ユーザーマニュアル
エンタープライズアクセスポイント

バージョン 3.45.0000

著作権に関する通知

Edgecore Networks Corporation

© Copyright 2019 Edgecore Networks Corporation.
本書に記載された情報は予告なく変更される場合があります。本書は参考情報の提供のみを目的としており、Edgecore Networks Corporationが提供するすべての機器、機能、サービスに対して、一切の明示的または暗示的な保証を提供しません。Edgecore Networks Corporationは本書の技術上または編集上の誤記や抜けに関して責任を負うことはありません。

目次

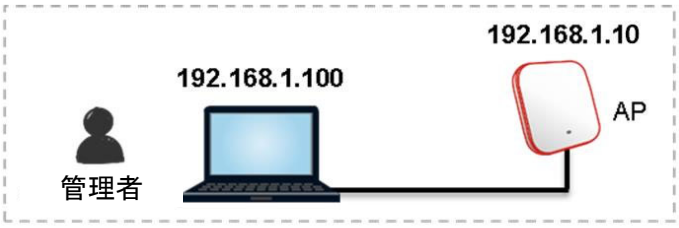
1. Edgecoreエンタープライズアクセスポイントの展開方法

このAP（アクセスポイント）を初めて設定する場合は、管理者が初期構成を実行し、APにIPアドレスや他の必要な情報を割り当て、APをローカルゲートウェイと通信させ、Wi-Fiデバイスを有線ネットワークに接続できるようにしてください。

1.1 APにログインする

APには、構成および管理用のWebベースのインターフェイスが搭載されています。初めて、Web管理インターフェイス（Web Management Interface/WMI）にアクセスする場合は、次の手順に従ってください。

1. **管理者用PCをAPと同じサブネット（192.168.1.10/255.255.255.0）の静的IPアドレスに手動で設定してください。イーサネットケーブルを経由して、APのLANポートにPCを直接接続してください。**

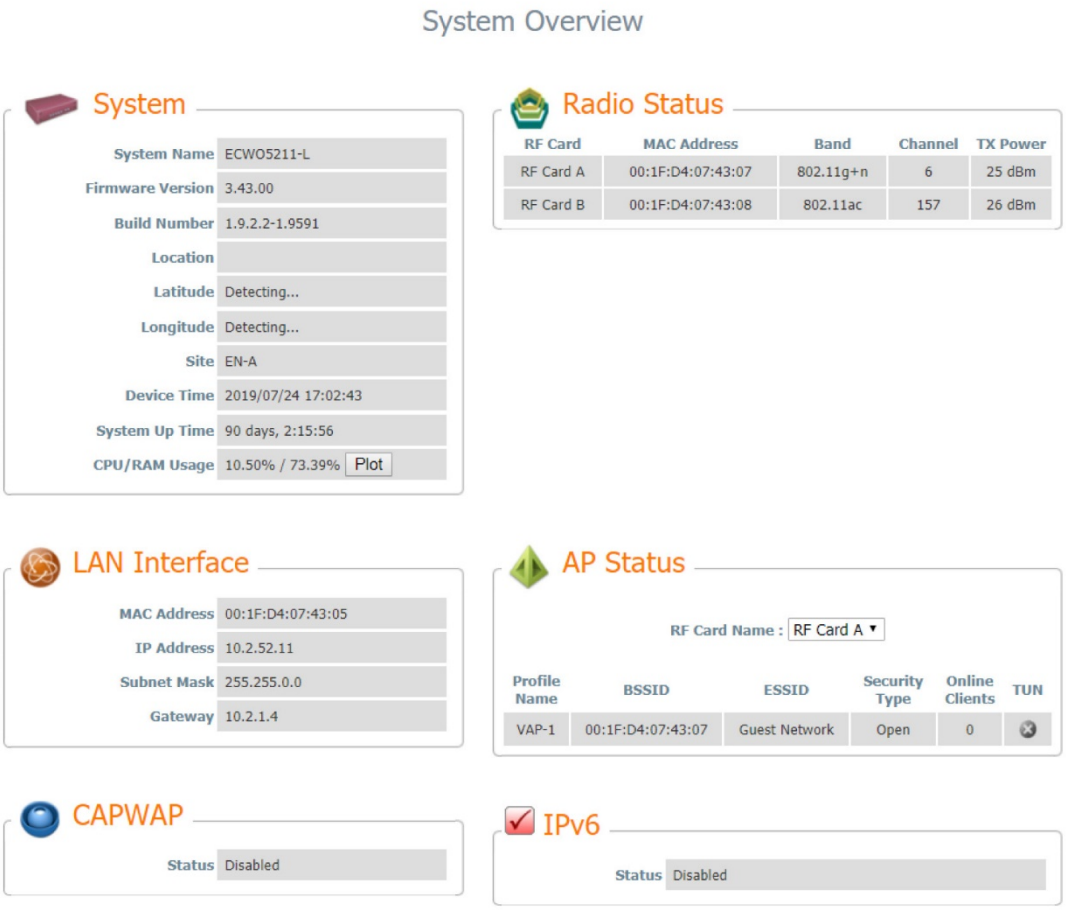


同じサブネット：192.168.1.0/255.255.255.0
（192.168.1.x）

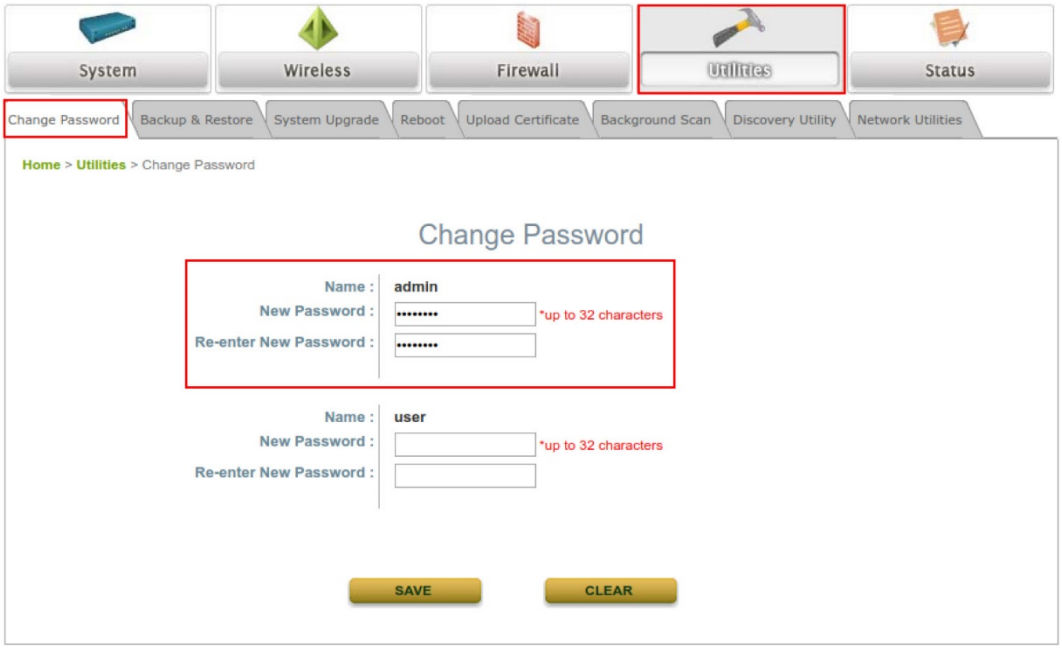
2. **Webブラウザーを起動して、アドレスフィールドにAPのデフォルトのIPアドレス（192.168.1.10）を入力してください。**

デフォルトのユーティリティ名（**admin**）とパスワード（**admin**）を使用して、[Administrator Login(管理者ログイン)]ページにログインしてください：

3. **ログインすると、WMIのシステム概要ページが表示されます。**

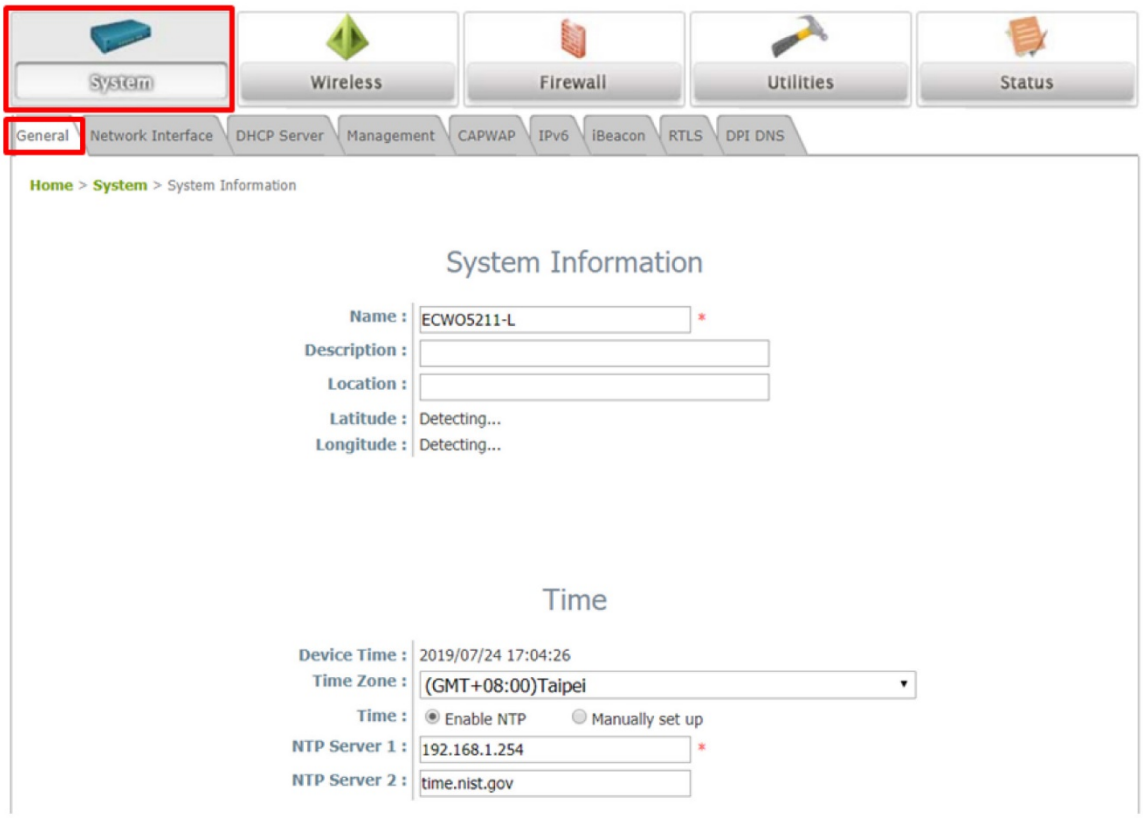


4. **セキュリティ上の理由により、管理者のパスワードを変更してください**
   - メインメニューの**[Utilities(ユーティリティ)]**アイコンをクリックし、**[Change Password(パスワードの変更)]**タブを選択してください。
   - **[New Password(新しいパスワード)]**フィールドにパスワードを入力し、**[Re-enter New Password(新しいパスワードの再入力)]**フィールドにパスワードを再入力してください。



1.2 一般情報構成

[General(一般)]ページ（Home(ホーム) > System(システム) > General(一般)）に移動して、APの一般情報を構成してください。



1. **System Information(システム情報)**：管理者がネットワークのAPを識別できるように、適切なシステム関連の情報（**Name(名前)**、**Description(説明)**、**Location(場所)**）を入力してください。

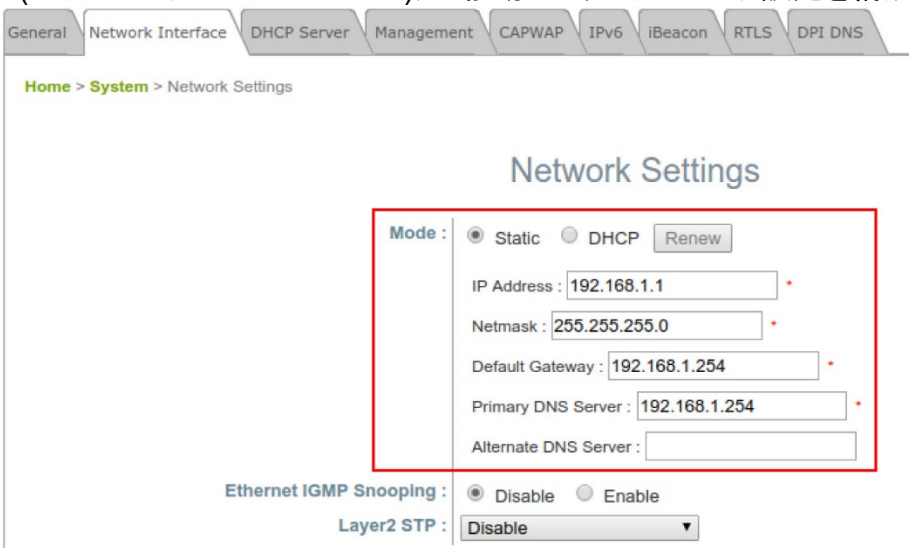
2. **Time(時刻)**：この初期構成の場合、**Enable NTP(NTPの有効化)**（システム時刻をネットワークタームプロトコル（Network Time Protocol/NTP）サーバーと同期させます）の方法を使用して、システム時刻を設定します。

1.3 APをネットワークに接続する

次の手順は、ネットワークの無線到達範囲を確立するための基本手順です。APは、そのLANポートを通して、有線ネットワークに接続し、ネットワークに対する無線アクセスを有効にします。

1. APのIP設定を変更する

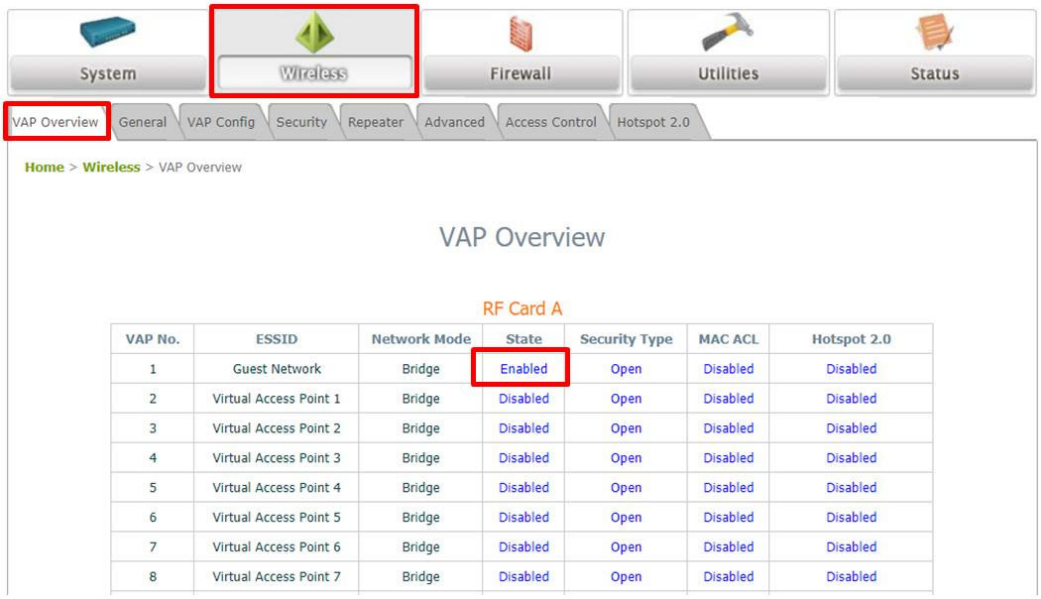
[Network Interface(ネットワークインターフェイス)]ページ（Home(ホーム) > System(システム) > Network Interface(ネットワークインターフェイス)）に移動して、ネットワーク設定を構成してください。



