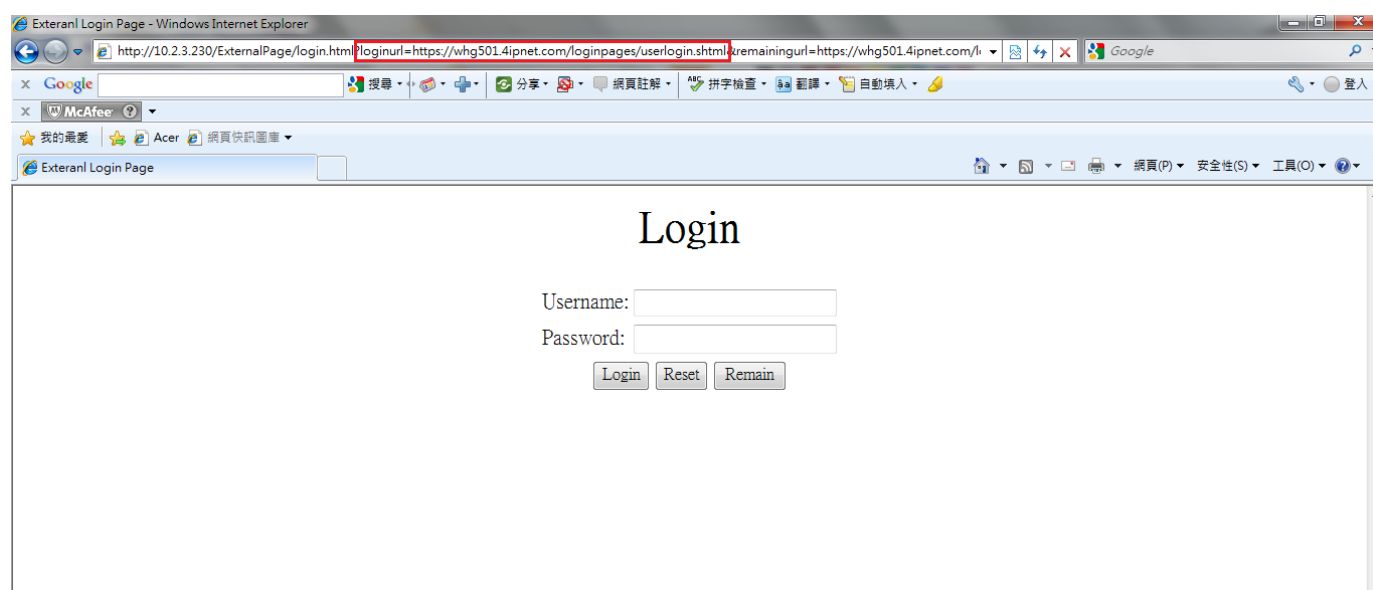
html コードで必要なパラメータを解析する必要があります。以下の HTML コードセグメントは、自己定義 JavaScript 関数を使用した loginurl パラメータの解析例です。

```
<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される、対応する自己定義 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]); }
}
```

ブラウザ起動時にユーザに表示される外部ページサンプルを示します。下図に赤色で強調表示された部分がシステムから送信された URL パラメータです。



外部ページ設計変数

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。
自分でデザインしたユーザを正しく機能させるためには、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	ストリング(URL エンコード)	ユーザがログインしたときに送信される URL。
remainingurl	ストリング(URL エンコード)	ユーザが残りのクォータを取得する場合に送信される URL。
vlanid	整数(1～4094)	VLAN ID
iface	整数(0～8)	サービスゾーン ID、デフォルトサービスゾーンの場合は 0
gwip	IP フォーマット	ゲートウェイがアクティブ化された WAN IP アドレス
gwmac	MAC フォーマット(“:”で区切る)	ゲートウェイがアクティブ化された WAN MAC アドレス
client_ip	IP フォーマット	クライアント IP アドレス
ipv6_addr	IPv6 フォーマット	クライアント IPv6 アドレス
umac	MAC フォーマット(“:”で区切る)	クライアント MAC アドレス
nat_ip	IP フォーマット	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	ストリング	ユーザ ID(ポストフィックスを含みます)
original_uid	ストリング	元のユーザ番号
utype	ストリング(LOCAL、RADIUS、ONDEMAND、POP3、LDAP、SIP、NT ドメイン)	認証サーバの名前
umac	MAC フォーマット(“:”で区切る)	クライアント MAC アドレス
sessionlength	整数(秒)	RADIUS ユーザセッションの長さ(RADIUS ユーザでのみ使用可能)
byteamount	整数(バイト)	RADIUS ユーザの音量制限(RADIUS ユーザでのみ使用可能)
idletimeout	整数(秒)	アイドルタイムアウト
acct-interim-interval	整数(秒)	RADIUS アカウンティングの中間アップデートインターバル(RADIUS ユーザでのみ使用可能)
logouturl	ストリング(URL エンコード)	ユーザがログアウトするときに送信される URL。
change_passwd_url	ストリング(URL エンコード)	ユーザがパスワードの変更を希望する場合に送信される URL。(ローカルユーザでのみ使用可能)
ondemand_creation_url	ストリング(URL エンコード)	ユーザがオンデマンドユーザを作成する場合に送信される URL。(ローカルユーザでのみ使用可能)
vlanid	整数(1～4094)	VLAN ID
gwip	IP フォーマット	ゲートウェイがアクティブ化された WAN IP アドレス
client_ip	IP フォーマット	クライアント IP アドレス

ipv6_addr	IPv6 フォーマット	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	グループ索引
Policy	整数	ポリシーインデックス
available_plan	課金プラン: 使用量、課金プラン: 使用量、	ローカルユーザがオンデマンドユーザを作成する場合
max_uplink	整数(b/s)	最大アップリンク速度
max_downlink	整数(b/s)	最大ダウンリンク速度
req_uplink	整数(b/s)	最小アップリンク速度
req_downlink	整数(b/s)	最小ダウンリンク速度
next_page	ストリング	クライアントから URL へのリード
CLASS	ストリング	DURAIS CLASS 属性(RADIUS ユーザでのみ使用可能)
WISPR-REDIRECTION-URL	ストリング	クライアントから URL へのリード
WISPR-SESSION-TERMINATE-TIME	ストリング、フォーマット: YYYY-MM-DDThh:mm:ssTZD	WISPr Session-Terminate-Time アトリビュート(RADIUS ユーザでのみ使用可能)
WISPR-SESSION-TERMINATE-END-OF-DAY	整数(0/1)	WISPr Session-Terminate-End-Of-Day 属性。終了ルールを示す 0 または 1。(RADIUS ユーザでのみ使用可能)
WISPR-BILLING-CLASS-OF-SERVICE	ストリング	WISPr Billing-Class-Of-Service アトリビュート(RADIUS ユーザでのみ使用可能)
WISPR-LOCATION-ID	ストリング	WISPr Location-ID アトリビュート (RADIUS ユーザでのみ使用可能)
WISPR-LOCATION-NAME	ストリング	WISPr Location-Name アトリビュート (RADIUS ユーザでのみ使用可能)
WISPR-BILLING-TIME	ストリング、フォーマット: HH:MM	WISPr Billing-Time アトリビュート (RADIUS ユーザでのみ使用可能)
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 フォーマット	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	ストリング	カスタマイズ・パラメーター

3. 外部エラーページ

変数:

フィールド	値	説明
msg	文字列、以下を含む。 システムがビジー状態です。後ほどやり直して下さい。 セッション関連情報が見つかりません。
よろしくお願いします。 ブラウザ設定で Cookie を有効にするか、Web サイトを開いて Cookie を取得します。 IP アドレスが不正です。IP アドレスを確認し、もう一度試してください。 MAC アドレスが不正です。MAC アドレスを確認し、もう一度試してください。 すみません。認証オプションが現在無効になっているため、アカウントを使用できません。
よろしくお願いします。ネットワーク管理者に問い合わせてください。 すみません。認証オプション(postfix に関連付けられています)が見つからないため、アカウントを使用できません。
ネットワーク管理者に問い合わせてください。 残念ながら、アカウントは現在ブラックリストに登録されているため、ログインすることはできません。 残念ながら、ログインは許可されていません。なぜなら、これは現在、あなたのアカウントのサービス時間ではないからです。 すでにログインしています。 申し訳ありませんが、あなたのアカウント(XXX)の情報をチェックしているシステム上の問題があります。
よろしくお願いします。 ネットワーク管理者に問い合わせてください。 無効なユーザー名またはパスワードです。
ユーザー名とパスワードを確認して、もう一度試してください。 考慮のポリシーを特定できません。
ネットワーク管理者にお問い合わせください。 このデバイスのユーザ(MAC アドレス)は、このアカウントを使用することができません。
ネットワーク管理者に問い合わせてください。 残念ながら、外部認証サーバは現在到達不能です。
ネットワーク管理者に問い合わせてください。 残念ながら、リモート VPN 接続を作成することはできません。 radius サーバからの応答メッセージ (radius 属性: Reply-Message)	エラーメッセージ
loginurl	ストリング(URL エンコード)	ユーザログイン時に送信される URL。

remainingurl	ストリング(URL エンコード)	ユーザが残りのクォータを取得する場合に送信される URL。
vlanid	整数(1~4094)	VLAN ID
iface	整数	サービスゾーン ID、デフォルトサービスゾーンの場合は 0
client_ip	IP フォーマット	クライアント IP アドレス
gwip	IP フォーマット	ゲートウェイがアクティブ化した IP アドレス
ipv6_addr	IPv6 フォーマット	クライアント IPv6 アドレス
umac	MAC フォーマット(“:”で区切る)	クライアント MAC アドレス
original_uid	ストリング	元のユーザ番号
nat_ip	IP フォーマット	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	ストリング	カスタマイズ・パラメーター

4. 外部ログアウト成功ページ

変数:

フィールド	値	説明
uid	ストリング	ユーザ ID(ポストフィックスを含みます)
original_uid	ストリング	元のユーザ番号
vlanid	整数(1~4094)	VLAN ID
gwip	IP フォーマット	ゲートウェイがアクティブ化した IP アドレス
used_time	整数	ユーザの使用時間

5. External On-Demand/Guest login successful ページ

変数:

フィールド	値	説明
uid	ストリング	ユーザ ID(ポストフィックスを含みます)
original_uid	ストリング	元のユーザ番号
utype	ストリング(LOCAL、RADIUS、ONDEMAND、POP3、LDAP、SIP、NTドメイン)	認証サーバの名前
umac	MAC フォーマット(“:”で区切る)	クライアント MAC アドレス
sessionlength	整数(秒)	オンデマンドユーザの時間割当て制限
byteamount	整数(バイト)	オンデマンドユーザのボリュームタイプのクォータ
chargetype	ストリング	ユーザ会計種別
idletimeout	整数(秒)	アイドルタイムアウト
logouturl	ストリング(URL エンコード)	ログアウト URL
redeemurl	ストリング(URL エンコード)	Redeem URL
vlanid	整数(1~4094)	VLAN ID
gwip	IP フォーマット	ゲートウェイがアクティブ化された WAN IP アドレス
client_ip	IP フォーマット	クライアント IP アドレス
ipv6_addr	IPv6 フォーマット	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	グループ索引
Policy	整数	ポリシーインデックス
next_page	ストリング	クライアントから URL へのリード
max_uplink	整数(b/s)	最大アップリンク速度
max_downlink	整数(b/s)	最大ダウンリンク速度
req_uplink	整数(b/s)	最小アップリンク速度
req_downlink	整数(b/s)	最小ダウンリンク速度

nat_ip	IP フォーマット	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	ストリング	ユーザ識別
gwip	IP フォーマット	ゲートウェイがアクティブ化された WAN IP アドレス
vlanid	整数(1~4094)	VLAN ID

外部ページ設計変数

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て表示します。いくつかは必須です。デザイナー参照にも宛先パスが指定されます。

1. ユーザログイン

パス:

(LAN IP address or Internal Domain Name) /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	ストリング	ユーザ識別
mypassword 代替変数 (passwd, Password, Pass)	必須	ストリング	ユーザパスワード
session	オプション	ストリング	コード化されたストリングは、このセッションの何らかのインフォメーションを含み、デフォルトは Cookie から取り出されます。

出力:

出力されず、ログイン成功画面にユーザを返します。

2. ユーザログアウト

パス:

(LAN IP address or Internal Domain Name) /loginpages/logoff.shtml

入力:

フィールド	必須	値	説明
uid	オプション	ストリング	ユーザ ID、デフォルトは Cookie から取得されます。

出力:

ログアウトに失敗しました。ログアウトに成功したページにユーザを返します。

3. 残りクォータ(クレジット残高)

パス:

(LAN IP address or Internal Domain Name)/loginpages/user_change_password.shtml

入力:

フィールド	必須	値	説明
myusername 代替変数: (Username, user, account)	必須	ストリング	ユーザ名称
mypassword 代替変数 (passwd, Password, Pass)	必須	ストリング	パスワード
ret_url	オプション	ストリング(URL エンコード)	返される URL。デフォルトは pop_reminder.shtml
command	オプション	ストリング	getValue: command が "getValue" に設定されている場合、返される URL は無視され、ページは使用可能なクォータのみを出力します。

出力:

"getValue" に設定すると、単に "value" となります。(ユーザの種類に応じた秒数またはバイト数)

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 ページへ案内され、UI スタイルの残りのクォータを表示します。ret_url が指定された場合、クライアントは ret_url に返され、ゲートウェイはこれらの 4 つの変数を URL に追加します。

フィールド	値	説明
msg	ストリング(以下を含みます): 残りのクォータ: XXX バイト 残高: XXXXXX 申し訳ありませんが、この機能はオンデマンドユーザでのみ使用できます。 申し訳ありませんが、このアカウントまたはパスワードは間違っています。 申し訳ありませんが、このアカウントはクォータ外です。 申し訳ありませんが、このアカウントは期限切れです。 申し訳ありませんが、このアカウントは解約されています。	結果およびエラーメッセージ
value	整数(秒またはバイト) またはエラー番号 -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: 期限切れです。 -4: 償還済み。	残りのクォータ。ユーザが time タイプの場合、値は残りの秒数、ユーザが volume タイプの場合、残りのバイト数です。
uname	ストリング	ユーザ名称

Type	文字列、以下を含む。 TIME: 時刻型 DATA: ボリュームタイプ CUTOFF: カットオフタイプ	オンデマンドユーザの請求の種類
------	---	-----------------

4. パスワードの変更

パス:

(LAN IP address or Internal Domain Name)/loginpages/user_change_password.shtml
--

入力:

フィールド	必須	値	説明
SAVE	必須	1 (1 にする必要があります)	
opw	必須	ストリング	古いパスワード
npw	必須	ストリング	新しいパスワード
npwc	必須	ストリング	確認済みの新しいパスワード
ret_url	必須	ストリング(URL エンコード)	URL を返します

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の変更結果を示す ret_url に結果を追加します。

フィールド	値	説明
Result	ストリング(以下を含みます): パスワードを正常に変更します ユーザの暗証番号が間違っています パスワードフォーマットが不正です。	結果およびエラーメッセージ

5. Redeem(オンデマンドユーザ)

パス:

(LAN IP address or Internal Domain Name) /loginpages/redeemuserlogin.shtml
--

入力:

フィールド	必須	値	説明
Username	オプション	ストリング	カレントユーザ ID(表示されない場合、Cookie に格納されているユーザ名がデフォルト)
upassword	オプション	ストリング	現行のユーザパスワード(表示されない場合、Cookie に保存されているパスワードがデフォルト値になります)
myusername	必須	ストリング	償還ユーザ番号
mypassword	必須	ストリング	ユーザパスワードを引き換えます
ret_url	オプション	ストリング(URL エンコード)	URL を返します。ログインに成功したページはデフォルトです。

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表示され、結果が表示されます。ret_url が指定された場合、クライアントは ret_url に返され、ゲートウェイは redeem プロシージャの結果を示す変数 rmsg を追加します。

フィールド	値	説明
rmsg	ストリング(以下を含みます): Redeem 処理が完了しました。 元のユーザ名が見つかりません。 償還ユーザの名前は、データベースから見つけることができません。 元のユーザの暗証番号が間違っています。 ユーザパスワードの使用が間違っています。 元のユーザタイプとオンデマンドユーザタイプが一致しません。 元のユーザがログインしていません。 すでにログインしているユーザを使用します。 以前に引き換えられたことがあります。 ユーザがクォータを使い果たしました。 最大許容時間を超えました。 最大許容メモリ容量を超えました。 間違ったポストフィックスをチェックしてください。 このアカウントは期限切れです。	結果およびエラーメッセージ

付録C 便利なマネジメント&バリュエーションツール

便利な管理ツール

HP、IBM、CA、BMC のビッグスイートを置き換える堅実な仕事をしている、オープンソース IT 管理製品の上位 6 製品は、次のとおりです。それぞれ、低価格のプロフェッショナルサービスと無料のソフトウェア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によって異なります。

QUEST BIG BROTHER

この Web ベースのシステムとネットワークモニタは、ほとんどの Windows、Unix、Linux OS をサポートしています。また、ユーザ提供スクリプトのリポジトリにより、Big Brother をネットワークに簡単にカスタマイズすることができます。その GUI は、一般的に理解されているカラーコードを特徴とし、赤は不良を意味し、緑は良好を意味します。

GROUNDWORK MONITOR PROFESSIONAL

2004 年に発売された、初めての企業規模のオープンソースマネジメント製品の 1 つです。Nagios、Apache、NMap など 100 以上のベストオブブリード方式のオープンソースプロジェクトを、Web ベースのインタフェースなどの機能を追加した 1 つの枠組みに統合します。Monitor Professional は、Linux、Unix、Windows サーバ、アプリ、データベース、ネットワークボックスなど、企業ネットワークの一元管理と監視を提供します。

HYPERIC HQ ENTERPRISE

[データセンタ](#)を目指して、ハイパリックのソフトウェアは、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すべての層の Web インフラストラクチャを管理・監視するために構築されています。また、トレンド分析も提供します。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、サービスポーリング、データ収集、およびイベントと通知の管理に焦点を当てています。現在、Linux、Mandrake、Solaris、および Mac OS X を含むさまざま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。Windows のサポートは OpenNMS2.0 用に計画されています。

OPENQRM

また、OpenQRM は、データセンター管理をターゲットにして、数千ものリナックスおよびウィンドウズサーバを管理し、データセンターの使用量と使用率を追跡できます。また、自動的なポリシーベースのプロビジョニングも行います。また、Nagios を統合して監視することもできます。

ZENOSS CORE

主にパイソンで書かれたこの管理プラットフォームは、イベント管理と、サーバ、ネットワークデバイス、OS 及びアプリケーションの利用可能性及びパフォーマンス監視とを提供します。ゼノスは Linux、FreeBSD、Mac OS X で運営されており、ウィンドウズで VM プレーヤーと Zenoss Virtual Appliance を搭載します。

評価ツール

Wireshark (パケットキャプチャおよびデバッグ解析用)

Wireshark は、世界最先端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で実行されているトラフィックをキャプチャしてインタラクティブに参照できます。これは、多くの業界や教育機関におけるデファクト(多くの場合、デジュール)標準です。

Wireshark の発展は、世界中のネットワーク専門家の貢献によって成長します。これは 1998 年に開始されたプロジェクトの継続です。

<http://www.wireshark.org/>

inSSIDer (ワイヤレススキャン&周波数アナライザ用)

inSSIDer は、近くの AP 信号および深度周波数について電波をスキャンするための有益なツールであり、設置場所のチャンネル分析です。

次のことができます。

- Wi-Fi および周辺のネットワークを点検します
- 近くにある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します
- 競合するアクセスポイントおよび詰まっている Wi-Fi チャンネルのトラブルシューティング
- Wi-Fi が集中している地域の接続先を反転表示
- 時間経過に伴う受信信号の強度を dBm 単位で追跡します
- MAC アドレス、SSID、チャンネル、RSSI、最終表示時刻で結果を並べ替えます
- Wi-Fi と GPS データを Google Earth の KML ファイルにエクスポート

<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には、主に次の 4 つのタイプがあります。

- **使用時間** （クォータの購入：使用可能時間）
- **ボリューム** （クォータの購入：使用可能なトラフィック量）

プリペイドコンセプト。使用中はクォータだけが差し引かれます。アカウントは、クォータが使い果たされたとき、またはアカウントの有効期限に達したときに期限切れになります。

- **ホテルの遮断** （有効なアカウントのインターバルを購入）
- **Duration-time** （有効なアカウントのインターバルを購入）

使用する時間間隔を定義します。カウントダウンは、アカウントが有効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

- ユーザは、残りのクォータが有効で、一定期間内に購入したアカウントを有効にする必要があるアカウントな限り、ログインしてインターネットにアクセスできます。
- Usage-time アカウントには、選択するオプションがあります。

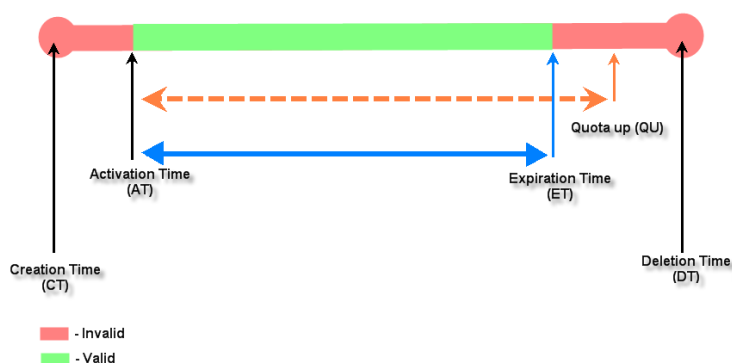
□ 有効期限あり

- ・ 最初のログインの直後にカウントダウンが開始されます。有効期限が切れるのは、Valid Period が使用されているか、クォータが使い果たされた場合です。

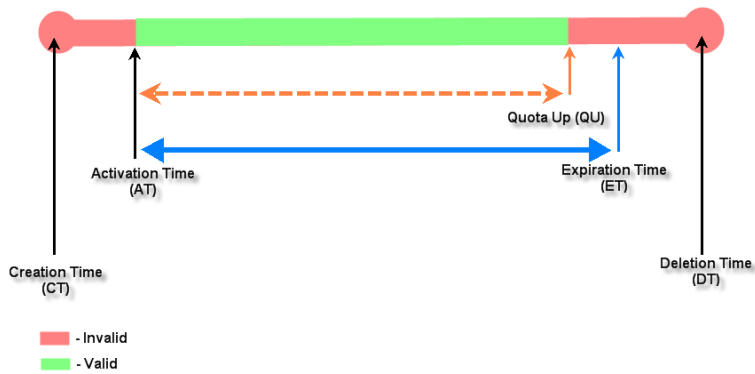
□ 有効期限なし

- ・ アカウントの有効期限は、クォータが使い果たされた場合にのみ切れます。

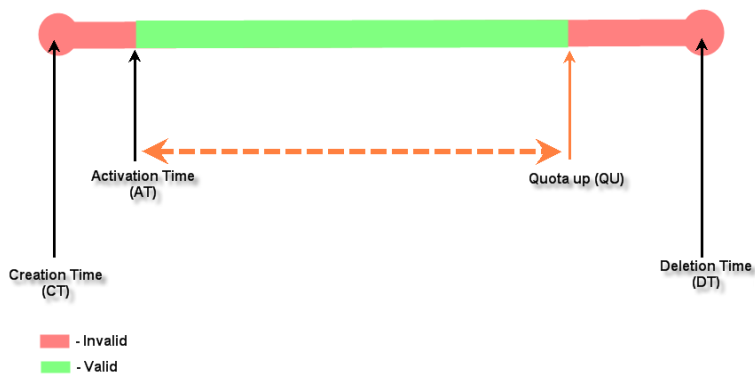
Usage-time account lifespan



Usage-time account lifespan



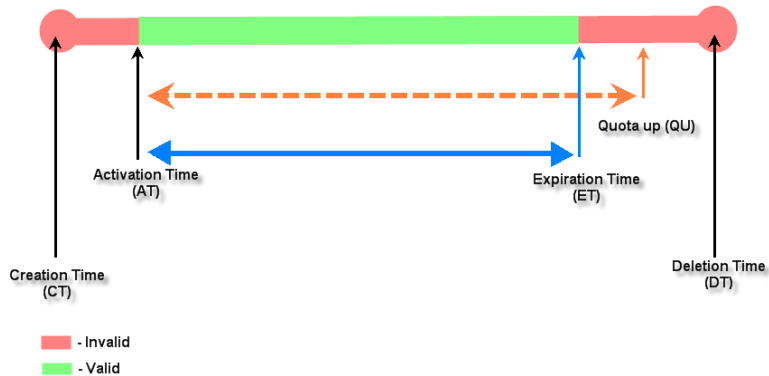
Usage-time account lifespan

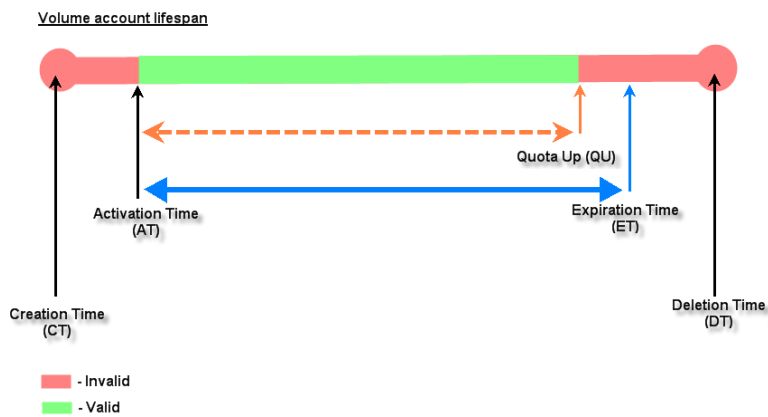


ボリューム

- ユーザは、アカウントが有効で、残りのクォータがあり、購入したアカウントを一定期間内に有効にする必要がある限り、ログインしてインターネットにアクセスできます。
- 有効期限が切れるのは、Valid Period が使用されているか、クォータが使い果たされた場合です。

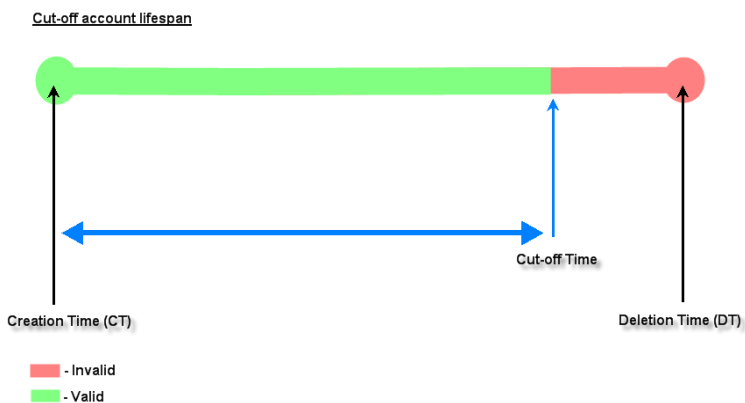
Volume account lifespan

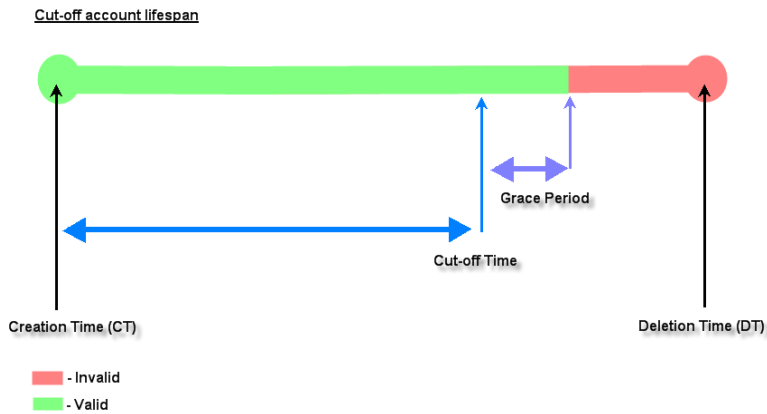




ホテル・カットオフ・タイム

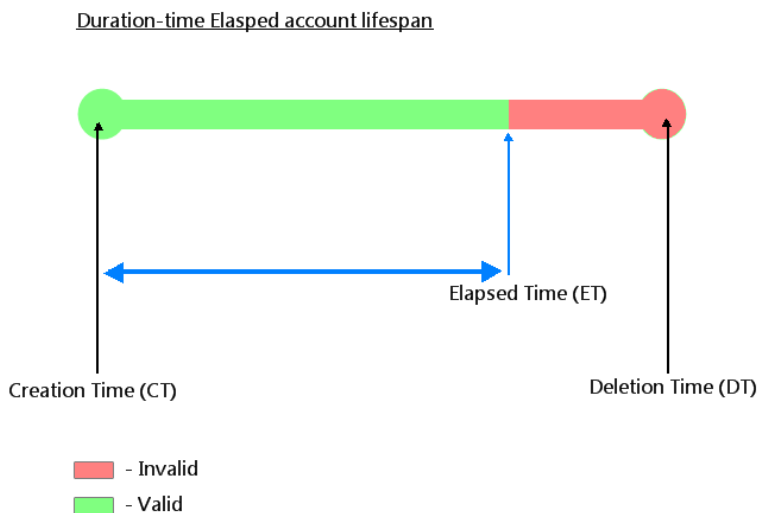
- オペレータは、アカウントの有効期限が切れる時刻を設定できます。
- アカウントは、作成時に自動的にアクティブ化されます。
- ユニットは、"Cut-off"を実行する日数です。たとえば、Unit=2days、Cut-off Time=10:00 の場合、アカウントは作成後 2 日後の 10:00AM に期限切れになります。
- 猶予期間が付与されていない限り、カットオフ時間に達すると無効になるアカウントのユーザビリティ。
- 主に、ゲストの滞在時間に応じたインターネットサービスを提供するホテルの会場で使用されます。



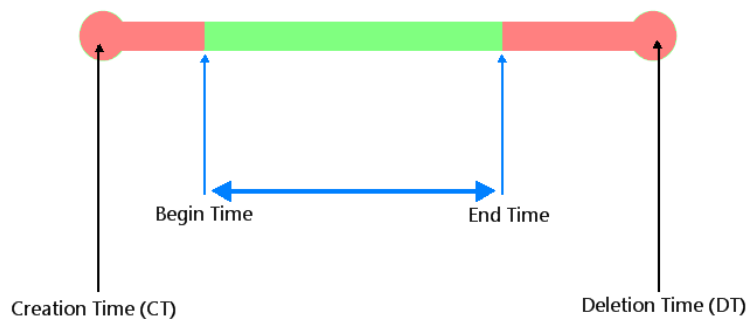


継続時間

- ユーザは、アカウントが有効な期間内であれば、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になると開始され、有効期限に達すると期限切れになります。
- 継続時間アカウントは、さらに次のように分類することができます。
 - 経過時間
 - ・ アクティブ化時間(アカウントの作成時間)を基準にした値。アカウントは、有効期限に達すると期限切れになります。
 - 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、終了時刻に達すると期限切れになります。
 - カットオフ時間
 - ・ 作成日内にクロック時間を明示的に Cut-off に定義します。



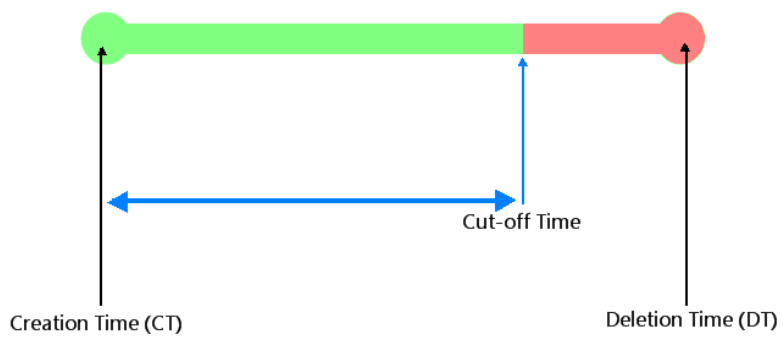
Duration-time Begin-End Account lifespan



Invalid

Valid

Duration-time Cut-off account lifespan



Invalid

Valid

注意事項

- 10 の請求プランしかないのですが、同じタイプですがさまざまな割当量を有するアカウントを作成したい場合、これは Unit フィールドを介して達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.

+ Create

✕ Cancel

ネットワークオペレータは、クォータに Unit フィールドの 1~9 の整数を掛けることができます。使用時間、ボリューム、および継続時間・経過時間のアカウントタイプのみが、1 つのアカウントに対して複数のユニットクォータ生成をサポートしていることに注意してください。



Welcome! SN:xxxxxx

Username	xxxx@ondemand
Password	xxxxxxxxxx
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!

付録E UI 参照インデックス

I. ダッシュボード

システムの全般設定、ネットワークインタフェース、オンラインユーザなど、管理者が一目で知っておく必要があるシステム関連の重要な情報を表示します。このページのインフォメーション更新速度を選択するためのドロップダウンメニューがあります。

右上隅の "Download" ボタンは、システムステータス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" を編集して、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、必要な情報のみを表示するようにカスタマイズできます。



II. セットアップウィザード

このウィザードでは、迅速なセットアップ手順を提供します。それぞれのステップに従って、システム管理者パスワードを変更します。タイムゾーンを選択し、WAN1 インタフェースを設定して、ローカルユーザアカウントを作成します。セットアップ手順が完了したら、設定を有効にするためにシステムを再起動する必要があります。最小限の構成で再起動すると、システムは動作可能な状態になります。

The screenshot displays the first step of a four-step setup wizard. The progress bar at the top shows '1 FIRST STEP Change Password' as the active step, followed by '2 SECOND STEP Configure WAN1', '3 THIRD STEP Create A Local User', and '4 YOU'RE DONE Restart the System'. On the left, 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 fields: 'New Password' and 'Verify Password', both masked with black dots and marked with a red asterisk, and a 'Time Zone' dropdown menu currently set to '(GMT+08:00)Taipei'. At the bottom right, there are 'Exit' and 'Next' buttons.

1 FIRST STEP
Change Password

2 SECOND STEP
Configure WAN1

3 THIRD STEP
Create A Local User

4 YOU'RE DONE
Restart the System

It is recommended to change administrator's password and select an appropriate time zone for the system.

General

New Password: [Masked] *

Verify Password: [Masked] *

Time Zone: (GMT+08:00)Taipei

Exit Next

A. System

システム: 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

General Settings

System Name	EWS101
Contact Information	
	When there is a warning of "Please contact your network administrator"
HTTPS Certificate	Default CERT
User HTTPS Login	☐ Enable ☒ Disable
	☐ Secure
HTTPS Automatic Redirect	☒ Allow ☐ Block ☐ Bypass
	Allow HTTPS Automatic Redirect with Certification Security Alert
Internal Domain Name	☒ Use the name on SSL certificate
	mknhhi.example.com
Portal URL Exceptions (User Agent)	IEMobile/7.0,XBLWP7
	(e.g. IEMobile/7.0,XBLWP7, separate by comma)
User Log Access	Enter IP Address Here
UAM Filter	Configure
Management IP Address	Configure
SNMP	☒ Enable ☐ Disable
	Configure
Suspend Warning Message	Sorry! The service is suspended. *
NMS Setting	Configure

System Time

Current Time	2019/06/25 17:26:12
Time Zone	(GMT+08:00)Taipei
Time Update	☒ NTP ☐ Manually set up
	NTP Server 1: time.nist.gov
	NTP Server 2: ntp1.fau.de
	NTP Server 3: clock.cuhk.edu.hk
	NTP Server 4: ntps1.pads.ufrj.br
	NTP Server 5: ntp1.cs.mu.OZ.AU
	☐ Use this controller as an NTP server

- **System Name:** これは、コントローラに指定できるニーモニック名です。設定されると、Web ブラウザのフレームに表示されます。

- **Contact Information:** インターネット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、携帯電話などの連絡先です。
- **HTTPS Certificate:** お客様独自のネットワーク証明書を、サイトセーフティペリファイアとしてここで選択することができます。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:** 暗号化されたコンテンツ転送のために HTTPS で認証されたエンドユーザを許可するオプションが表示されます。Secure オプションは、High 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ための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、証明書セキュリティの警告が表示される場合があります。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。このオプションは、ユーザのデバイスに表示されるすべてのセキュリティ警告を効果的に防止します。HTTPS 要求がタイムアウトすると、一部のブラウザでは自動的に HTTP Web ページがキャプティブポータルにリダイレクトされます。
 - **Enable HTTPS Automatic Redirect:** ユーザが HTTPS を使ってキャプティブポータルにアクセスする前にブラウズすると、証明書セキュリティ警告が表示される場合があります。
 - **Block HTTPS Automatic Redirect:** ユーザが HTTPS を使ってブラウズするとタイムアウトし、宛先には到達しないため、Web ページは空白で表示されます。
 - **Bypass non-HTTP Traffic Prior to Sign-In:** すべての HTTPS Web サイトは、ユーザが免責事項ページを受け入れていないか、キャプティブポータルでサインイン処理を完了していても、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ネーム(FQDN)。LAN インタフェースの IP アドレスを記憶するのではなく、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が LAN IP アドレスの代わりに Login Success 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は、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により、ログインに成功したクライアントがログイン成功ページにリダイレクトされます。
- **Portal URL Exceptions (User Agent):** ユーザの初回ログイン後に、ここにリストされている特定の開いているブラウザを除いて、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:** 設定が完了すると、入力した IP からのみユーザログにアクセスできます。
- **UAM Filter:** Universal Access Method (UAM) フィルタは、ユーザエージェントからの非ブラウザ HTTP 要求を認証前にドロップして、過剰なトラフィックからシステム過負荷を防止します。
- **Management IP Address List:** この設定により、ネットワーク管理者は、Web Management インタフェースの表示を許可されている予約済み 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 プロトコルによるシステム情報の取得を有効または無効にするためのオプションが表示されます。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を選択できます。CPU 使用率、メモリー使用率、DHCP スコープ、ハートビート周期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停止されたときに、管理者がユーザするメッセージを入力するためのフィールド。
- **Time:** 外部 NTP サーバを指定して、手動のシステム時刻設定オプションまたは自動時間同期を行います。
 - **Current Time:** 以下の設定に従い、直ちにシステム時刻を返します。
 - **Time Zone:** ドロップダウンリストで、システムが存在するローカルタイムゾーンを選択します。
 - **Time Update (NTP):** NTP サーバ 1~5 の順序で外部 NTP サーバを指定することで、自動的に時間同期を完了します。Use this controller チェックボックスは、管理対象 AP の時刻を同期するためにデフォルトでオンになっています。
 - **Time Update (Manually Set Up):** システム時刻は手動で設定します。

Management Service

SSH Service ☒ Enable ☐ Disable
Telnet Service ☒ Enable ☐ Disable

Management Service Zone List

Active	Status	Service Zone	IP Address/Segment
☒	☒	Default	192.168.1.254/255.255.0.0
☒	☒	SZ1	10.1.1.254/255.255.0.0
☐	☒	SZ2	10.2.1.254/255.255.0.0
☐	☐	SZ3	10.3.1.254/255.255.0.0
☐	☐	SZ4	10.4.1.254/255.255.0.0
☐	☐	SZ5	10.5.1.254/255.255.0.0
☐	☐	SZ6	10.6.1.254/255.255.0.0
☐	☒	SZ7	10.7.1.254/255.255.0.0
☐	☐	SZ8	10.8.1.254/255.255.0.0

Management IP Address List

No.	Active	IP Address/Segment
1	☒	0.0.0.0/0.0.0.0
2	☒	10.71.1.1/255.255.0.0
3	☐	
4	☐	

- **Management Service:** リモートコンソールマネジメントインタフェースを有効または無効にするためのオプションです。
 - **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フェース。セキュリティ上の理由から、悪意のあるユーザがシステムにアクセスしないように無効にすることをお勧めします。ただし、Edgecore サポートチームがリモートでトラブルシューティングを行う必要がある場合は、事前にサポートを有効にしてください。
 - **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フェース。セキュリティのために、悪意のあるユーザがシステムにアクセスしないように、Telnet サービスはデフォルトで無効になっています。
- **Management Service Zone List:** System>Service Zone、第 2.4 章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、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、アクティブ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/セグメントをカスタマイズして、管理者がシステムの WMI にアクセスするようにできます。チェックボックスにチェックを入れて、テーブル内のエントリがアクティブであることを確認してください。たとえば、192.168.3.1 と 192.168.1.0/24 と入力すると、192.168.3.1 のデバイスと 192.168.1.0～192.168.1.255 のデバイスのみが Web マネジメントインタフェースに到達できます。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 と入力します)

2) WAN

WAN1 Configuration

Physical Mode: Auto

Interface Type: ☒ Static (Use the following IP settings)

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

Alternate DNS Server:

☐ Dynamic (IP settings assigned automatically)

☐ PPPoE

☐ PPTP

- **Physical Mode:** ドロップダウンリストを使用して、管理者は WAN コネクションのスピードとデュプレックスを選択できます。オートネゴシエーションを ON にすると、インタフェースに接続されているデバイスとシステムの両方がサポートする最高性能の伝送モード(速度/デュプレックス/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:** アップストリームネットワークで DHCP サーバが使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 を選択します。
- **PPPoE:** ISP が提供する PPPoE ダイアルアップ接続用であり、設定を完了するために、ISP はパスワードを使用してアカウントを発行します。
- **PPTP:** 一部の IPS(ヨーロッパ諸国)では、ダイアルアップ接続に PPTP プロトコルが提供されている場合があります。PPTP サーバ用に発行された PPTP アカウントと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。
 - **Ether Port:** 銅線イーサネット WAN ポートを保守用にデプロイします。
 - **Fiber Port:** 保守用の SFP ファイバーポートをデプロイします。
 - **Fiber Port and Ether Port:** ブリッジファイバポートとイーサネットポート。SFP ポートまたはイーサポートのいずれかを介してアップリンクは物理的には 1 ポートのみを接続します。
 - **Bonding:** 保守用に SFP ポートと銅線イーサネットポートの両方をデプロイします。このオプションにより、2 つの接続が集約され、集約されたスループットが向上します。

WAN2 Configuration

Physical Mode: 100Mb/s Half

Interface Type: ☐ None

☐ Static (Use the following IP settings)

☒ Dynamic (IP settings assigned automatically) Renew

☒ Obtain DNS server address automatically.

Preferred DNS Server: 168.95.1.1

Alternate DNS Server:

☐ PPPoE

- **Physical Mode:** ドロップダウンリストを使用して、管理者は WAN コネクションのスピードとデブプレックスを選択できます。オートネゴシエーションを ON にすると、インタフェースに接続されているデバイスとシステムの両方がサポートする最高性能の伝送モード(速度/デブプレックス/フロー制御)を選択します。
- **None:** WAN2 インタフェー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:** アップストリームネットワークで DHCP サーバが使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 を選択します。
- **PPPoE:** ISP が提供する PPPoE ダイアルアップ接続用であり、設定を完了するために、ISP はパスワードを使用して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。
 - **Ether Port:** 銅線イーサネット WAN ポートを保守用にデプロイします。
 - **Fiber Port:** 保守用の SFP ファイバーポートをデプロイします。
 - **Fiber Port and Ether Port:** ブリッジファイバポートとイーサネットポート。物理的には、SFP ポートまたはイーサポートのいずれかを介して 1 つのアップリンクのみを接続します。
 - **Bonding:** 保守用に SFP ポートと銅線イーサネットポートの両方をデプロイします。これにより、2 つの接続がオプション集約され、集約されたスループットが向上します。

WAN Traffic Settings

Bandwidth Limitation

Function of WAN2

Target for Detecting Internet Connection

☒ Enable Bandwidth Limitation on WAN

Max Uplink Bandwidth Kbps

Max Downlink Bandwidth Kbps

☒ 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

☒ 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になっています。この制限は、WAN1 および WAN2 の両方について組み合わせられますが、一方、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:** WAN2 が有効になっている場合にのみ、次の機能が実行されます。
 - **Disable:** WAN2 は、ロードバランシングおよび 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機能します。
 - **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 WAN1 および WAN2 ポート全体にシステムトラフィックを分散するオプションを選択します。
 - **WAN Failover:** WAN1 が停止している場合に、WAN1 によって最初に処理されたトラフィックを処理する WAN2 のオプションを選択します。ネストされたオプションが選択されている場合、再びアップリンクになると、WAN1 に戻ります。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稼働中か停止中かを確認するための検知対象として、最大 3 つの送信側サイトを指定します。警告メッセージテキストのフィールドは、3 つのターゲットがすべて応答しないことを検出した場合にユーザの Web ブラウザに表示されるようにカスタマイズすることができます。

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 go6 transition

- **Status:** 選択した WAN インタフェースで IPv6 サポートを有効または無効にします。
- **Interface:** IPv6 アドレスで設定する機器の外部インタフェースを選択します。
- **Type:** IPv6 方式のいずれかを選択します。
 - **Static:** 関連するすべての IPv6 情報を手動で入力します。赤色のアスタリスクは必須フィールドです。入手したインターネットパッケージに ISP が発行した固定 IPv6 アドレスが含まれていれば理想的です。
 - **6to4:** 6to4 は、IPv4 から IPv6 へ移行するためのインターネット移行メカニズムであり、明示的なトンネルを構成する必要なく IPv6 パケットが IPv4 ネットワーク(一般に IPv4 インターネット)を介して送信されることを可能にするシステムです。6to4 オプションは、選択した WAN インタフェースがスタティック IPv4 アドレスで設定されている場合にのみ選択できます。

4) LAN Ports

デフォルトでは、システムの"Service Zone"には、組織内の有線およびワイヤレスのサービスエリアが含まれています。このページでは、サービスゾーンマッピングを識別するためのオプションを提供します。

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

Default

LAN1

Default

LAN2

SZ1

LAN3

SZ1

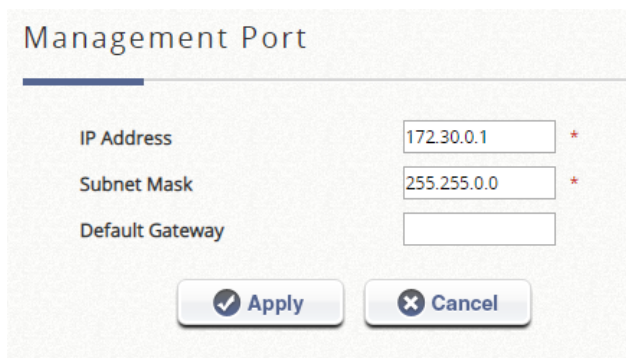
LAN4

- **LAN Port Mode:** ポートおよびサービスゾーンマッピングを識別するための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数は、コントローラの 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 ポートにかかわらず、VLAN ID によって異なるサービスゾーンが識別されます。つまり、タグベースのモードは、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:** Port-based モードが選択されている場合に、有効になっているサービスゾーン別の物理 LAN ポートの構成。

5) MGMT Port

(EWS5207 で使用可能)



The image shows a 'Management Port' configuration window. It has a title bar with the text 'Management Port'. Below the title bar, there are 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 input field has a red asterisk to its right. At the bottom of the window, there are two buttons: 'Apply' with a checkmark icon and 'Cancel' with an 'X' icon.

Management Port	
IP Address	172.30.0.1 *
Subnet Mask	255.255.0.0 *
Default Gateway	
✓ Apply ✗ Cancel	

管理ポートの IP 構成ページで設定できます。

6) High Availability

(EWS5203、EWS5204、EWS5207 で使用可能)

Current Status

Dedicated Port	LAN1
Status	No Peer
Link to Peer's UI	HA Configuration ▼ <button>Goto</button>
Version	10000

Configuration

Status	☒ Enabled ☐ Disabled
Number of Active(s)	1 ▼
Mode	☒ Active ☐ Standby
HA Port IP Address	172.31.0.1 *
HA Port Subnet Mask	255.255.0.0 *
Peer IP Address	*
Shared Key	*
Action	<button>Sync & Swap</button>

Configuration:

- **Status:** この機能は、ここでオン/オフを切り替えることができます。
- **Number of Active(s):** N+1 HA のために最大 3 つのアクティブを選択可能。
- **Mode:** このコントローラのロールは、ここで手動で決定する必要があります。
- **HA Port IP Address:** 専用 HA ポートに設定された IP アドレス。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:** 高可用性通信のサブネットマスク。
- **Peer IP Address:** ピアコントローラの高可用性ポートの IP アドレスを入力します。
- **Shared Key:** 両方のコントローラにシークレットストリングを入力します。HA 接続が成功するには、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、関連する LAN ポートおよび VLAN ID は HA の発生時に自動的に変更される可能性があるため、Edgecore SW1024 を強くお勧めします。管理者が VLAN101、41、42 を持つ #1 アクティブ AC に対してポート 1、ポート 4、およびポート 2 を SW1024 に設定する場合は、#1 アクティブ関連ポートに 1、4、2 と入力し、#1 アクティブ LAN ポート VLAN ID に 101、41、42 と入力します。
- **Action:** この機能は、プライマリコントローラで起動され、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で LAN1 に設定されています。
- **Status:** 高可用性リンクの現状を反映します。
- **Link to peer's UI:** ページを選択すると、ピア Web UI にすばやくアクセスできます。アクティブのものにのみ使用できます。
- **Version:** 高可用性機能のリビジョンを表示します。

7) Service Zones

このテーブルには、サービスゾーンと関連する設定が一覧表示されます。

- **Status:** サービスゾーンの状態。デフォルトサービスゾーンの場合は、必ず"ON"になります。
- **Service Zone Name:** サービスゾーンの名前。
- **IP Address:** サービスゾーンごとのコントローラの IP アドレス。
- **IPv6 Address:** サービスゾーンごとのコントローラの IPv6 アドレス。
- **VLAN Tag:** (タグベースのモードのみ)各サービスゾーンにマッピングされた VLAN タグ番号。
- **LAN Port Mapping:** (Port-based モードのみ)LAN ポートとサービスゾーン間の対応付け。
- **Default Auth. Option:** サービスゾーンごとに指定されたデフォルト認証サーバ。
- **Network Alias:** サービスゾーンごとのエイリアスサブネット。
- **DHCP Pool:** DHCP サーバステータスまたは DHCP プールの IP 範囲。

Service Zone Settings

Status	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
	Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
	SZ1	10.1.1.254	N/A	1	Server 1	N/A	10.1.1.1 ~ 10.1.1.100
	SZ2	10.2.1.254	N/A	2	Server 1	N/A	10.2.1.1 ~ 10.2.1.100
	SZ3	10.3.1.254	N/A	3	Server 1	N/A	10.3.1.1 ~ 10.3.1.100
	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

SZ1

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

[Configure](#)

This list defines other IP Addresses (range) that are routable in this Service Zone.

DHCP

Enabled

[Configure](#)

Router モード

Basic Settings

Service Zone Status	☐ Enabled ☒ Disabled
Service Zone Name	SZ1
Network Interface	VLAN Tag 1 * (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 172.21.0.254 * Subnet Mask 255.255.0.0 *
	Network Alias List Configure
	This list defines other IP Addresses (range) that are routable in this Service Zone.
DHCP	Enabled Configure

NAT モード

- **Service Zone Status:** デフォルト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(タグベースのモードのみ):** サービスゾーンにマップされる VLAN タグ番号。
- **Tag-Based Isolation(タグベースのモードのみ):** 管理者は、サービスゾーンごとに異なる分離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 つのクライアントは、さまざまな VLAN およびさまざまな LAN ポートから入ってくる場合、お互いに目にすることはありません。分離は、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 を導入する場合は、AP/スイッチでステーション隔離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内で互いに隔離されます。
 - **None:** このサービスゾーンのクライアントには分離は適用されません。
- **Port-Based Isolation(ポートベースのモードのみ):** 管理者は、サービスゾーンごとに異なる分離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 つのクライアントは、異なるポートからの着信時に互いを認識しません。分離は、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 を導入する場合は、AP/スイッチでステーション隔離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内で互いに隔離されます。
 - **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、このサービスゾーン内で隔離されてから認証されます。
 - **None:** このサービスゾーンのクライアントには分離は適用されません。
- **Operation Mode**
 - **NAT:** Network アドレス Translation モードの略。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 に変換してから、アップリンクネットワークに転送します。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表示されません。NAT を展開するコントローラのみが対応する変換を認識します。このモードは、LAN 上のユーザが外部装置から見られることを防ぐだけでなく、限られたパブリック IP アドレス問題を解決します。

- **Router:** コントローラとの間でアドレス変換を行わないネットワークオペレーティングモード。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します。
- **IP Address:** このサービスゾーンの IP アドレス。
- **Subnet mask:** このサービスゾーンのサブネットマスク。
- **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)。
- **Network Alias List:** 管理者は、サービスゾーンに多数のエイリアスネットワークセグメントをオプションで設定できます。この機能により、単一のサービスゾーンを多数のサービスゾーンと見なすことができます。また、サービスゾーンのネットワークインタフェースの IP アドレスを隠し、ある程度まで LAN クライアントからの攻撃を防ぎます。Configure ボタンを押すと、Network Alias List ページが表示されます。

Network Alias List - SZ1

Enable	No.	IP Address	Subnet Mask	Operation Mode
☐	1		255.255.255.255 (/32)	☒ NAT ☐ Router
☐	2		255.255.255.255 (/32)	☒ NAT ☐ Router
☐	3		255.255.255.255 (/32)	☒ NAT ☐ Router
☐	4		255.255.255.255 (/32)	☒ NAT ☐ Router
☐	5		255.255.255.255 (/32)	☒ NAT ☐ Router
☐	6		255.255.255.255 (/32)	☒ NAT ☐ Router
☐	7		255.255.255.255 (/32)	☒ NAT ☐ Router

- ◆ 所望のエイリアス IP アドレスを入力し、所望のサブネットマスク、オペレーションモードを選択し、有効ボックスをオンにして、Apply ボタンをチェ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 サーバを無効、有効、またはリレーに設定できます。
"Enable DHCP Relay"が有効になっている場合は、外部 DHCP サーバの IP アドレスを入力します。クライアントの IP アドレスは外部 DHCP サーバによって割り当てられます。外部 DHCP サーバからの DHCP 情報のみが、このサービスゾーンのダウストリームクライアントに中継されます。DHCP サーバ中継モードに設定すると、冗長 DHCP サーバを設定できます。コントローラは、DHCP サーバと同じサブネット内にある必要があります。

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	☒	Scope 1	172.21.0.1	172.21.0.100	172.21.0.254		domain.com	1440		☐ Enable ☒ Disable
2	☐	Scope 2						1440		☐ Enable ☒ Disable
3	☐	Scope 3						1440		☐ Enable ☒ Disable
4	☐	Scope 4						1440		☐ Enable ☒ Disable
5	☐	Scope 5						1440		☐ Enable ☒ Disable
6	☐	Scope 6						1440		☐ Enable ☒ Disable

Reserved IP Address List
Configure

DHCP Lease Protection
☐ Enable ☒ Disable

- **Start IP Address / End IP Address:** DHCP サーバに組み込まれている一連の IP アドレスがクライアントに割り当てられます。
注記: 管理者がネットワークインタフェースのデフォルト IP アドレスを変更した後に管理者が EWS CONTROLLER 管理ページにアクセスできるようにするには、それに応じて(System Configuration >> System Information >> Management IP Address List で)Management IP アドレス List を変更してください。

- **Preferred DNS Server:** このサービスゾーンで使用するプライマリ DNS サーバ。
 - **Alternate DNS Server:** このサービスゾーンで使用する代替 DNS サーバ。
 - **Domain Name:** このサービスゾーンのドメインネームを入力します。
 - **WINS Server:** WINS サーバがこのサービスゾーンに適用可能な場合にサーバする WINS(Windows Internet Naming Service)の IP アドレス。
 - **Lease Time:** DHCP サーバから発行された IP アドレスが有効で使用可能である期間です。
 - **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、無効を選択した場合は、IP アドレス発行時に機器の名前が記録されます。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 IP 範囲内に特定の IP を予約するための設定リスト(内部ファイルサーバなど)。Configure を選択すると、リザーブ IP リストが変更されます。
 - **DHCP Lease Protection:** これはオプションのチェックメカニズムで、有効にすると、リースの有効期限が切れた IP が現在オンラインであるかどうかを確認します。存在する場合、ユーザセッションが終了するまで、コントローラはこの 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たときに、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。

Assigned IP Address for AP Management

IP Range

Start IP Address

192.168.10.1

End IP Address

192.168.10.254

This defines the range of IP addresses Access Points would use for Local Access Point Management.

Authentication Settings

このシステムは、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などの認証オプションをサポートしています。すべての認証オプションは、同時に有効化および適用できます。この点については、次節“Users”で述べます。

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

Configure

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

Configure

Authentication Options

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	☒	☒
Server 2	RADIUS	.	☐	☒
Server 3	RADIUS	radius	☐	☒
Server 4	LDAP	ldap	☐	☒
Server 5	POP3	pop3	☐	☒
On-Demand	ONDEMAND	ondemand	☐	☒
SIP	SIP	N/A	☐	☐
Guest	FREE	N/A	☐	☐
Social Media Login	SOCIAL	N/A	☐	☐
One Time Password	OTP	N/A	☐	☐

- **Authentication Options:** 管理者は、設定された認証サーバを使用するように指定できます。複数の認証サーバが有効になっている場合、Postfix は認証 OOBID として使用されます。
- **Portal URL:** 目的のランディングページの仕様は、ここで設定できます。有効にすると、管理者はユーザの初回ログイン後に開いているブラウザの URL を設定できます。
- **MAC Authentication:** RADIUS MAC 認証機能を有効にすると、接続された機器の MAC アドレスが設定された RADIUS サーバに入力されている場合、認証が成功すると、コントローラは自動的に認証を行い、すぐにアクセスを許可します。ユーザには透過的なログインが行われます。
- **PPP Authentication:** Point-to-Point Protocol(PPP)は、2 つのネットワークノード間の直接接続を確立する際に一般的に使用されるデータリンクプロトコルです。この機能を有効にすると、エンドユーザは有効なユーザ名とパスワードを使用してダイヤルアップ接続設定を行うことができます(ローカルおよび RADIUS ユーザ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、ユーザは UAM ログインなしで正常に認証されます。
- **Assign IP Address From:** PPP が IP アドレスをダイヤルアップ仮想インタフェースに割り当てることができる開始 IP 範囲。割り当てられたインタフェース IP アドレスは、トンネルの両側のネットワーク間の経路情報に使用されます。

Page Customization

各サービスゾーンは、一意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、一般ログインページ、PLM オープンタイプログインページ(ポート場所マッピングフリーアクセス用)、PMS 請求予定選択ページの 3 種類があります。Service Disclaimer page は、必要に応じて有効にすることができます。これらのページは、管理者に完全な柔軟性を与えるために完全にカスタマイズできます。メッセージページはカスタマイズすることもでき、メッセージページには、ログイン成功ページ、オンデマンドユーザ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が含まれます。

The screenshot shows the 'Page Customization' header. Below the title, there are two rows: 'Login Page Customization' and 'Message Page Customization'. Each row has a 'Configure' button to its right.

The screenshot shows two sections of the configuration interface. The top section, 'Login Page Customization', has a sidebar with four items: 'Service Disclaimer' (Default), 'General Login Page' (Default), 'PLM Open Type Login Page' (Default), and 'PMS Billing Plan Selection Page' (Default). The main area has four radio buttons: 'Edgecore Default' (selected), 'Customize with Template', 'Upload Your Own', and 'Use External Page'. Below these are a checkbox for 'Enable Disclaimer' (unchecked) and a 'Preview' button. At the bottom are 'Apply' and 'Cancel' buttons. The bottom section, 'Theme for Template', has a 'Button Color' row with seven color swatches (grey, orange, green, blue, black, etc.). Below that is an 'Upload Logo' section with a file selection button labeled '選擇檔案' and '未選擇任何檔案'. It shows 'No File' and a message: '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.' At the bottom are 'Apply' and 'Cancel' buttons.