Mode(モード):
Static(静的)：ネットワークインターフェイス（**IP Address(IPアドレス)、Netmask(ネットマスク)、Default Gateway(デフォルトゲートウェイ)、Primary DNS Server(プライマリDNSサーバー)**）に適切な値を手動で入力してください。上の例では、APは、デフォルトIPアドレス192.168.1.10を使用しています。
DHCP：展開のため、APがLANから動的IPアドレスを取得する必要がある場合は、Mode(モード)を**DHCP**に設定し、***[Save(保存)]***をクリックして、変更を送信してください。

2. Wi-Fiアクセス用の最初のSSIDを有効にする

デフォルトでは、1つのサービスセット識別子（Service Set Identifier/SSID）は、Radio A(無線A)（**RFカードA**）に対して有効になっており、1つのSSIDは、Radio B(無線B)（**RFカードB**）に対して有効になっています。上の**[VAP Overview(VAP概要)]ページ**（Home(ホーム) > Wireless(無線) > VAP Overview(VAP概要)）に示すように、Virtual Access Point No.1(仮想アクセスポイント1番)（VAP-1）のプロファイルは、利用可能な1番目のSSIDを表しています。

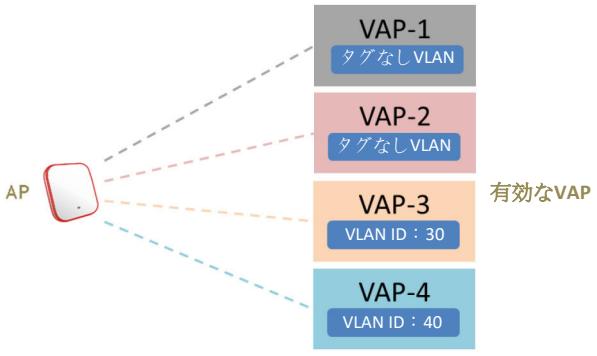


VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled
4	Virtual Access Point 3	Bridge	Disabled	Open	Disabled	Disabled
5	Virtual Access Point 4	Bridge	Disabled	Open	Disabled	Disabled
6	Virtual Access Point 5	Bridge	Disabled	Open	Disabled	Disabled
7	Virtual Access Point 6	Bridge	Disabled	Open	Disabled	Disabled
8	Virtual Access Point 7	Bridge	Disabled	Open	Disabled	Disabled

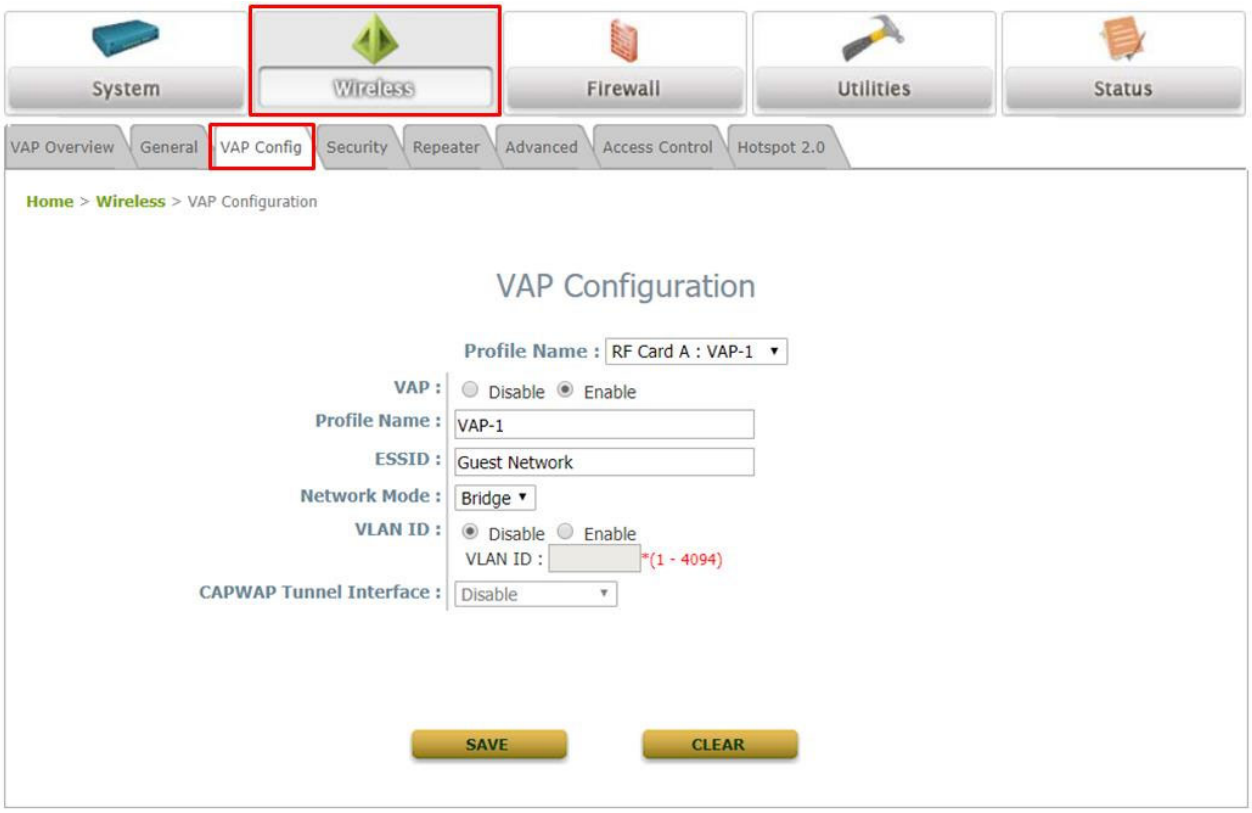
Virtual Access Point（仮想アクセスポイント/VAP）:

- VAP機能により、単一の物理APデバイス（一意の単一BSSIDを持つ）は、下図の例に示すように、それ自身を複数の離散APとして表すことができます。
- 各VAPは、独自の設定（たとえば、SSID、Network Mode(ネットワークモード)、VLAN ID、Security(セキュリティ)）を使用して、個別に有効または無効にできます。これにより、APは、複数のSSIDを通して、異なるクライアントをサポートできます。

注:

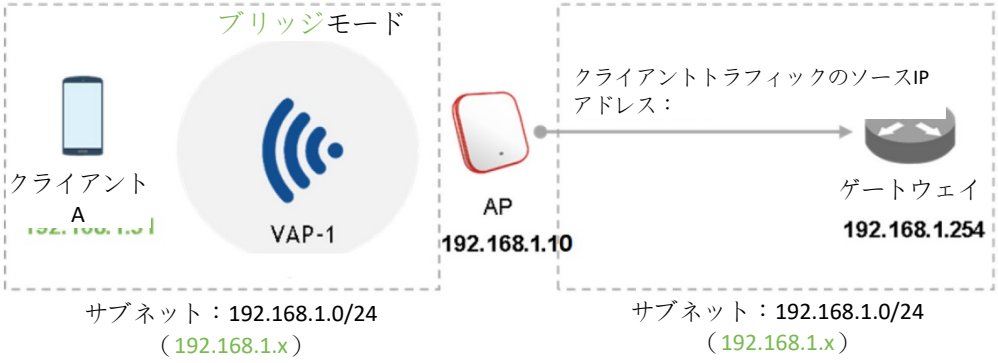


VAP-1の状態（**Enabled(有効)**）をクリックして、プロファイルを構成してください。これにより、次の[VAP Configuration(VAP構成)]ページに移動します。

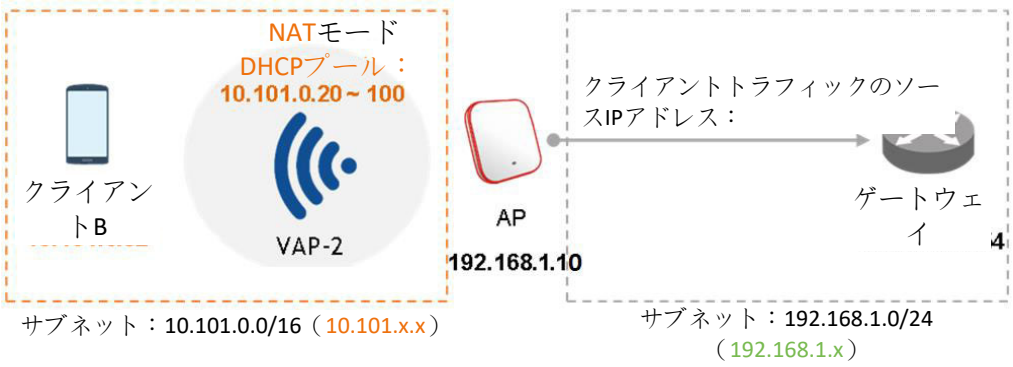


特定のVAPプロファイル（この場合は、「RF Card A:VAP-1」）を選択してください。プロファイルに収集されるVAPの基本設定は次の通りです：

- **VAP**：このVAPを無効または有効にします。
- **Profile Name（プロファイル名）**：識別/管理目的用のVAPプロファイル名。
- **ESSID**：拡張サービスセット識別子（Extended Service Set Identifier/ESSID）は、特定のVAPに関連するクライアントの識別子として機能します。
- **Network Mode（ネットワークモード）**：
  - **Bridge(ブリッジ)**モード：VAPは透過的（つまり、非NAT、非DHCP）に動作します。したがって、クライアントデバイスは、LAN側のDHCPサーバーから動的IPアドレスが割り当てられます。アップリンクゲートウェイ/スイッチによって認識されるクライアントトラフィックのソースIPアドレスは、クライアントの元のIPアドレスのままです（この場合、下図に示す通り、192.168.1.31です）。



- **NAT mode（NATモード）**：VAPは、このSSID上の内蔵SSIDと共にネットワークアドレス変換（Network Address Translation/NAT）デバイスとして動作します。つまり、クライアントデバイスには、このSSID上に構成されたDHCPプールから動的IPアドレスが割り当てられます。NAT変換後、アップリンクゲートウェイ/スイッチによって認識されるクライアントトラフィックのソースIPアドレスは、APのIPアドレスになります（この場合、下図に示す通り、192.168.1.10です）。



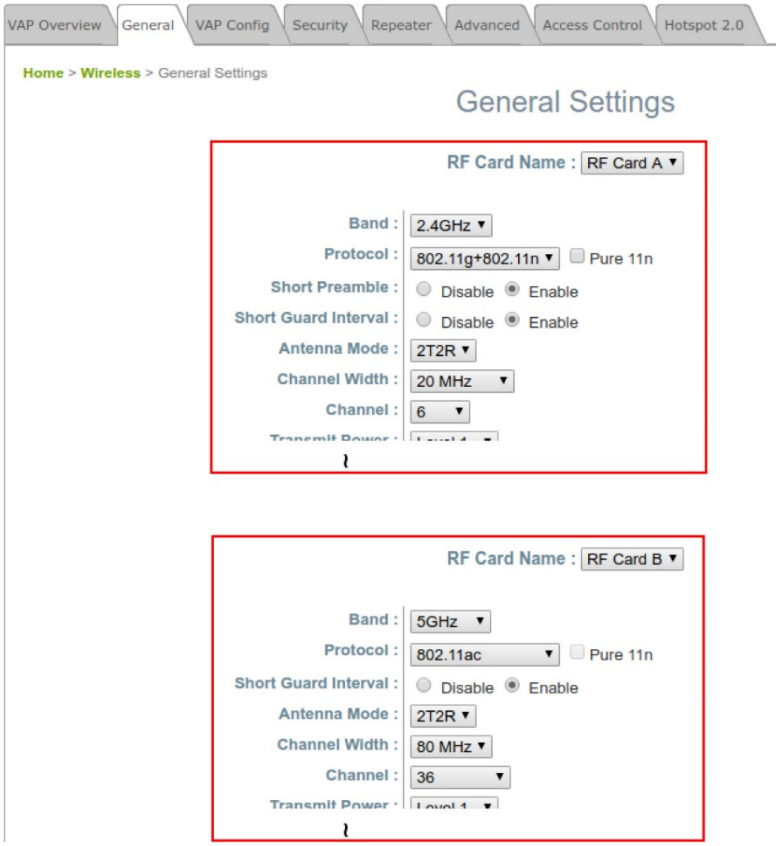
- **VLAN ID**：SSIDごとのVLANタグ付け機能 - 有効にすると、このSSIDを通してAPに入るクライアントのトラフィックは、構成されたVLAN IDによりタグ付けされます。
- **DHCP Profile（DHCPプロファイル）**：内蔵DHCPサーバーのプロファイルです。DHCPサーバーのIP設定は、Home(ホーム) > System(システム) > DHCP Server(DHCPサーバー)にあります。
- **CAPWAP Tunnel Interface（CAPWAPトンネルインターフェイス）**：APがコントローラーにより管理されるとき、APとコントローラーの間の接続状態を示す3つの状態です。
  - **Disable(無効)**（トンネルなし）：APは、コントローラーに対するCAPWAPトンネル接続のない状態で動作します。
  - **Split Tunnel（スプリットトンネル）**：APは、CAPWAPトンネルを経由して、コントローラーに「コントロール」トラフィックのみを通過させます。つまり、「データ」トラフィックは、トンネルを通過せずにローカルに送信されます
  - **Complete Tunnel（完全トンネル）**：APは、CAPWAPトラフィックを経由して、「コントロール」トラフィックと「データ」トラフィックの両方を通過させます

注：
- VAPがブリッジモードであるときのみ、VLAN IDはサポートされます。
- VAPがNATモードに設定されているときのみ、DHCPプロファイルとDHCPサーバーがアクティブになります。
- VAPがNATモードである場合、CAPWAPトンネルインターフェイスは、次の2つの状態でのみ動作します：

無効（トンネルなし）またはスプリットトンネル。

3. 一般無線設定を構成する

Home(ホーム) > Wireless(無線) > General(一般)の下にRF Card A(RFカードA)およびRF Card B(RFカードB)用のグローバル設定があります。RF Card A(RFカードA)は、2.4 GHz帯で動作し、RF Card B(RFカードB)は、5 GHz帯で動作します。両方は、デフォルトで有効になっています。
初期構成では、下記のデフォルトの基本設定の変更が必要となる場合があります:
RF Card A(RFカードA):2.4 GHz、802.11g+802.11n、アンテナモード2T2R、チャンネル幅40 MHz、チャンネル6
RF Card B(RFカードB):5 GHz、802.11ac、アンテナモード2T2R、チャンネル幅80 MHz、チャンネル36(後で他の設定に変更できます)。



完了です!システムを再起動後、APは、これらの設定で動作します。

注:

SSID、ESSID、BSSID:

- サービスセット識別子(Service Set Identifier/**SSID**)は、無線LANの名前を識別するためのキーです。
- 拡張サービスセット識別子(Extended Service Set Identifier/**ESSID**)= SSID。複数の物理APを同じSSIDを使用するように構成できます。つまり、複数の物理AP間のローミングがサポートされます。
- 基本サービスセット識別子(Basic Service Set Identifier/**BSSID**)= APのMACアドレス。複数の物理APが同じESSIDをブロードキャストすると、一意のBSSIDが(ビーコン管理フレームで)送信されます。

2. Web管理インターフェイスを操作する

APには、構成および管理用のWebベースのインターフェイスが搭載されています。本章では、APの詳細設定について説明します。APは、APモードまたはCPEモードとして設定でき、2つのモードには、相互に異なるメニューがあります。次の表は、APのWeb管理インターフェイス（Web Management Interface/WMI）の**Main Menu(メインメニュー)**の下にあるすべての機能タブを示します。

APモード

システム	無線	ファイアウォール	ユーティリティ	ステータス
一般	VAP概要	ファイアウォールリスト	パスワードの変更	概要
ネットワークインターフェイス	一般	サービス	バックアップおよび復元	インターフェイス
ポート	VAP構成	詳細	システムアップグレード	関連クライアント
DHCPサーバー	セキュリティ		再起動	DHCPリース
管理	リピーター		証明書のアップロード	リンクステータス
CAPWAP	詳細		バックグランドスキャン	イベントログ
IPv6	アクセスコントロール		検出ユーティリティ	無線ログ
iBeacon	ホットスポット2.0		ネットワークユーティリティ	モニター
RTLS				
DPI DNS				