Edgecore Default Page 以外にも、Customize with Template、Upload Your Own、Use External Page の 3 つのカスタマイズオプションがあります。

- **Edgecore Default:** ゲートウェイには、Edgecore ロゴの付いた標準の 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を選択できます。
- **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。全般的なレイアウトは管理者用に設定されていますが、コンテンツは自分の優先順位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でき、テンプレートプレゼンテーションレイアウト内にサービス免責事項、テキストカラーなどのコンテンツフィールドを入力できます。
- **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"では、管理者は編集元のサンプル HTML コードを使用できます。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"を選択します。ファイルが.html フォーマットに保存されている限り、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。このオプションには、メッセージページと連動する 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 ECW100 ▼

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。この一覧は AP 種別ごとに整理されており、AP 名(Main>Access Points>Local Area AP Management>List>AP Configuration へのリンク)のショートカットリンクをクリックして AP を設定できます。これは概要のように機能し、管理者に簡単なステータスチェックを提供します。

8) Port Location Mapping

ポートロケーションマッピング機能により、各サービスゾーンは(各 VLAN がポートであるかのように)複数の VLAN を所有し、クライアントがどこから来ているかを識別することができます。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、場所(ホテルルームなど)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、各部屋を別々のサービスゾーンに割り当てて、別々のポリシーを取得することもできます。さらに、アプリケーションに応じて、さまざまな部屋をさまざまなポートタイプ (Authentication Required、Open または Block)に設定できます。

Create

Status ☒ Enable ☐ Disable Apply

Mapping Create

Subinterface

Use LAN Port LAN1 ▼

Subinterface ID Enter a Number Here

Remark Optional

Add Cancel

Lists

PLM List Show

Subinterface List Show

Tunnel PLM List Show

- **Open:** このポートタイプは、ユーザがこの部屋のインターネットに無料でアクセスできることを意味します。
- **Block:** 部屋にインターネットアクセス権を付与しない場合は、部屋のポートを Block に変更できます。ユーザがブラウザを開き、インターネットにアクセスしようすると、ユーザに通知するブロックメッセージがポップアップ表示されます。
- **Auth. Required:** このポートタイプは、主にユーザを請求するホスピタリティアプリケーションに使用されます。ユーザがブラウザを開き、インターネットにアクセスしようすると、免責事項と課金プランのオプションが記載されたページが表示されます。ユーザは希望するプランを選択し、確認ボタンを押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 に送られ、構成されたミドルウェアを介してホテル請求書に追加されます。

➤ Create Single Mapping

The screenshot shows a web interface for creating a single mapping. At the top, there is a 'Method' dropdown menu set to 'Create Single Mapping'. Below this is a section titled 'Create One'. The form contains several fields with labels on the left and input areas on the right:

- Port Type:** A dropdown menu with 'Open' selected.
- Choose LAN Port:** A dropdown menu with 'LAN1' selected.
- Service Zone:** A dropdown menu with 'Default' selected.
- DHCP Scope:** A dropdown menu with 'None' selected.
- Assign VLAN ID:** A text input field containing 'Range from 1 - 4094' with a red asterisk to its right.
- Location ID:** A text input field containing 'A number'.
- Location Description:** A text input field containing 'Optional'.
- User Limit:** A text input field containing 'Unlimited if left blank'.
- NAS Identifier:** A text input field containing 'NAS Identifier'.
- Class:** An empty text input field.
- HTTP Parameter:** An empty text input field.

- **Port Type:** 部屋のデフォルトステート。オープン、ブロック、認証のいずれかです。必須。
- **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。
- **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。
- **Location ID:** 数値の ID 番号(通常は部屋番号)。
- **Location Description:** 参照のためのオプションの記述。
- **User Limit:** 対応するポートの一括ユーザの最大数
- **NAS Identifier:** RADIUS 属性のオプションパラメータ。
- **CLASS:** RADIUS 属性のオプションパラメータ。
- **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	Open ▼
Choose LAN Port	LAN1 ▼
Service Zone	Default ▼
DHCP Scope	None ▼
Assign VLAN ID From	Range from 1 - 4094 *
Number of VLANs	A number *
Location ID From	A number
Location Prefix	Optional
Location Postfix	Optional
User Limit Per Port	Unlimited if left blank
NAS Identifier From	Optional
NAS Identifier Prefix	Optional
NAS Identifier Postfix	Optional

- **Port Type**: 部屋のデフォルトの状態。フリー、ブロック、単一ユーザ、複数ユーザ。
- **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。
- **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。
- **Number of VLAN**: VLAN の総数。
- **Location ID**: 数値の ID 番号(通常は部屋番号)。
- **Location ID Prefix**: プレフィックス(部屋番号)。
- **Location ID Postfix**: ポストフィックス(部屋番号)。
- **User Limit Per Port**: 対応するポートの一括ユーザの最大数。
- **NAS Identifier From/Prefix/Postfix**: オプションの RADIUS アトリビュート

➤ Subinterface

サブインタフェース 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、さらに分離するために 1 つ以上の VLAN ヘッダーを必要とする大規模なネットワークで一般的に使用されます。

➤ Port Location Mapping List

Port Location Mapping List

Delete Export List Import List Change All Port Types All Search							
☐	VLAN ID	Room Number (Location ID)	Room Description (Location Name)	Port Type	From	Service Zone	Availability
☐	100	1000		Single User	LAN1	Default	
☐	101	1001		Single User	LAN1	Default	
☐	102	1002		Single User	LAN1	Default	
☐	103	1003		Single User	LAN1	Default	

Port Location Mapping List には、すべてのプロファイルエントリが、その VLAN ID、部屋番号/ロケーション ID、ポートタイプ、サービスゾーンなどの情報とともに表示されます。

- **Delete:** 個別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:** 既存の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:** すべての部屋のポートタイプ(フリー、ブロック、単一ユーザ、複数ユーザ)を設定します。

➤ Tunnel PLM List

Tunnel Port Location Mapping List						
Delete All Search						
☐	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ルで戻される VAP の場合。管理者は、NAS 識別子を割り当て、サービス用の IP プールを指定することを望むかもしれません。

ワイドエリア AP 管理の管理対象 AP リストで、管理者は NAS 識別子を割り当て、管理対象 AP の VAP ごとにサービスの IP プールを指定できます。これは、AP とコントローラ間のトンネルを確立するときに設定できます。

9) PMS Interface

PMS インタフェースへの接続を設定することで、PMS サーバからのメッセージを個別に聴くことができます。ホテルのゲストがインターネットアクセスのために部屋内課金プランを購入する場合、システムはレコードを PMS サーバにポストします。

- **PMS Interface Type:** 統合するインタフェースの種類を選択します。

Micros Opera / IDS

- **PMS IP:** Micros Opera PMS で使用される IP を入力します。
- **PMS Port:** Microsoft 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)、または G+(プロフィール名)の組合せを使用してユーザアカウント資格情報を定義し、ユーザ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、大文字と小文字の区別は、PMS サーバに保存されている情報に正確に従います。このオプションを有効にして、大文字と小文字を無視します。
- **Room Bill Description:** 入力された内容は、システムインテグレーションにより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します。
- **User Account Log:** この機能に関連する背景で発生したイベントが記録され、ここに表示される場合があります。
- **Synchronize Data with PMS:** Sync を選択すると、PMS サーバとデータが同期され、データベースが最新であることが確認されます。
- **PMS External Page Customization API:** PMS API は、管理者がカスタマイズされたログインページを柔軟に実装できるようにします。このページでは、ログイン情報、選択された課金プラン、購買ユニットなどがアクセスプロセスを完了できます。
 - **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

サーバと WLAN 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:** ダウンロード可能なサンプルがあり、管理者はどのように統合および変更するかを容易に理解できます。
- すべての req_type は、JSON でフィールド"format"を使用できます。
- req_type=1(equals: bpinfo) 課金プラン情報が表示されます。フィールド"all"を追加すると、無効を含むすべての課金プランが表示されます。
- req_type=2(equals: check) 利用可能な課金プラン、ユニット、およびユーザーに、特定の課金プランの購入が許可されているかを確認します。エラーがある場合は、管理者にエラーコードとメッセージが返されます。
- req_type=3(equals: userinfo) ユーザの情報とステータスが表示されます。項目 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。
- テストの前に、send_req 関数で使用する WLAN コントローラの管理者パスワードを確認してください。
- 対応するサービスゾーンについては、Use External Page で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: Password:

Case and Diacritics Insensitive for Password: ☒ Disable ☐ Enable

Login Error Message:

User Account Log:

Innkey PMS

- **Query API:** クエリーAPI の IP を入力します。
- **Post API:** POST API の IP を入力します。
- **Shared Key:** インキーPMS API の共有鍵を入力します。
- **Account Credential:** 部屋番号とゲスト番号は、ユーザログインのユーザ名とパスワードになります。
- **Case and Diacritics Insensitive for Password:** このオプションを有効にすると、パスワードの検証時に大文字と小文字の区別が無視されます。
- **Login Error Message:** エラーメッセージの内容をカスタマイズします。
- **User Account Log:** この機能に関連する背景で発生したイベントが記録され、ここに表示される場合があります。

B. Users

Users: このセクションでは、ユーザ認証、許可、アカウントिंगについて説明します。これには、グループ構成、内部/外部認証構成、オンデマンドアカウント、ポリシー構成、権限リスト構成、およびその他の制御が含まれます。

1) Groups

Group Overview ページには、対応するグループに使用されている認証サーバの概要が表示されます。

Main › Users › Groups › Overview

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	

グループオプション(モデル依存関係)とゾーン権限設定とポリシー割り当ての 16 セットをそれぞれ定義して、異なるサービスゾーンの異なるユーザグループに対してアクセス管理を実施できます。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 1 ▼

Group Name Group 1

Remark

Number of devices which are allowed to login 1
(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 ▼
☒	Service Zone : Default	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ1	Policy 1 ▼	Policy 1 ▼
☒	Service Zone : SZ2	Policy 1 ▼	Policy 1 ▼
☒	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を使用してログインできるようにするには、ここで"Number of devices which are allowed to login"に数字を定義します。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、選択した料金プランで設定できます。

2) Internal Authentication

このシステムは、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、"Local"、"On-Demand"、および"Guest"が含まれます。

Authentication Option - Server 1

Server No. 1

Name Server 1 *

User Postfix local *

Remark

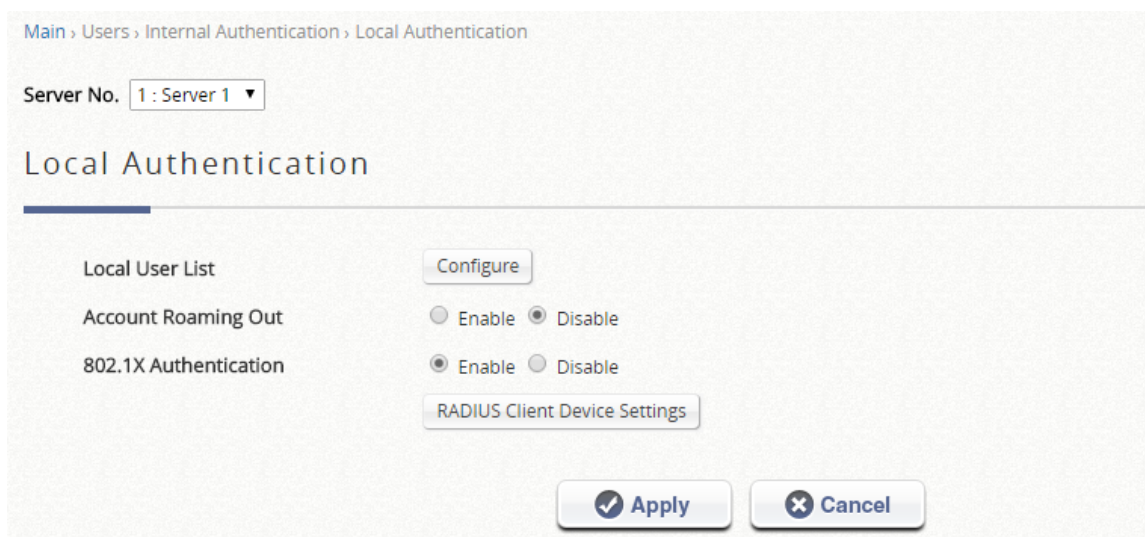
Blacklist None ▼

Authentication LOCAL ▼

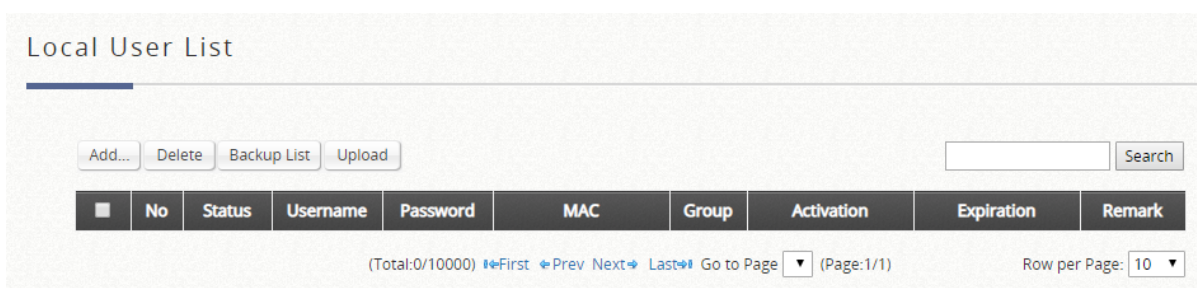
a) Local Authentication

この種の認証方式では、ユーザを格納するローカルデータベース(多くの場合は職員と資格情報)が内部でチェックされます。ローカルユーザデータベースは、管理者が手動で実行しない限り削除されないスタティックアカウントを格納するように設計されています。

"Local"のデフォルト認証は、認証サーバ 1 に設定されています。ユーザポストフィックスは、複数のオプションが同時に使用されている場合に、特定のユーザアカウントでどの認証オプションを使用するかを識別するために使用されます。ローカルアカウントを操作するには、ローカルユーザリストの"Configure"に移動します。



- **Local User List:** "Configure"を選択すると、ローカルアカウント一覧が表示され、アカウントが設定されます。
- **Account Roaming Out:** 外部 RADIUS 認証要求の RADIUS サーバとして使用する場合は、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:** 外部 802.1X 認証要求の RADIUS サーバとして使用する場合は、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 認証が許可されているデバイスのクライアントリストとシークレットキーを設定します。



- **Add:** ユーザ名、パスワード、MAC アドレス、グループ、アカウントスパン、備考などのアカウントを含む 1 つまたは複数のアカウントを作成します。
- **Delete:** Select All にチェックを入れると、個別または全体を削除します。
- **Backup:** ユーザ資格情報をテキストファイルとして新しいウィンドウの CSV フォーマットにエクスポートします。
- **Upload:** 大量のローカルアカウントを作成するのに便利な方法で、アカウントをローカルユーザに再度インポートします。
- **Edit Account Information:** 既存のユーザアカウントでは、ページ上のユーザ名ハイパーリンクをクリックしてアカウント属性を再設定するだけで、さらに修正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
			Group 1 ▼	☐	
			Group 1 ▼	☐	
			Group 1 ▼	☐	
			Group 1 ▼	☐	

- **Username:** 新しいローカルアカウントのユーザ名。新しいアカウントを追加する場合は必須です。
- **Password:** 新しいローカルアカウントのパスワード。新しいアカウントを追加する場合は必須です。
- **MAC Address:** この特定のアカウントは、指定された MAC アドレスを持つデバイスを使用したアクセスのみが許可されるという条件でバインドします。
- **Group:** 作成するアカウントのグループプロファイル。
- **Account Span:** このアカウントに適用される時間制約。
- **Remark:** 管理者が強調したい追加のメモ。ユーザー一覧に表示されます。

b) On-Demand Authentication

通常、オンデマンド認証オプションは、一般的に公共のホットスポットなどの短期の利用に使用されます。請求書プランプロファイル、POS チケットのカスタマイズ、端末サーバリスト、外部決済ゲートウェイの設定など、オンデマンド認証オプションに関連する設定をここで行うことができます。

On-Demand Authentication

User Postfix

ondemand

Billing Plans

Configure

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

30 day(s)

Out-of-quota Account Cache

30 day(s)

Set Ticket's Serial Number

000001

Set

Web Printout

Configure

This will be applied to the regular printer printout when creating a single On-Demand account.

POS Tickets

Configure

Number of Tickets

☒ 1
☐ 2

This will be applied to printouts from the POS ticket printer.
Templates can be edited for customization.

Terminal Server

Configure

Terminal Servers are add-on devices such as the SDS100 or SDS200W.

Payment Gateway

Configure

SMS Gateway

Configure

Account Roaming Out

☐ Enable
☒ Disable

- **User Postfix:** ユーザ Postfix は、複数のオプションが同時に使用されている場合に、特定のユーザアカウントでどの認証オプションが使用されるかを識別するために使用されます。
- **Billing Plans:** Configure を選択すると、料金プランを変更できます。

- **Currency:** オンデマンド認証情報に料金を指定します。
- **Expired Account Cache:** すでに期限切れになっているオンデマンドアカウントをデータベースから削除する日。
- **Out-of-quota Account Cache:** すでにクォータ外になっているオンデマンドアカウントをデータベースから削除する日。
- **On-Demand Access Code:** ユーザ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ログインを許可/禁止します。
- **Smart Login:** オンデマンドユーザのログインを一定期間内に自動的に許可/禁止します。
- **Set Ticket's Serial Number:** 次回の POS チケット印刷時のシリアル番号を設定します。
- **Web Printout:** Configure を選択すると、単一の On-Demand アカウントを作成するときにアカウント情報ページがカスタマイズされます。ここで結果をプレビューすることもできます。
- **POS Tickets:** Configure を選択すると、POS プリンターで印刷するアカウントチケットをカスタマイズできます。
- **POS Printer:** Configure を選択すると、POS プリンタの追加/削除ができます。
- **Payment Gateway:** Configure ボタンを押下すると、ユーザ自身でアカウントを購入できる決済ゲートウェイインタフェースが設定されます。
- **SMS Gateway:** Configure を選択し、SMS ゲートウェイ統合を設定します。オンデマンドアカウントは、アカウント作成時にショートメッセージ(SMS)で送信できます。
- **Email Verification:** Configure を選択すると、メール照合機能が設定されます。ユーザは、メールで送信されたリンクを有効にすることで、アカウントの追加割り当てにアクセスできます。
- **Account Roaming Out:** 外部 RADIUS 認証要求の RADIUS サーバとして使用する場合は、On-Demand 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 認証が許可されているデバイスのクライアントリストとシークレットキーを設定します。

Billing Plans

No	Plan Type	Quota	Price	Active	Group	Function
1	N/A			☐	Group 1	<button>Reset</button>
2	N/A			☐	Group 1	<button>Reset</button>
3	N/A			☐	Group 1	<button>Reset</button>
4	N/A			☐	Group 1	<button>Reset</button>
5	N/A			☐	Group 1	<button>Reset</button>
6	N/A			☐	Group 1	<button>Reset</button>
7	N/A			☐	Group 1	<button>Reset</button>
8	N/A			☐	Group 1	<button>Reset</button>
9	N/A			☐	Group 1	<button>Reset</button>
0	N/A			☐	Group 1	<button>Reset</button>

最大で 10 の課金プランを構成することができます。料金プランには、Usage-time、Volume、Hotel Cut-off Time、および Duration-time の 4 種類があります。料金プランタイプのコンセプトについては、付録 D をご覧ください。

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

<https://www.paypal.com/cgi-bin/webscr>

*

Identity Token

*

Instant Payment Notification (IPN)

☒ Enable ☐ Disable

☐ Behind NAT

Verify SSL Certificate

☒ Enable ☐ Disable

Default ▾

Currency

USD (U.S. Dollar) ▾

*

- **Payment Page Configuration:** 決済ゲートウェイの種類ごとに、入力が必要な情報が異なります。これらの情報は決済ゲートウェイ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 はトランザクション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 の下にある場合は、決済側ユーザがトランザクション結果を受信するために、IP 転送情報を設定する必要があることに注意してください。
- **Choose Billing Plans for Payment Page:** 購入アカウントをユーザするときに、利用可能な請求計画を選択します。
- **Web Page Customization:** Configure を選択して、サービス免責事項ページ、課金プラン選択ページ、およびアカウント資格情報ページをカスタマイズします。

SMS Gateway

- **Selection:** 統合する SMS ゲートウェイの種類。
- **Clickatell:** Clickatell API に接続して、SMS メッセージを送信します。
- **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。コントローラは、設定されたパラメータを使用して、指定された API URL に HTTP 要求を送信し、定義されたパターンで要求が成功したかどうかを識別します。
- **Version (Clickatell のみ):** 旧バージョン(2016 年 11 月より前)は、API ID、ユーザ名、およびパスワードの JSON フォーマットの残りの部分プロトコルの Clickatell API です。新しいバージョンは、統合のために HTTPs プロトコルの API キーのみが必要です。
- **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:** ユーザによる自己登録と SMS による Wi-Fi アカウントの受信を許可します。
- **Account Purchases via Payment Gateway:** オンライン決済ゲートウェイを介してオンデマンドアカウントを購入した Wi-Fi ユーザの SMS 機能を有効にします。購入したアカウントを携帯端末に送信するオプションが表示されます。
- **Both:** 両方のオプションを有効にします。
- **API Key (Clickatell のみ):** Clickatell API の認証キー。特定のインテグレーションサービスの呼び出しとロック解除に使用されます。

- **API URL:** Clickatell API サーバに SMS 要求を送信するためのリンク。デフォルトは <http://api.clickatell.com/http/sendmsg> です。
- **Registration before Accounts Expired:** 第 1 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、同じ携帯電話番号が第 2 オンデマンドアカウントを要求できるようにするには、allow を選択します。1 番目のアカウントが期限切れになった後にのみ 2 番目のオンデマンドアカウントを送信するようにユーザを制限するには、block を選択します。

SMS Gateway

Selection

☐ Disable
☒ Clickatell
☐ SMS API

Version

☐ Old (Prior to November 2016)
☒ New

Send SMS for

Account Registration

API key

API URL

<http://api.clickatell.com/http/sendmsg>

Registration before Accounts Expired

☒ Allow
☐ Block

Billing Plans

Plan	Activation	Quota	Price	Remark
1	☐			
2	☐			
3	☐			
4	☐			
5	☐			
6	☐			
7	☐			
8	☐			
9	☐			
10	☐			

Account Registration Control

☒ Disable
☐ Black List
☐ White List

Web Page Customization

Configure

- **Parameter(SMS API のみ):** SMS 要求を送信するための API パラメータと値。
- **Response Format(SMS API のみ):** JSON または HTML。選択肢は、SMS サービスが提供する応答の種類によって異なります。レスポンスフォーマットは、SMS テキストメッセージが正常に送信されたかどうかを決定するために無線 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):** JSON フォーマットでの SMS 要求の応答からの値のキーパス。例: ['data'][0]['status']
- **Return Value of Successful Request (SMS API のみ):** 成功したレスポンスのテキストをここに入力します。
- **Send Test Message (SMS API のみ):** 携帯電話番号を入力し、テスト SMS メッセージを送信します。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 要求のトラブルシューティングを行い、SMS プロバイダから送信された応答メッセージを表示することができます。
- **Message Content (SMS API のみ):** Wi-Fi ユーザが受信する SMS テキストメッセージを、メッセージエディタボックスでカスタマイズします。作成された On-Demand アカウントに関する 4 つのパラメータを入力できます。username、username without the postfix、password、および quota description です。

パラメータ	定義
\$username	作成されたオンデマンドアカウントのユーザー名。
\$Username_without_postfix	\$username と同じですが、ポストフィックスは使用しません。
\$password	作成したオンデマンドアカウントのパスワード。
\$quota	作成した On-Demand アカウントのクォータ説明。

SMS Gateway

Selection

Send SMS for

API URL

Registration before Accounts Expired

Parameter

Response Format

Key of JSON Array

Return Value of Successful Request

Send Test Message

Message Content

Billing Plans

Account Registration Control

Web Page Customization

☐ Disable
☐ Clickatell
☒ SMS API

Account Registration

http://api.clickatell.com/http/sendmsg

☒ Allow
☐ Block

No.	Parameter	Parameter Value	Remark
-			Phone Number
-			SMS Content
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

☒ JSON
☐ HTML

Please enter the path of the key. ex ['data'][0]['status']

Please enter String, Number, Boolean, or null.

Please check the response sample code to identify the object for indicating the success of the request.

Phone Number

Send

Please apply the changes in this page before sending test message.

Message Editor

Parameter

\$username
▼
Insert Parameter

On-Demand Username

Plan	Activation	Quota	Price	Remark
1	☐			
2	☐			
3	☐			
4	☐			
5	☐			
6	☐			
7	☐			
8	☐			
9	☐			
10	☐			

☒ Disable
☐ Black List
☐ White List

Configure

- **Billing Plans:** 作成されたアクティブ料金プランが表示され、ショートメッセージ(SMS)によるオンデマンドアカウントの作成に使用されます。少なくとも 1 つの請求計画を選択する必要があることに注意してください。

- **Account Registration Control:** ブラックリスト、ホワイトリストを無効にします。特定の携帯電話番号を制限しない、または、許可することを無効にします。ブラックリストは、特定の携帯電話番号の登録を拒否します。ホワイトリストでは、特定の携帯電話番号のみを登録できます。
- **Web Page Customization:** デフォルトを使用してサービス免責事項と請求書プラン選択ページをカスタマイズし、テンプレートを使用してカスタマイズし、独自のページをアップロードし、外部ページオプションを使用します。

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	☐		D H M		
2	☐		D H M		
3	☐		D H M		
4	☐		D H M		
5	☐		D H M		
6	☐		D H M		
7	☐		D H M		
8	☐		D H M		
9	☐		D H M		
10	☐		D H M		

SMTP Server Settings

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!

Web Page Customization
Configure

- **Selection:** 機能を有効または無効にします。
- **Choose Billing Plan for Redeeming Account via Email(選択可能な使用時間のみ):** 設定された請求計画を選択します。この機能は、使用状況タイプの請求計画のみがサポートされます。
- **Activation:** どの課金プランで許可される電子メール検証機能を選択します。
- **Quota:** それぞれの請求予定の最新サマリーを表示します。
- **Redeem Quota:** 使用時間。これは、再利用時に追加で使用することができます。
- **Price:** それぞれの請求書プランの最新料金を表示します。
- **Remark:** ウォールドガーデンエントリーごとの ID のカスタムエントリー。
- **SMTP Server Settings:** 引き換えクライアント用にメールを送信するための SMTP サーバを割り当てます。この SMTP はゲスト電子メール検証と共有されます。
- **Sender Name:** 送信者名がクライアントメールボックスに表示されます。

- **Activation Email Subject:** カスタマイズ可能な電子メールの件名がクライアントメールボックスに表示されます。
- **Activation Email Content:** メールボックスに表示されるメールの内容をカスタマイズできます(最大 2000 文字)。
- **Activation Link:** クライアント電子メールコンテンツのアカウントを引き換えるハイパーリンクの名前。
- **Web Page Customization:** さまざまなカスタマイズタイプを選択できますが、Edgecore デフォルトとテンプレートを使用したカスタマイズのみがサポートされるようになりました。

c) Guest Authentication

ゲスト認証オプションは、技術的にはユーザデータベースではなく、ユーザがユーザ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、サーフィンできるように特別に設計されたオプションです。この機能を使用すると、ユーザを特定のサービスゾーンに関連付け、管理者が定義したソーシャルセキュリティ番号などのゲストアンケートによってゲスト電子メールまたはテキストの指定した文字列を入力し、実際の認証なしでネットワークを使用できます。

- **Group:** ゲストログインクライアントが属するユーザグループ。これは、特定のサービスゾーンにマッピングでき、ユーザポリシープロファイルの制限付きで適用できます。
- **Guest Information:** アカウントの一部の情報は、管理者の詳細な解析またはマーケティング目的で使用できます。アカウントメールなどのアンケート対応フィールドは、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、1000 件(11000/12000、最大 12000 件)のエントリが残っている場合に電子メール通知が送信されます。
- **Download:** 管理者は、収集されたゲストインフォメーションをダウンロードできます。
- **Delete All:** 管理者は、保存されているすべてのデータを削除できます。管理者は、リストを最新の状態に保つために、エクスポート後にすべてのエントリを削除できます。

- **Questionnaire:** ゲストログインのログインページで追加の質問をカスタマイズするオプションを管理者に提供します。ゲストユーザからのアクセス情報が収集され、Guest Information list に表示されます。
- **Guest Access Time:** MAC アドレスに基づいてユーザタイム制約を定義します。
 - **Unlimited:** 使用可能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制約で強制されます。
 - **Multi-Day Access:** クライアントは使用時間制約で強制されます。
- **Quota:** ゲストクライアントごとに許可される持続時間とボリューム。
- **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できます。
- **Access Limit(1 Day Access のみ):** 1 日に何回、デバイスが空きアカウントを要求できるか定義します。
- **Email Verification:** 入力し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。メールサーバから送信されたメールのリンクをクリックすることで、利用時間を延長するには、有効化時間内にこのアカウントを有効化する必要があります。アクティブ化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にメールを送信するための SMTP サーバを割り当てます。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 サーバの例として挙げると、以下のような構成になります。
 - **SMTP server address:** smtp.gmail.com
 - **SMTP port:** 465
 - **Encryption:** SSL
 - **Authentication: Login:** アカウント名: 管理者の Gmail 電子メールアドレス
 - **Authentication: Login:** パスワード: admin の Gmail メールパスワード
 - **Sender Email Address:** 管理者の Gmail 電子メールアドレス。
- **Sender Name:** 送信者名がクライアントメールボックスに表示されます。
- **Activation Email Subject:** カスタマイズ可能な電子メールの件名がクライアントメールボックスに表示されます。
- **Activation Email Content:** カスタマイズ可能なメール内容が、クライアントメールボックスに表示されます(最大 2000 文字)。
- **Activation Link:** クライアント電子メールコンテンツのアカウントを引き換えるハイパーリンクの名前。
- **Guest Quota List:** MAC アドレスと電子メールアドレスで、アクセス制限付きゲストアカウントの残りの容量を確認します。(毎日深夜に自動的に更新され、最大に達すると最も古いエントリが削除されます)。
- **Email Denial List:** ジャンクメールボックスを防ぐ必要がある場合は、電子メールドメインのログイン権限を確認します。

d) One Time Password

ワンタイムパスワード(OTP)認証オプションでは、クライアントは自身の携帯電話番号を入力し、認証画面に入力する必要があるワンタイムパスワードで SMS メッセージを受信することによって、インターネットにアクセスすることができます。その後、クライアントはインターネットサーフィンを開始できます。

One Time Password Authentication

Group	Group 1 ▼
OTP Client Information	View
Default Country Code	AF - AFGHANISTAN (+93) ▼ ☐ 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 認証されたクライアントは、設定されたユーザポリシーによってそれぞれのサービスゾーンに適用されます。
- **OTP Client Information:** ワンタイムパスワードを要求したクライアントの情報。
 - **Download:** 管理者は、収集された 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、保存されているすべてのデータを削除できます。管理者は、リストを最新の状態に保つために、エクスポート後にすべてのエントリを削除できます。
- **Default Country Code:** ログインページに表示されるデフォルトの国番号を設定します。
- **Length of Mobile Number:** 携帯電話番号フォーマットを桁数で設定します。
- **Quota(継続時間):** OTP 認証されたクライアントの継続時間を指定します。最大期間は 364 日 23 時間 59 分です。
- **Questionnaire:** 5 つのエントリが OTP 登録ページに表示されます。
- **SMS Gateway:** Clickatell (Legacy/New)、および SMS API(テキストコンテンツのカスタマイズを確認)。関連する設定については、オンデマンドユーザデータベースの SMS ゲートウェイ設定を参照してください。
- **Web Page Customization:** さまざまなカスタマイズタイプを選択できますが、Edgecore デフォルトとテンプレートを使用したカスタマイズのみがサポートされるようになりました。

3) External Authentication

最大 5 つの外部認証サーバを同時に設定および有効にして、ネットワーク上の既存のユーザアカウントデータベースを容易にすることができます。外部認証オプションには、RADIUS、POP3、LDAP、NTドメイン、および SIP が含まれます。

Authentication Options				
Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	☒	☒
Server 2	RADIUS	.	☐	☒
Server 3	NTDOMAIN	ntdomain	☐	☒
Server 4	LDAP	ldap	☐	☒
Server 5	POP3	pop3	☐	☒
On-Demand	ONDEMAND	ondemand	☐	☒
SIP	SIP	N/A	☐	☐
Guest	FREE	N/A	☐	☒
Social Media Login	SOCIAL	N/A	☐	☐
One Time Password	OTP	N/A	☐	☐

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グループ。これは、特定のサービスゾーンにマップし、ユーザポリシープロファイルの制限付きで適用することができます。
- **Social Media Account Information:** アカウントの一部の情報は、管理者の詳細な解析またはマーケティング目的で使用できます。ソーシャルメディアアカウント一覧のアカウント名、アカウントメール、性別、誕生日、および場所は、管理者のデータ操作のためにダウンロードできます(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、1000 件(11000/12000、最大 12000 件)のエントリが残っている場合に電子メール通知が送信されます。
- **Download:** 管理者は、収集されたゲストインフォメーションをダウンロードできます。
- **Delete All:** 管理者は、保存されているすべてのデータを削除できます。管理者は、リストを最新の状態に保つために、エクスポート後にすべてのエントリを削除できます。
- **Social Media Account Access Time:** “Limited”に設定すると、MAC アドレスに基づいて使用時間の制約が適用されます。

- **Quota:** ソーシャルメディアログインクライアントごとに許可される持続時間とボリューム。
- **Reactivation:** 時間が経過すると、新しいセッションを定義できます。
- **Access Limit:** 1日に何回、デバイスが空きアカウントを要求できるか定義します。

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:** MAC アドレスと電子メールアドレスで、アクセス制限付きゲストアカウントの残りの容量を確認します。(毎日深夜に自動的に更新され、最大に達すると最も古いエントリが削除されます)。
- **Punishment:** 処罰メカニズムを有効/無効します。事前に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テーブルに表示されます。クライアントがソーシャルログインボタンを 3 回再試行しても失敗する場合は、処罰として 15 分かかります。
- **Punishment List:** 罰せられるクライアントがここに表示されます。管理者は、処罰リストで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

- **Account Creation:** 管理者は、"Batch Create"機能を使用して、単一のアカウントまたは複数のアカウントを作成できます。アカウントを作成するには、少なくとも 1 つの請求書プランを設定して有効化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を使用して作成するか、手動で作成できます(最大 8 文字)。ユーザー名とパスワードは、バッチ作成のために手動で作成することもできます。(例: Prefix=ABC、Postfix=DEF、Serial Number0001)

On-Demand Account List

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

☐	Username	Remaining Quota	Status	Group	Reference	External ID	Redeem
☐	28v2	Until 2013/02/07-02:00	Expired	Group 1	roomN-3154-00:09:6B:CD:82:47		
☐	e69w	Until 2013/02/19-01:00	Expired	Group 1			
☐	9u2u	Until 2013/02/19-03:03	Expired	Group 1			
☐	ep4r	Until 2013/02/19-05:01	Expired	Group 1			

(Total:4/9000) Go to Page (Page:1/1) Row per Page:

- **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がこのページに表示されます。また、管理者は、オンデマンドアカウントに対してアカウントの復元/削除や管理者による回復などの操作をできます。

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さまざまなログイン時間権限を設定できます。設定したスケジュールプロファイルを適用するには、グループ設定に移動します。

Schedule Permitted Login Hours - Profile 1

Select Schedule	Schedule 1
-----------------	------------

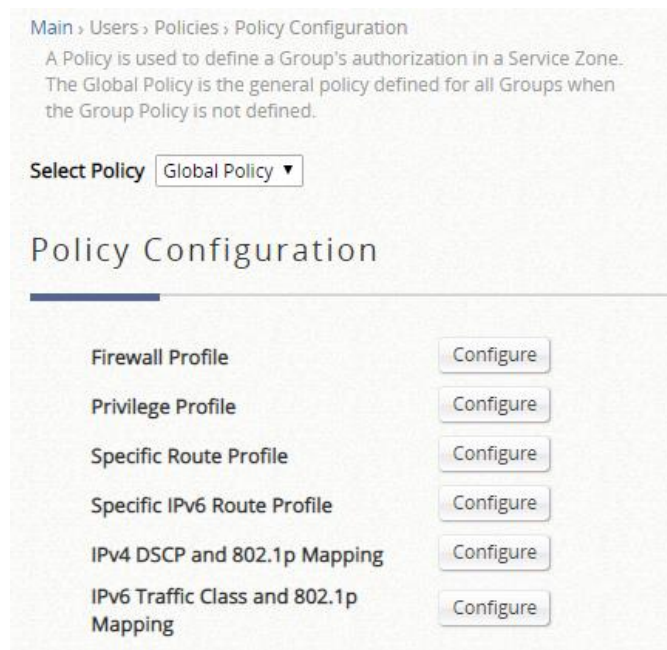
Schedule Name	Schedule 1
---------------	------------

☐	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
☐	SUN	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	MON	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	TUE	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	WED	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	THU	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	FRI	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	SAT	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

☐ Log off authenticated users during unauthorized periods

6) Policies

グローバルポリシーとは、ユーザが規制され、他のポリシーに適用されない限り、すべてのユーザに適用される、Firewall Profile、Specific Route Profile、Schedule Profile、Maximum Concurrent Sessions 管理を含むシステムの普遍的なポリシーです。



それぞれのポリシーは、Firewall Profile、Specific Route Profile、Schedule Profile、Maximum Concurrent Sessions 管理から構成されています。ポリシーはポリシータブで定義できます。管理者は、定義されたポリシーのいずれかを選択して、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のグループは、異なるポリシーで適用できます。たとえば、販売部門の地域または財務部門の地域からアクセスしながら、異なるネットワークアクセス権を使用して販売を適用できます。

- **Select Policy:** 使用可能なポリシープロファイルの数は、モデルの種類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、独自のカ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:** このリンクは、プロトコル(TCP/UDP/ICMP/IP)ごとにサービスの一覧を定義できるポリシーのサービスリストページにつながります。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、ポリシーのファイアウォールルールページが表示されます。ルール No.1 が最も優先順位が高く、ルール No.2 が 2 番目の優先順位、というように続きます。それぞれのファイアウォールルールは、送信元、宛先、ポリシーのサービスリスト外のサービス、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、Firewall Rule Schedule を設定して、ファイアウォールルールを適用する時間を指定できます。常時、定期的、または 1 回限りに設定できます。
 - **DoS Protection(グローバルプロファイルのみ):** DoS 攻撃から保護するためのオプションを設定します。
- **Privilege Profile:** ユーザ生成されたセッション番号の制限は、ここで設定できます。ネットワークの使用状況に応じて、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):** 許可を設定して、適用された権限プロファイルを持つユーザがログインパスワードを柔軟に変更できるようにします。
 - **Maximum Concurrent Sessions:** この権限プロファイルを持つユーザがセッション制限に達すると、このユーザは一定期間、新しい接続から暗黙的に中断されます。
 - **Disable timeout for this group(非グローバルプロファイルのみ):** 有効を設定することで、このポリシーによって適用されるクライアントが自動的にログアウトされなくなります。このオプションを有効にすると、装置の負荷が高くなることがあります。
- **QoS Profile(非グローバルポリシーのみ):** トラフィック構成を編集します。帯域幅スロットリングが必要な場合、管理者はこのチェックボックスをオンにして、クライアントが認証を完了したときに、特定の期間が経過した後の 2 番目の QoS を選択できます。
 - **Traffic Class:** 各ポリシー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 に別々のトラフィッククラスリマークを設定できます。
 - **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許可される最低保証帯域幅を定義します。個々の要求ダウンリンクは、Group Total Downlink および 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許可される最低保証帯域幅を定義します。個々の要求アップリンクは、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に適用されるルーティングルールは、ここで設定できます。
- **Specific IPv6 Route Profile:** このポリシーでユーザに適用されるルーティングルールは、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):** この条件は、管理対象 VLAN ネットワークで送信するために、IPv4DSCP タグから目的の 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有効にします。
- **IPv6 traffic class and 802.1p mapping(グローバルポリシーのみ):** この条件は、管理対象 VLAN ネットワークで送信するために、IPv6 トラフィックタグから目的の 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有効にします。

Policy1～x(モデル依存)は、さまざまなサービスゾーンの特定のユーザグループに適用できます。Policy1 が最も優先順位が高く、優先順位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。

ここでは、優先 DHCP プール(サービスゾーンの DHCP 構成で定義)も選択できます。

7) Blacklists

ブラックリストプロファイルを定義し、それぞれのアクティブ認証オプションにこれらのブラックリストプロファイルのいずれかを設定できます。ブラックリストにリストされているユーザアカウントは、システムへのログインが許可されていないため、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 1 つのブラックリストを選択することができ、このブラックリストは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

Case Insensitive with blacklist ☒ Disable ☐ Enable

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

8) Privilege Lists

Privilege 関数は、IP アドレス、MAC アドレス、IPv6 アドレスの 3 タイプの権限リストをサポートしています。リストに指定されたデバイスは、ネットワークにアクセスするために認証を必要としません。ユーザグループは、IP アクセス権リストのデバイスに割り当てることができますが、MAC アクセス権リストには割り当てることができません。

SYSTEM **USERS** ACCESS POINTS NETWORK UTILITIES STATUS

Main > Users > Privilege List > IP Address

IP Privilege List

No.	IP Address	MAC Address	Group	Remark
(Total:0/200) First Prev Next Last Go To Page (Page:1/1) Row per Page: 10				

- **Privilege List:** 管理者が認証なしで特権的な個別アクセスを指定できる認証フリー・リストには、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使用して実現できます。

5) Additional Control

このセクションでは、追加設定について説明します。これらは、ユーザセッション制御、内蔵 RADIUS サーバ設定、カスタマイズ、残り時間リマインダ、および MAC ACL です。管理者は、ユーザセッション制御でアイドルタイムアウトなどのユーザセッションを制御できます。内蔵 RADIUS サーバ設定には、セッションタイムアウトなどの 3 つの機能があります。カスタマイズで、管理者は証明書をシステムにアップロードできます。残り時間リマインダは、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、システムへのアクセス制御を管理できます。

User Session Control

Idle Timeout	10 minute(s) *(1-5040)
Detection Interval	60 second(s) *(1-600)
Traffic Direction for Idle Timeout	Uplink & Downlink
Timeout Threshold	0 byte(s) *(0-1048576, 0 is Disabled)
User Options	☐ Charge Traffic to/from Hosts in Walled Garden List
	☐ Kick user when user's IP change
	☐ Log NAT Mapped in User Session Log

Built-in RADIUS Server Settings

Session Timeout	120 minute(s) *(5-43200)
Idle Timeout	10 minute(s) *(1-5040)
Interim Update	5 minute(s) *(1-120)
Certificate	Default CERT

Remaining Quota Reminder

Time and Cut-off Reminder	☐ Enable ☒ Disable
Volume Reminder	☐ Enable ☒ Disable
Reminder Refresh Time	☒ 10mins ☐ 15mins ☐ 20mins

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.	

User Session Control

- **Idle Timeout:** アクティビティなしでタイムベースを設定して、アイドルタイムアウトと見なします。
- **Idle Detect Interval:** アイドル基準に達したかどうかを確認するためのインターバル。上記のアイドル時間設定を超えてアイドル時間が連続して累積されると、ユーザがログアウトされ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:** ユーザのアクティビティインスペクションは、アップリンクトラフィックのみまたは両方向でチェックできます。
- **Threshold for Idle Traffic Detection:** 設定した値より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・データベース内の使用量または量のタイプアカウントについて、管理者は、ウォールガーデンまたはウォールガーデン広告リストにリストされた Web サイトへの訪問に課金するか、または課金しないオプションを有します。
- **Kick out user when user's IP change:** ユーザが IP アドレスを変更するたびに、強制的に切断するかどうかを管理者にオプションします。
- **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/ポートへの接続ごと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:** 内蔵 RADIUS サーバで認証されたユーザによって生成された作成済みセッション(アカウントローミングユーザの場合もあります)では、ここでタイムアウト範囲を手動で設定できます。このアトリビュートは慎重に設定してください。
- **Idle Timeout:** 内蔵 RADIUS サーバで認証されたユーザ(アカウントローミングユーザの場合もあります)の場合、アイドルタイムアウトレンジはここで手動で設定できます。このアトリビュートは慎重に設定してください。
- **Interim Update:** 内蔵 RADIUS サーバで認証されたユーザ(アカウントローミングユーザの場合もあります)の場合は、ここでアカウント間隔を手動で設定できます。このアトリビュートは慎重に設定してください。
- **Certificate:** 内蔵 RADIUS サーバの証明書を選択できます。

Remaining Quota Reminder

- **Time and Cut-off reminder:** これは、タイムベースのアカウント割当量が切れようとしていることをオンデマンドユーザに警報するオプションです。
- **Volume Reminder:** これは、On-Demand ユーザに対して、ボリュームベースのアカウントクォータが使い果たされシステムとしていることを示す警告メッセージを表示するオプションです。
- **Reminder Refresh Time:** 残りのクォータを含むログイン成功ページでは、10/15/20 分ごとに更新するように設定して、更新された残りのクォータを表示できます。

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で、MAC アドレスの制限方法を設定できます。

C. Devices

Devices: AP およびスイッチを管理するために使用します。AP およびスイッチのさまざまな属性を表示するほかに、さまざまな構成で提供されるさまざまな機能があります。

Welcome to Device Management

Local Area AP Management

Enable

Enter

Wide Area AP Management

Enable

Enter

Switch Management

Enable

Enter

1) Local Area AP Management

a) Overview

サマリは、各 AP タイプの基本情報を一覧表示するために使用されます。これには、AP の数、オンラインの数、オフラインの数、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。

システムの管理下にあるすべてのサポート対象 AP がこの表に表示され、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

必要に応じて、チェックボックスをオンにして任意の AP を選択し、下のボタンをクリックして、選択した AP を Reboot、Enable、Disable、Delete、Apply template および Apply Service Zone します(タブベース)。

b) List

種別、名前、IP アドレス、MAC アドレス、オンラインステータスなど、管理対象 AP ごとの情報を一覧表示するために使用されます。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、サービスゾーンやその他の構成による適用などの操作も含まれます。

システムの管理下にあるサポートされているすべての AP がリストに表示されます。管理者は、Discovery 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、AP 種別、AP 名、IP アドレス、MAC アドレス、サービスゾーン、状態など、現在の管理対象 AP が一覧表示されます。管理者は、各 AP の前にあるチェックボックスをオンにするか、トップチェックボックスをオンにしてすべての AP を一緒に選択すること

で、管理対象 AP の再起動、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の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)

	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をオンにして任意の 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 を Reboot、Enable、Disable、Delete、Apply template、Reset to Default、Apply by Service Zone および Add to Floor Plan します。

c) Adding

Adding 機能は、AP に必要な情報を入力して、AP を手動で設定するために使用します。システムには、AP 構成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"を選択することで、サポートされている AP をリスト表に手動で追加できます。システムは指定された値で AP を設定しようとします。処理後、AP のステータスは AP リストに "online" または "offline" と表示されます。

Add Method Add AP

Add An AP

AP Type ECW100

AP Name *

Admin Password admin

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。
- **AP Name:** 特定の AP のニックネーム。
- **Admin Password:** この AP に必要なパスワード。
- **IP Address:** 指定した AP の IP アドレス。
- **MAC Address:** 指定した AP の MAC アドレス。
- **Apply AP Template:** この追加された 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が追加した 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 を手動または自動で検出し、検出されたそれぞれの AP に一意の IP アドレスを自動的に割り当てる機能です。AP リストから "Add" をクリックし、"Find Multiple APs" を選択します。

Background AP Discovery 機能を有効にすると、10 分ごと、または管理者が設定した時間に基づいてスキャンされます。いずれかの AP が検出され、Auto Adding AP to the List が有効になっている場合、チェックされたサービスゾーンプロファイルに設定されている開始 IP アドレスから利用可能な IP 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:** システムで検索する AP モデル名を選択します。
- **Service Zone:** 接続先の 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 の管理に使用する VLAN を設定します。
- **Admin Settings Used to Discover:** 接続されている AP のインタフェースと管理資格情報が変更されていない場合は、出荷時のデフォルトを選択します。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、検出処理中に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:** 設定されている場合、新しく接続された AP デバイスの設定された IP 範囲が定期的にスキャンされ、検出結果が自動的に表示されます。
- **Discovery Results:** 上記で設定した検出基準に一致する AP デバイスが表示されます。

e) Templates

AP 設定テンプレートを定義できます。"Adding"および"Discovery"セクションでは、最大 8 つのテンプレートを編集、保存、および使用できます。

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、AP 管理インタフェースをログに記録する代わりに、設定をテンプレートにまとめて構成して、設定を 1 つずつ設定できます。AP Type を選択し、Edit をクリックして Template Editing ページに入ります。

AP Template

AP Model: ECW100 Add Template

Template Name	Copy Settings from	Remark	Action
TEMPLATE1	NONE	Template 1	 

- **Template Editing:** 管理者は、テンプレート設定を手動で設定するか、Copy Settings From オプションで管理対象 AP から設定をコピーできます。Configure を選択すると、詳細な設定を行うことができます。
 - **Name:** この特定のテンプレートに表示される名前。
 - **Copy Settings From:** 設定済みの AP を選択し、Apply を選択して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注釈または追加情報。
 - **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: 255.255.0.0 *

Default Gateway: 192.168.1.254 *

Primary DNS: 192.168.1.254 *

Secondary DNS:

NTP: Time Zone (GMT 00:00)Greenwich Mean Time:Dublin,Lisbon,London

NTP Server 1: 192.168.1.254 *

NTP Server 2: time.nist.gov

SNMP: Disabled

SYSLOG: Enabled

SYSLOG Server IP Address: 127.0.0.1 *

SYSLOG Server Port: 514 *

Log Level: Debug

Port Configuration: LAN 1 Disabled

VLAN ID: *(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 Subnet mask を修正し、ここを Default Gateway します。NTP Servers と Time Zone を設定します。また、管理者は、SYSLOG サーバが 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 では、管理者が LAN ポートごとに 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 ▼

☐ 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:** このオプションを選択すると、AP の SSID がネットワークにブロードキャストされます。プライベートで使用するために認証が無効になっている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、選択するモードは異なります。802.11a、802.11b、802.11g、802.11a+802.11n、802.11b+802.11g、802.11g+802.11n、および 802.11ac です。
- **Channel Width(802.11g+n、802.11a+n、および 802.11ac のみ):** 20MHz、40MHz、または自動から選択します。スループットを向上させるために、40MHz までのダブルチャネル帯域幅がサポートされています。802.11ac モードでは、80MHz を選択できます。
- **Antenna Mode(802.11g+n、802.11a+n、および 802.11ac のみ):** MIMO に使用するストリーム番号を選択します。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、最大電力から 1dBm ずつ減少することを意味します。Level 1 は実際の最大電力、Level 2 は最大電力から 1dBm を引いた値などです。

- **Beacon Interval(ミリ秒)**: 20~1000 ミリ秒の間で入力します。デフォルトは 100 ミリ秒です。入力される時間とは、アクセスポイントと無線ネットワーク間でビーコン信号が送信される頻度を意味します。
- **ACK Timeout**: ACK フレームの受信待ち時間です。インターバル内に ACK が受信されなかった場合、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または悪化します。
- **Airtime Fairness**: "Fair Access"に設定すると、帯域互換性の異なるすべてのデバイスが同じエアタイムを持つようになります。"Preferred Access"に設定すると、N クライアントが優先されます。この機能は、異なる帯域をサポートするデバイスがあるネットワークに最適です。
- **Packet Delay Threshold(ms)**: 送信キューフラッシュメカニズムです。これは、パケットをドロップし、キューが x ミリ秒を超えて処理された場合にすぐに他のパケットを処理するためのメカニズムです。デフォルトでは無効です(=0)。
- **Idle Timeout(秒)**: 非アクティブが設定された秒数(デフォルト=300 秒)に達すると、クライアントは切断されます。
- **Band Steering**: 有効にすると、5GHz 接続のクライアントは 5GHz 帯域に向けて 2.4GHz 帯域の輻射を低減します。これは、AP が 2 つの RF カードで 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 接続のクライアントは強制的に 5GHz 帯に接続されます。
- **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えます。
- **Transmission Rate Threshold**: 通信速度が設定したしきい値を下回ると、関連付けられたクライアントがキックされます。これにより、関連付けられているすべてのクライアントの接続速度が高速になります。
- **UAPSD**: 有効/無効 USPAD に対応しています。
- **WME Configuration**: アクセス優先順位は、さまざまなパラメータを使用して設定できます。AP 側パラメータ、クライアント側パラメータをそれぞれ設定できます。CW Min: Contention Window Minimum、CW Max: Contention Window Maximum、AIFS: Arbitration Inter Frame Spacing、TXOP Limit: Transmission Opportunity Limit.
- **VAP Configuration**: "Status"列の VAP を有効/無効します。VAP の設定は、"Action"の下にある編集アイコンをクリックすることで行うことができます。

VAP Edit - ECW5211-L: TEMPLATE1

Status	☒ Enable ☐ Disable
Profile Name	VAP-1 *
Service Zone	Default ▼
VLAN ID	0 ▼
SSID	Guest Network *
RTS Threshold	2346 *(Default: 2346 ; Range: 1 ~ 2346)
DTIM Period	1 *(Default: 1; Range: 1 ~ 15)
Consecutive Dropped Packets	0 *(2 - 50, 0:Disable)
Broadcast SSID	Enable ▼
Wireless Station Isolation	Enable ▼
IAPP	Enable ▼
Multicast-to-Unicast Conversion	Disable ▼
TX STBC	Enable ▼
Multicast/Broadcast Rate	5.5M ▼
Management Frame Rate	5.5M ▼
Receiving RSSI Threshold	-85 *(-95 ~ 0 dbm, 0:Disable)
Service Schedule	24/7 Service ▼
Security ▼	
Authentication	Open System ▼
Encryption	None ▼
Access Control ▼	
Maximum Number of Clients	128 *(Limit per RF Card)
Access Control Type	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/管理を目的とした、特定の RF カードとその VAP のプロファイル名。
- **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、特定の VAP に関連付けるクライアントの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:** 1～2346 の値を入力します。RTS (Request to Send) Threshold では、非表示ノードの問題を回避するためにフラグメントを送信する前に送信する要求(RTS)を発行するパケットサイズを指定します。データサイズが指定された値を超えると、RTS メカニズムがアクティブになります。RTS しい値の設定を低くすると、多くのクライアントデバイスが AP に関連付けられている領域、またはクライアントが離れており、AP のみを検出し、相互には検出ししない領域で役立ちます。
- **DTIM Period:** 定期的なビーコン内で生成される DTIM Interval を指定した周波数で入力します。DTIM が大きいほど、ワイヤレス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、パケット送信が失敗した場合に AP が送信範囲外であると

判断するまでに試行する送信リトライ最大数です。設定された回数の送信再試行が失敗すると、アクセスポイントはクライアントにキックして、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、SSID のブロードキャストが中止されます。SSID のブロードキャストが無効になっている場合、正しい SSID を持つデバイスのみ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、システムに関連付けられているすべてのステーションが隔離され、システムとのみ通信できます。
- **IAPP:** IAPP(Inter Access Point Protocol)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ためのプロトコルです。この機能を有効にすると、システムは関連する無線局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無線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:** マルチキャストからユニキャストへの変換が有効な場合、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。レジストレーション情報は記録され、マルチキャストグループに分類されます。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にのみインテリジェントにトラフィックを転送できます。マルチキャストからユニキャストへの変換がない場合、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るため、ネットワークの非効率が発生します。
- **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。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無線クライアントの帯域幅が必要な場合、管理者はここで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カスタマイズできます。
- **Management Frame Rate:** この機能は、マネジメントフレームの帯域幅を制御します。レートが高いほど、伝送がカバーする範囲は短くなります。
- **Receiving RSSI Threshold:** 接続局の通信速度を速く保つため、受信感度がしきい値を下回ると接続局をキックアウトします。
- **Security:** アクセスポイントは、VAP プロファイルごとに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。セキュリティの種類には、オープン、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:** 無効を選択した場合、クライアント装置からのアクセスは制限されません。
 - **MAC ACL Allow List:** MAC ACL Allow List を選択すると、許可リスト(許可 MAC アドレス)にリストされているクライアント装置(MAC アドレスで識別)のみがシステムへのアクセスを許可されます。管理者は、Disable をチェックすることで、リストされた MAC を再度有効にするまでの間、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、拒否リスト(拒否 MAC アドレス)にリストされているデバイスを除き、すべてのクライアントデバイスにアクセス権が付与されます。管理者は、Disable をチェックすることで、拒否された MAC アドレスが一時的にシステムに接続できるようにすることができます。
 - **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 アドレスを持つ RADIUS 要求を設定された RADIUS サーバに送信します。RADIUS サーバが受け入れる MAC アドレスのみが AP に関連付けることができます。ここでの RADIUS サーバ設定は、同じ VAP の WPA-Enterprise および 802.1X 設定と共有されることに注意してください。
- **Hotspot 2.0:** Hotspot 2.0 は、公衆 Wi-Fi 加入者により良い帯域幅とサービスを提供するために、Wi-Fi Alliance によって開始された Wi-Fi 認定パスポイントとも呼ばれます。Hotspot 2.0 機能は、サービスプロバイダとそのパートナーのみを対象としています。設定を完了するには、サービスプロバイダまたは当社のサービスチームにお問い合わせください。

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。設定パラメータは、選択した AP モデルによって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	☒	ACCEPT	ARP	ARP	To RF Card A	Edit
2	☐	DROP	BOOTPC	IPv4	To RF Card A	Edit
3	☒	ACCEPT	BOOTPS	IPv4	To RF Card A	Edit
4	☐	DROP	Broadcast	ALL	To RF Card A	Edit
5	☐	DROP	IAPP	IPv4	To RF Card A	Edit
6	☐	ACCEPT	IPv4 Multicast	IPv4	To RF Card A	Edit
7	☐	ACCEPT	IPv6 Multicast	ALL	To RF Card A	Edit
8	☒	DROP	All Multicast	ALL	To RF Card A	Edit
9	☐					Edit
10	☐					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

Rule name *

EtherType

Interface ☐ From ☒ To

Opcode

Source

MAC Address: Mask:

ARP IP: Mask:

ARP MAC: Mask:

Destination

MAC Address: Mask:

ARP IP: Mask:

ARP MAC: Mask:

Action ☐ Block ☒ Pass

Remark

- **State:** 各ルールを有効または無効にします。
- **Rule:** このルールの番号は、テーブル内の利用可能なファイアウォールルールの中でその優先順位を決定します。
- **Rule name:** 規則名称をここで指定できます。
- **EtherType:** ドロップダウンリストには、この規則に従うトラフィックの使用可能なタイプが表示されます。
- **Interface:** 目的のインタフェースで受信側/送信側の方向を示します。
- **DSAP/SSAP(ethertype が IEEE802.3 の場合):** 802.2LLC フレームヘッダーのフィールドにさらに指定できます。
- **Type(ethertype が IEEE802.3 の場合):** カプセル化トラフィックの種類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、IP アドレス/マスクは送信元 IP アドレス(ethertype が

- IPv4 の場合)、ARP IP/MAC および 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、IP アドレス/マスクは宛先 IP アドレス(ethertype が IPv4 の場合)、ARP IP/MAC および 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 から選択できます。
- **Remark:** この規則の注意事項は、ここで指定できます。

f) Firmware

ファームウェア機能には、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が用意されています。

システムは、新しいファームウェアをアップロードし、既存のファームウェアを削除し、ファームウェアを管理対象 AP にダウンロードするための AP のファームウェア管理をサポートします。AP のファームウェアバージョンは、統合されたバージョンである必要があることに注意してください。

Firmware Upload は、AP のファームウェアの現行バージョンを表示します。ここで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アップデートできます。アップロードするには、まず Add をクリックし、Browse してファイルを選択してから Upload をクリックします。

Add... Delete						
	Filename	AP Type	Version	Size	Checksum	Actions
☐	Edgecore_ECW5211-L_3.43.00-EN-E_1.32-1.9276.rom	ECW5211-L	3.43.00	6304078	d12806c08a4417cbae8265aede810571	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。
- **AP Type:** ファームウェアの AP 種別
- **Version:** ファームウェアのバージョン
- **Size:** ファームウェアのファイルサイズ
- **Checksum:** 自動的に検出されたファームウェアの OOCID。
- **Download:** Download を選択して、選択したファームウェアをローカルディスクに保存します。
- **Delete:** Delete を選択すると、選択したファームウェアが削除されます。

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、Selection 列の AP のチェックボックスをオンにして、選択した AP のファームウェアを個別にアップグレードすることも、同時にアップグレードすることもできます。なお、アップグレード前と次のバージョンは、システムに統合されているものでなければなりません。

AP Model ECW100

List

	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)は、AP(アクセスポイント)をワイヤレス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 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
Add

Move WDS Connection

Update Parent AP
Update Child AP
Move

Delete WDS Link

Delete

- **WDS Status:** Status には、WDS ツリーに追加された AP と、セキュリティおよびチャネル設定が表示されます。WDS は複数のツリーに設定できます。Edit を選択して、関連付けられた WDS ツリーの WDS connection settings を変更します。
- **WDS Update:** 以下の操作で WDS 接続をアップデートします。
 - **Add:** WDS がない子 AP との新しい WDS 接続を追加し、AP リストから親 AP 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含まれていない場合は、新しい WDS ツリーが追加されます。Edit を選択して、新しい追加された WDS ツリーの WDS connection settings を変更します。
 - **Move:** WDS から子 AP との WDS 接続を更新し、WDS で接続可能な親 AP を更新すると、子 AP と以前の親 AP の間の WDS 接続は削除されます。
 - **Delete:** 選択した AP のすべての WDS 接続が、その子 AP への WDS 接続を含めて削除され、有線接続されていない子 AP は到達不能になります。

i) Rogue AP Detection

デプロイされた環境で、管理対象外または悪意のある可能性のある AP を検出するように設計されています。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 をセンサーとして使用して非管理対象 AP を検索します。AP の BSSID、ESSID、Type、Channel、Encryption、およびレポート時間が表示されます。

The screenshot shows the 'General Configuration' tab with the following settings:

- Rogue AP Detection:** ☐ Enable ☒ Disable
- Scanning Interval:** 0 minutes
- Sensor List:** 0/1
- Trusted APs:** 0/40

Below this is the 'Rogue AP List' section, which includes a table with the following columns: No, Rogue AP BSSID, ESSID, Type, Channel, Encryption, and Report Time. The table is currently empty. Above the table are buttons for 'Add to Trusted AP List', 'Delete', and a search bar for ESSID. At the bottom of the list section, there is a pagination bar showing '(Total:0) First Prev Next Last Go to Page: (Page:1/1)' and a 'Row per Page: 10' dropdown.