CPEモード（ECWO5212-Lのみ）

システム	無線	ファイアウォール	ユーティリティ	ステータス
一般	VAP概要	IP/ポート転送	パスワードの変更	概要
ネットワークインターフェイス	一般	DMZ	バックアップおよび復元	インターフェイス
ポート	VAP構成	詳細	システムアップグレード	関連クライアント
DHCPサーバー	セキュリティ		再起動	イベントログ
管理	詳細		証明書のアップロード	モニター
	アクセスコントロール		バックグランドスキャン	DHCPリース

	サイト調査		検出ユーティリティ	UPnP
			ネットワークユーティリティ	

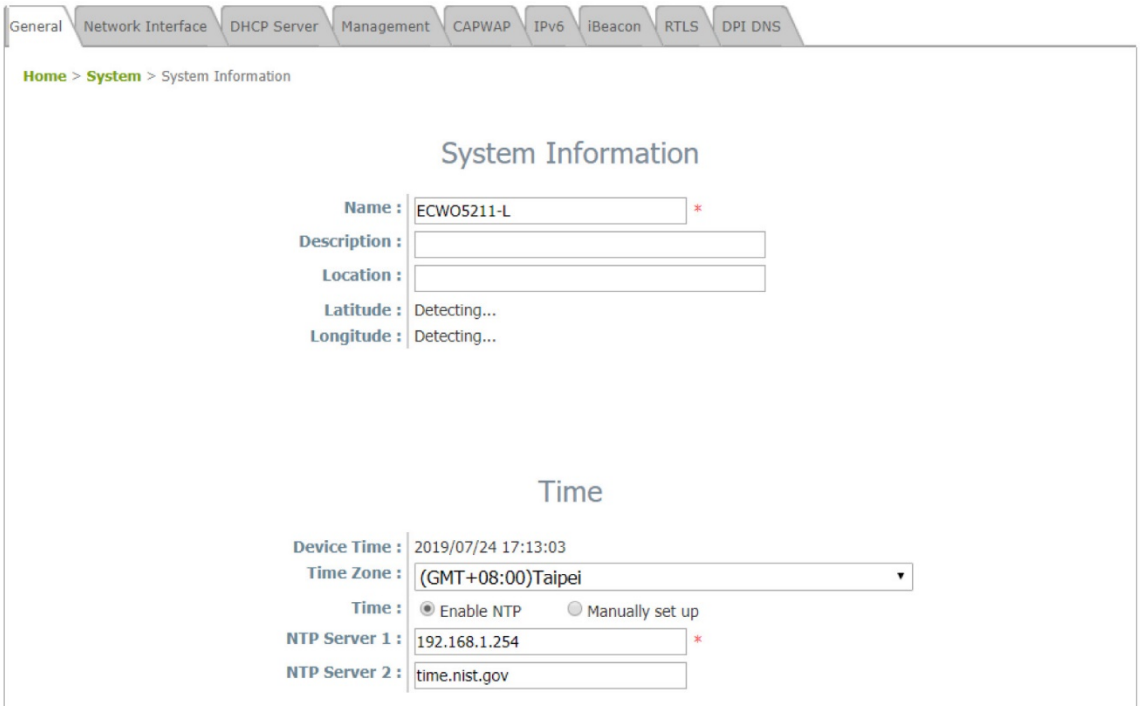
注:

各構成ページで、***[SAVE(保存)]***をクリックして、構成した設定の変更を保存できますが、変更を有効にするには、システムを再起動する必要があります。***[SAVE(保存)]***をクリックすると、次のメッセージが表示されます:**「一部の変更が保存され、再起動後に有効になります。」**再起動または再開中は、すべてのオンラインユーザーは切断されます。

3. システム

[Sysytem(システム)]アイコンをクリックすると、管理者は、APの一般構成用にこのセクションを利用できます。

3.1 General(一般)

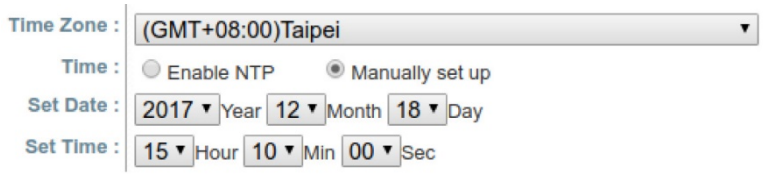


System Information(システム情報)
Name(名前):このシステムを識別するために使用されるシステム名。
Description(説明):システムに関する詳細情報(たとえば、デバイスモデル、ファームウェアバージョン、アクティブ日)。
Location(場所):管理者がシステムを容易に検索できるようにするためのシステムの地理情報に関する情報。

Time(時刻)
Device Time(デバイス時刻):現在のシステム時刻を表示します。
Time Zone(タイムゾーン):ドロップダウンリストボックスから、適切なタイムゾーンを選択してください。
Time(時刻):時刻を設定するには、2つの方法があります –

- **Enable NTP(NTPの有効化)**:システムクロックをネットワークタイムプロトコル(Network Time Protocol/NTP)サーバーと同期させます。ローカルNTPサーバー(利用可能な場合、または、最も近くのNTPサーバーをオンライン検索します)のIPアドレスまたはドメインを入力して、*[SAVE(保存)]*をクリックします。

- **Manually set up(手動設定)**:システムクロックを手動で設定します。これは、デフォルトの方法で、システムを起動するたびに、設定が必要となります。タイムゾーンを選択し、それに応じで、日付と時刻を入力し、*[SAVE(保存)]*をクリックします。

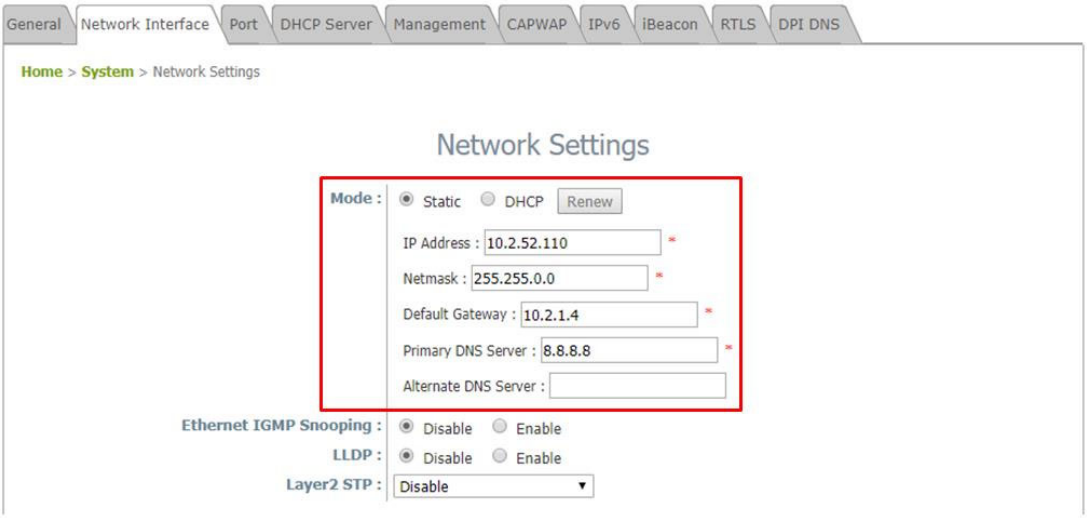


アラートメッセージ「* 一部の変更が保存され、適用後に有効なります」がWMIIに表示されたら、[APPLY(適用)]をクリックします。

インターネット接続またはNTPが利用不可にならない限り、時刻を同期するために、NTPサーバーを使用することをお勧めします（再起動時にシステム時刻を構成する必要がなくなります）。

3.2 Network Interface(ネットワークインターフェイス)

このページで、デバイスのネットワーク設定を構成できます。赤いアスタリスク付きのフィールド（つまり、**IP Address(IPアドレス)、Netmask(ネットマスク)、Default Gateway(デフォルトゲートウェイ)、Primary DNS Server(プライマリDNSサーバー)**）は必須です。



Mode(モード) – Static(静的)：管理者は、静的LAN IPアドレスを手動で設定できます。すべての必須フィールドには、赤いアスタリスクが付いています。

- **IP Address(IPアドレス)**：LANポートのIPアドレス。
- **Netmask(ネットマスク)**：LANポートのサブネットマスク。
- **Default Gateway(デフォルトゲートウェイ)**：LANポートのゲートウェイIPアドレス。
- **Primary DNS Server(プライマリDNSアドレス)**：プライマリDNS（Domain Name System/ドメインネームシステム）サーバーのIPアドレス。
- **Alternate DNS Server(代替DNSサーバー)**：代替DNSサーバーのIPアドレス。

Mode(モード) – DHCP：この構成タイプは、システムがDHCPサーバーが存在するネットワークに接続されている場合に適用されます。必要なすべての関連IP情報は、DHCPサーバーによって自動的に提供されます。

LTE（EAP100のみ）：LTEモジュールをSIMカードと共にUSBポートに接続すると、次の2つのオプションが表示されます。

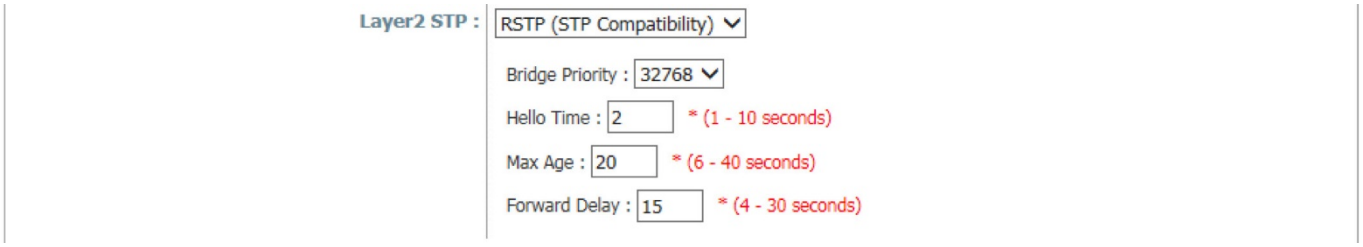
- **No LTE(LTEなし)**：アップリンクとして、LANポートを選択します。
- **LTE**：アップリンクとして、LTEを選択します。

Ethernet IGMP Snooping(イーサネットIGMPスヌーピング)：有効にすると、スイッチはトラフィックを転送し、IGMPパケットはアクセスポイントのネットワークインターフェイスとIPマルチキャストホストを経由して転送されます。登録情報は記録され、マルチキャストグループに保存されます。内部スイッチは、マルチキャストトラフィックを必要とするこれらのポートのみにトラフィックを転送します。逆に、IGMPスヌーピングがない場合、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、ネットワークが非効率になります。

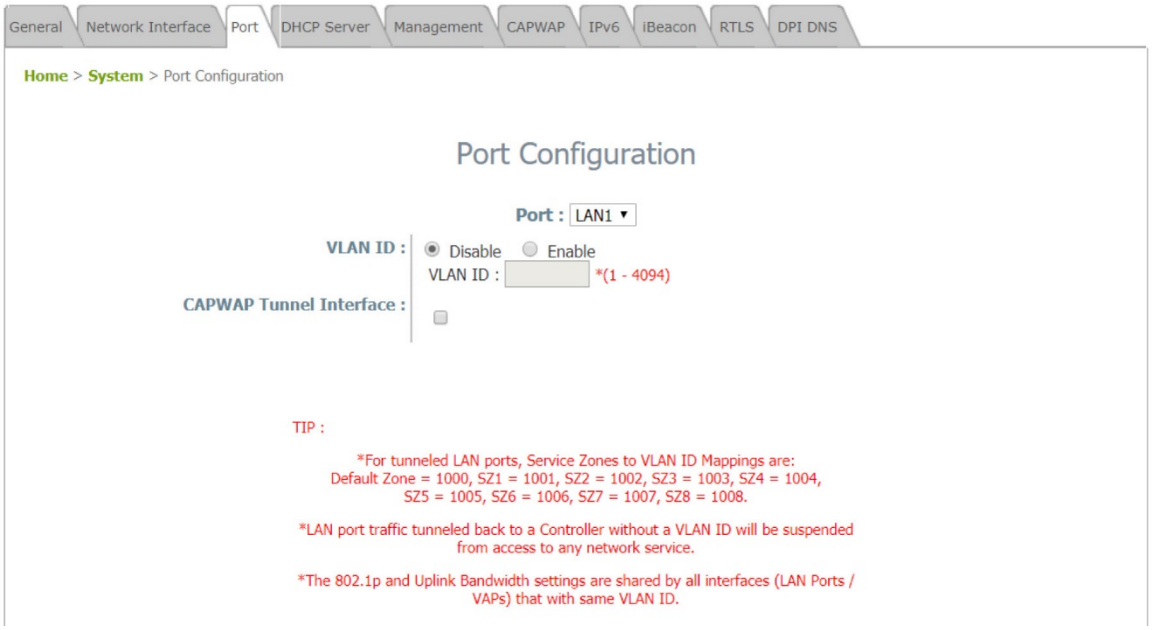
エンタープライズアクセスポイント**LLDP**：LLDP（Link Layer Discovery Protocol）は、（**TxInterval * TxHold**）秒ごとに定期的に再送信することで、基本デバイス情報をLAN（Local Area Network/ローカルエリアネットワーク）上の他のデバイスに通知する手段を提供するため。イーサネットフレームにカプセル化されたメッセージを定義するIEEE標準プロトコル（IEEE 802.1ab）です。

- **TxInterval**：パケットを送信する間隔を設定します。
- **TxHold**：パケットを送信する間隔の回数を設定します。

Layer 2 STP(レイヤー2 STP)：APが他のネットワークコンポーネントをブリッジするように設定されている場合、ブロードキャストストームがスイッチ間のエンドレスループで転送されるマルチスイッチ環境でブロードキャストストームが発生する可能性があるため、このオプションを有効にして不要なループを防ぐことができます。さらに、ブロードキャストストームは、利用可能な帯域幅に加えて、利用可能なシステムリソースのほとんどを消費する可能性があります。したがって、レイヤー2 STPを有効にすると、このような望ましくない発生を減らし、ネットワーク通信に使用可能な最良のデータパスを導出できます。また、APはRSTP動作をサポートします。構成可能なパラメーターには、**Bridge Priority(ブリッジ優先度)、Hello Time(ハロー時間)、Max Age(最大経過時間)、Forward Delay(転送遅延)**が含まれます。推奨されるパラメーター値については、IEEE標準を参照してください。



3.3 Port(ポート)



Port(ポート)：詳細構成用に1つのポートを選択します。

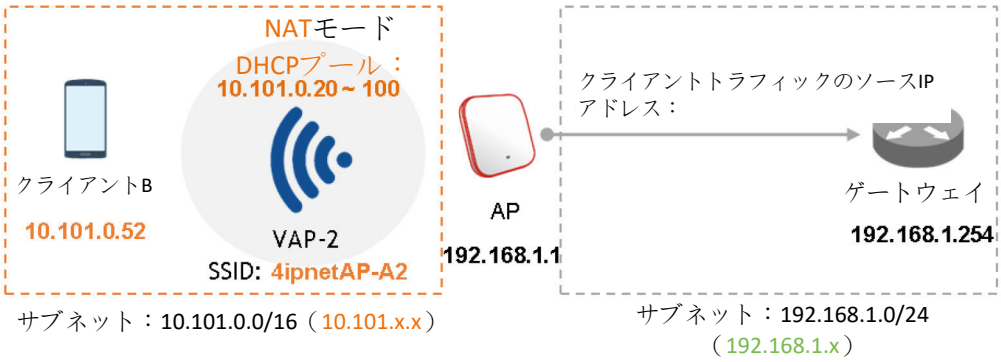
VLAN ID：[Enable(有効)]を選択すると、このLANポートからアップストリームに送信されるネットワークトラフィックは、下のフィールドで構成されたVLAN IDでタグ付けされます。[Disable(無効)]を選択すると、このLANポートからのトラフィックは、VLAN IDでタグ付けされません。