- **General Config:** この設定アイテムには、このタブページ内で機能を有効にするためのスイッチが含まれています。つまり、Rogue AP Detection およびオプションの"Channel Switching"機能です。
- **Sensor List Config:** この設定アイテムには、現在管理されているすべての AP のリストがワイドエリアネットワーク AP マネジメントに含まれています。管理者は、不正なアクセスポイントを検索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:** この設定アイテムを使用すると、管理者は検出された不正なアクセスポイントの一覧を維持し、信頼できる AP として注釈を付けることができます。
- **Rogue AP List:** このウィンドウには、検出されたすべての不正なアクセスポイントが表示されます。それぞれの不正なアクセスポイントには、BSSID、チャンネル、暗号化、レポート時間などの関連情報が表示されます。ウィンドウの下部にあるラジオボタンから、このリストで選択した不正なアクセスポイントを信頼済み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:** このフィールドのユニットは分です。"Rogue AP Detection"を無効にする場合は 0 を入力し、"Rogue AP Detection"を有効にする場合は、検知間隔を 1~999 の整数で入力してください。

- **Sensor List Config**

- **AP Type:** ドロップダウンメニューには、選択可能な管理可能なモデルタイプが表示されます。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一覧表示されます。

管理者は、リストされている AP の 1 つ以上をチェックし、下部にある Apply ボタンをクリックして、これらの AP をスキャナとして指定できます。

- **Trusted AP Config**

- **BSSID:** 管理者は、このリストにある既知のトラステッド AP の BSSID を静的に割り当てることができます。AP がこのリストに入力されても、管理対象外である場合は、不正なアクセスポイントデバイスリストには表示されません。
- **Remark:** 管理者は、信頼できる AP に関連する追加情報を入力できます。

j) AP Load Balancing

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。システムが、事前定義されたしきい値を超える AP の関連クライアント数の発生を検出し、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、バランス機能がアクティブになり、過負荷 AP の送信電力が減少し、他の利用可能な AP の送信電力が増加します。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、グループしきい値と、AP 負荷分散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

Apply

Balance Interval

minute(s)

Cluster

0/3

Configure

Device List

Add to

None

Apply

AP Type

All AP

List

	Cluster	Device Name	MAC Address	IP Address	Power Level	Clients	Log
☐	None	123		192.168.123.123	Highest	Offline	View

- **Load Balancing:** この構成アイテムを使用すると、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、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:** 設定画面に入ると、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、すべての管理対象 AP が、グループ、名前、MAC、IP、パワーLv、ロードなどの関連情報とともにモデル名でソートされて表示されます。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どの AP グループに属しているかを示す Group 列があります。

2) Wide Area AP Management

a) AP List

リストには、種別、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、地理的な場所など、各管理対象 AP の情報が表示されます。このセクションの機能には、Delete、Add to Map、Backup Config、Restore Config、Upgrade、Applying Settings、およびリブートなどの操作も含まれます。

システムの管理下にあるサポートされているすべての AP が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 タブからサポート対象の AP を追加できます。AP が追加されると、このリストには、AP 種別、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、地理的な場所など、現在の管理対象 AP が表示されます。管理者は、各 AP の前にあるチェックボックスをオンにするか、トップチェックボックスをオンにしてすべての AP を一緒に選択することで、管理対象 AP を削除、マップに追加、設定の復元、設定のアップグレード、設定の適用、管理対象 AP のリブートを実行できます。

AP List

Type All ▼
 Status All ▼
 Tunnel None ▼
 Name ▼

Refresh Interval 30 seconds ▼

■	Type	Name	IP	MAC	Map	Template	Status	# of Users	Tunnel	AP Admin Web	CAPWAP	AP Ver.	Serial Number
---	------	------	----	-----	-----	----------	--------	------------	--------	--------------	--------	---------	---------------

管理対象リストに AP を追加した後、リストされた AP を管理するためにいくつかの操作を実行できます。

- **Go:** EWS Controller から Wide Area AP の設定をリモートで直接行うことはできません。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、リストされた AP のステータスがオンライン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 ▼

Refresh Interval 120 seconds ▼

■	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:** チェックした AP をリストから削除します。
- **Add to Map/Floor Plan:** 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、マップまたはフロアプランで選択した AP にマークを付けることができます。マッププロフィー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 の設定を EWS コントローラのストレージに保管されている.db ファイルにバックアップできます。バックアップファイルは、ダウンロードまたは削除のために Backup Config タブページの下に一覧表示されます。
- **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 Controller のストレージにローカルに保存されている.db ファイルを使用して、選択した AP の設定を復元できます。
- **Upgrade:** ポップアップウィンドウが表示されます。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)にローカルに保存されている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:** 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 管理者パスワードを変更したりするために、選択した AP に準備済みの WAPM テンプレートを適用します。
- **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:** 選択可能な列を持つ現行の 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、管理者がデバイス名と SNMP コミュニティを指定できる AP の属性編集ページに入ります。AP をマップにマークする場合、このページでは、地理的な場所、カバレッジ、関連リンクを設定し、マップに表示されるマーカーまたはアイコンイメージをカスタマイズすることもできます。
- **Edit(トンネルステータス):** OOCVAP のポート場所マッピングパラメータを設定します。管理者は、NAS 識別子を割り当て、管理対象 AP の完全なトンネル VAP ごとにサービスの IP プールを指定できます。

Main >> Devices >> Wide Area AP Management >> AP List に移動します。

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	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:** この項目には、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 を発行するために割り当てられる IP プールを指定できます。
- **User Limitation:** 管理者は、この VAP から 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 の場所 ID を説明する文字列を入力できます。

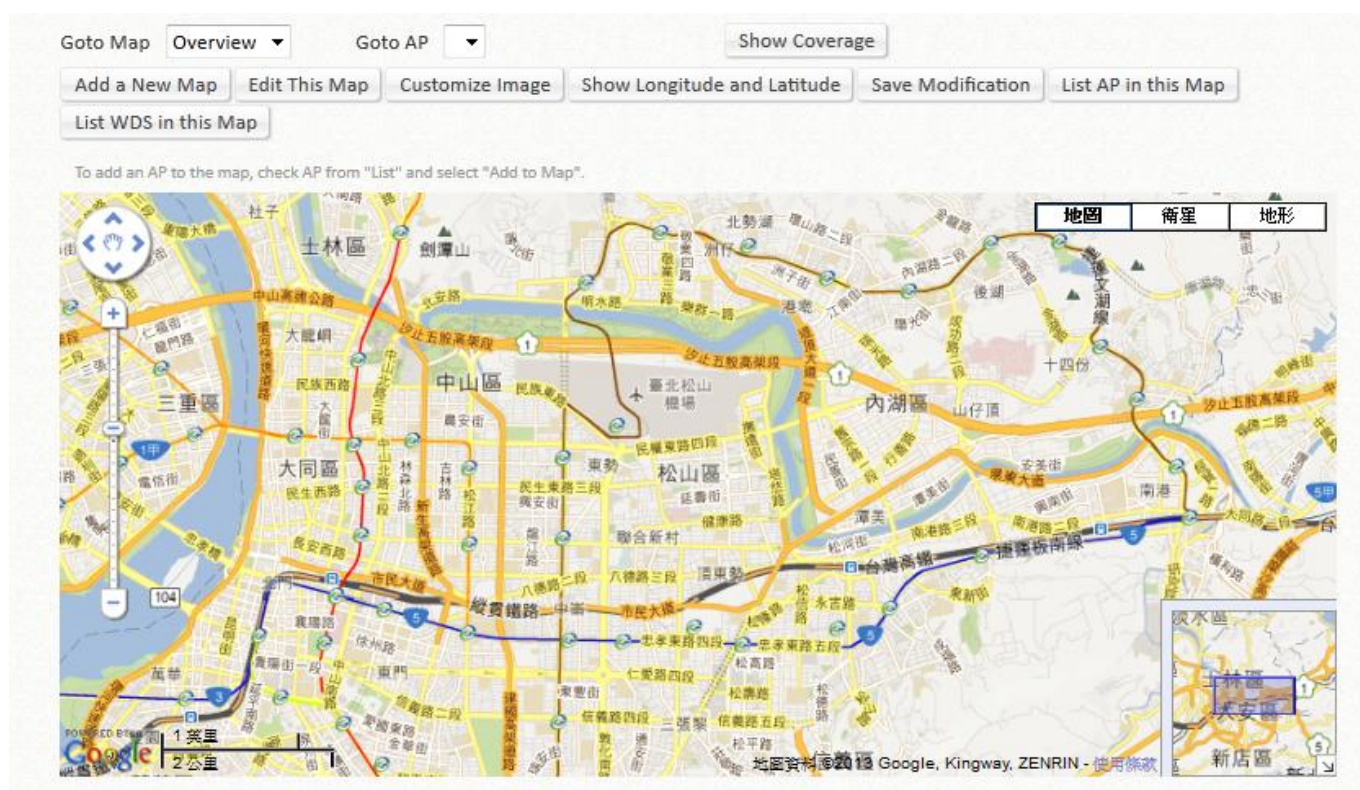
- **Room Description/ Location Name:** 管理者は、この VAP の場所の名前を説明する文字列を入力できます。
- **NAS Identifier:** 管理者は、追加の NAS ID を割り当てて、必要に応じてこの VAP と組み合わせることができます。

b) AP Grouping

Map Configuration

Map タブページは、Google Map API バージョン 3 で実装されています。これにより、管理者は Wide Area AP Management の下にあるすべての AP の場所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。

管理者が管理対象リストに AP を追加すると、次のように、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 AP の地理的な場所を表示したりできます。



マップの作成手順

- 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 インタフェースに設定します。
- ステップ 2:** Google マップ登録キーに適用します。
- ステップ 3:** マップ画面で Add a New Map を選択します。設定マップ名とレジストレーションキー。
- 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 ページから、作成したマップに AP を追加します。

AP 情報を使用してマップを設定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 管理で新しいマップを追加する前に、Google アカウントにサインアップするか、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できます。このアカウントは、Google マップ API v3 鍵の適用に使用されます。詳細については、<https://cloud.google.com/maps-platform/> の Google からの指示に従い、そのような Map API v3 キーを取得し、Map Configuration ページの "[Google Maps Registration Key](#)" 欄に

tony.chen@cipherium.com.tw | My favorites

Google code

Search

e.g. "ajax apis" or "open source"

★ Google Maps JavaScript API V2 ([Deprecated](#))

HomeDocsFAQArticlesBlogForumTerms

What is the Google Maps Javascript API?

Note: The Google Maps Javascript API Version 2 has been officially deprecated as of May 19, 2010. The V2 API will continue to work as per our [deprecation policy](#), but we encourage you to migrate your page to [version 3 of the Maps Javascript API](#).

The Google Maps API lets you embed Google Maps in your own web pages with JavaScript. The API provides a number of utilities for manipulating maps (just like on the <http://maps.google.com> web page) and adding content to the map through a variety of services, allowing you to create robust maps applications on your website.



How Do I Start?

1. [Sign up for a Google Maps API key](#).
2. Read the [Maps API Developer's Guide](#)
3. Read the [Maps API Reference](#).
4. Join the [announcements](#) group to receive important updates.

enter email

1. Your relationship with Google.

1.1 Use of the Service is Subject to these Terms. Your use of any of the Google Maps/Google Earth APIs (referred to in this document as the "Maps API(s)" or the "Service") is subject to the terms of a legal agreement between you and Google Inc., whose principal place of business is at 1600 Amphitheatre Parkway, Mountain View, California 94043, United States ("Google"). This legal agreement is referred to as the "Terms".

1.2 The Terms include Google's Legal Notices and Privacy Policy.

☒ I have read and agree with the terms and conditions ([printable version](#))

My web site URL:

Controller's WAN IP address

Tip: Signing up a key for <http://yourdomain.com> is usually the best practice, as it will work for all subdomains and directories. See this [FAQ](#) for more information.

Generate API Key

Thank You for Signing Up to Google Maps API Key!

Your key is:

```
ABQIAAAAKf_mMpRETFZUaDr5paUTBTQNSWw9wiT7VEiW-QmsIzKiVcN7BTEWPYnI5GqXOpgcOYJAEfkFgw6A
```

Note: for more information on the API key system, consult <http://code.google.com/apis/maps/faq.html#keysystem>.

How you use your key depends on what Maps API product or service you use. Your key is valid for use within the entire family of Google Maps API solutions. The following examples show how to use your key within the Maps API product family.

JavaScript Maps API Example

Within the JavaScript Maps API, place the key within the script tag when you load the API:

```
<script src="http://maps.google.com/maps?file=api&v=2&sensor=true_or_false&key=ABQIAAAAKf_mMpRETFZUaDr5paUTBTQNSWw9wiT7VEiW-QmsIzKiVcN7BTEWPYnI5GqXOpgcOYJAEfkFgw6A"></script>
```

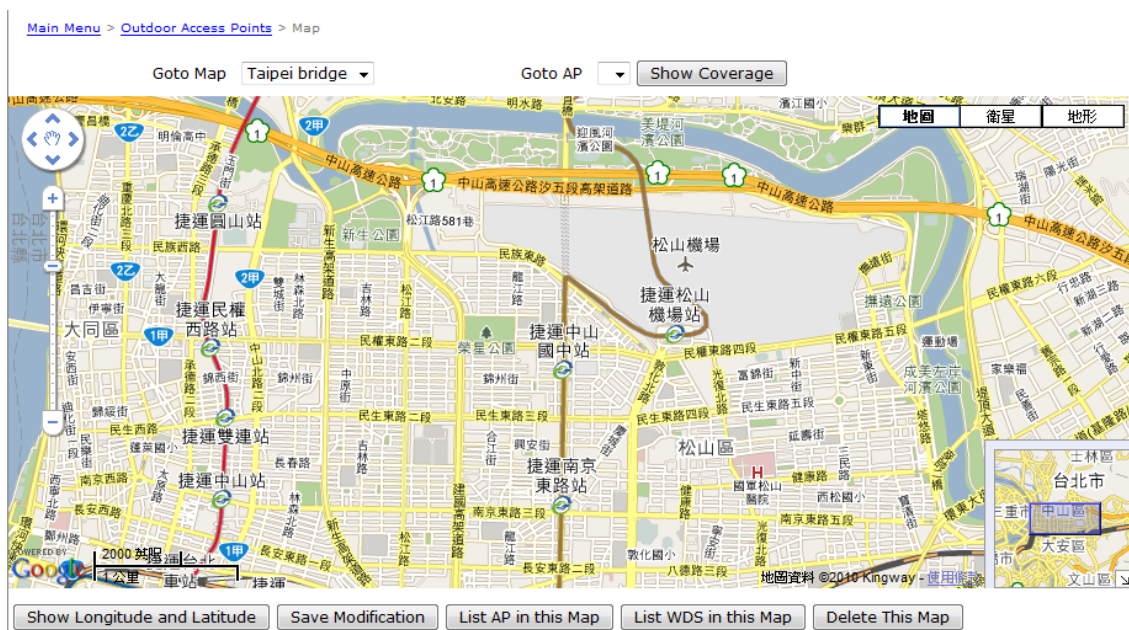
See [Loading the Maps API](#) in the JavaScript Maps API documentation for more information.

261

MAP Configuration

Map Name	Taipei Bridge
Latitude	25
Longitude	121
Google Maps Registration Key	AlzaSyDzjF1tWlf6158aJw7zGAxBYscY-L8Dtd8
Zoom Level	1
Map Type	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 と、Longitude と Latitude で定義されている地理的な場所を入力してください。また、Google が発行した Key も記入してください。最後に、Zoom Level と Map Type を選択し、SAVE を選択します。



上記のスクリーンショットは、地図名が台北ブリッジ、ズームレベルが 14、法線マップタイプの台北市を示す例です。

複数の AP が展開されていて、Wide Area AP Management の List にリストされている場合、それらの AP の地理的な場所を特定のマップ上でマークできます。

まず、List タブページに移動し、マップ上でマークする AP の Edit をクリックします。AP 設定ページで、この AP の座標(Latitude および Longitude)と信号カバレッジの半径を設定します。

Device : ECW5211-L

Device Name: ECW5211-L *

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

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

Latitude: 0.0 *-85 ~ 85

Longitude: 0.0 *-180 ~ 180

Remark:

Link 1: Name: , Description: , URL:

Link 2: Name: , Description: , URL:

Link 3: Name: , Description: , URL:

この AP をマークする座標を入力します。Link1～Link3 は、この AP に関連する追加情報を参照するためにマップ上のダイアログボックスに表示される http リンクを設定します。たとえば、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 Venue Web サイトの URL などです。

管理者は、マップに表示されるカスタマイズされたサムネイルイメージをアップロードできます。すべての設定を行い、画像をアップロードしたら、Apply を押して APList ページに戻ります。

マップ上でマークする AP を確認し、Add to Map/Floor Plan ボタンを選択し、これらの AP をマークするマップの名前を選択して、OK ボタンを選択します。

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	N/A

Add to Map - Google Chrome

⚠ 不安全 | https://10.71.36.101/OutdoorEquipmentManagement/AddToMap.shtml

Add to Map

Add AP(ECW5211-L)

☒ Add into a map

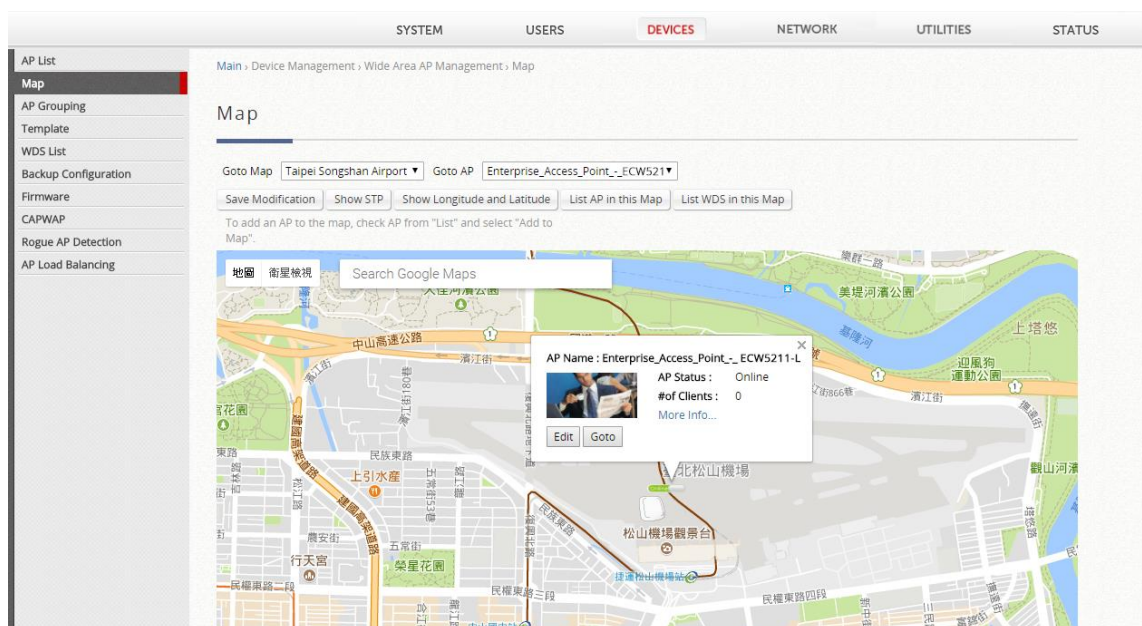
Select Map: Taipei

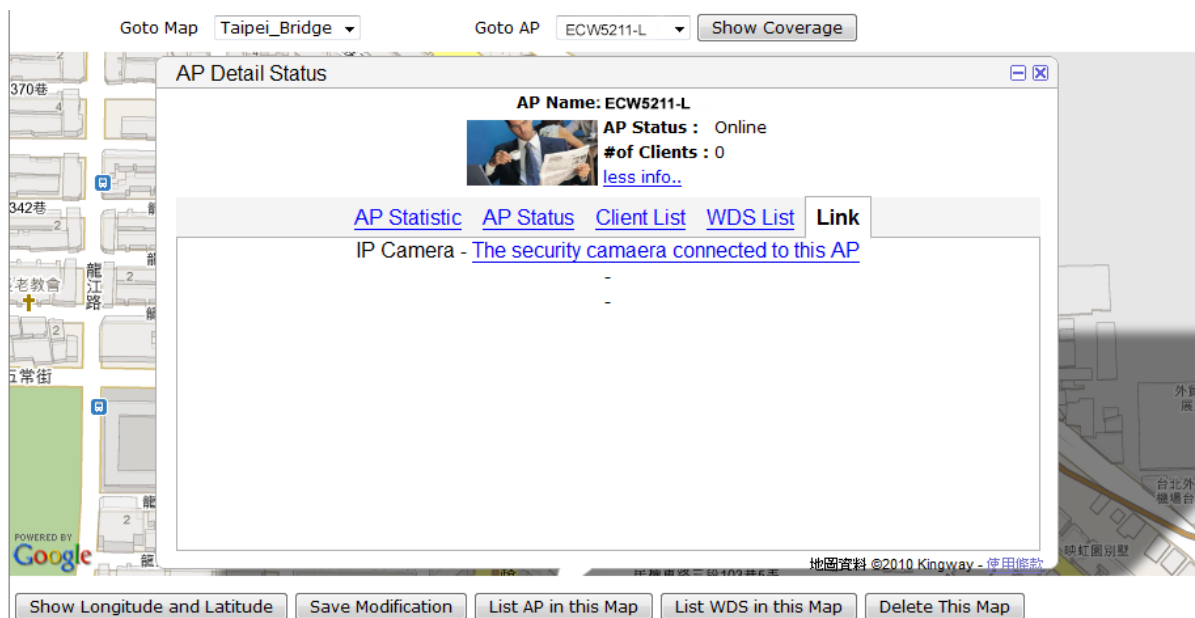
Apply Cancel

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ップ上にマーカーイメージとして表示されます。



AP アイコンをクリックすると、設定した追加情報またはリンクのダイアログボックスが表示されます。この AP に関連する AP status、Client List、WDS List および Links については、more info を選択してください。



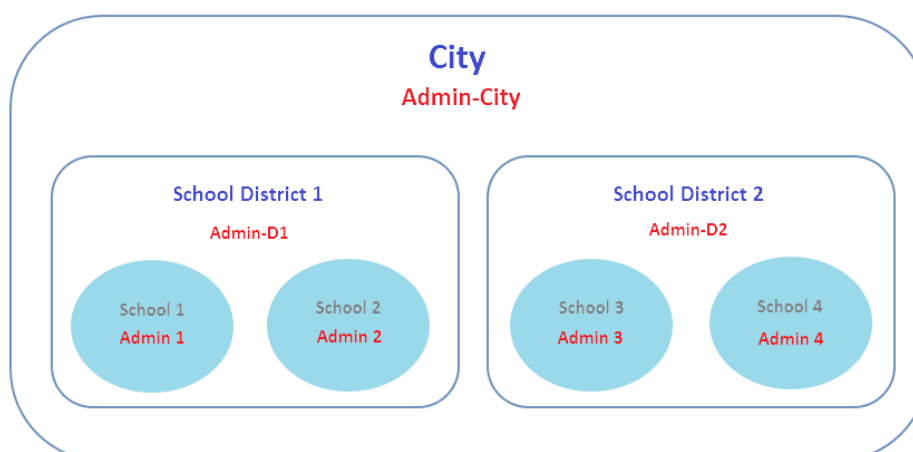


リストされた AP status、Client List および WDS List 情報は、リモート AP から SNMP を介して収集されます。

AP Grouping

ワイドエリア AP 管理では、すべての管理対象 AP をマップ別 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 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、マップは、異なる AP グループによって含めることができます。AP グループごとに異なる読み取り/書き込み権限を持つ異なる管理者グループを割り当てることができます。



Edgecore コントローラは、Google マップへの AP の追加をサポートしています。以下にプロセスを示します。

1. 一番下のページの Map List の 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フィールドに入力します。Apply を選択します。
2. AP の属性プロファイル(経度と緯度)に AP の配置場所を追加します。Main Menu>Devices>Wide Area AP Management>List - AP Attribute(Edit)
3. List 画面に戻り、AP を選択して Add to Map/Floor Plan を選択し、目的のマップを選択します。設定後、admin は選択したマップ上の AP のアイコンを表示できるようになります。

4. Overview path: "Main Menu>Devices>Wide Area AP Management>Map"
5. Main Menu>Devices>Wide Area AP Management>AP Grouping>AP Grouping List 移動して、AP グループを追加または削除します。

AP Grouping

■	AP Group	Map	Template
☐	456	123	☐ 1 ☐ 3 ☐ 5

6. Add をクリックして AP グループを追加すると、各 AP グループに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

Template2
 Template4
 Template5
 Template7
 Template8

Selected

Template1
 Template3
 Template6

7. AP グループが作成されたら、管理者グループを管理者グループリストに追加して、各 AP グループにアクセス権限を割り当てることができます。

Main > Utilities > Administrator Accounts > Administrator Group List

Administrator Group List

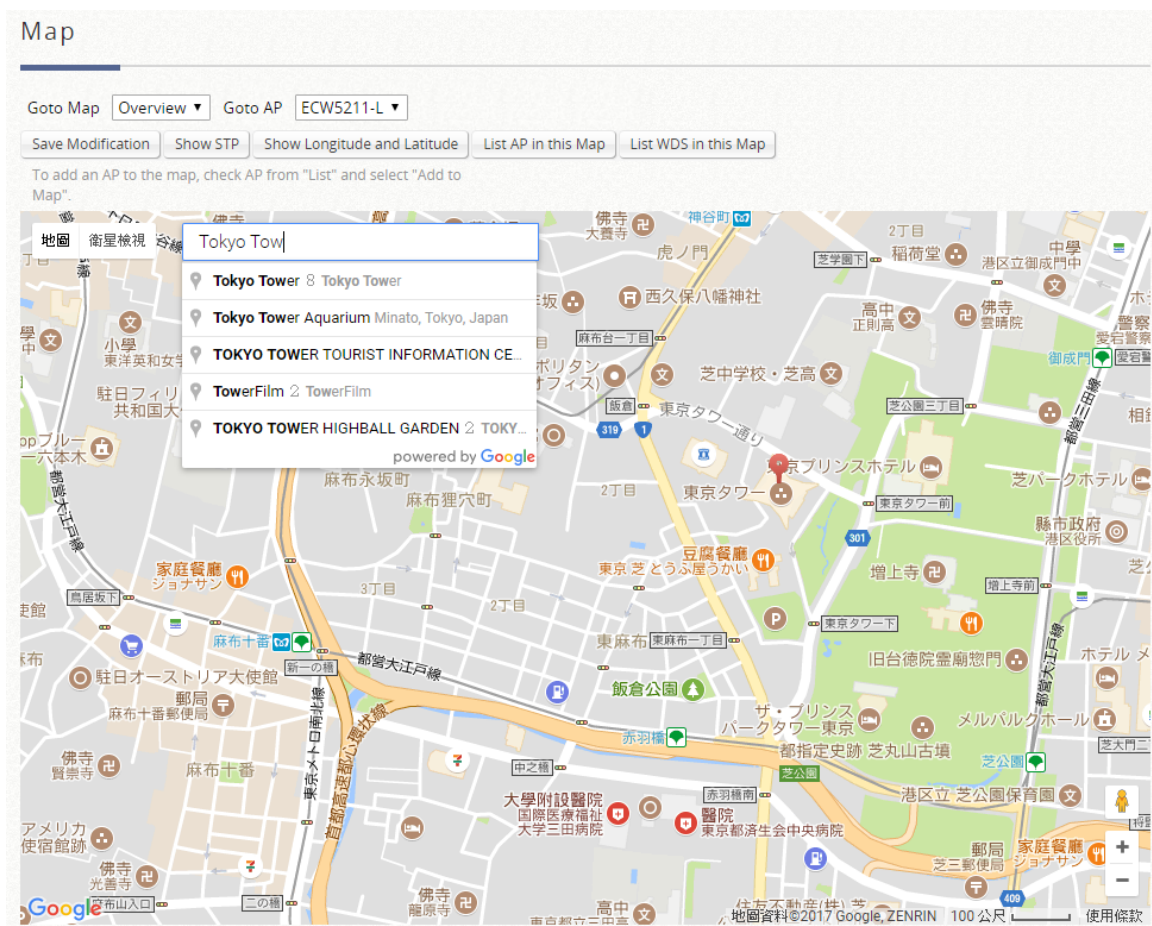
■	name	remark
☐	Super Group	remark
☐	Manager	remark
☐	Operator	remark
☐	On Demand	remark
☐	Custom 1	remark
☐	Custom 2	remark
☐	Custom 3	remark