CAPWAP Tunnel Interface（CAPWAPトンネルインターフェイス）：LAN、VAP、またはWDSインターフェイスを選択して、APとコントローラーの間に確立されたCAPWAPトンネルを通過するトラフィックを指定します。オンにされていないネットワークインターフェイスについて、このAPがコントローラーのWAN側にリモートで配置されている場合、トラフィックはローカルでインターネットに転送されます。

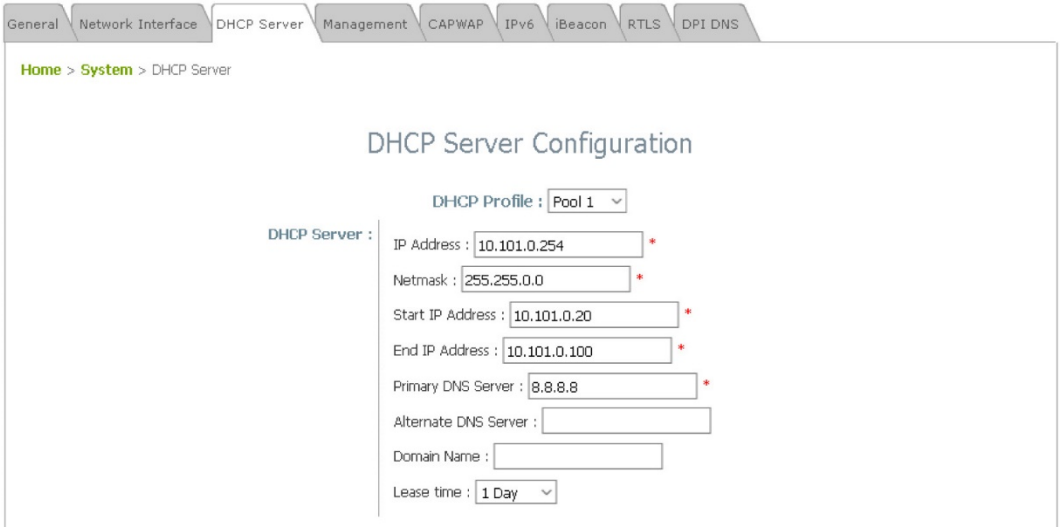
ページの下部にある赤色の「TIP(ヒント)」では、CAPWAPを使用する場合、デフォルトからService Zone 8(サービスゾーン8)までの各サービスゾーンに固定の事前に定義されたVLAN ID番号があることを説明しています。管理者は、トラフィックを特定のService Zone（サービスゾーン）に戻すために、いずれかの番号を入力する必要があります。

3.4 DHCP Server(DHCPサーバー)

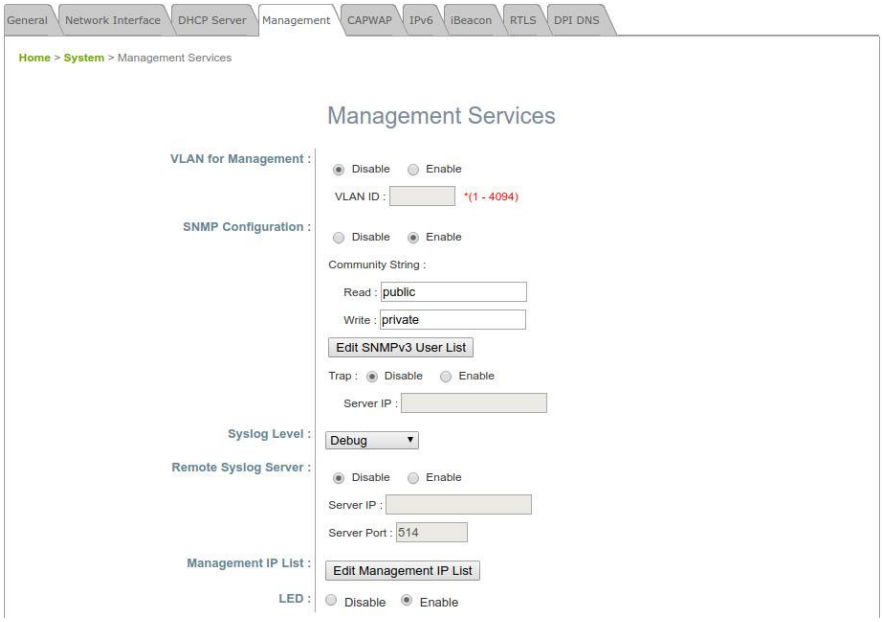
1つのVAPがNATモードで動作するように有効にされている場合、関連付けられたクライアントデバイスには、SSIDで構成されたDHCPプールから動的DHCP IPアドレスが割り当てられます。NATおよびDHCPモードは、トンネルなしで実行するか、スプリットトンネルを備えたEdgecore WLANコントローラーで管理できます。



Pool1(プール1)～Pool16(プール16)は、すべてデフォルト値としてAクラスDHCP IPアドレスとして構成され、APのWeb管理インターフェイスでのみ構成可能であることに注意してください。これは、16個のDHCPプロファイルに対して10.101.0.254/16から10.116.0.254/16で始まり、DHCPリース時間はデフォルトで1440分です。



3.5 Management(管理)



VLAN for Management(管理用VLAN):これを有効にすると、システムからの管理トラフィックにVLAN IDのタグが付けられます。つまり、WMIにアクセスする必要がある管理者は、同じVLAN IDを持つ特定のVAPに接続するなど、同じVLAN IDを持つ管理トラフィックを送信する必要があります。オプションが有効な場合は、VLAN IDに1～4094の値を入力してください。

SNMP Configuration(SNMP構成):システム情報をリモートで取得します。

- **Enable(有効化)/Disable(無効化)**:この機能を*有効*または*無効にします*。
- **Community String(コミュニティストリング)**:コミュニティストリングは、システムの管理情報ベース(Management Information Base/MIB)にアクセスするときに必要です。**Read(読み取り)**:コミュニティストリングを入力して、読み取り権限でMIBにアクセスします。**Write(書き込み)**:コミュニティストリングを入力して、書き込み権限でMIBにアクセスします。
- **Edit SNMPv3 User List(SNMPv3ユーザーリストの編集)**:システムは、5人のSNMPユーザーに読み取りまたは読み取りおよび書き込みアクセスを許可します。
  SNMP Account List(SNMPアカウントリスト)で、Name(名前)とAuthentication Password(認証パスワード)を決定します。
- **Trap(トラップ)**:有効にすると、Cold Start(コールドスタート)、Interface UP & Down(インターフェイスのアップとダウン)、およびAssociation & Disassociation(関連付けと関連付け解除)に関するイベントを、割り当てられたサーバーに報告できます。
- **Server IP Address(サーバーIPアドレス)**:トラップレポートを受信する割り当てられたサーバーのIPアドレスを入力します。

Syslog Level(Syslogレベル):ドロップダウンメニューから希望する受信イベントレベルを選択します。「Debug(デバッグ)」レベルはデフォルト設定です。

Remote Syslog Server(リモートSyslogサーバー):この機能が有効になっている場合は、システムからリモートでSYSLOGメッセージを受信する外部SYSLOGサーバーを指定してください。

- **Enable(有効化)/Disable(無効化)**:この機能を*有効*または*無効にします*。
- **SYSLOG Server IP(SYSLOGサーバーIP)**:報告されたイベントを受信するSyslogサーバーのIPアドレス。

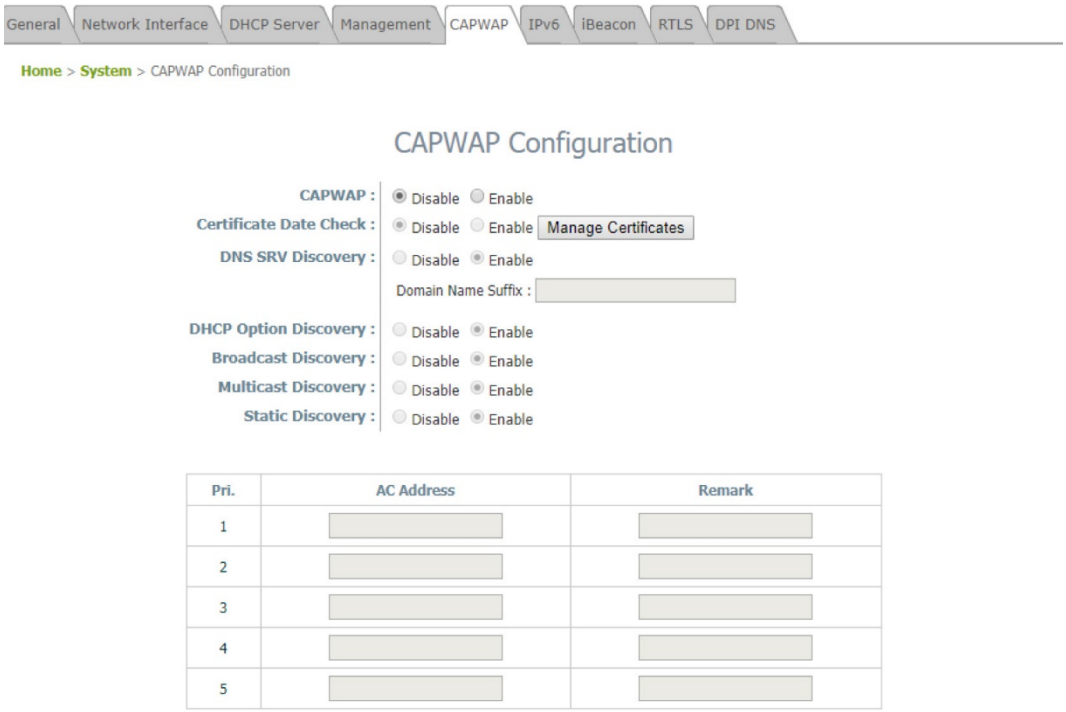
- **Server Port(サーバーポート)**：Syslogサーバーのポート番号。

Management IP List(管理IPリスト)：このAPのWMIへのアクセスを許可されている管理者PCのソースIPアドレス/サブネットを入力します。このリストに含まれていない他のユーザーは、WMIアクセスを拒否されます。デフォルトのエントリ0.0.0.0/0.0.0.0は、管理者がどこからでもWMIにアクセスできることを意味します。

LED：APのステータスLEDインジケーターをオンまたはオフにします。

3.6 CAPWAP

CAPWAPとは、コントローラーが無線アクセスポイントのコレクション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。自動AP検出には、DNS SRV、DHCPオプション、Broadcast(ブロードキャスト)、Multicast(マルチキャス)ト、Static(静的)の5つの方法があります。



CAPWAP：CAPWAP機能を有効または無効にします。

Certificate Date Check(証明書日付チェック)：この項目を有効にする場合は、*[Enable(有効化)]*を選択し、*[Manage Certificates(証明書の管理)]*をクリックして[Upload Certificate(証明書のアップロード)]ページに入ります。セクション4.4.5「証明書のアップロード」を参照してください。
DNS SRV Discovery(DNS SRV検出)：DNS SRVを使用して、アクセスコントローラーを検出します。

- **Domain Name Suffix(ドメイン名サフィックス)**：アクセスコントローラーのサフィックス（example.comなど）を入力します。

DHCP Option Discovery(DHCPオプション検出)：DHCPオプションを使用して、アクセスコントローラーを検出します。

Broadcast Discovery(ブロードキャスト検出)：ブロードキャストを使用して、アクセスコントローラーを検出します。

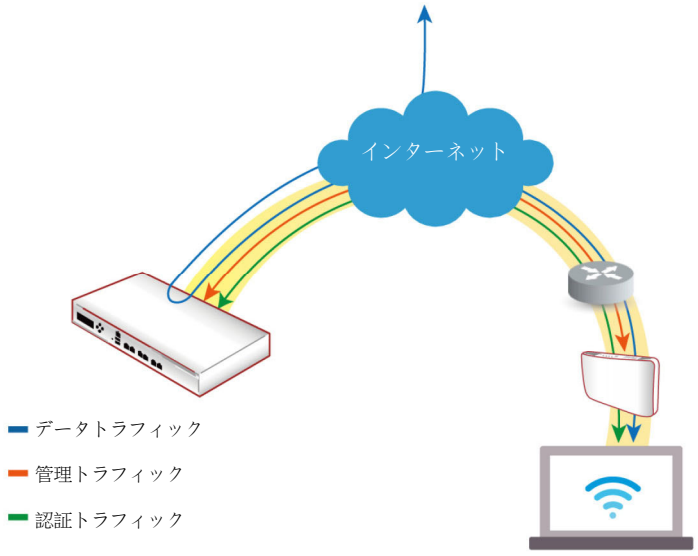
Multicast Discovery(マルチキャスト検出)：マルチキャストを使用して、アクセスコントローラーを検出します。

Static Discovery(静的検出)：静的アプローチを使用して、アクセスコントローラーを検出します。

- **AC Address(ACアドレス)**：アクセスコントローラーのIPアドレス。最初のACを検出できない場合は、2番目のACを検出しようとします。

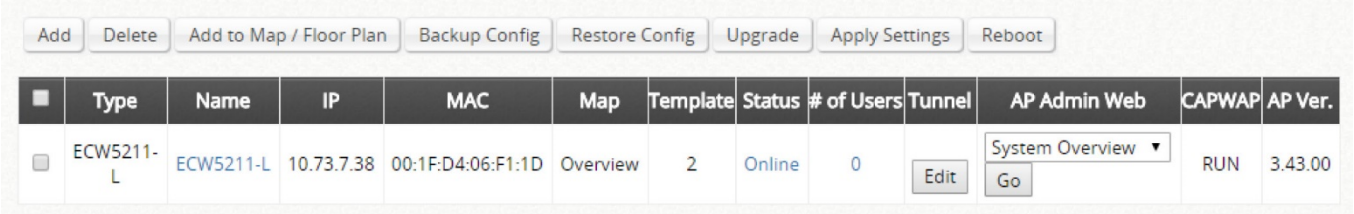
3.6.1 完全トンネルを備えたWLANコントローラーで管理する

完全トンネルは、CAPWAPプロトコルを使用してアクセスポイントと通信するため、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は、データトラフィックをインターネットに転送する前にコントローラーに送信されます。WLANコントローラーは、レイヤー3ネットワークを介してロールベースのポリシーを実装でき、リモートサイトでユーザーアクセスコントロールを利用できます。この機能により、WLANコントローラーは、一元化されたAP管理とユーザー管理を完全にサポートできます。