8. AP グループへの権限の割り当て。

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

c) Map

マップには、管理対象 AP とその WDS リンクが Google マップに表示されます。これは、ワイヤレス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:** マルチマッププロファイルを設定すると、この機能により、さまざまなマップ間で切り替えることができます。
- **Goto AP:** この機能は、管理者が一覧から AP を選択するためのもので、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します。
- **Save Modification(オーバービューマップを除きます):** 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機能です。たとえば、元のマップを変更またはパンした場合、このボタンをクリックすると変更が保存されます。

- **Show Longitude and Latitude:** この機能を押すと、ポップアップウィンドウに地図の現在の中心点の経度と緯度が表示されます。
- **List AP in this Map:** このボタンをクリックすると、ブラウザ上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、マップに AP の一覧が表示されます。
- **List WDS in this Map:** このボタンをクリックすると、ブラウザ上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、マップに WDS リンクの一覧が表示されます。
- **Map/Satellite:** グラフィック表示または実際の衛星画像の表示を切り替えます。
- **Search:** 管理対象 AP を検索する代わりに、Google マップから場所を検索します。
- **Distance Calculation:** 選択した 2 つの AP 間の distance 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 を検出するためのものです。検出された AP を管理対象デバイスに追加し、定期的なステータス収集に使用される 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。AP を検出するには、AP 一覧から Add を選択し、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 を検出しようとする場合は、Device Type を選択します。次に、AP の現在の IP 範囲(ログイン ID とパスワード)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

Search

Device Type ECW100 ▼

Admin Settings Used to Discover

Start IP Address

End IP Address

Login ID

Password

Device Results

Add Delete

	Device Type	IP Address	Device Name	SNMP Community	SNMP Write Community	Map
--	-------------	------------	-------------	----------------	----------------------	-----

- **Start / End IP address:** 管理者は、AP 探索の IP アドレス範囲を指定する必要があります。また、指定された IP アドレスは、外部または内部ネットワーク IP アドレスにすることができます。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。指定された範囲内にない 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:** 対象の AP の管理インタ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 を検出しようとするときに、Device Type を選択します。次に、AP、Login ID、および Password のカレント IP 範囲を入力します。Discover を選択します。新しい AP が検出されると、次の Discovery Results list に表示されます。管理者は、検出処理中にいつでもコントローラのスキャンを停止できます。
- **Device Results:** 検出処理が完了すると、検出された AP がここに表示されます。管理者は Add をクリックすると、管理対象の AP をリストに登録できます。

- **Device Type:** 検出された AP の AP モデル。
- **IP Address:** 検出された AP の IP アドレス。
- **Device Name:** デバイス名を設定してデバイスを識別します。
- **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ストリング。
- **SNMP Write Community:** 設定変更で使用される SNMP 書き込みコミュニティストリング。
- **Map:** 階層管理またはグラフィカル・ビュー用に、特定のマップで管理対象デバイスを指定します。

e) Adding

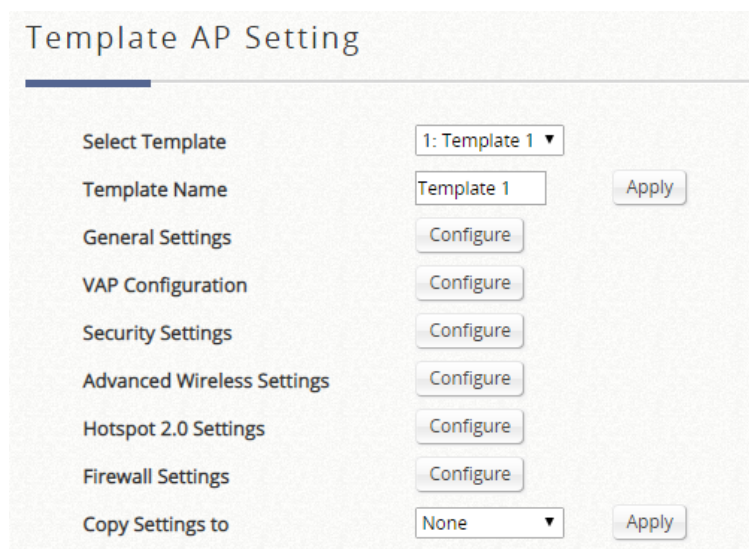
Adding 機能は、AP に必要な情報を入力して、AP を手動で設定するために使用します。

管理者は、管理リストに追加するために複数の AP を検索および一覧表示できる Discovery 機能のほかに、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、およびログインクレデンシャルを設定し、SNMP コミュニティストリングを設定し、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 テーブルに手動で追加できます。手動で追加された AP は、最初は AP リストに"offline"のステータスで表示されます。システムは、SNMP プロトコルによって AP に接続しようと試みます。SNMP 読み取りが成功すると、手動で追加した AP がオンラインになります。

- **Device Type:** ワイドエリアネットワーク AP の装置種別。
- **Device IP:** 管理リストに追加する AP の IP アドレス。
- **Device Name:** この AP デバイスに付けられたニーモニック名。
- **Login ID:** 本機のマネージメントインタフェースのログイン名です。
- **Password:** 本機のマネージメントインタ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ストリング。
- **SNMP Write Community:** 設定変更で使用される SNMP 書き込みコミュニティストリング。
- **Map:** 階層管理またはグラフィカル・ビュー用に、特定のマップで管理対象デバイスを指定します。

f) Template



Template AP Setting

Select Template	1: Template 1 ▼	
Template Name	Template 1	Apply
General Settings	Configure	
VAP Configuration	Configure	
Security Settings	Configure	
Advanced Wireless Settings	Configure	
Hotspot 2.0 Settings	Configure	
Firewall Settings	Configure	
Copy Settings to	None ▼	Apply

アクセスポイントのファームウェアバージョンに応じて、国番号を選択します。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 ▼ ☐ Pure 11n
Short Preamble	☐ Disable ☒ Enable
Short Guard Interval	☐ Disable ☒ Enable
Channel Width	20 MHz ▼
Channel	6 ▼
Antenna Mode	Max ▼
Transmit Power	Level 1 ▼
ACK Timeout	0 *(0 - 255, 0:Auto, Unit:4 micro seconds)
Beacon Interval	100 millisecond(s) *(100 - 500ms)
Airtime Fairness	☒ Disable ☐ Fair Access ☐ Preferred Access
Packet Delay Threshold	0 millisecond(s) *(100 - 5000ms, 0:Disable)
Idle Timeout	300 second(s) *(60 - 60000)
Band Steering	☒ Disable ☐ Enable ☐ Aggressive
Interference Detection	Adjacent Channel Utilization Threshold 0 % *(60 - 99, 0:Disable) Latency 10 second(s) *(10 - 999) Co-Channel Utilization Threshold 0 % *(60 - 99, 0:Disable) Invalid Packet Rate 90 % *(60 - 99) Latency 10 second(s) *(10 - 999)
WME Configuration	Configure
Transmission Rate Threshold	1001 kbps *(0:Disable)
CCA Minimum Power	☒ Auto ☐ Dense Deployment ☐ Sparse Deployment ☐ Other -95 *(≤ -75)
UAPSD	☐ Disable ☒ 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、選択するモードは異なります。802.11a、802.11b、802.11g、802.11a+802.11n、802.11b+802.11g、802.11g+802.11n、および 802.11ac です。
- **Short Preamble:** 56 ビットの同期フィールドを持つ短いプリアンプルを使用すると、無線 LAN の伝送効率が向上します。Enable を選択すると 128 ビットの同期フィールドで Short Preamble を使用し、Disable で Long Preamble を使用します。
- **Short Guard Interval(帯域が 802.11g+802.11n または 802.11a+802.11n の場合に使用可能):** ガードインターバルは、符号間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 で処理能力をさらに向上させるために、ショートガードインターバルは以前の半分の値です。ショートガードインターバルを使用するには Enable を、通常のガードインターバルを使用するには Disable を選択してください。
- **Channel Width(802.11g+n、802.11a+n、および 802.11ac のみ):** 20MHz、40MHz、または自動から選択します。スループットを向上させるために、40MHz までのダブルチャネル帯域幅がサポートされ

ています。802.11ac モードでは、80MHz を選択できます。

- **Channel:** ドロップダウンメニューから、ネットワーク設定に対応する適切なチャネルを選択します。"Auto"として設定され、Band が"802.11a"、"802.11a+n"、または"802.11ac"の場合、選択したチャネルが干渉されるか、DFS チャネル信号が検出されると、チャネルセレクトアテーブルが表示されます。
- **Antenna Mode(802.11g+n、802.11a+n、および 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、最大電力から 1dBm ずつ減少することを意味します。Level 1 は実際の最大電力、Level 2 は最大電力から 1dBm を引いた値などです。
- **Beacon Interval(ミリ秒):** 20~1000 ミリ秒の間で入力します。デフォルトは 100 ミリ秒です。入力される時間とは、アクセスポイントと無線ネットワーク間でビーコン信号が送信される頻度を意味します。
- **ACK Timeout:** ACK フレームの受信待ち時間です。インターバル内に ACK が受信されなかった場合、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または悪化します。
- **Airtime Fairness:** "Fair Access"に設定すると、帯域機能が異なるすべてのデバイスが同じエアタイムであることが保証されます。"Preferred Access"に設定すると、802.11n および 802.11ac クライアントが優先されます。この機能は、異なる帯域をサポートするデバイスがあるネットワークに最適です。
- **Packet Delay Threshold(ms):** 送信キューフラッシュメカニズムです。これは、パケットをドロップし、キューが x ミリ秒を超えて処理された場合にすぐに他のパケットを処理するためのメカニズムです。デフォルトでは無効です(=0)。
- **Idle Timeout(秒):** 非アクティブが設定された秒数(デフォルト=300 秒)に達すると、クライアントは切断されます。
- **Band Steering:** 有効にすると、5GHz 接続のクライアントは 5GHz 帯域に向けて 2.4GHz 帯域の輻射を低減します。これは、AP が 2 つの RF カードで 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 接続のクライアントは強制的に 5GHz 帯に接続されます。
- **Interference Detection:** 現在のチャネルまたは隣接するチャネルの使用率、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 は別のチャネルに切り替えます。
- **Transmission Rate Threshold:** 通信速度が設定したしきい値を下回ると、関連付けられたクライアントがキックされます。これにより、関連付けられているすべてのクライアントの接続速度が高速になります。
- **WME Configuration:** Wireless Multimedia Extensions(WME)は、Wi-Fi Multimedia(WMM)とも呼ばれ、IEEE802.11e 標準に基づく Wi-Fi Alliance 相互運用性認証です。IEEE802.11 ネットワークに基本的な Quality of service(QoS)機能を提供します。アクセス優先順位は、さまざまなパラメータを使用して設定できます。CW Min: Contention Window Minimum、CW Max: Contention Window Maximum、AIFS: Arbitration Inter Frame Spacing、TXOP Limit: Transmission Opportunity Limit。
- **UAPSD:** U-APSD は、WMM で動作する 802.11 省電力メカニズムである Unscheduled Automatic Power Save Delivery の略です。クライアントデバイスが省電力モード(つまり、レシーバの電源が切断され、データフレームを受信できません)の場合、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します。

➤ VAP Configuration

VAP Configuration - 1: Template 1

Profile Name	RF Card A : VAP-1 ▼
VAP	☐ Disable ☒ Enable
Profile Name	VAP-1
ESSID	Guest Network
Network Mode	Bridge ▼
VLAN ID	☒ Disable ☐ Enable
	VLAN ID *(1 - 4094)
CAPWAP Tunnel Interface	Disabled ▼
Service Schedule	24/7 Service ▼
Access Control Type	☒ Disable ☐ MAC ACL Allow List ☐ MAC ACL Deny List

- **VAP:** この VAP を Enable または Disable します。
- **Profile Name:** ID/管理を目的とした、特定の RF カードとその VAP のプロファイル名。
- **ESSID:** ESSID(拡張サービスセット ID)は、特定の VAP に関連付けるクライアントの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。
 - **Bridge モード:** VAP は透過的に動作します(つまり、NAT なし、DHCP なし)。これにより、クライアントデバイスに LAN 側の DHCP サーバからダイナミック 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 モード:** VAP は、この SSID に DHCP サーバが組み込まれている Network Address Translation (NAT)デバイスのように動作し、クライアント装置には、この SSID で設定された DHCP プールからダイナミック 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 で Kbps 単位で設定できます。帯域幅を無制限に制御するには、0 を設定します。VLAN が有効な場合にのみ設定可能です。同じ VLAN ID を持つ VAP には、同じアップリンク帯域幅制限が必要です。
- **Downlink Bandwidth:** ダウンリンク帯域幅制御は、VAP で Kbps 単位で設定できます。帯域幅を無制限に制御するには、0 を設定します。VLAN が有効な場合にのみ設定可能です。
- **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 関数を有効にするために、各 VAP は、1 から 4094 の範囲の有効な値を持つ一意の VLAN ID を与えられなければなりません。VLAN が有効になると、VAP で QoS がサポートされます。
- **CAPWAP Tunnel Interface:** AP とコントローラ間で確立された CAPWAP トンネルを通過する VAP のトラフィックを指定するには、ドロップダウンを選択します。CAPWAP トンネルインタフェースが Complete または Split トンネルの場合、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:** Complete-Tunnel または Split-Tunnel VAPs で、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:** デバイス(MAC アドレス)の一覧を設定して、VAP に関連付けることが許可されているデバイスを決定します。
 - **Disable:** クライアント装置からのアクセスに制限はありません。
 - **MAC ACL Allow List:** 一覧表示されているクライアント装置(MAC アドレス)のみにアクセス権が付与されます。

- **MAC ACL Deny List:** クライアント装置(MAC アドレス)には、拒否リストにリストされているデバイスに対するアクセス権が付与されます。

➤ Security Settings

Security Settings - 1: Template 1

Profile Name: RF Card A : VAP-1

Security Type: Open (selected from dropdown: Open, WEP, WPA-Personal, WPA-Enterprise, OSEN)

Buttons: Apply, Cancel

ドロップダウンメニューから目的の Security Type を選択します。ドロップダウンメニューには、Open、WEP、WPA-Personal、WPA-Enterprise と OSEN が含まれます。

➤ 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: ☐ Disable ☒ Enable

Wireless Station Isolation: ☐ Disable ☒ Enable

WMM: ☐ Disable ☒ Enable

IAPP: ☐ Disable ☒ Enable

Multicast-to-Unicast Conversion: ☒ Disable ☐ Enable

TX STBC: ☐ Disable ☒ Enable

Multicast/Broadcast Rate: 5.5M

Management Frame Rate: 5.5M

Receiving RSSI Threshold: -80 *(-95 ~ 0, 0:disable)

- **RTS Threshold:** 1～2346 の値を入力します。RTS (Request to Send) Threshold では、非表示ノードの問題を回避するためにフラグメントを送信する前に送信する要求(RTS)を発行するパケットサイズを指定します。データサイズが指定された値を超えると、RTS メカニズムがアクティブになります。RTS しきい値の設定を低くすると、多くのクライアントデバイスが AP に関連付けられている領域、またはクライアントが離れており、AP のみを検出し、相互には検出ししない領域で役立ちます。
- **Fragmentation Threshold(802.11a、802.11b、および 802.11g モード):** 256～2346 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、送信前に断片化されます(1 つのチャンクではなく複数の断片で送信されます)。値を小さくするとフレームは小さくなりますが、送信フレーム数は多くなります。

Fragmentation Threshold の設定を低くすると、通信状態が悪くなったり、大量の無線干渉により通信が妨害されたりするような場所で役立ちます。

- **DTIM Period:** 定期的なビーコン内で生成される DTIM Interval を指定した周波数で入力します。DTIM が大きいほど、ワイヤレス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、パケット送信がドロップされてからクライアントが送信範囲外であると判断するまでに、AP が試行する送信再試行の最大回数です。設定された回数の送信再試行が失敗すると、アクセスポイントはクライアントにキックして、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、SSID のブロードキャストが中止されます。SSID のブロードキャストが無効になっている場合、正しい SSID を持つデバイスのみ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、システムに関連付けられているすべてのステーションが隔離され、システムとのみ通信できます。
- **IAPP:** IAPP(Inter Access Point Protocol)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ためのプロトコルです。この機能を有効にすると、システムは関連する無線局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無線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:** マルチキャストからユニキャストへの変換が有効になっている場合、アクセスポイントはマルチキャストトラフィックをリクエストするポートにのみインテリジェントにトラフィックを転送します。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るため、ネットワークの非効率が発生します。
- **TX STBC:** STBC は、単一の RF レシーバ(非 MIMO)であっても信号対ノイズ比を改善できるようにする、MIMO トランスミッタ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。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無線クライアントの帯域幅が必要な場合、管理者はここで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カスタマイズできます。
- **Management Frame Rate:** この機能は、マネジメントフレームの帯域幅を制御します。レートが高いほど、伝送がカバーする範囲は短くなります。
- **Receiving RSSI Threshold:** 接続されているステーションの接続速度を速くするために、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

Hotspot 2.0 は、公衆 Wi-Fi 加入者により良い帯域幅とサービスを提供するために、Wi-Fi Alliance によって開始された Wi-Fi 認定パスポイントとも呼ばれます。Hotspot 2.0 機能は、サービスプロバイダとそのパートナーのみを対象としています。設定を完了するには、サービスプロバイダまたは当社のサービスチームにお問い合わせください。

➤ Firewall Settings

- **Proxy ARP:** 有効にすると、AP はダウンリンクステーションの代わりに ARP 要求に応答します。AP によって維持されている ARP テーブルは、AP アップリンクから ARP 要求を受信するとルックアップテーブルとして使用されます。逆に、プロキシ ARP がない場合、ARP 要求は AP の無線ネットワークにブロードキャストされ、ネットワークの非効率性を引き起こします。

➤ Linkyfi's Location Engine

Linkyfi は、公共の Wi-Fi ホットスポット向けに AVSystem によって設計されたプラットフォームです。EdgecoreAP は、位置追跡およびトラフィック解析のために専用の Linkyfi サーバと統合できます。

- **Real Time Location System:** 室内およびリアルタイムナビゲーション用の Linkyfi Real Time Location System (RTLS)サーバとの統合を有効にします。
- **DNS DPI:** DNS トラフィックを解析するために、Linkyfi DNS DPI サーバと統合できるようにします。

g) WDS List

このリストには、管理対象 AP に設定されている WDS リンク(Peer AP、Band、Channel、Security、TX Power、Link Speed、RSSI、TX Bytes、TX Packets、STP や Status など)が表示されます。

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	

リストにリストされている AP 間で確立されている場合、WDS リンクは、リンクの帯域とチャネル、セキュリティ設定(存在する場合)、および送信電力、バイト、パケットなどの関連情報とともにここにリストされます。

h) Backup Config

バックアップされた設定ファイルを使用して、List で AP の設定を復元できます。管理者が AP の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

☐	Device Type	Version	Size	Backup Time	File Name	Actions
☐	ECW5211-L	1.21.00	39947	2013/02/21 17:55:22	ECW5211-L	Download

また、自動的に Daily Backup することもできます。バックアップ時刻を 24 時間形式で設定すると、AP のバックアップ設定がその時間に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格納できます。Firmware タブページの管理者は、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して、AP List ページから簡単にリモート AP のアップグレードおよび復元操作を行うことができます。必要に応じて、このページの下にリストされている AP ファームウェアを 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。

AP Firmware List

Add...

Delete

☐	File Name	Device Type	Version	Size	Actions
--------------------------	-----------	-------------	---------	------	---------

j) CAPWAP

CAPWAP は、EWS コントローラがワイヤレス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。

Main > Device Management > Wide Area AP Management > CAPWAP

CAPWAP Configuration

CAPWAP Status ☒ Enable ☐ Disable

Apply Certificate to APs

Trusted Certificate Authority(CA)

IP Address For Control Channel

IP Netmask For Control Channel

Control Channel IP Range 100.64.144.1 ~ 100.64.145.253

Access Controller IP List

No.	IP Address	Remark
1		
2		
3		
4		
5		

- **CAPWAP Status:** CAPWAP 関数の構成状態 Enable を選択してアクセス EWS コントローラをオンにすると、CAPWAP がサポートする AP が管理対象 AP リストに自動的に追加されます。
- **Apply Certificate to APs:** この設定アイテムを使用すると、管理者は、AC と AP 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な場合、ネゴシエーションは失敗し、AP は自動的に管理対象リストに追加されません。
- **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ための、AC 側の IP アドレス。
- **IP Netmask For Control Channel:** 管理対象 AP の最大数に応じて、ネットマスクサイズを自動的に/手動で設定できます。
- **Control Channel IP Range:** AP 側に割り当て、通信する制御チャネルを確立するための IP プール。IP の数は、上記の制御チャネルの IP アドレスおよび IP ネットマスクで定義されています。
- **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 対応 AC を CAPWAP AP のバックアップ AC として静的に指定できます。この番号は、これらのバックアップ AC の AP への優先順位を指定します。元の AC がダウンしている場合、AP は最初に No.1 バックアップ AC への参加を試み、以下同様に続きます。

k) Rogue AP Detection

設置された環境で、管理対象外または悪意のある可能性のある AP を検出するように設計されています。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 をセンサーとして使用して非管理対象 AP を検索します。AP の BSSID、ESSID、Type、Channel、Encryption、および見つかった時間が表示されます。

General Configuration

Rogue AP Detection

☒ Enable ☐ Disable

Apply

Scanning Interval

0 minutes

Channel Switching

☐ Enable ☒ Disable

Sensor List

0/1

Configure

Trusted APs

0/40

Configure

Rogue AP List

Add to Trusted AP List

Delete

ESSID

Search

	No	Rogue AP BSSID	ESSID	Type	Channel	Encryption	Report Time
--	----	----------------	-------	------	---------	------------	-------------

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

l) AP Load Balancing

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。システムが、事前定義されたしきい値を超える AP の関連クライアント数の発生を検出し、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、バランス機能がアクティブになり、過負荷 AP の送信電力が減少し、他の利用可能な AP の送信電力が増加します。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、グループしきい値と、AP 負荷分散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 間で可能な限り均等にネットワーク負荷を分散します。

WAPM Load Balancing

Load Balancing ☐ Enable ☒ Disable

AP Distance meter(s)

Interval minute(s)

Threshold ☒ Number of Clients clients
☐ Number of Packets

Apply

Map Cluster Setting

Map

Cluster

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

- **WAPM Load Balancing:** この構成アイテムを使用すると、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:** 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す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が離れている AP は、同じグループと見なされます。
- **Interval:** このパラメータを使用すると、管理者は、コントローラが同じグループ内の各 AP のロードを確認し、必要に応じてロードバランシングを開始する間隔を指定できます。
- **Threshold:** このパラメータを使用すると、管理者は、クライアントのロード Number of Client またはトラフィックのロード Number of Packets を、AP のシステムロードの尺度として選択できます。管理者は、負荷分散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ーと AP を表示します。
- **Cluster:** このマップ上のクラスターの数を表示します。
- **Configure:** クラスターごとに AP ロードバランシング機能を有効/無効にします。
- **Create:** アクセスポイントの distance に応じて、カレントマップにクラスターを作成します。
- **Delete:** 現在のマップ上のクラスターを削除します。
- **Cluster and Device List:** スクロール可能なウィンドウには、すべての管理対象 AP が、グループ、名前、IP、電力レベル、負荷などの関連情報とともにモデル名でソートされて表示されます。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どの AP クラスターに属するかを示す Group 列があります。"View" ボタンをオフにすると、各 AP の AP 負荷分散のログが表示されます。

m) Third Party AP Management

デバイスタイプから THIRDPARTYAP 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 AP の IP アドレス、名前、および 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。

Add Method Add an AP ▾

Add an AP

Device Type 3rd Party AP ▾

Device IP 192.168.1.1 *

Device Name ThirdAP001 *

VLAN ID 1 *

サードパーティ AP の一覧を確認および管理するには、次の URL に移動します。Access Points >> Enter Wide Area AP Management >> List
 このサードパーティの AP をタイプリストから管理します。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 マップ機能およびすべてのマップ機能に配置することもできます。

3) Switches

Switches: 本機の管理に関する設定を行います。

a) Switch List

EWS コントローラは、Edgecore スイッチを管理できます。このリストには、システムの管理下にあるスイッチが表示されます。

Switch List

Status All ▾

Add Delete Restart Backup Restore

■	Name	Type	Status	IP address	MAC address	Total allocated/Used/Max supply power [W]	Switch UI
---	------	------	--------	------------	-------------	---	-----------

スイッチの名前はハイパーリンクとして表示されます。スイッチの設定(全般設定、PoE 設定、VLAN メンバシップ設定、ポート設定、PoE スケジュール)については、管理対象スイッチのハイパーリンクを選択します。
 AP の詳細ステータス情報(General Setting、PoE Setting、VLAN Membership Setting、Port Setting、PoE Schedule)については、各管理対象 AP の表示されているステータスのハイパーリンクをクリックします。

- **Add:** "Add"機能を使用して、必要な情報を入力してスイッチを設定します。リストにスイッチを追加すると、スイッチのステータスが"online"または"offline"になります。
- **Delete:** リストから削除したいスイッチを選択するには、対応するチェックボックスをクリックし、次に Delete ボタンをクリックします。
- **Restart:** リストから再起動するスイッチを選択します。対応するチェックボックスをクリックし、Restart をクリックします。
- **Backup:** "Backup"を選択すると、コントローラ上のスイッチ用の構成.db ファイルが保存されます。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をコントローラに保存する場合は、スイッチのチェックボックスをオンにし、Restore を選択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デフォルトテンプレートであり、削除することはできません。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ている"Configure"をクリックして、テンプレートの設定を入力します。PoE Schedule Template では、以下の設定が可能です。

- 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
☐	Sun	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Mon	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Tue	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Wed	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Thu	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Fri	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	Sat	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

- 適用先: 帯域、チャネル幅、送信電力など。

Apply to

Refresh

Switch Name ▼

☐	Port	PoE Mode	Connected Device	☐	Port	PoE Mode	Connected Device
☐	1			☐	13		
☐	2			☐	14		
☐	3			☐	15		
☐	4			☐	16		
☐	5			☐	17		
☐	6			☐	18		
☐	7			☐	19		
☐	8			☐	20		
☐	9			☐	21		
☐	10			☐	22		
☐	11			☐	23		
☐	12			☐	24		

既存の管理対象スイッチがオンラインであり、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 Apply を選択します。

管理者の参照用に、Remark セクションに追加の備考を追加することができます。

c) Backup Configuration

リストには、バックアップされた構成の概要が表示されます。管理者は、リストアのために構成ファイルをダウンロードすることができます。または、チェックボックスをオンにして、選択した設定ファイルを削除します。

Backup Configuration

Delete

☐	Device Type	Size	Backup time	File Name	Action
--------------------------	-------------	------	-------------	-----------	--------

E. Network

Network: セクションは、全ての回路網設定を構成するために使用されます。

1) NAT

アドレス変換機能は、DMZ(Demilitarized Zone)、Public Accessible サーバ、IP/Port 転送の 3 種類をサポートします。

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		WAN1 ▾		
2		WAN1 ▾		
3		WAN1 ▾		
4		WAN1 ▾		

システムは、スタティック割り当ての内部 IP アドレス(LAN)と外部 IP アドレス(WAN)のマッピングの設定をサポートします。自動 WAN IP 割り当ての外部 IP アドレスは、WAN1 インタフェースが動的の場合に動的に変化する外部インタフェース(WAN1)の IP アドレスです。Assign WAN IP Automatically にチェックを入れると、入力した内部 IP アドレスが WAN1 インタフェースにバインドされます。それぞれの Static Assignment は、選択した外部インタフェース、WAN1、または WAN2 でバインドできます。利用可能なスタティック Internal IP Address と External IP Address の設定があります。Internal、ExternalIP アドレスが設定されます。設定後、WAN にアクセスすると、内部 IP アドレスにアクセスするようにマッピングされます。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。

Public Accessible Servers

Public Accessible Server

Enable	No.	External Port	Local Server IP Address	Local Server Port	Type	Remark
☐	1				☒ TCP ☐ UDP	
☐	2				☒ TCP ☐ UDP	
☐	3				☒ TCP ☐ UDP	
☐	4				☒ TCP ☐ UDP	
☐	5				☒ TCP ☐ UDP	
☐	6				☒ TCP ☐ UDP	
☐	7				☒ TCP ☐ UDP	
☐	8				☒ TCP ☐ UDP	
☐	9				☒ TCP ☐ UDP	
☐	10				☒ TCP ☐ UDP	

Public Accessible Servers を使用すると、管理者は仮想サーバを設定して、管理対象ネットワーク外のクライアント装置が管理対象ネットワーク内のこれらのサーバにアクセスできるようになります。仮想サーバは、TCP サービスや UDP サービスなど、物理サービスのセットごとに構成できます。External Service Port、Local Server IP Address、Local Server Port 入力し、種類を TCP、UDP から選択します。有効(Enable)で、有効にするサーバを選択します。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。

Port & IP Forwarding

Port and IP Forwarding

No.	Destination		Translated to Destination		Type	Remark
	IP Address	Port	IP Address	Port		
1					☒ TCP ☐ UDP	
2					☒ TCP ☐ UDP	
3					☒ TCP ☐ UDP	
4					☒ TCP ☐ UDP	
5					☒ TCP ☐ UDP	
6					☒ TCP ☐ UDP	
7					☒ TCP ☐ UDP	
8					☒ TCP ☐ UDP	
9					☒ TCP ☐ UDP	
10					☒ TCP ☐ UDP	

この機能を使用すると、管理者は、リダイレクトのために IP アドレスの特定のセットを最大でも設定できます。ユーザがここにリストされている宛先 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 の IP Address と Port、Translated to Destination の IP Address と Port を入力し、サービスの種類として TCP または UDP を選択してください。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 関数では、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オンラインステータスを電子メールで定期的に報告できます。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 モードで運用されている場合、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	
2	http ▾		Create	
3	http ▾		Create	

3) Walled Garden and Walled Garden Ad

本関数では、ユーザがログインや認証を行う際に、ここに記載されている Web サイトにアクセスするためのサービスを無料で提供しています。このリストでは、Web サイトの特定のアドレス名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がないユーザでも、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 Web サイトの IP Address または Domain Name 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一覧は、バックアップまたは復元することができます。

Walled Garden List

200 entries can be added to the Walled Garden List.
40 advertisement entries can be displayed on the user login page.