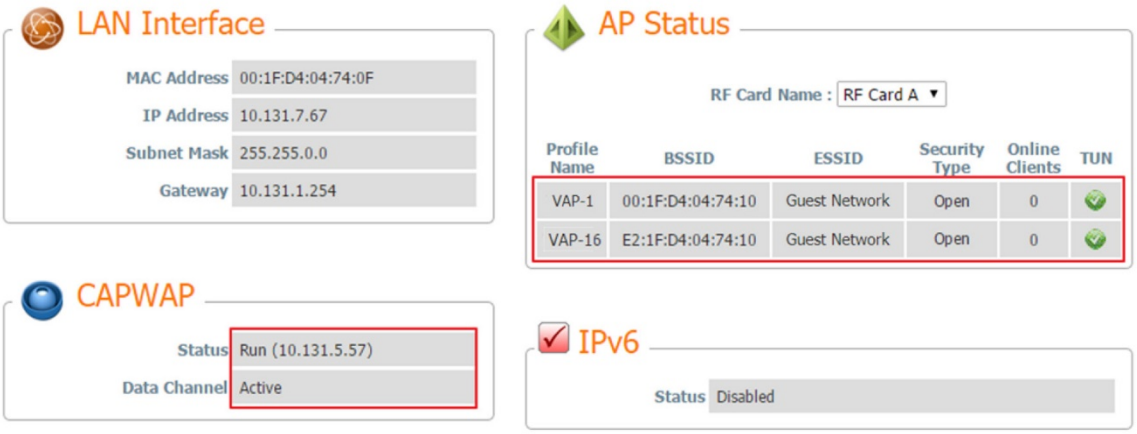


次の手順が役立つ場合があります

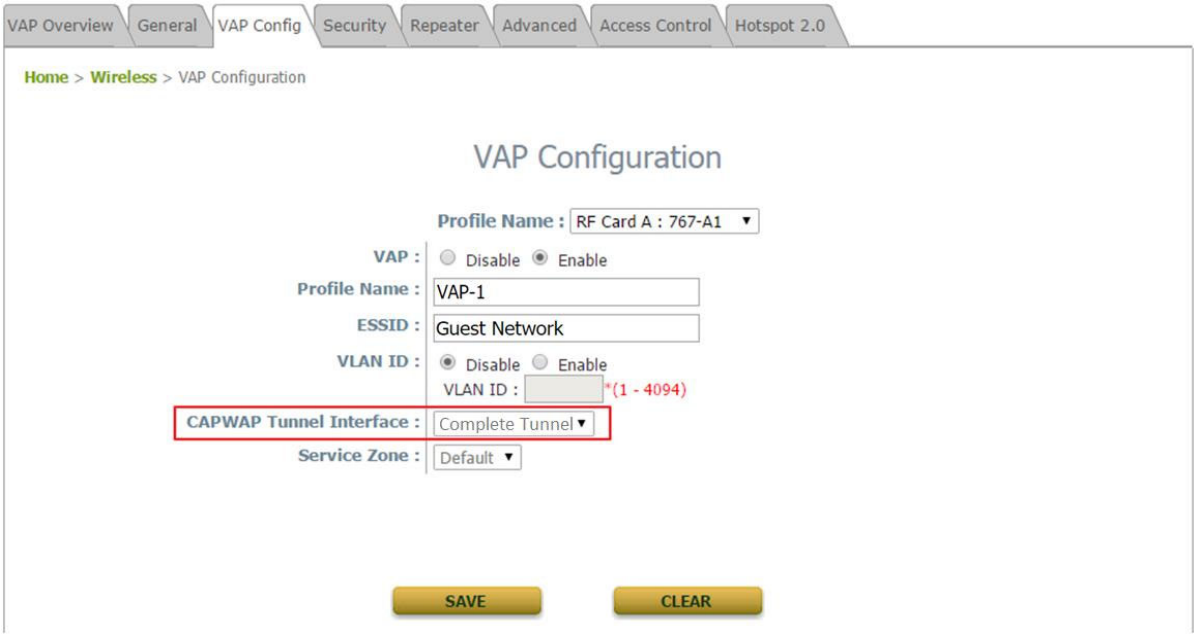
1. APの場合：**Static Discovery(静的検出)**のIPアドレスを入力し、CAPWAP列に「RUN(実行)」ステータスが表示されるまで待機します。
2. EWSの場合：**CAPWAPトンネルインターフェイス – 「完全トンネル」でVAP構成**のテンプレートを準備します
3. EWSの場合：VAPがトンネリングされてコントローラーに戻るように構成されている場合、準備されたテンプレートをCAPWAP確立APに適用すると、トンネルステータスにクリック可能な「Edit(編集)」ボタンが黒で表示されます。



4. APの場合：[System Overview(システム概要)]ページの[Green(緑)]ライトのVAPトンネルステータスで、Data Channel(データチャンネル)が「Active(アクティブ)」であることを示すAP WMIを確認します

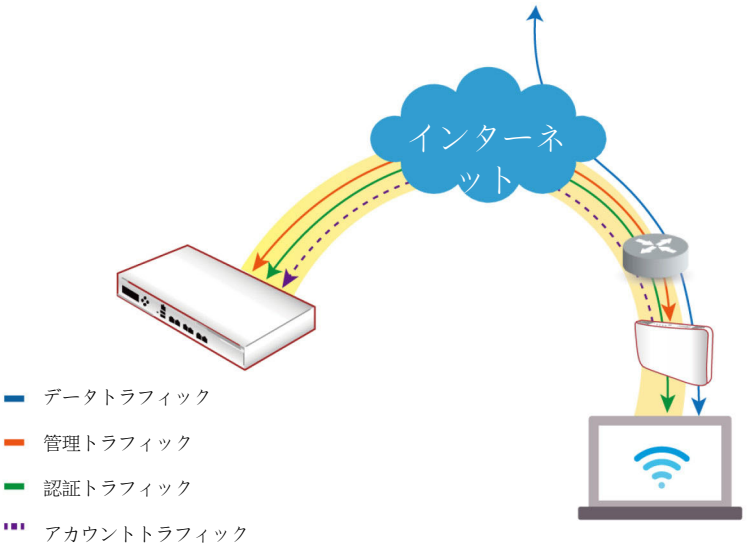


5. APの場合：特定のVAP構成が**Complete Tunnel(完全トンネル)**の下にあることを再確認します



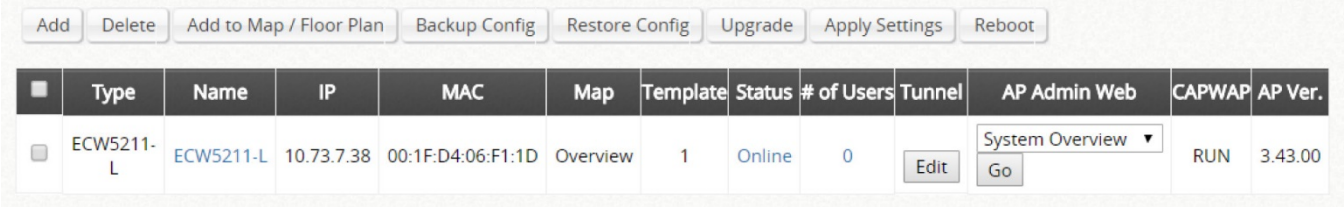
3.6.2 完全トンネルを備えたWLANコントローラーで管理する

スプリットトンネルの場合、ユーザー認証関連のトラフィックのみがコントローラーにリダイレクトされます。認証されたユーザーの場合、データトラフィックは、ローカルネットワークを介して直接インターネットに送られます。ユーザーデータは、より短い経路で送信でき、コントローラーのネットワーク負荷も軽減できます。

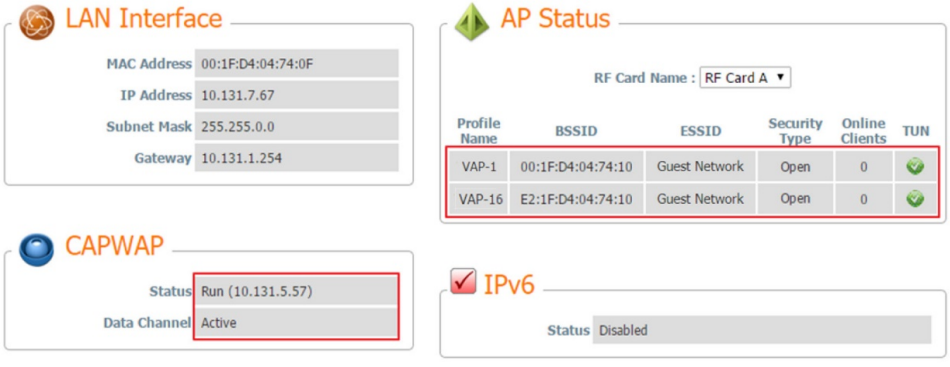


次の手順が役立つ場合があります

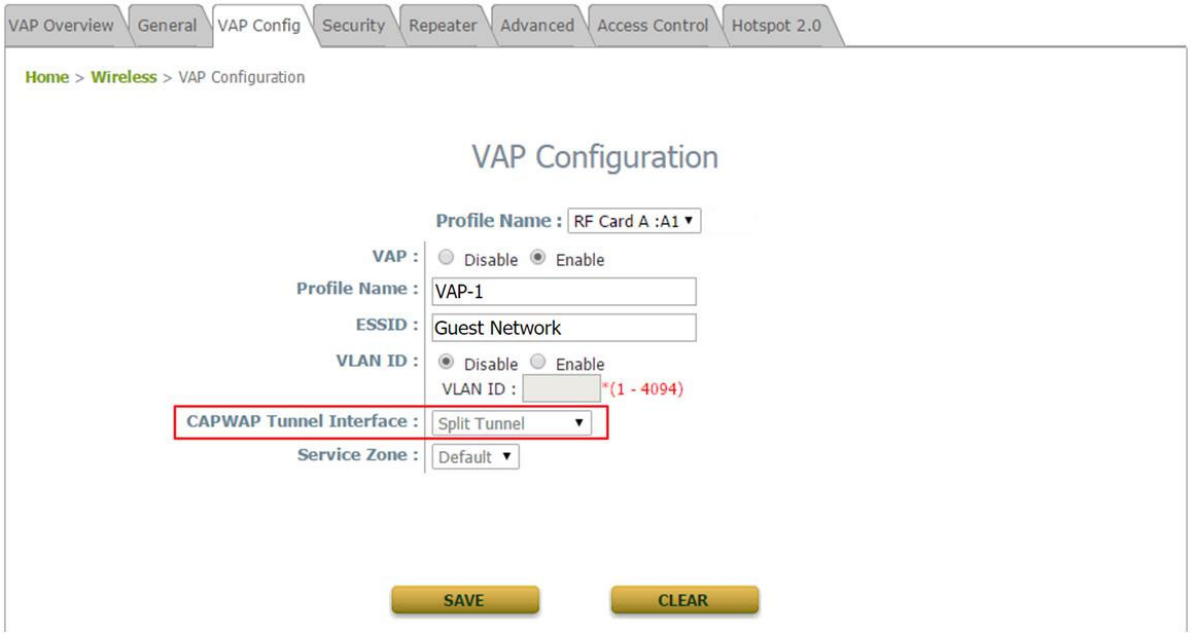
1. APの場合：**Static Discovery(静的検出)**のIPアドレスを入力し、CAPWAP列に「RUN(実行)」ステータスが表示されるまで待機します。
2. EWSの場合：**CAPWAPトンネルインターフェイス – 「スプリットトンネル」でVAP構成**のテンプレートを準備します
3. EWSの場合：VAPがトンネリングされてコントローラーに戻るように構成されている場合、準備されたテンプレートをCAPWAP確立APに適用すると、トンネルステータスにクリック可能な「Edit(編集)」ボタンが黒で表示されます。



4. APの場合：[System Overview(システム概要)]ページの[Green(緑)]ライトのVAPトンネルステータスで、Data Channel(データチャンネル)が「Active(アクティブ)」であることを示すAP WMIを確認します

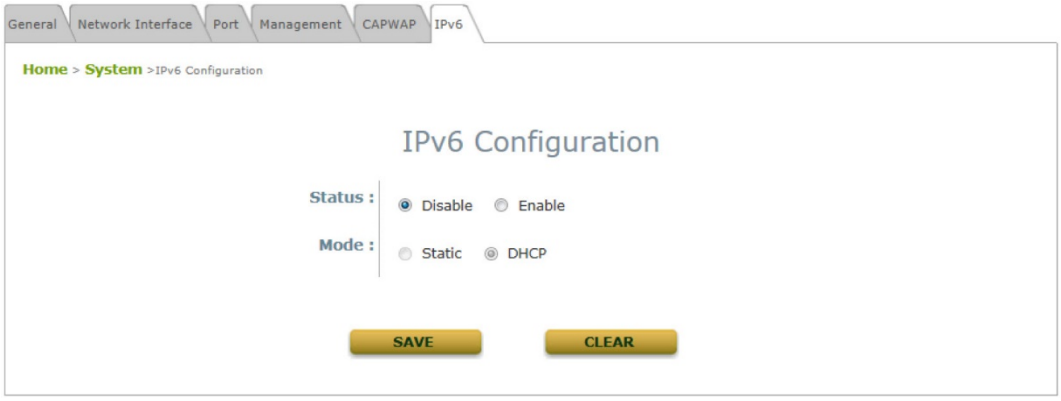


5. APの場合：特定のVAP構成が**Split Tunnel(スプリットトンネル)**の下にあることを再確認します



3.7 IPv6

IPv6およびIPv4デュアルスタックアドレス指定機能がサポートされています。



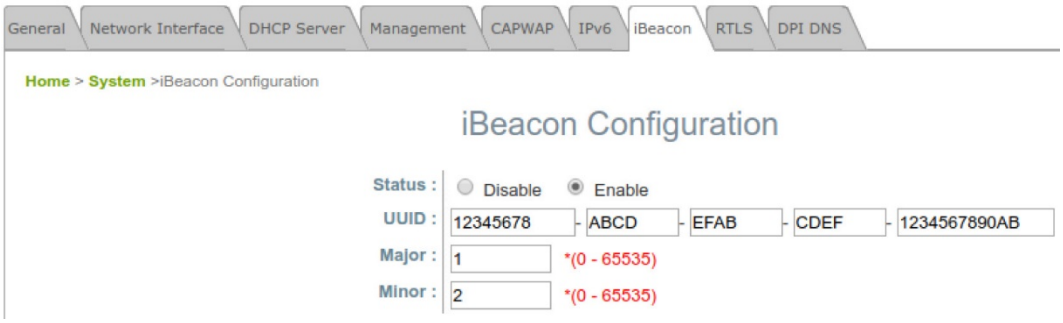
Status(ステータス):IPv6はデフォルトで無効になっていますが、このタブページで有効にできます。

Mode(モード):このデバイスのIPv6アドレスを取得するには、2つのオプションがあります。

- **Static(静的)**:操作用の永続的なIPv6アドレスを既に取得している場合は、このオプションを経由して、IPv6アドレスを手動で構成します。
- **DHCP**:アップストリームサーバーからIPv6アドレスを自動的に取得します。

3.8 iBeacon

iBeaconは、2013年にAppleによって導入された技術で、新しい位置認識サービスを可能にします。適切に構成されている場合、APは、iBeacon互換のハードウェアトランスミッターになり、Bluetooth Low Energy（BLE、無線接続技術）を経由して、近くのデバイスに情報をブロードキャストします。



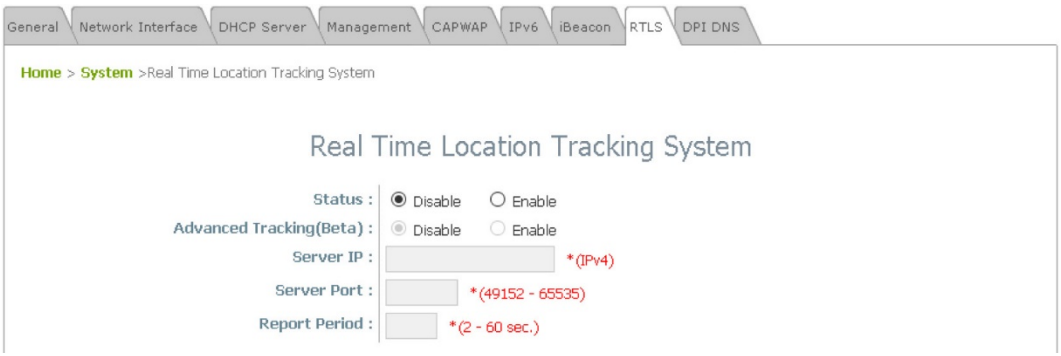
UUID、Major(メジャー)、およびMinor(マイナー)は、APによって継続的に送信されるiBeaconの「アドバタイズパケット（Advertising Packets）」の主要コンポーネントを構成するために使用される識別パラメーターです。

UUID：Universally Unique Identifier、ネットワーク内の独自のAPを、コントロール外のネットワーク内の他のすべてのiBeaconトランスミッターと区別するための番号。これは32桁の16進数を含み、5つのグループに分割され、次のようになります：12345678-ABCD-EFAB-CDEF-1234567890AB

Major(メジャー)/Minor(マイナー)：これらは、UUIDのみを使用するよりも高い精度でAPを識別するために独自のAPに割り当てられた番号（0～65535の整数値）です。通常、Major(メジャー)値は、グループを識別して区別することを目的としていますが、Minor(マイナー)値は、個人を識別して区別することを目的としています。たとえば、ショッピングセンターに同じUUIDで展開された多くのiBeaconトランスミッターがあり、それらが異なるフロア/店舗に配置されている場合です。次に、これらのトランスミッターは、異なるMajor(メジャー)（たとえば、1階の場合は1）とMinor(マイナー)（たとえば、2階の場合は2）の値によって識別および区別できます。

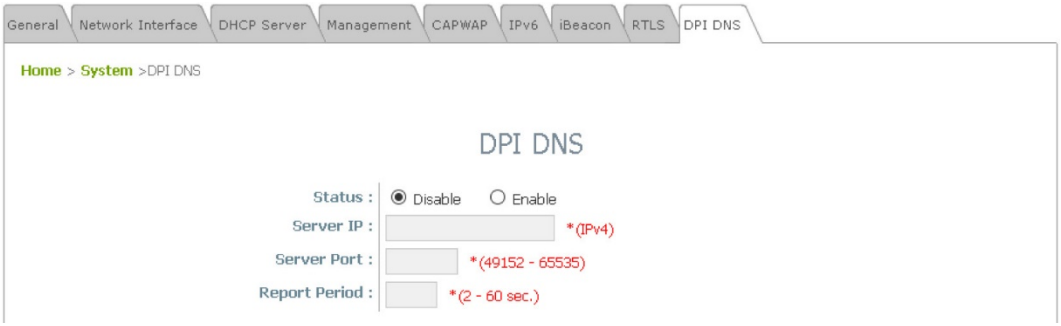
3.9 RTLS

Wi-Fiベースの位置情報ソリューションを実装する場合は、この機能を有効にしてAPをリアルタイム位置情報システム（RTLS）の専用Linkyfi（Edgecore技術パートナー）サーバーと統合できます。これは、Linkyfi Location Engine（すべてのタイプの会場での屋内位置情報とリアルタイムナビゲーションのための高度なソフトウェアソリューション）の一部です。



3.10 DPI DNS

Wi-Fiマーケティング分析を実行する場合は、この機能を有効にして、APをLinkyfiのDNSサーバーに統合できます。これは、ディープパケットインスペクション（Deep Packet Inspection/DPI）技術を経由して、DNSトラフィックを分析するLinkyfi Location Engineの一部でもあります。

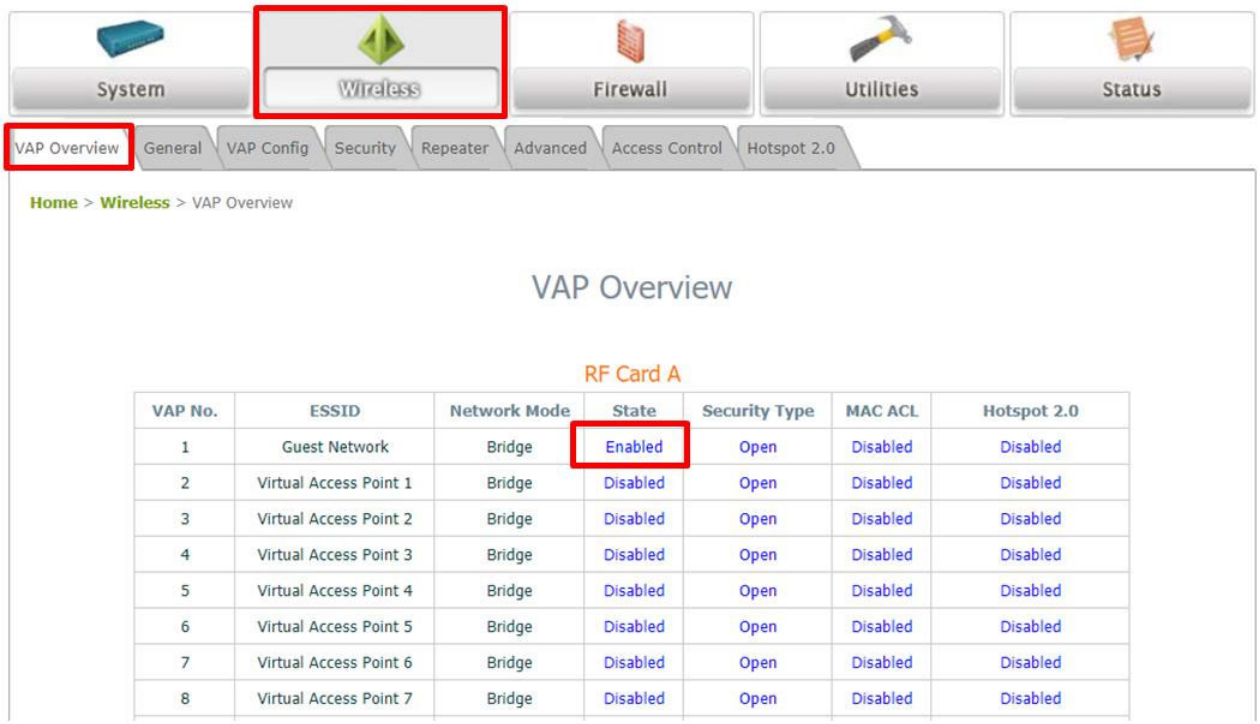


4. 無線

このセクションには、以下の機能が含まれます：**VAP Overview(VAP概要)、General(一般)、VAP Configuration(VAP構成)、Security(セキュリティ)、Repeater(リピーター)、Advanced(詳細)、Access Control(アクセスコントロール)**および**Hotspot 2.0(ホットスポット2.0)**。Edgecoreアクセスポイントは、RFカードごとに最大16の仮想アクセスポイント（Virtual Access Point/VAP）をサポートします。各VAPには、独自の設定（ESSID、VLAN ID、セキュリティ設定など）があります。このようなVAP機能を使用すると、さまざまなレベルのサービスを構成して、ネットワーク要件を満たすことができます。

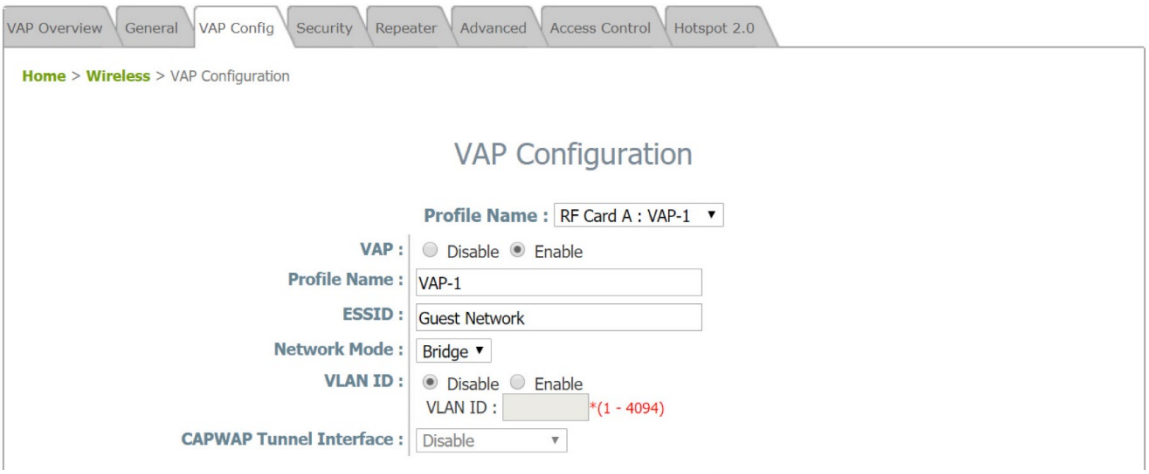
4.1 VAP Overview(VAP概要)

このページでは、**ESSID、Network Mode(ネットワークモード)、State(状態)、Security Type(セキュリティタイプ)、MAC ACL、Hotspot 2.0(ホットスポット2.0)**などの全体的なステータスが収集されます。APは、各設定で無線ごとに16個のVAPを備えています。この表で、ハイパーリンクをクリックして、各VAPをさらに構成してください。



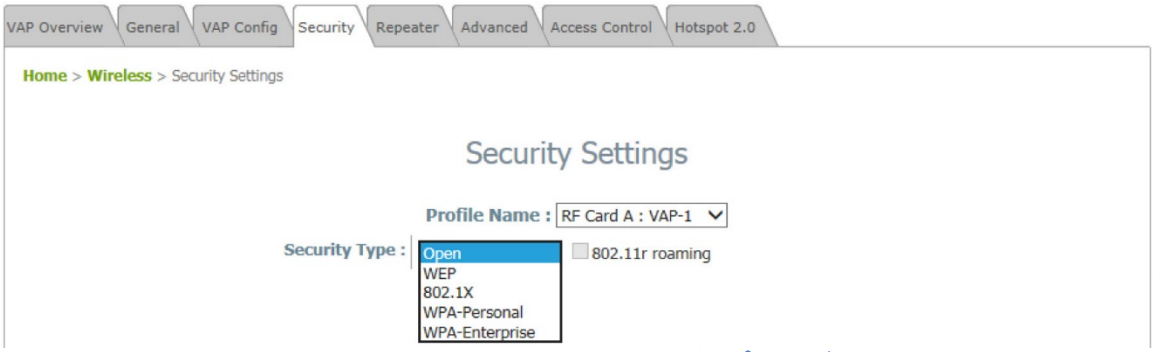
VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled
4	Virtual Access Point 3	Bridge	Disabled	Open	Disabled	Disabled
5	Virtual Access Point 4	Bridge	Disabled	Open	Disabled	Disabled
6	Virtual Access Point 5	Bridge	Disabled	Open	Disabled	Disabled
7	Virtual Access Point 6	Bridge	Disabled	Open	Disabled	Disabled
8	Virtual Access Point 7	Bridge	Disabled	Open	Disabled	Disabled

State(状態):**[VAP Configuration(VAP構成)]**ページへの***Enable(有効化)***または*****Disable(無効化)***リンクを示すハイパーリンク。



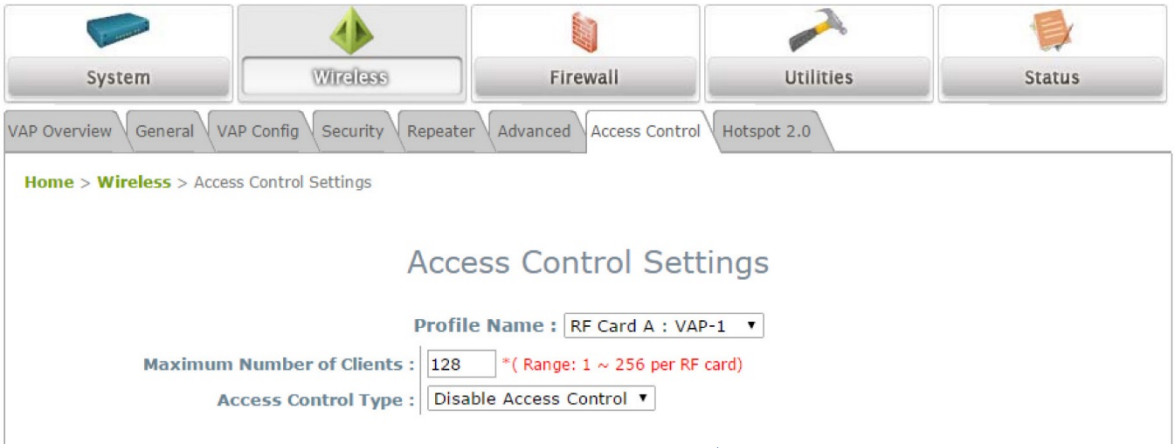
VAP – [State(状態)]ページ

Security Type(セキュリティタイプ):**[Security Settings(セキュリティ設定)]**ページへのセキュリティタイプリンクを示すハイパーリンク。



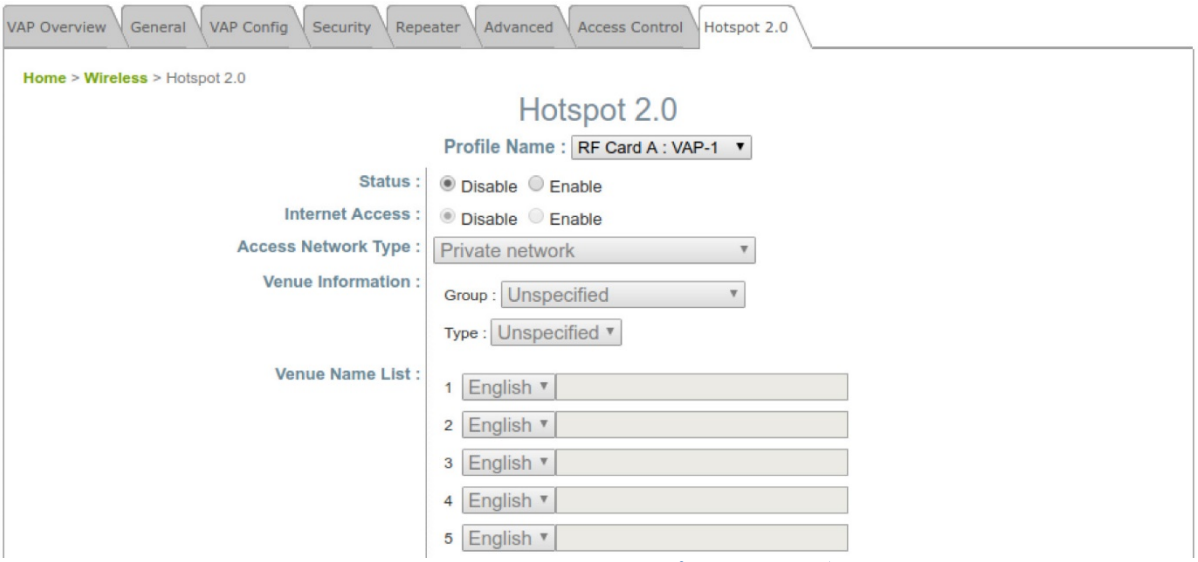
VAP – [Security Type(セキュリティタイプ)]ページ

MAC ACL:**[Access Control Settings(アクセスコントロール設定)]**ページへの**Allow(許可)**または**Disable(無効化)**リンクを示すハイパーリンク。



VAP – [MAC ACL]ページ

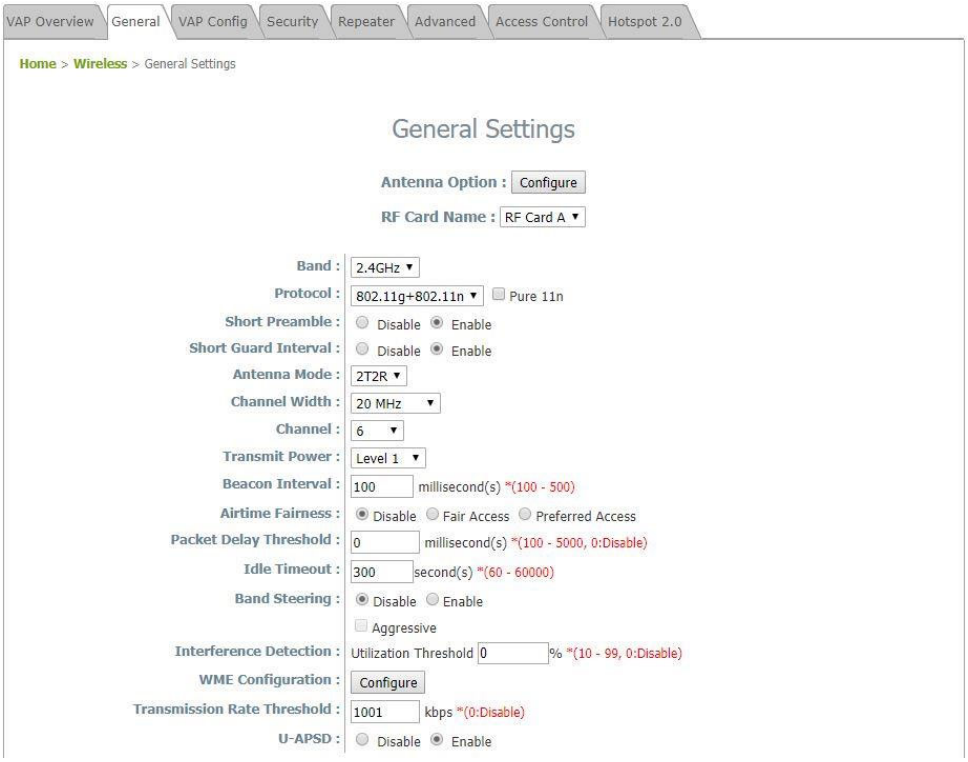
Hotspot 2.0(ホットスポット2.0)：**[Hotspot 2.0(ホットスポット2.0)]**ページへの詳細設定用ハイパーリンク。