Add Delete Backup Walled Garden List Restore Walled Garden List

No.	Domain Name/IP Address/URL	Walled Garden / Advertisement
-----	----------------------------	-------------------------------

(Total:0/200) ⚡First ⚡Prev Next⚡ Last⚡ Go to Page (Page:1/1) Row per Page: 50 ▾

Walled Garden Advertisements は、クライアントがアクセスするためのアドバタイズメントリンクで、システムによって認証されます。たとえば、ホテルのネットワークアクセス権を持たないゲストは、これらのサイトに無料でアクセスできます。

200 件までのウォールドガーデンエントリがサポートされ、200 件のうち 40 件をウォールドガーデンアドバタイズメントとして選択できます。

Add Walled Garden List

Domain Name/IP Address/URL:	
Walled Garden	Advertisement
Active: ☐	Display: ☐
Service Zone: All ▼	Protocol: http ▼
Remark:	Topic:
	Description:

- Add をクリックして、新しいエントリを追加します。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 を選択すると、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、サービスゾーンの設定に対応するアドバタイズメントハイパーリンクがログインページに表示されます。

ウォールドガーデン Ad として選択されたエントリは URL である必要があり、プレフィックス付きの 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アドバタイズメント機能を有効にするには、ウォールドガーデンとアドバタイズメントチェックの両方のチェックボックスをオンにする必要があることに注意してください。

4) VPN

このタブでは、システムでリモート VPN とサイト間 VPN の 2 タイプの VPN を使用できます。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 トンネルが iKEv2 を介したデータ転送を暗号化できるようにします。サイト間 VPN では、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	☐
Server 2	RADIUS	.	☐
Server 3	NTDOMAIN	ntdomain	☐
Server 4	LDAP	ldap	☐
Server 5	POP3	pop3	☐

Site-to-Site VPN

Local Sites

	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
--	-----	-------------------	-----------------	--------------------	--------------------	---------------

Remote Sites

	No.	Name	IP Address	Pre-shared Key
--	-----	------	------------	----------------

5) Proxy Server

内蔵プロキシサーバと外部プロキシサーバ機能を備えています。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に戻ります。

基本的に、プロキシサーバは、クライアントがネットワークリソースにより迅速にアクセスするのに役立ちます。ここでは、EWS CONTROLLER のプロキシサーバ設定を構成するための基本的な例を示します。

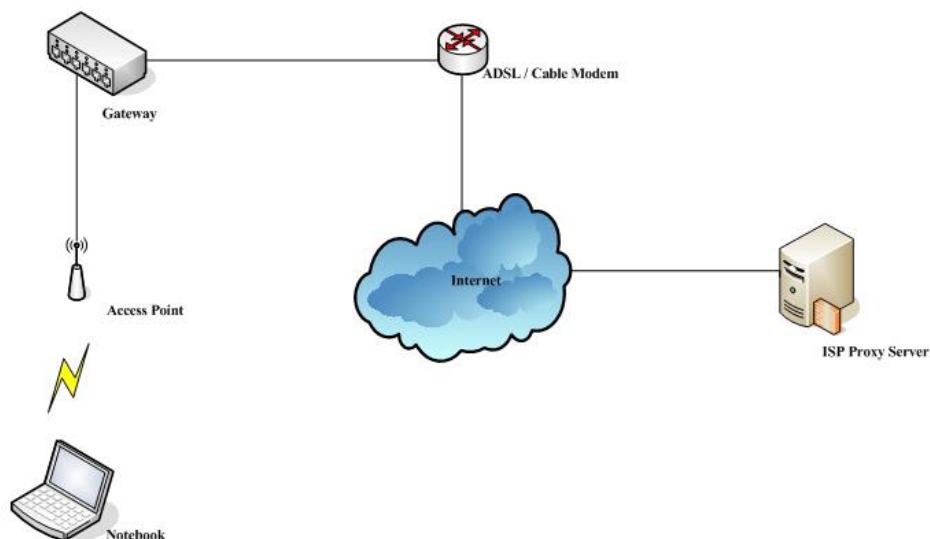
Web Proxy Settings

Proxy Server

☐ Enable Built-in ☒ Disable Built-in ☐ External

■ Using Internet Proxy Server

本機に内蔵されているプロキシサーバは、プロキシサーバが LAN 環境外やインターネット上にあっても有効にすることができます。たとえば、次の概略図は、プロキシサーバがどのように使用されるかを示しています。



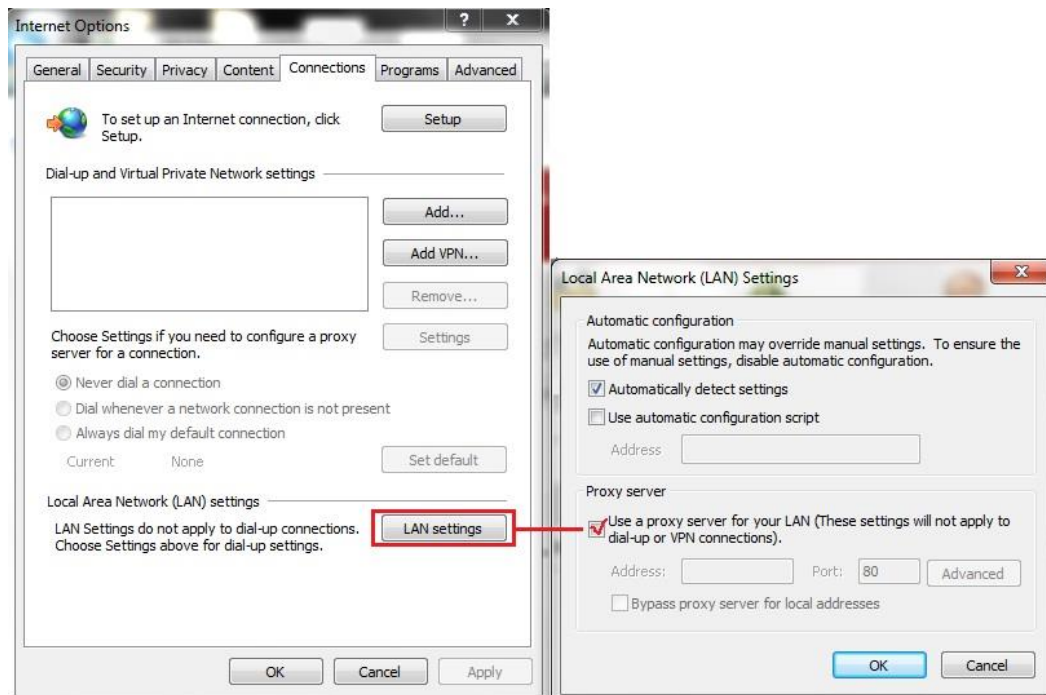
次の手順に従って、プロキシ設定を完了します。

- Step 1.** 管理者アカウントを使用してログインします。
- Step 2.** Network >> Proxy Server >> Web Proxy Settings ページ
Built-in Proxy Server を有効にします。Apply を選択して設定を保存します。

Web Proxy Settings

Proxy Server ☒ Enable Built-in ☐ Disable Built-in ☐ External

- Step 3.** Client Stations のインターネットオプションでプロキシサーバ設定を有効にします。



内蔵プロキシサーバを有効にすると、すべてのトラフィックがコントローラのローカルプロキシサーバに転送されます。

■ Using an External Proxy Server

外部プロキシサーバを指定するには、外部オプションを選択し、プロキシサーバの適切な IP アドレスと使用されている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ます。

- Step 1.** 管理者アカウントを使用してログインします。
- Step 2.** Network >> Proxy Server >> Web Proxy Settings. プロキシサーバで External を選択します。プロキシサーバの IP アドレスとポート番号を外部プロキシサーバ設定に追加します。Apply を選択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

10.168.1.100

External Proxy Port

6588

- Step 3.** Client Stations のインターネットオプションでプロキシサーバ設定を有効にします。

注意事項

プロキシサーバを有効にすると、クライアントステーションのインターネットオプションでプロキシサーバ設定を手動で確認する必要があります。Transparent Proxy を適用するには、Port and IP 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の 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。この機能を使用して、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することができます。

Local DNS Records Configuration

DNS time-to-live

120

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		
2		
3		
4		

7) Dynamic Routing

この関数は、RIP、OSPF と IS-IS の 3 つのダイナミックルーティングプロトコルをサポートします。

- ISIS 構成:** 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のグループ、または同様のデバイス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。それぞれのインタフェース回線種別をレベル 1 またはレベル 2 に設定できます。

IS-IS

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: ISO アドレスネットワークエンティティタイトル(NET)です。
NET は、IP アドレスと同様に、ネットワーク間でルータを一意に識別するために使用されます。
- Route Level: レベル 1 のシステムは、エリア内を経路情報します。宛先がエリア外にある場合は、レベル 2 のシステムに経路情報します。レベル 2 の中間システムは、エリア間および他のルーティングドメインに経路情報します。それぞれのインタフェースの階層型を割り当てることができます。
- **OSPF 構成:** 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ルーティングプロトコルです。それぞれのインタフェース領域、スタブ、および認証を設定できます。

OSPF

Function ☒ Enable ☐ Disable

Setup Table

Interface	Status	Area	Stub	Authentication
WAN1	Enabled		☐	None ▾
WAN2	Disabled		☐	None ▾
Default	Enabled		☐	None ▾
SZ1	Disabled		☐	None ▾
SZ2	Disabled		☐	None ▾
SZ3	Disabled		☐	None ▾
SZ4	Disabled		☐	None ▾
SZ5	Disabled		☐	None ▾
SZ6	Disabled		☐	None ▾
SZ7	Disabled		☐	None ▾
SZ8	Disabled		☐	None ▾

☐ Advertise as default gateway

☐ Advertise Global Policy Route

☐ Re-distribute RIP

- Area: エリアは、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。エリア 0 はバックボーンエリアと呼ばれ、レベルの最上位にあり、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 外部アドバタイズメントがフラッディングされないエリア。
- Authentication: OSPF ネイバーの認証を許可します。認証方式 none は、OSPF に認証が使用されておらず、デフォルト方式であることを意味します。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隣接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経路情報を隣接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が配信されます。

- **OSPF v3 構成:** IPv6 ダイナミックルーティング構成

OSPF v3

Function

☒ Enable
☐ Disable

Setup Table

Configuration

Interface	Status	Area
WAN	Disabled	
Default	Enabled	
SZ1	Disabled	
SZ2	Disabled	
SZ3	Disabled	
SZ4	Disabled	
SZ5	Disabled	
SZ6	Disabled	
SZ7	Disabled	
SZ8	Disabled	

☐ Advertise Global Policy Route

- **RIP 構成:** ローカルおよびワイドエリアネットワークで使用するダイナミックルーティングプロトコルです。それぞれのインタフェースを受動バージョンまたはサポートバージョンに設定し、認証を行うことができます。

RIP

Function

☒ Enable
☐ Disable

Setup Table

Configuration

	Status	Passive	Version	Authentication
WAN1	Enabled	☐	Both ▼	None ▼
WAN2	Disabled	☐	Both ▼	None ▼
Default	Enabled	☐	Both ▼	None ▼
SZ1	Disabled	☐	Both ▼	None ▼
SZ2	Disabled	☐	Both ▼	None ▼
SZ3	Disabled	☐	Both ▼	None ▼
SZ4	Disabled	☐	Both ▼	None ▼
SZ5	Disabled	☐	Both ▼	None ▼
SZ6	Disabled	☐	Both ▼	None ▼
SZ7	Disabled	☐	Both ▼	None ▼
SZ8	Disabled	☐	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 パケットがパッシブとしてチェックされている場合、RIP パケットはネットワークインタフェースから送信されません。
- **Version:** このインタフェースの 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、RIP パケットはブロードキャストとマルチキャストの両方を使用します。
- **Authentication:** RIP ネイバーの認証を許可します。認証方式 none は、RIP に認証が使用されておらず、デフォルト方式であることを意味します。RIP 認証が有効になっているインタフェースでの認証の 2 つのモード (プレーンテキスト認証と MD5 認証)。
- **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隣接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経路情報を隣接ノードに通知します。
- **Redistribute OSPF:** 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する場合は、このオプションをオンにします。
- **RIP Timer:**
 - ◆ **Update timer:** ルーティング情報の即時更新を要求するシステムを秒単位で指定します。
 - ◆ **Timeout Timer:** 経路情報は限られた期間だけルーティングテーブルに保存されます。経路情報がルーティングテーブルにインストールされるたびに、特別なタイムアウトタイマが開始されます。ルータは、その経路情報に関する別の RIP 応答を受信するたびに、経路情報は "refreshed" と見なされ、タイムアウトタイマがリセットされます。このタイマの有効期限が切れると、経路情報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不正な経路情報を消去するまでの秒数を指定します。

8) DDNS

この機能を有効にする前に、動的 DNS プロバイダに動的 DNS ホスト名を登録しておく必要があります。EWS CONTROLLER は、WAN ポートのダイナミック IP アドレスからスタティック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 サーバの IP アドレスが定期的にアップデートされます。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。
- **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)。
- **Password/Key:** DNS プロバイダの登録パスワード。

9) Client Mobility

- **IP PNP:** この機能を有効にすると、スタティック/DHCP IP、DNS、および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アクセスを取得できます。
- **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 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:** 設定マスタノードでは、1 台のマスタが最大 15 個のスレーブノード設定をアクティブできます。

Cross Gateway Roaming

Mode ☐ Disable ☒ Master Mode ☐ Slave Mode

Status

Slave Nodes Setting	No.	Active	Remote IP Address *	Secret Key *	Remark
	1	☐			
	2	☐			
	3	☐			

- **Slave Node:** スレーブノードの設定中に、そのマスタノードの設定を入力します。

Cross Gateway Roaming

Mode ☐ Disable ☐ Master Mode ☒ Slave Mode

Status

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、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、サービスの再起動、ネットワークユーティリティ、および証明書を変更する関数について説明します。

1) Administrator Account

これを使用して、管理者アカウントの作成、編集、削除、および確認を行うことができます。

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、admin Name 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。また、"Elementary School's Name"欄には、管理者のユーザ名や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。電子メールと小学校の名前は両方とも空であるか、両方とも記入することに注意してください。

Generate Admin Account

Admin Username

*

Password

*

Confirm Password

*

Email

Elementary school's name

Assign SMTP server

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

Super Group

また、管理者は別の権限で他の管理者アカウントを作成することもできます。

Administrator Accounts

Add ...DeleteLock AdminUnlockBackup ListRestore List

	Name	IP Address	MAC Address	Group	Status
☐	admin	10.28.128.188	0A:1F:D4:00:DA:D1	Super Group	Current Page: /Utilities/MlaUser.shtml
☐	admin	10.30.42.168	0A:1F:D4:00:DA:D1	Super Group	Current Page: /SystemConfiguration/ServiceZoneConf.shtml?sz_id=0

管理者には、自分のパスワードを変更したり、管理者リストにアカウントを追加して(管理者の一部を)担当する権限があります。

General Settings

Password Complexity

☒ Enable ☐ Disable

Min Password Length * (2~20)

Min Password Category * (2~4)

Limit Login Attempts

☒ Enable ☐ Disable

Block access after * tries

Password Expiration

☒ Enable ☐ Disable

Password expires * day(s) after creation

Password Limits

☒ Enable ☐ Disable

Users to choose passwords different from their past * passwords

Access Permission

[Configure](#)

- **Password Complexity** を使用すると、管理者は、サブ管理者が使用するパスワードの作成方法を制限できます。
Min password Length は、パスワードストリング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どれくらい複雑であるかを定義できます。各番号の意味を以下に示します。

数	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 つの形成(大文字/小文字/数字/特殊文字)を含めること。
2	パスワードには、少なくとも 2 つの形成を含めること。
3	パスワードには、少なくとも 3 つの形成を含めること。
4	パスワードには、少なくとも 4 つの形成を含めること。

- **Limit Login Attempts(有効な場合)**: サブ管理者がパスワードを再試行する回数を入力します。この数を超えて試行すると、サブ管理者は文字列を再度入力することができなくなります。
- **Password expiration(有効な場合)**: これは、パスワードの有効期限が切れる日数を管理者が決定するための機能です。有効期間は、最初のログインから数えて、パスワードごとに定義できます。パスワードの有効期限が切れると、オペレータは今後使用する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の数を確認する必要があります。たとえば、admin が 5 と入力すると、新しく追加されたパスワードが最新の 5 つのパスワードのいずれかと同じかどうかを確認されます。同じ場合、サーバは管理者に新しいパスワードストリングを再度選択するように要求します。

■ Sub-admin creation

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 Super Group

[Assign SMTP server](#)

Generate テーブルに移動して、サブ管理を作成し、その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、電子メールと小学校名の両方を入力すると、割り当てられた電子メールアドレスにアカウント信用証明情報が電子メールで送信されます。電子メールリマインダを送信するには、SMTP サーバを設定する必要があることに注意してください。

Send Password

Username	
Elementary school's name	

(下位管理者には、Super Group、Manager、Operator、On-Demand Manager、Custom1、Custom2、Custom3 の 6 つのカテゴリがあります。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確認および変更します。'Super Group'の権限制限は変更できません。)設定が完了したら、Apply を押してリストへのアカウントを作成します。

Select Group Custom 2

Note: Left checkbox means Read-Write, right checkbox means Read-Only.

Permission Settings

Service Zone	☐ ☐ Select All ☐ ☐ Default ☐ ☐ SZ1 ☐ ☐ SZ2 ☐ ☐ SZ3 ☐ ☐ SZ4 ☐ ☐ SZ5 ☐ ☐ SZ6 ☐ ☐ SZ7 ☐ ☐ SZ8
Map	☐ ☐ Select All ☐ ☐ Overview ☐ ☐ EL
AP Management	☐ ☐ Select All ☐ ☐ Local Area AP Management ☐ ☐ Wide Area AP Management

- **The admin list** は、管理者が各管理アカウントの動態(オンライン管理者の人数と各サブ管理者の状態)を追跡するためのリストとして機能します。

Administrator Accounts

Add ... Delete Lock Admin Unlock Backup List Restore List					
☐	Name	IP Address	MAC Address	Group	Status
☐	admin	10.28.128.188	0A:1F:D4:00:DA:D1	Super Group	Current Page: /Utilities/MlaUser.shtml
☐	admin	10.30.42.168	0A:1F:D4:00:DA:D1	Super Group	Current Page: /SystemConfiguration/ServiceZoneConf.shtml?sz_id=0

作成されたサブ管理者のみを削除できることに注意してください。特定のサブ管理者が管理ページにアクセスできないようにするには、Lock または Unlock のチェックボックスをオンにします。また、admin は Name 列のハイパーリンクをクリックして、admins/sub-admins 関連の設定を編集することもできます。

2) Backup & Restore

システム設定のバックアップと復元に使用します。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 Backup を選択すると、現在のシステム構成が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されます。バックアップファイルは、現行のシステム設定とローカルユーザアカウントを保持します。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 ボタンをクリックすると、バックアップファイルをシステムに復元できます。

バックアップは FTP 経由で定期的に実行できます。この機能を有効にするには、Period Backup の Configure 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

Day
0
:
0

- Restore System Settings:** Browse を選択して db を検索します。コントローラによって作成されたデータベースバックアップファイルを Restore をクリックして、バックアップファイルが保管された時間と同じ設定に復元します。Keep WAN1 setting と Management IP Address List のオプションを選択して、リモートアクセス用の WAN1 設定を保持することができます。
- Reset to Factory Default:** Reset を選択すると、コントローラの出荷時のデフォルト設定が読み込まれます。

3) Certificates

このタブでは、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"欄には、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設定するには、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=mknghi.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。コントローラには組み込みのファクトリーデフォルト証明書(gateway.example.com)があり、これを削除することはできませんが、証明書をアップロードできます。"Regenerate"ボタンをクリックすると、一意の 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、該当する"View"ボタンをクリックし、"Get CERT"と"Get Key"をクリックして証明書と公開鍵をローカルディスクにダウンロードします。

System Certificate

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

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、プライベート使用のためにルート CA を生成できます。作成されたルート CA 証明書をダウンロードし、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、1 つの内部ルート CA 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	View Delete

Generate Root CA

Common Name

Email Address

Country Name

State or Province Name

Locality Name

Organization Name

Organization Unit Name

Key Type

RSA ▾

Key Length

512 ▾

Generate Certificate

Upload Root CA

Certificate

Browse...

Private Key

Browse...

Upload Files

ルート CA 証明書は、一致する秘密鍵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、内部的に発行された証明書に署名することができます。

Certificate Information

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/キーペアを Get CERT、Get KeyinView でダウンロードできます。

- Trusted Certificate Authorities

管理者は、自己署名証明書およびシステムのルート CA 以外に、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決済ゲートウェイまたは CAPWAP 対応 AP の証明書を認識し、信頼することを目的としています。

信頼できる CA をアップロードするには、browse をクリックし、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ます。

Trusted Certificate Authorities (CA)

Cert Name	Common Name	Operation
Certificate Authorities (CA)		
N/A	N/A	<button>View</button> <button>Delete</button>

Upload Trusted CAs

Certificate

Browse...

Upload Files

4) Network Utilities

Web ベースの Ping、Trace 経路情報、ARP テーブルなどのネットワークユーティリティがサポートされています。

Network Utilities

Type

☒ IPv4 ☐ IPv6 ☐ Sniff ☐ IP Discovery

Ping

Ping

Trace Route

Start Stop

ARPing

Interface WAN1 ▾ ARPing

VLAN ID

Find

ARP Table

Show

Status

Result

項目	説明
IPv4	▪ Ping: 管理者は、IP アドレスまたはホストドメインネームを使用してデバイスを検出し、デバイスが稼働しているかどうかを確認できます。 ▪ Trace Route: 管理者は、IP アドレスまたはホストドメインネームを使用して、ゲートウェイから宛先へのパケットの実際のパスを復元できます。 ▪ ARPing: 管理者は、特定の IP アドレスまたはドメイン名の ARP 要求を送信できます。 ▪ ARP Table: 管理者は、Address Resolution Protocol (ARP) で使用される IP から物理アドレスへの変換テーブルを表示できます。
IPv6	▪ Ping: 管理者は、IPv6 アドレスまたはホストドメインネームを使用してデバイスを検出し、デバイスが稼働しているかどうかを確認できます。 ▪ Trace Route 6: 管理者は、IPv6 アドレスまたはホストドメインネームを使用して、ゲートウェイから宛先へのパケットの実際のパスを復元できます。 ▪ Neighbor Discovery: 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ネーム上にある IPv6 ネイバーノードについて学習できます。 ▪ Neighbor Cache: ネイバーキャッシュ内のネイバー情報を管理するノード。この機能により、管理者は、システムのネイバーキャッシュに保存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	この機能を使用すると、コントローラは同じレイヤ 2 ネットワーク内に接続されている 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の機能を実行している場合、動作のステータスがここに表示されます。
Result	演算結果が表示されます。

5) Restart

Restart を選択して再起動します。点滅タイマーが終了するのを待ってから、もう一度 Web Management インタフェースにアクセスしてください。

Restart

Restart the system in Regular ▼ Mode

Reason for Restart :

6) System Upgrade

管理者は、Web 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 を選択してファームウェアファイルを検索し、Apply を選択してファームウェアアップグレードを行います。アップグレードプロセスが完了し、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後で再起動する必要があるまで、数分かかる場合があります。

FTP ファームウェアアップグレードもオプションです。FTP サーバ IP アドレス、FTP サーバポート、および FTP アカウント名とパスワードを入力し、システムのアップグレードに使用する FTP サーバに保存されている完了ファームウェアファイル名を最後に指定します。

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処理を実行します。ファームウェアのアップグレードが成功した後にシステムを再起動するように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。確認メッセージが表示されるまでお待ちください)

ファームウェアアップグレード後に出荷時のデフォルトにリセットするには、事前にシステムをリブート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		Browse...	Apply
Upgrade Firmware Via FTP	Anonymous	☒ Yes ☐ No	
	IP Address		Port
	File Name	File Name or Dir/File Name	
			Apply

G. Status

Status: システムステータス、インタ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、セッションリスト、ユーザログ、および通知設定に関する情報を提供します。

1) System Summary

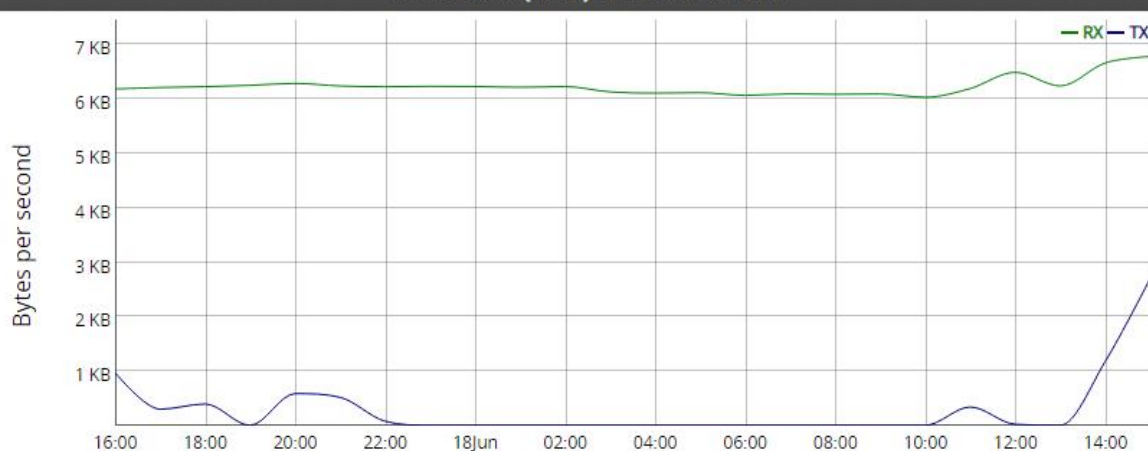
システムの現在の設定の表示。

システムの概要は、管理者のためにここに記載されています。

System Summary

[See Reports](#)

Network Traffic (WAN1) for the Last 24 Hours



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
		N/A

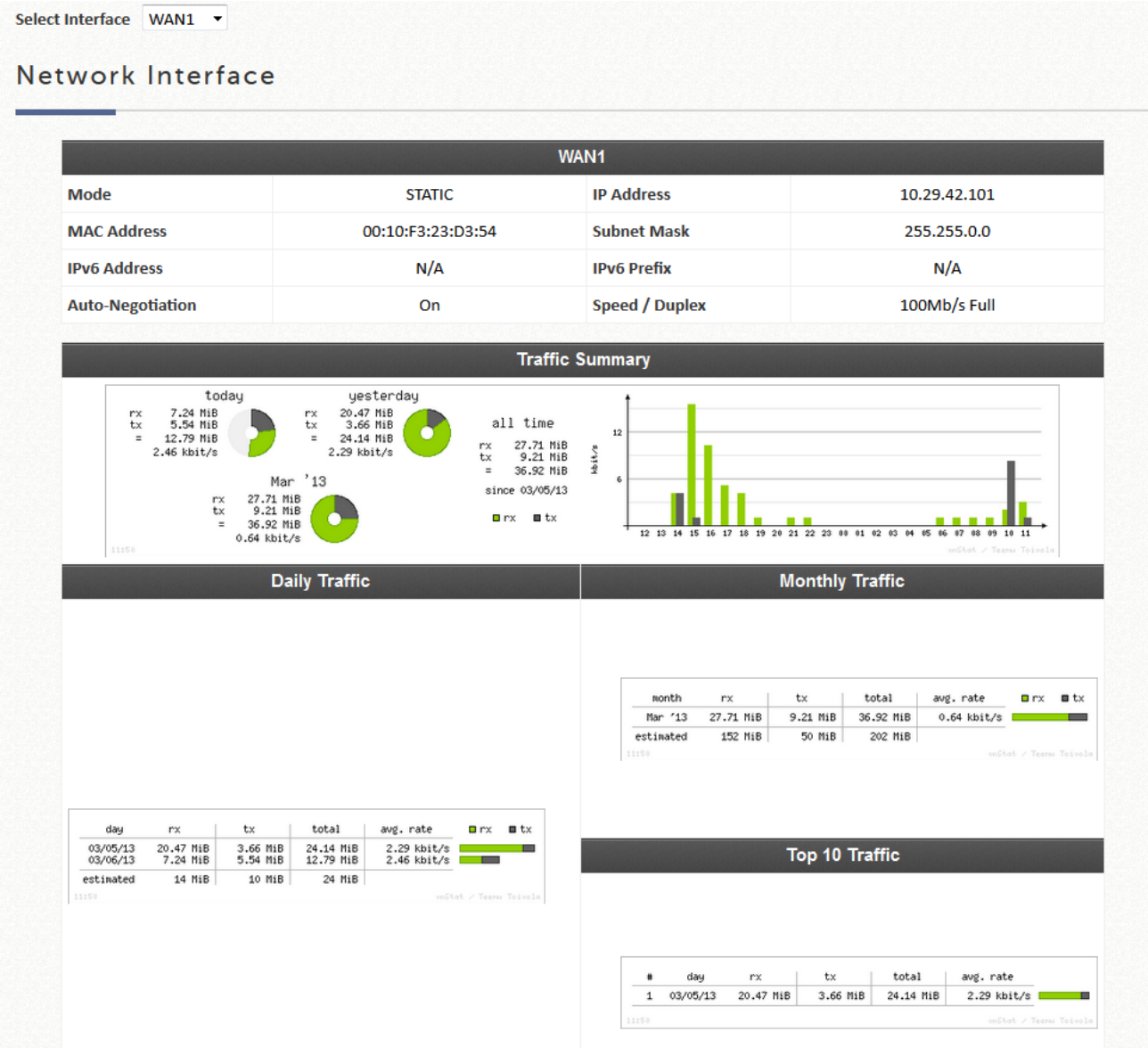
一般			
System Name	システム名。デフォルト名称は型番です。	Firmware Version	現在の EWS CONTROLLER のファームウェアバージョン。
System Up Time	システムの動作時間を表示します。	Build Number	現在のビルド番号。
System Time	ローカル時刻はシステム時刻として表示されます。	NTP Server	アライメントするように設定されているネットワークタイムサーバ。
Preferred DNS Server	優先 DNS サーバの IP アドレス。	Alternate DNS Server	代替 DNS サーバの IP アドレス。
Proxy Server	Enabled/Disabled/External	APM Version	AP 管理モジュールのバージョン。
WAN Failover	Enabled/Disabled	Load Balancing	Enabled/Disabled
SNMP	Enabled/Disabled	Warning of Internet Disconnection	Enabled/Disabled
Idle Timeout	アカウントが自動的に期限切れになるまでのユーザの無効時間(分)。	Traffic Direction for Idle Timeout	アップリンク/アップリンク&ダウンリンク。 ユーザのアクティビティインスペクションは、アップリンクトラフィックのみまたは両方向でチェックできます。
Num of Current Users	カレントオンラインユーザの数。	Num of Maximum Users	オンラインユーザの上限回数。
報告			
Syslog server 1		外部 Syslog サーバの IP アドレスとポート番号。N/A は、構成されていないことを意味します。	
Syslog server 2		外部 Syslog サーバの IP アドレスとポート番号。N/A は、構成されていないことを意味します。	
User Logs	Retained Days		ユーザの情報を保持する最大日数。
	Receiver Email Address (es)		トラフィック履歴またはユーザのトラフィック履歴情報が送信されるメールアドレス。