VAP – [Hotspot 2.0(ホットスポット2.0)]ページ

4.2 General(一般)

APのシステムの一般的な無線設定を構成できます



Antenna Option(アンテナオプション)(OAP100のみ):デバイスは、4台のアンテナで構成され、2台は2.4GHz用、2台は5GHz用です。異なるサービスには2つのオプションがあります。

- **Hotspot(ホットスポット)**:ホットスポットの目的で使用します。2つの2.4GHzは、クライアントにサービスを提供するために使用される無指向性アンテナを採用しています。 2つの5GHzは、30度の方位角と仰角を持つ指向性アンテナを採用し、ポイントツーポイント接続に使用されます。
- **Point to Point(ポイントツーポイント)**:ポイントツーポイントの目的で使用します。2つの2.4GHzと2つの5GHzはどちらも、方位角90度、仰角30度の指向性アンテナを採用しています。

RF Card Name(RFカード名):詳細構成用に1つのRFカードを選択します。

Band(バンド):無線機能が必要ない場合は、***[Disable(無効化)]***を選択してください。

Protocol(プロトコル):次の適切な無線プロトコルを選択してください:***802.11a***、***802.11a+802.11n***、***802.11ac***または***802.11b***、***802.11g***、***802.11b+802.11g***、***802.11g+802.11n***。プロトコルは、**Band(バンド)**または**RF Card(RFカード)**によって異なります。

- **Pure 11n(ピュア11n)**:802.11nネットワークのみを有効にしてください。

Short Preamble(短いプリアンブル):56ビットの同期フィールドを持つ短いプリアンブルは、WLAN伝送効率を向上させることができます。短いプリアンブルを使用する場合は***[有効化]***を選択し、128ビットの同期フィールドを持つ長いプリアンブルを使用する場合は***[無効化]***を選択してください。

Short Guard Interval(ショートガードインターバル)(バンドが802.11g+802.11nまたは802.11a+802.11nまたは802.11acの場合に使用可能):ガードインターバルは、シンボル間干渉を排

除するために送信されるシンボル（文字）間のスペースです。**802.11n**でスループット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になります。ショートガードインターバルを使用する場合は***[有効化]***、通常のガードインターバルを使用する場合は***[無効化]***を選択してください。

Antenna Mode(アンテナモード)：RFカードの空間ストリームの数を選択します。1つの空間には1T1Rを選択します
1つの空間ストリームには1T1R、2つの空間ストリームには2T2Rを選択します。

Channel Width(チャンネル幅)（バンドが802.11g+802.11nまたは802.11a+802.11nまたは802.11acの場合に使用可能）：スループットを向上させるための40 MHzまたは80 MHzへのダブルチャンネル帯域幅。

Channel(チャンネル)：規則性を満たすために、ドロップダウンメニューから適切なチャネルを選択します。

- 無線カードBで「Auto(自動)」として構成されている場合、選択したチャネルが干渉したり、DFSチャンネル信号が検出された場合のチャネル切り替え用のチャンネルセレクターテーブルがあります
- 屋外APモデルの場合、「Outdoor mode(屋外モード)」は、チャンネル選択に影響します

Channel Selector(チャンネルセレクター)：このオプションは、Band(バンド)が5GHzに設定され、チャンネルがAuto(自動)またはDFSチャネルに設定されている場合に、RFカードBに対して表示されます。以下を行うため、操作用に目的のチャンネルを選択します

- システムが起動し、Channel(チャンネル)がAuto(自動)に設定されている場合、システムは、どちらのチャンネルがよりクリアであるかに基づいて、選択されたチャンネルからチャンネルを選択します。
- DFSチャンネルでレーダー信号が検出されたとき、または干渉しきい値（設定されている場合）に達したときなどの理由により、システムが別のチャンネルに切り替えると決定した場合、どちらのチャネルがよりクリアであるかに基づいて、選択したチャネルの1つにのみ切り替えます。

Transmit Power(送信電力)：システムから送信される信号強度は、レベルによって選択できます。

- 各レベルは、最大電力からの1dBmの減少を意味します。
- レベル1は実際の最大電力であり、レベル2は最大電力から1dBmを引いたものです（以下同様です）。

Distance(距離)：これは、WDS経由で接続されている場合の、システムからクライアントまたは別のアクセスポイントまでの距離を指します。距離の値を入力すると、以下のACKタイムアウトの値が自動調整されます。

ACK Timeout(ACKタイムアウト)：これは、システムが再送信せずにステーションから送り返された確認応答フレームを待つ期間を示します。つまり、タイムアウト時に確認応答フレームがまだ受信されていない場合、フレームは再送信されます。このオプションを使用すると、カバレッジを拡大するためにネットワークパフォーマンスを調整できます。通常の屋内展開の場合は、デフォルト設定を維持してください。

Beacon Interval (ms)(ビーコン間隔（ミリ秒）)：入力した時間は、ビーコン信号がアクセスポイントから送信される頻度を示します。

- 7つを超えるVAPが有効になっている場合、Beacon Interval(ビーコン間隔)は500ミリ秒より長くする必要があります。
- 3つを超えるVAPが有効になっている場合、Beacon Interval(ビーコン間隔)は250ミリ秒より長くする必要があります。

Airtime Fairness(エアタイムフェアネス):802.11a/b/g/nレガシーデバイスが通信時間を占有すると、802.11acデバイスのスループットが影響を受けます。

- **Enable(有効化)**:バンドの互換性が異なるすべてのデバイスが同じ通信時間を持つようにします。この機能は、さまざまなバンドをサポートするデバイスを備えたネットワークに最適です。
- **Preferred Access(優先アクセス)**:Nバンドのクライアントが優先されます。この機能は、さまざまなバンドをサポートするデバイスを備えたネットワークに最適です。

Packet Delay Threshold (ms)(パケット遅延しきい値(ミリ秒)):アクセスポイントは、ビジー状態のクライアントまたは範囲外のクライアントにパケットを送信しようとして占有されているため、接続されている他のクライアントへの送信が遅れている可能性があります。有効にすると、このTxキューフラッシュメカニズム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、他のパケットの処理をすぐに開始します。デフォルトは0(無効)です。この機能により、複雑な無線ネットワークのパフォーマンスが向上しますが、一部のパケットを再送信する必要がある場合があります。

Idle Timeout (s)(アイドルタイムアウト(秒)):非アクティブが構成された時間(秒単位)に達すると、クライアントは切断されます。デフォルトは300秒です。

Band Steering(バンドステアリング):有効にすると、5GHz接続のクライアントは5GHzバンドに誘導され、2.4GHzバンドの輻輳を軽減します。これは、2つのRFカードでAPが2.4GHzおよび5GHzに設定されている場合にのみ適用されます。

- **Aggressive(アグレッシブ)**:5GHz接続のクライアントは、5GHz帯域に接続する必要があります。
- これはアクセスポイントの一般的な設定であり、RFカードごとには設定されないことに注意してください。

Interference Detection(干渉検出):現在のチャンネルまたは隣接チャネルのUtilization(使用率)、Latency(遅延)(およびInvalid Packet Rate(無効なパケットレート))が構成済みのしきい値(%単位)に達すると、APは別のチャンネルに切り替わります。

WME Configuration(WME構成):WMM(Wi-Fi Multimedia)としても知られるWME(Wireless Multimedia Extensions)は、IEEE 802.11e標準に基づくWi-Fi Alliance相互運用性認定です。IEEE 802.11ネットワークに基本的なサービス品質(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ーを使用して構成できます。CW Min:Contention Window Minimum(最小コンテンションウィンドウ)、CW Max:Contention Window Maximum(最大コンテンションウィンドウ)、AIFS:Arbitration Inter Frame Spacing(仲裁フレーム間の間隔)、TXOP Limit:Transmission Opportunity Limit(送信機会の制限)。

Transmission Rate Threshold(伝送速度しきい値):伝送速度が設定されたしきい値よりも低い場合、クライアントはキックされます。これにより、関連するすべてのクライアントの接続速度が高速になります。

CCA Minimum Power(CCA最小電力):CCA(Clear Channel Assessment/クリアチャネルアセスメント)は、無線周波数が占有されているかどうかを判断する方法です。CCA最小電力(CCA Minimum Power)は、システムが解決可能と見なす最小信号強度です。つまり、電力レベルがCCA最小電力よりも低い場合、受信信号はノイズとして扱われます。

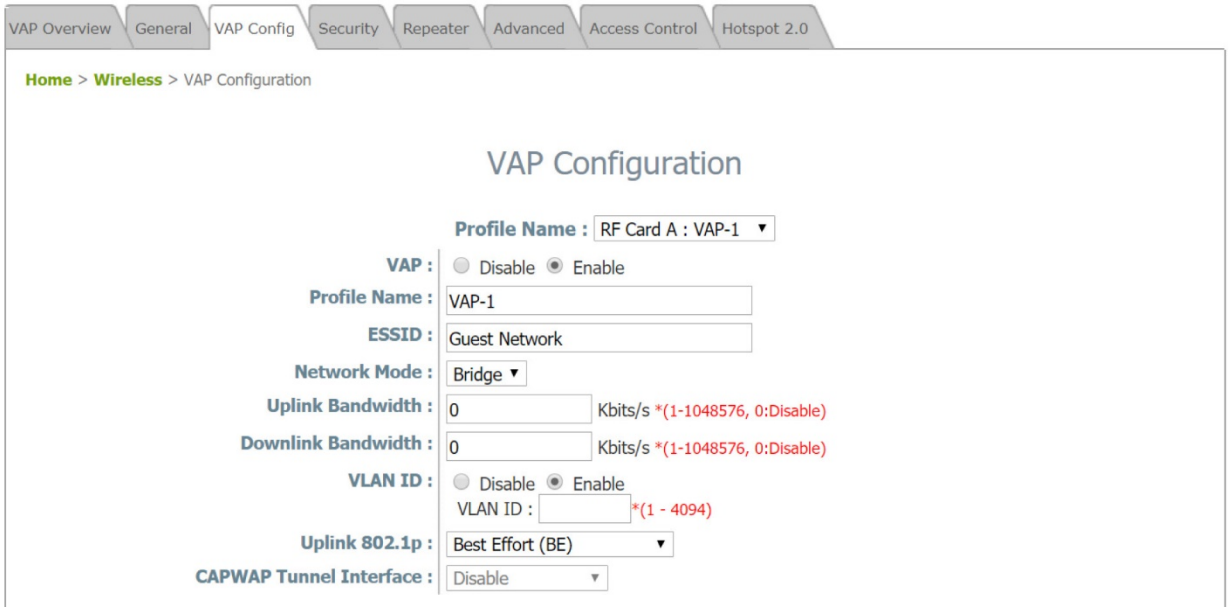
U-A SD：U-APSDとは、WMMで機能する802.11省電力メカニズムである**U**nscheduled **A**utomatic **P**ower **S**ave **D**eliveryの略です。クライアントデバイスが省電力モードの場合（つまり、受信機がオフになっているため、データフレームを受信できない場合）、APはクライアント宛てのすべてのフレームを一時的にバッファーします。

» 注：

Short Preamble(短いプリアンブル)、ACK Timeout(ACKタイムアウト)などの機能は、RFカードBで制限される場合があります。

4.3 VAP Config(VAP構成)

このセクションでは、各仮想アクセスポイントの構成と、**Profile Name(プロファイル名)**、**ESSID**、**VLAN ID**などの設定について説明します。特定のVAPを有効にする場合は、Profile Name(プロファイル名)のドロップダウンリストからVAPを選択してください。

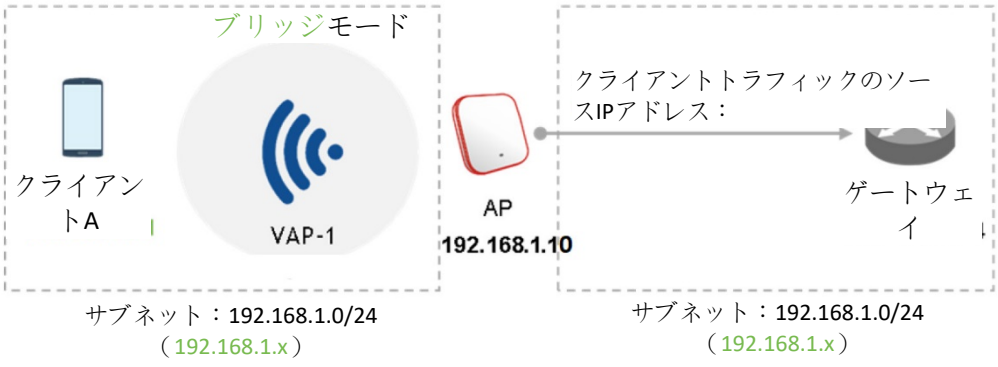


VAP:このVAPを無効または有効にします。

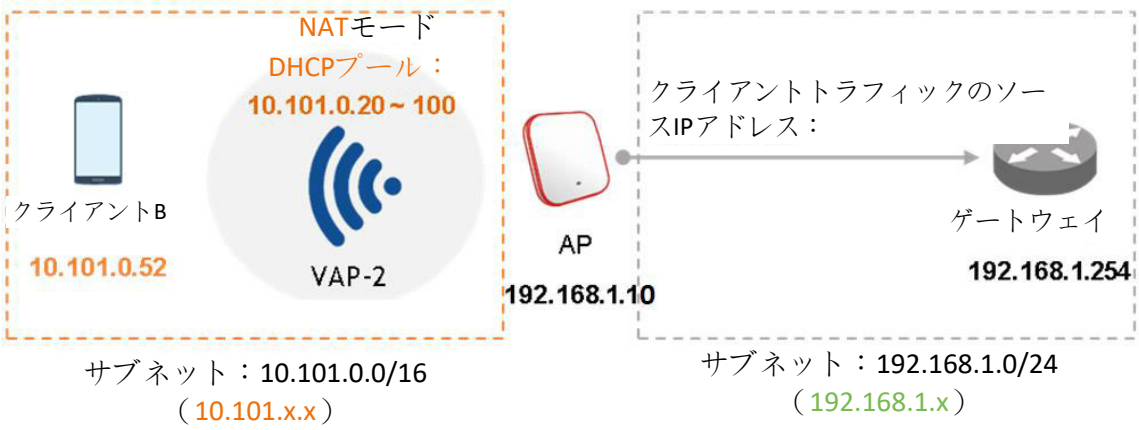
Profile Name(プロファイル名):識別/管理目的用のVAPプロファイル名。

ESSID:拡張サービスセット識別子(Extended Service Set Identifier/ESSID)は、特定のVAPに関連するクライアントの識別子として機能します。