ネットワークトラフィック、CPU ロード、CPU 温度、メモリー使用量、ストレージ使用量、オンラインユーザ、ログインの成功、セッション、DHCP リース、および DNS クエリのインタフェース別にソートされた、使用可能なレポートの [See Reports](#) をクリックします。レポートは、時間範囲と間隔を選択して、優先順位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 を介して送信できます。

2) Interface

すべてのネットワークインタ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インタフェースを選択します。

各サービスゾーンは仮想システムを表すため、システムのネットワークインタフェースの情報はサービスゾーンごとにグループ化されます。



項目		説明
Interface(WAN1/WAN2)	Mode	このインタフェースの動作モード。
	MAC Address	WAN ポートの MAC アドレス。
	IP Address	WAN ポートの IPv4 アドレス。
	Subnet mask	WAN ポートのサブネットマスク。
	IPv6 Address	選択したインタフェースの IPv6 アドレス
	IPv6 Prefix	IPv6 アドレスのプレフィックス
	Auto-Negotiation	オートネゴシエーションを ON にすると、インタフェースに接続されているデバイスとシステムがサポートする最高性能の伝送モード(速度/デュプレックス/フロー制御)を選択します。
	Speed/Duplex	選択したインタフェースのスピードとデュプレックスを表示します。
Traffic Summary		このインタフェースの送受信速度の日次、月次、およびすべての時間のサマリーがグラフィカルに表示されます。
Daily Traffic		その日のトラフィック情報をテーブルでテーブル示します。
Monthly Traffic		テーブル内のトラフィック情報を表示します。
Top 10 Traffic		日付レコードの上位 10 件のトラフィックを表示します。
Service Zone - デフォルト、SZ1～SZ8	Mode	SZ の動作モードです。
	MAC Address	SZ の MAC アドレス。
	IP Address	SZ の IP アドレス。
	Subnet mask	SZ のサブネットマスク。
	IPv6 Address	SZ の IPv6 アドレス
Service Zone - DHCP スコープ(デフォルト、SZ1～SZ8)	Status	有効/無効は、デフォルトサービスゾーンの DHCP サーバのステータスを表します。
	WINS IP Address	DHCP サーバ上の WINS サーバ IP。N/A は、構成されていないことを意味します。
	Start IP Address	DHCP IP 範囲の先頭 IP アドレス。
	End IP address	DHCP IP 範囲のエンド IP アドレス。
	Lease Time	IP アドレスのリース時間の分。

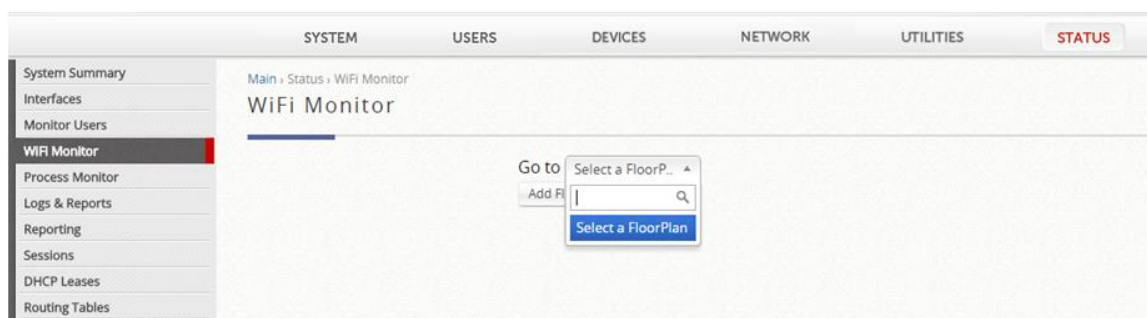
3) Monitor Users

すべてのオンラインユーザ/デバイスがここに表示されます。管理者は、Kick Out をクリックすると、任意のユーザを終了できます。ログインしていないユーザもここに表示されます。

- **Online Users:** 正常に認証されたローカルユーザ。
- **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(クロスゲートウェイローミング用)。
- **Roaming Out User:** RADIUS プロトコルを介して外部コントローラで On-Demand ユーザを認証します。
- **Non-Login Local User:** IP アドレスを取得しましたが、まだローカルユーザ認証されていません。
- **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はなく、MAC ログインデバイスリストで MAC 認証が可能です。
- **Authenticated Users:** IP が未知の認証完了ユーザ(802.1X、MAC 認証、PPP 認証、CoA ログイン)。
- **Smart Login Users:** スマートログイン期間内のオンデマンドユーザ。このリストのユーザは、次回アクセス時に自動的にログインされます。

4) WiFi Monitor

Wi-Fi モニタを実行するには、まず管理対象 AP モニタリングまたはシミュレーションを開始するフロアプランを作成し、次に 2D 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。フロアプランを追加するには、Add Floor Plan を選択します。

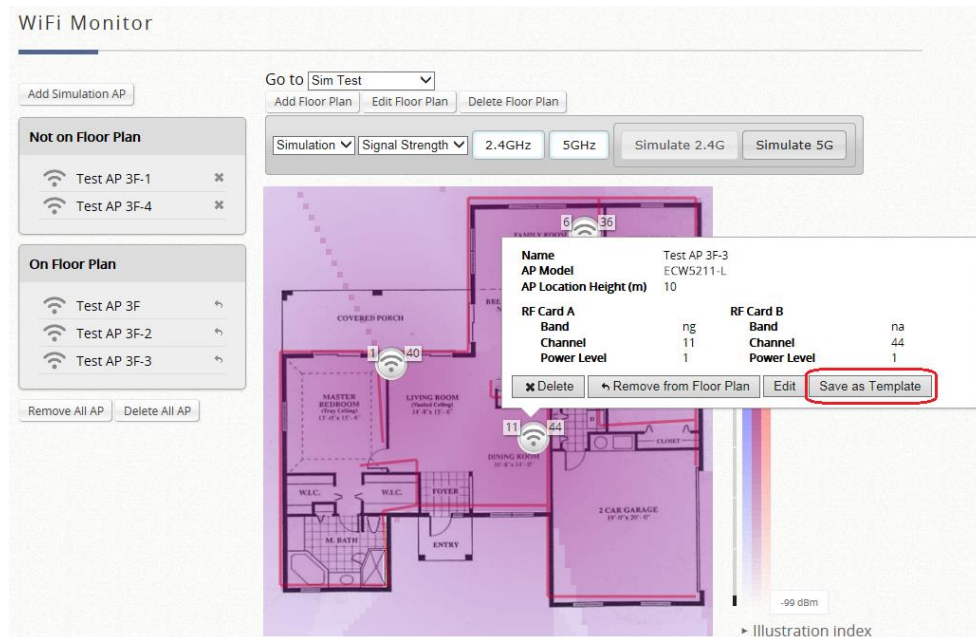


Add Floor Plan

Floor Plan Type	Local ▼	
Floor Plan Name		*
Floor Plan (.jpg)	選擇檔案 未選擇任何檔案	* (under 256k, .jpg)
Wall (.xml / .osm)	選擇檔案 未選擇任何檔案	*
Map Width (m)		* (1~200)
Map Length (m)		* (1~200)
Country Code	EUROPE ▼	
Height of Receiving Device (m)	1	* (1~10)

- **Floor Plan Type:** フロアプランの種別。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、AP シミュレーションの場合は"Virtual"を選択します。
- **Floor Plan Name:** 管理者用の自己定義の名前。
- **Floor Plan:** フロアプラン(.jpg フォーマット)のファイルを選択します。
- **Wall:** ウォール用のファイル(.xml または .osm フォーマット)を選択します。

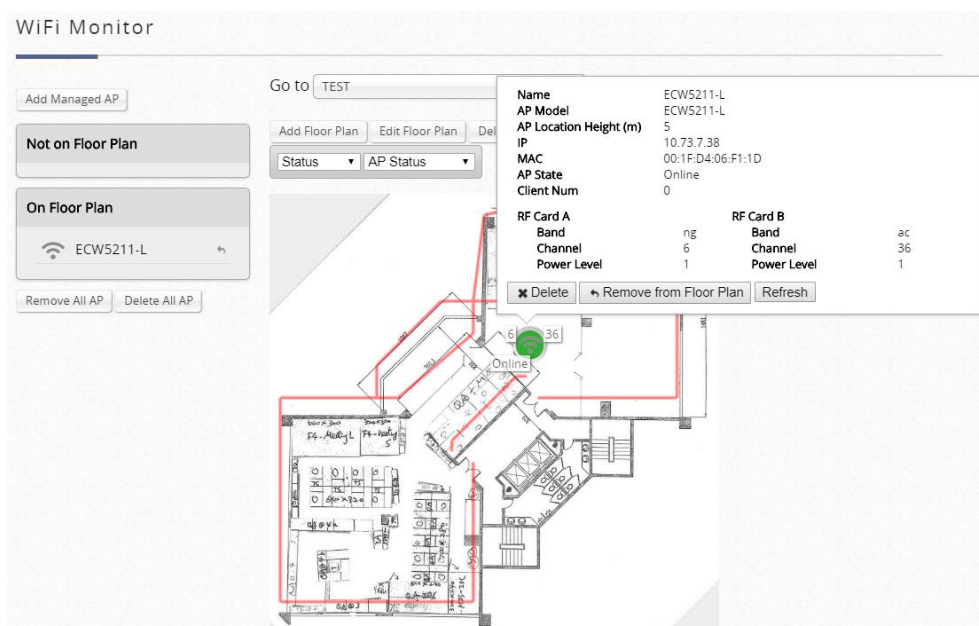
- **Map Width:** フロアプランの実際の幅。
- **Map Length:** フロアプランの実際の長さ。
- **Country Code:** 国番号(EU/US)を選択します。これにより、アクセスポイントの最大出力電力が決まります。
- **Height of Receiving Device(m):** 受信するクライアントデバイスの想定される高さ。



Virtual Type

Simulate 2.4G または Simulate 5G をクリックすると、シミュレーションを実行できます。結果が満足できるものであれば、各 AP の設定をテンプレートとして保存し、AP 管理の AP に適用することができます。

- **Signal Strength:** 色が暗いほど、電波状態が強くなります。
- **Coverage:** 各 AP のカバレッジ領域は、異なる色で表示されます。
- **Distribution:** 信号の強度を示すために、さまざまな色を使用します。



Local & Wide Type

- **AP status:** オンライン/オフライン状態、CPU 使用率(ワイドタイプのみ)、メモリー使用率(ワイドタイプのみ)を視覚化します。
- **Statistics:** AP ごと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:** 仮想タイプに似ており、それぞれの AP のカバレッジを異なる方法で表示します。

6) Process Monitor

処理・監視は、ゲートウェイ上の処理・デーモンのアクティブ状態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して、プロセッサモニタの Enable または Disable を選択できます。

Process Monitor		
Enable Monitor ☒ Enable ☐ 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。ユーザログはユーザーイベントにまとめられており、ユーザごとに発生したトラフィックデータも、直近の暦月に累積されて記録されています。ただし、これらの情報はすべて揮発性メモリに保存されるため、再起動/リブート時に失われます。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:** コントローラと CAPWAP が有効な AP 間で通信された 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 構成を変更したユーザのアカウントと IP が表示されます。
- **Local Monthly Usage:** ローカルユーザごとに生成されたトラフィックデータの累積レコードが、直近の 2 カレンダー月間に保存されます。ローカルユーザレコードの月次ネットワーク使用量の各行は、System Name、Connection Time Usage、Packets In、Bytes In、Packets Out、および Bytes Out の 6 つのフィールドで構成されます。
- **Local Web Log:** このページは、Web ページのどれが Controller 組み込み Web サーバでアクセスされたかを示します。
- **On-Demand Billing Report:** このページでは、オンデマンドアカウントトランザクションの概要を示します。
- **RADIUS Server Log:** 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、起動時刻、発信者、着信者、持続時間(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:** イベントトレースのシステム関連ログを表示します。
- **UAMD Log:** UAM デーモンから出力された UAM 関連情報を表示します。
- **User Events:** 管理者の優先順位に合わせてカスタマイズ可能なユーザ関連のすべての情報が表示されます。

User Events

Display Mode Configure

From 2019-07-01 Display

To 2019-07-01

User Type ☐ Local ☐ On-Demand ☐ Guest ☐ Roaming Out ☐ Roaming In ☐ External ☐ Social ☐ OTP

Download

Type ▼ Search

Type	Date	Name	IP	MAC	Event
(Total:0) First Prev Next Last Go to Page ▼ (Page:1/1) Row per Page: 20 ▼					

Download を選択すると、表示されているユーザイベントがカンマ区切りの .txt 形式でダウンロードされます。これはセル(MS Excel)に読み込むことができます。

なお、ユーザの種類によってユーザ内容が異なります。ユーザの種類に該当しない場合は、カテゴリは空白のままになります。

ローカルユーザの適用可能なユーザイベントカテゴリ:

Date、Type、Name、IP、IPv6、MAC、Pkts In、Bytes In、Pkts Out、Bytes Out、VLAN ID、Group、Policy、MaxDnLoad、MaxUpload、ReqDnLoad、および ReqUpload

オンデマンドユーザの適用可能なユーザイベントカテゴリ:

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、および ReqUpload

ローミングアウトユーザに適用可能なユーザイベントカテゴリ:

Date、Type、Name、NSID、NASIP、NASPort、UserMAC、SessionID、SessionTime、Bytes in、Bytes Out、Pkts In、Pkts Out、および Message

ローミングインユーザに適用可能なユーザイベントカテゴリ:

Date、Type、Name、NSID、NASIP、NASPort、UserMAC、UserIP、SessionID、SessionTime、Bytes in、Bytes Out、Pkts In、Pkts Out、および Message

- **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。アラームは、障害が解決されるまでアラームリストに残ります。
- **Management Events:** 選択したアイテムの管理関連ログ。

8) Reporting

設定された E メールアドレス、SYSLOG サーバ、または FTP サーバに、さまざまな種類のユーザおよび/またはシステム関連のレポートを自動的に送信できます。

Notification Settings ページ:

この設定画面では、選択した時間間隔に基づいて、あらかじめ設定された電子メール、SYSLOG サーバ、または FTP サーバに送信するログタイプを選択できます。

■ Sending Logs to E-mail

"SMTP Settings"で設定された電子メールアドレスに送信できるログの種類は、監視 IP レポート、ユーザログ、オンデマンドユーザログ、試用ユーザログ、ローミングアウトユーザログ、ローミングインユーザログ、外部ユーザログ、セッションログ、ファイアウォールログ、ローカルエリアネットワーク AP ステータス変更、オンデマンドユーザ請求レポート、ワイドエリアネットワーク AP ステータス変更、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。目的の E-mail アドレスプロファイル(1～5)を選択し、レポートまたはログを送信する間隔を選択します。

Notification Settings

	Receiver E-mail Address(es)						SYSLOG	Primary FTP	Interval
	1	2	3	4	5	Detail / Test			
Monitor IP Report	☐	☐	☐	☐	☐	 	N/A	N/A	1 Hour ▼
Local Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
On-Demand Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
Guest Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
Roaming Out Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
Roaming In Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
External Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
Social Media Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
One Time Password Users Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
Session Log	☐	☐	☐	☐	☐	 	☐ 	☐ 	1 Hour ▼
Firewall Log	☐	☐	☐	☐	☐	 	☐ 	N/A	1 Hour ▼
Online User Limit Notification	☐	☐	☐	☐	☐	 	N/A	N/A	N/A
Local Area AP Status Change	☐	☐	☐	☐	☐	 	N/A	N/A	2 Mins ▼
On-Demand User Billing Report	☐	☐	☐	☐	☐	 	N/A	☐ 	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report
Wide Area AP Status Change	☐	☐	☐	☐	☐	 	N/A	N/A	2 Mins ▼
Wide Area AP Report									
☐ CPU Loading ☐ Memory Usage ☐ Network Delay ☐ Network Traffic ☐ Associated Clients ☐ VAP Traffic ☐ WDS Traffic							N/A	☐ 	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Guest Information	☐	☐	☐	☐	☐	 	N/A	N/A	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report
Social Account Information	☐	☐	☐	☐	☐	 	N/A	N/A	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report
Guest/Social Account Info Full	☐	☐	☐	☐	☐	 	N/A	N/A	2 Mins ▼
Local HTTP Web Log							N/A	☐ 	1 Hour ▼
HTTP Web Log							N/A	☐ 	1 Hour ▼
Configuration Change Log	☐	☐	☐	☐	☐	 	N/A	☐ 	1 Hour ▼

- **Detail:** このラジオ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:** 選択した E-mail アドレスにテストログを送信します。

■ Sending Logs to SYSLOG

"SYSLOG Settings"で設定された外部 SYSLOG サーバに送信できるログタイプは、ローカルユーザログ、オンデマンドユーザログ、試用ユーザログ、ローミングアウトユーザログ、ローミングインユーザログ、外部ユーザログ、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、および DHCP サーバログです。目的のログタイプをクリックし、ログの送信間隔を選択します。

Notification Settings

	Receiver E-mail Address(es)					SYSLOG	Primary FTP	Interval
	1	2	3	4	5			
Monitor IP Report	☐	☐	☐	☐	☐		N/A	1 Hour ▼
Local Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
On-Demand Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
Guest Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
Roaming Out Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
Roaming In Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
External Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
Social Media Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
One Time Password Users Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
Session Log	☐	☐	☐	☐	☐		☐	1 Hour ▼
Firewall Log	☐	☐	☐	☐	☐		N/A	1 Hour ▼
Online User Limit Notification	☐	☐	☐	☐	☐	N/A	N/A	N/A
Local Area AP Status Change	☐	☐	☐	☐	☐	N/A	N/A	2 Mins ▼
On-Demand User Billing Report	☐	☐	☐	☐	☐	N/A	☐	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report
Wide Area AP Status Change	☐	☐	☐	☐	☐	N/A	N/A	2 Mins ▼
Wide Area AP Report	N/A					N/A	☐	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
☐ CPU Loading								
☐ Memory Usage								
☐ Network Delay								
☐ Network Traffic								
☐ Associated Clients								
☐ VAP Traffic								
☐ WDS Traffic								
Guest Information	☐	☐	☐	☐	☐	N/A	N/A	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report
Social Account Information	☐	☐	☐	☐	☐	N/A	N/A	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report
Guest/Social Account Info Full	☐	☐	☐	☐	☐	N/A	N/A	2 Mins ▼
Local HTTP Web Log	N/A						☐	1 Hour ▼
HTTP Web Log	N/A						☐	1 Hour ▼
Configuration Change Log	☐	☐	☐	☐	☐	N/A	☐	1 Hour ▼
DHCP Server Log	N/A						N/A	N/A

- **Detail:** このボタンをクリックすると、タグ、重大度、ファシリティなどの SYSLOG 属性を設定構成します。これらの属性は、SYSLOG サーバのフィルタ要件を満たすために、対応するログに割り当てられます。

注記: 選択したログを設定済みの SYSLOG サーバに送信するには、SYSLOG Settings で"System Log"オプションを有効にする必要があります。

■ Sending Logs to FTP

"FTP Settings"で設定された外部 FTP サーバに送信できるログの種類は、ローカルユーザログ、オンデマンドユーザログ、試用ユーザログ、ローミングアウトユーザログ、ローミングインユーザログ、外部ユーザログ、セッションログ、オンデマンド課金レポートログ、ワイドエリアネットワーク 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。目的のログタイプをクリックし、ログの送信間隔を選択します。

Notification Settings

	Receiver E-mail Address(es)						SYSLOG	Primary FTP	Interval	
	1	2	3	4	5	Detail / Test				
Monitor IP Report	☐	☐	☐	☐	☐		N/A	N/A	1 Hour ▼	
Local Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
On-Demand Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
Guest Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
Roaming Out Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
Roaming In Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
External Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
Social Media Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
One Time Password Users Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
Session Log	☐	☐	☐	☐	☐		☐		1 Hour ▼	
Firewall Log	☐	☐	☐	☐	☐		☐	N/A	1 Hour ▼	
Online User Limit Notification	☐	☐	☐	☐	☐		N/A	N/A	N/A	
Local Area AP Status Change	☐	☐	☐	☐	☐		N/A	N/A	2 Mins ▼	
On-Demand User Billing Report	☐	☐	☐	☐	☐		N/A	☐	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report	
Wide Area AP Status Change	☐	☐	☐	☐	☐		N/A	N/A	2 Mins ▼	
Wide Area AP Report	N/A						N/A	☐	☐ CPU Loading ☐ Memory Usage ☐ Network Delay ☐ Network Traffic ☐ Associated Clients ☐ VAP Traffic ☐ WDS Traffic	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Guest Information	☐	☐	☐	☐	☐		N/A	N/A	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report	
Social Account Information	☐	☐	☐	☐	☐		N/A	N/A	☐ 0 ▼ Daily Report ☐ Sun ▼ Weekly Report ☐ 1 ▼ Monthly Report	
Guest/Social Account Info Full	☐	☐	☐	☐	☐		N/A	N/A	2 Mins ▼	
Local HTTP Web Log	N/A						☐		1 Hour ▼	
HTTP Web Log	N/A						☐		1 Hour ▼	
Configuration Change Log	☐	☐	☐	☐	☐		N/A	☐	1 Hour ▼	
DHCP Server Log	N/A						☐		N/A	
DHCP Lease Log	N/A						N/A	☐	1 Hour ▼	
System Report	N/A						N/A	☐	☐ CPU Loading ☐ Memory Usage ☐ Storage Usage ☐ Network Traffic ☐ Online User ☐ Successful Login ☐ Session ☐ DHCP Lease ☐ DNS Query	☐ Daily Report ☐ Weekly Report ☐ Monthly Report
Traffic Report (Text)	N/A						N/A	☐	1 Hour ▼	
Service Zone	N/A						N/A	☐	1 Hour ▼	
VLAN	N/A						N/A	☐	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 サーバに保存される FTP サーバフォルダーを指定できます。

Note: FTP サーバに出力されるログファイルは、フォーマット

\$Topic_\$ExtraDesc_\$SystemName_\$Date_Time.txt に従って命名されます。

例: HTTPWebLog_GW1_2010-10-15_0800.txt

- **FTP Settings:** 選択したユーザログとシステムログを送信する外部 FTP サーバの設定を許可します。

FTP 設定ページ

The screenshot shows the 'FTP Settings' page. It is divided into two main sections: 'Primary FTP Server' and 'Secondary FTP Server'. Each section contains the following fields: 'IP Address' (text input), 'Port' (text input), 'Login' (radio buttons for 'Anonymous' and 'Normal'), 'Username' (text input), and 'Password' (text input). Below these fields is a 'Send Test File' button with a 'Send' sub-button. The 'Normal' login option is selected for both servers.

- **FTP Destination:** FTP サーバの 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、FTP 宛先の設定をテストするためのテストログを送信することができます。
- **SMTP Settings:** 5 つの受信者 E-mail アドレスと、さまざまなユーザ関連のログが送信される必要なメールサーバ設定を構成できます。

The screenshot shows the 'SMTP Settings' page. It contains the following fields: 'SMTP Server' (with 'Server Address' and 'Port' text inputs), 'Encryption' (radio buttons for 'Disable', 'TLS', 'SSL'), 'Authentication' (a dropdown menu set to 'None'), 'Sender E-mail Address' (text input), and 'Receiver E-mail Address' (five separate text input fields labeled 'Receiver 1' through 'Receiver 5'). At the bottom is a 'Send Test E-mail' button with a 'Send' sub-button. Red asterisks are visible next to the 'Server Address', 'Port', and 'Sender E-mail Address' fields.

- **SMTP Server:** 送信者の SMTP サーバの 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 サーバで SMTP over SSL を実行する場

合、管理者は他のポートを指定できます。

- **Encryption:** SMTP サーバで SMTP over TLS または SSL を実行する場合は、このオプションを有効にします。
- **SMTP Authentication:** Plain、Login、CRAM-MD5 と NTLMv1、または"None"の 4 つの認証方法があり、これらのいずれも使用されません。選択した認証方法に応じて、Account Name、Password と Domain を入力します。
 - NTLMv1 は、現在のところ、一般的な用途には使用できません。
 - Plain と CRAM-MD5 は標準化された認証メカニズムで、Login と NTLMv1 は Microsoft 独自のメカニズムです。Plain と Login のみが、UNIX ログインとパスワードを使用できます。ネットスケープは Plain を使っています。Outlook および Outlook Express は、NTLMv1 を使用するように設定できますが、Login をデフォルトとして使用します。
 - Pegasus は CRAM-MD5 または Login を使用しますが、どのメソッドを使用するかは設定できません。
- **Sender E-mail Address:** 監視を担当する管理者の電子メールアドレス。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):** 通知を受信するために、ここで最大 5 つの E-mail アドレスを設定できます。
- **SYSLOG Settings:** 選択したユーザログとシステムログの送信先となる 2 つの外部 SYSLOG サーバを設定できます。

SYSLOG 設定ページ

SYSLOG Settings

SYSLOG ☒ Enabled ☐ Disabled

SYSLOG Server

Server 1

IP Address:

Port:

Server 2

IP Address:

Port:

Severity Level emergency ▼

- **SYSLOG Destinations:** 最大 2 つの外部 SYSLOG サーバを設定できます。外部 SYSLOG サーバの IP アドレスとポート番号を入力してください。
- **Severity Level:** このレベルよりも重大なログは、外部 SYSLOG サーバに送信されます。
- **Alarms & Events Settings:** 監視する項目をアラームまたは管理イベントとして設定します。アラームは、Alarms ページおよびダッシュボードに表示される、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す。アラームは、障害が解決されるまでアラームリストに残ります。管理イベントは、Management Events ページに表示する、選択したアイテムのログです。最新のいくつかのイベントもダッシュボードに表示されます。

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	☒	☒	
AP Backup Configuration	☒	☒	
AP Restore Configuration	☒	☒	
AP Firmware Upgrade	☒	☒	
AP Template Applying	☒	☒	
AP High CPU Usage	☒	☒	70% ▼
AP High Memory Usage	☒	☒	70% ▼
AP High Airtime Utilization	☒	☒	70% ▼
Controller High CPU Usage	☒	☒	70% ▼
Controller High Memory Usage	☒	☒	70% ▼
Controller High Storage Usage	☒	☒	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間で現在確立されているセッションを検査できます。それぞれの結果には、送信元および宛先の IP およびポートの値が表示されます。フィルタ条件を定義し、必要な結果のみを表示することができます。

Session List

Filter					
Address Family	Protocol	Source IP	Port	Destination IP	Port
IPv4 ▼	All ▼				

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

このページでは、DHCP IP リース情報を表示できます。

- Statistics of IP Offered

Last 10 Minutes、Hours と Days の有効なリース数がここに表示されます。ヘッダ 1～10 はユニット乗算器です。たとえば、列 2 の下の数字は過去 20 分/時/日のリースカウントを示し、列 3 の下の数字は過去 30 分/時/日のリースカウントを示しています。

- Statistics of IP Expired

Last 10 Minutes、Hours と Days で期限切れになったクライアントにリースされた IP がここに表示されます。ヘッダ 1～10 はユニット乗算器です。たとえば、列 2 の下の数字は過去 20 分/時/日の期限切れカウントを示し、列 3 の下の数字は過去 30 分/時/日の期限切れカウントを示します。

の数字は過去 30 分/時/日の期間有効なカウントを示します。

Refresh

Refresh Disable ▾

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

	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

ここには DHCP リースログが表示され、IP アドレス、MAC アドレス、またはサービスゾーンで検索を実行できます。

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 アドレスを使用しているクライアントの関連情報が表示されます。

DHCP Lease List						
Refresh Delete		Refresh Disable ▾				
☐	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 1 (Page:1/1) Row per Page: 50						

11) Routing Table

このルーティングテーブルには、すべての IPv6 および IPv4 経路情報ルールが一覧表示されます。経路情報ユーティリティのルールもここに表示されます。ポリシー・経路情報・ルールの優先順位順位はグローバル・ポリシー・経路情報・ルールより高く、システム・経路情報・ルールの優先順位順位は最も低くなります。

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
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、ポリシーまたはインタフェースごとのルーティングルールが表示されます。

- **Policy1～n:** 1 から n までの個々のポリシーを表示します。
- **Global Policy:** グローバルポリシーの内容を表示します。
- **System:** システム管理の情報を表示します。
 - **Destination:** 機器の宛先 IP アドレス。
 - **Subnet mask:** ポートのサブネットマスク IP アドレス。
 - **Gateway:** ポートのゲートウェイ IP アドレス。
 - **Interface:** WAN1、WAN2、Default、またはトラフィックインタフェースに適用する名前付き Service Zones を含む、インタフェースネットワークの選択肢。

P/N: V345000020191018JP