Network Mode(ネットワークモード) –Bridge(ブリッジ)モード:VAPは透過的(つまり、非NAT、非DHCP)に動作します。したがって、クライアントデバイスは、LAN側のDHCPサーバーから動的IPアドレスが割り当てられます。アップリンクゲートウェイ/スイッチによって認識されるクライアントトラフィックのソースIPアドレスは、クライアントの元のIPアドレスのままです(この場合、下図に示す通り、192.168.1.31です)。



Network Mode(ネットワークモード) –NATモード:VAPは、このSSID上の内蔵SSIDと共にネットワークアドレス変換(Network Address Translation/NAT)デバイスとして動作します。つまり、クライアントデバイスには、このSSID上に構成されたDHCPプールから動的IPアドレスが割り当てられます。NAT変換後、アップリンクゲートウェイ/スイッチによって認識されるクライアントトラフィックのソースIPアドレスは、APのIPアドレスになります(この場合、下図に示す通り、192.168.1.10です)。



Uplink/Downlink Bandwidth(アップリンク/ダウンリンク帯域幅):帯域幅制御は、VAPでKbps単位で設定できます。無制限の帯域幅制御の場合は、0を設定してください。

VLAN ID:SSIDごとのVLANタグ付け機能 - 有効にすると、このSSIDを通してAPに入るクライアントのトラフィックは、構成されたVLAN IDによりタグ付けされます。

Uplink 802.1P per VAP(VAPごとのアップリンク802.1P):ここでは、アップリンクトラフィックの優先度レベルを選択できます。利用可能なオプションは、Background(バックグラウンド)、Best Effort(ベストエフォート)、Excellent Effort(エクセレントエフォート)、Critical Applications(クリティカルアプリケーション)、Video(ビデオ)、Voice(音声)、Internetwork Control(インターネットワーク制御)、Network Control(ネットワーク制御)です。詳細については、IEEE標準802.1Pを参照してください。

DHCP Profile(DHCPプロファイル)(NATモードの場合):内蔵DHCPサーバーのプロファイルです。DHCPサーバーのIP設定は、Home(ホーム) > System(システム) > DHCP Server(DHCPサーバー)にあります。

CAPWAP Tunnel Interface(CAPWAPトンネルインターフェイス):APがコントローラーにより管理されるとき、APとコントローラーの間の接続状態を示す3つの状態です。

- **Disable(無効)**(トンネルなし):APは、コントローラーに対するCAPWAPトンネル接続のない状態で動作します。
- **Split Tunnel(スプリットトンネル)**:APは、CAPWAPトンネルを経由して、コントローラーに「コントロール」トラフィックのみを通過させます。つまり、「データ」トラフィックは、トンネルを通過せずにローカルに送信されます
- **Complete Tunnel(完全トンネル)**:APは、CAPWAPトラフィックを経由して、「コントロール」トラフィックと「データ」トラフィックの両方を通過させます

注:
- VAPがブリッジモードであるときのみ、VLAN IDはサポートされます。
- VAPがNATモードに設定されているときのみ、DHCPプロファイルとDHCPサーバー

がアクティブになります。

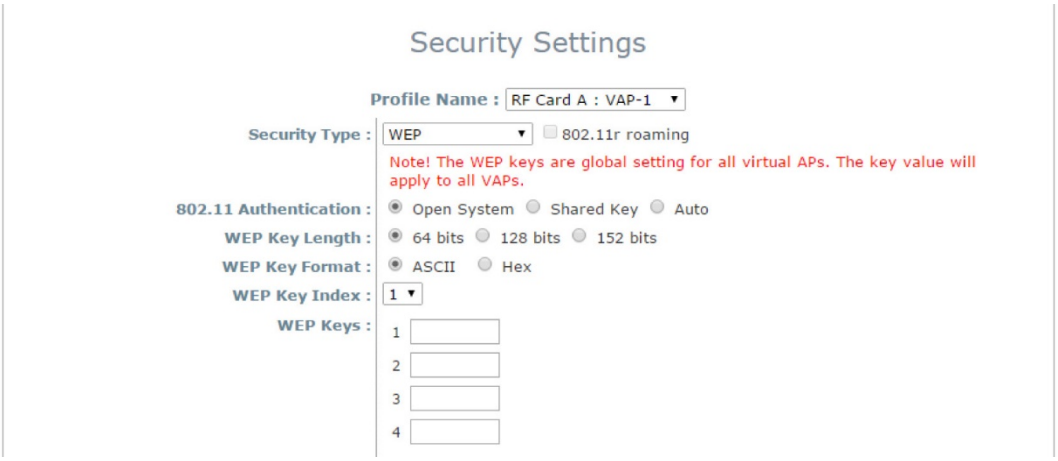
- VAPがNATモードである場合、CAPWAPトンネルインターフェイスは、次の2つの状態でのみ動作します：無効（トンネルなし）またはスプリットトンネル。

4.4 Security(セキュリティ)

APは、各VAPプロファイルでさまざまな無線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さまざまな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、**Open(オープン)**、**WEP**、**WPA-Personal(WPAパーソナル)**、**WPA-Enterprise(WPAエンタープライズ)**、**OSEN**があります。

Open(オープン):認証は必要なく、データは送信中に暗号化されません。

WEP:Wired Equivalent Privacy(有線と同等のプライバシー/WEP)は、64ビット、128ビット、または152ビットの共有キーアルゴリズムに基づくデータ暗号化メカニズムです。

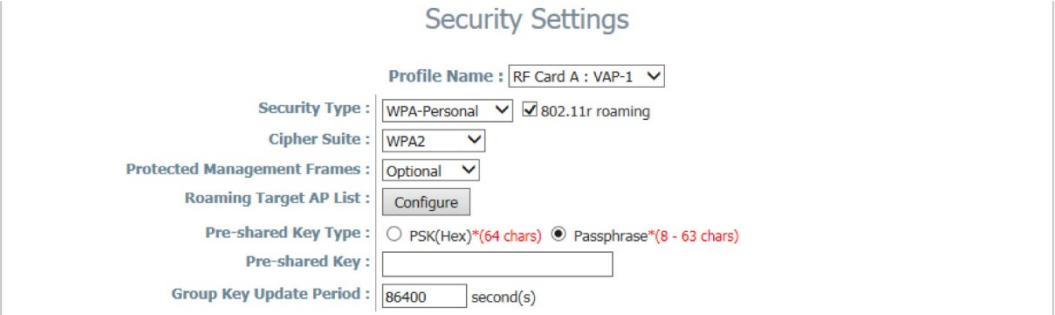


- **802.11 Authentication(802.11認証)**:*Open System(オープンシステム)*、*Shared Key(共有キー)*、または*Auto(自動)*から選択します。
- **WEP Key Length(WEPキーの長さ)**:キーの長さを*64-bit(64ビット)*、*128-bit(128ビット)*、または*152-bit(152ビット)*から選択します。
- **WEP Key Format(WEPキーの形式)**:WEPキーの形式を***ASCII***または***Hex(16進数)***から選択します。
- **WEP Key Index(WEPキーインデックス)**:キーインデックスを***1～4***から選択します。WEPキーインデックスは、データ送信中に無線フレームの暗号化に使用されるWEPキーを指定する番号です。
- **WEP Keys(WEPキー)**:事前定義されたWEPキー値を入力します。システムは最大4セットのWEPキーをサポートします。

注: 一部のAPモデルでは、WEPキーの長さが制限されている場合があります。

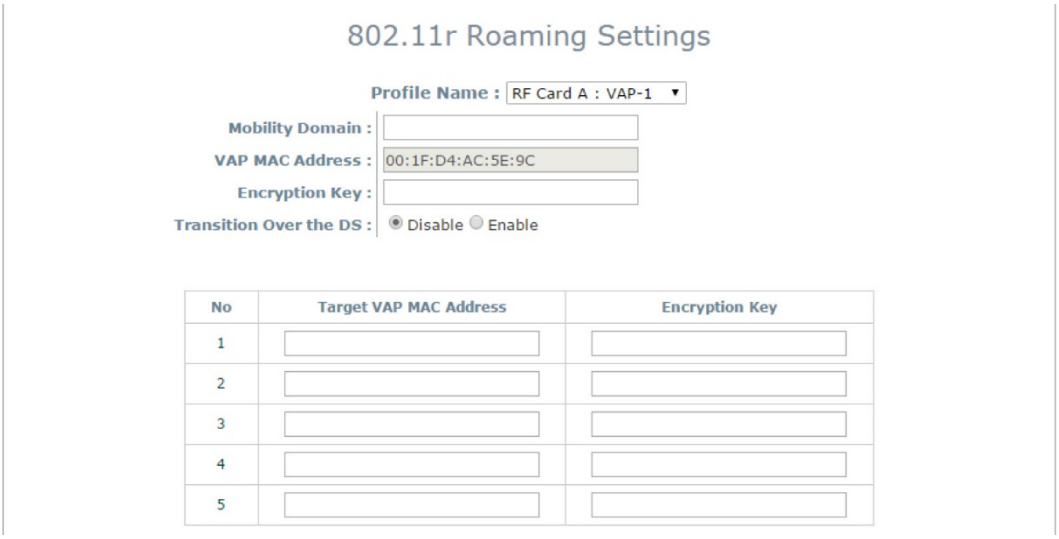
WPA-Personal(WPAパーソナル):WPA-Personal(WPAパーソナル)は、事前共有キー(PSK)認証方法です。

- **802.11r Roaming(802.11rローミング)**:ローミングは、同じAPの同じモビリティドメイン内で同じ暗号化キーを持つクライアントに対して行うことができます。



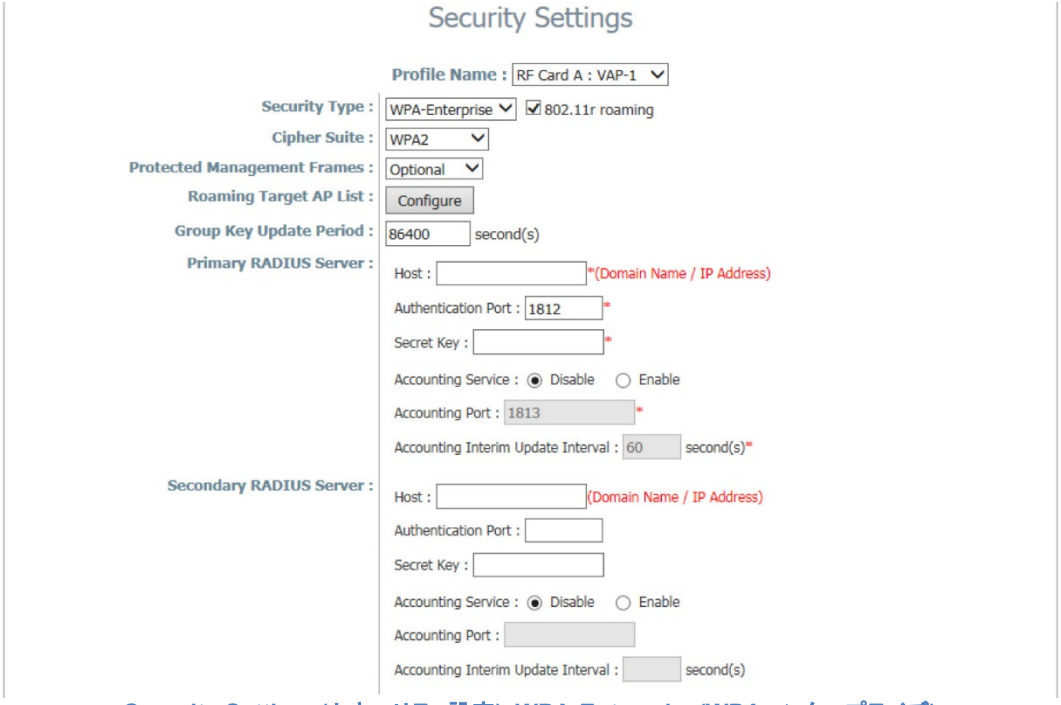
Security Settings(セキュリティ設定):WPA-Personal(WPAパーソナル)

- **Cipher Suite(暗号スイート)**:暗号化方法を***WPA2***または***WPA2/WPA***から選択します。
- **Protected Management Frames(保護された管理フレーム)**:Disable(無効化)、Optional(任意)またはMandatory(必須)を選択します。
- **Roaming Target AP List(ローミングターゲットAPリスト)**(802.11rが有効である場合)



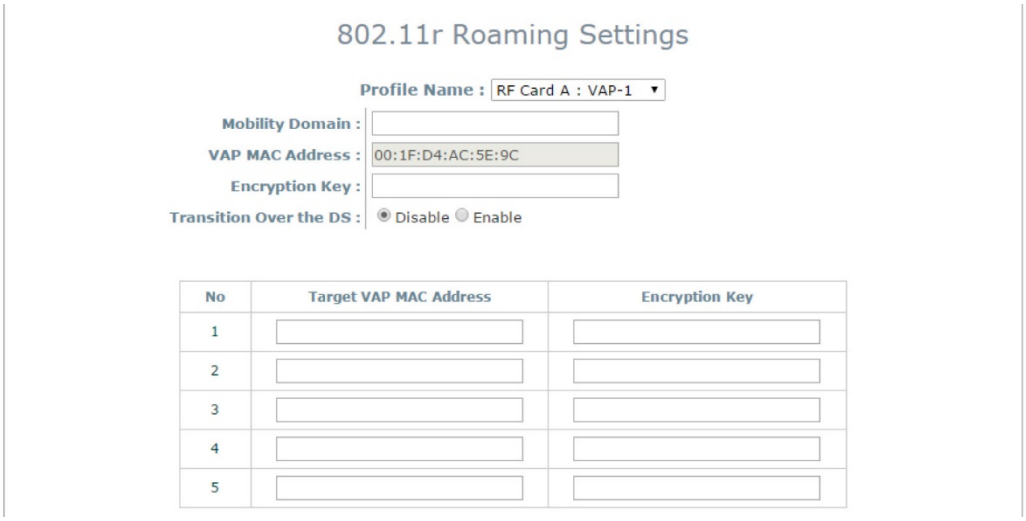
- **Pre-shared Key Type(事前共有鍵タイプ)**:事前共有鍵のタイプ(PSK(16進数)またはPassphrase(パスフレーズ))を選択します。
- **Pre-shared Key(事前共有鍵)**:事前共有鍵のキー値を入力します。キー値の形式は、選択した鍵のタイプによって異なります。
- **Group Key Update Period(グループキーの更新期間)**:グループキーを更新する時間間隔。時間の単位は秒です。

WPA-Enterprise(WPAエンタープライズ):選択すると、RADIUS認証とデータ暗号化の両方が有効になります。



Security Settings(セキュリティ設定):WPA-Enterprise(WPAエンタープライズ)

- **Cipher Suite(暗号スイート)**:暗号化方法を***WPA2***または***WPA2/WPA***から選択します。
- **Protected Management Frames(保護された管理フレーム)**:Disable(無効化)、Optional(任意)またはMandatory(必須)を選択します。
- **Roaming Target AP List(ローミングターゲットAPリスト)**(802.11rが有効である場合)



- **Group Key Update Period(グループキーの更新期間)**:グループキーを更新する時間間隔。時間の単位は秒です。
- **RADIUS Server Settings (Primary/Secondary)(RADIUSサーバー設定(プライマリ/セカンダリ))**:
  - **Host(ホスト)**:RADIUSサーバーのIPアドレスまたはドメイン名を入力します。
  - **Authentication Port(認証ポート)**:RADIUSサーバーが使用するポート番号。ポート番号を指定するか、デフォルトの1812を使用します。
  - **Secret Key(秘密鍵)**:システムがRADIUSサーバーと通信するための秘密鍵。

- **Accounting Service(アカウンティングサービス)**:このオプションを*有効にする*と、RADIUSサーバーを介したログインおよびログアウトのアカウンティングが可能になります。
- **Accounting Port(アカウンティングポート)**:RADIUSサーバーがアカウンティングのために使用するポート番号。
  ポート番号を指定するか、デフォルトの1813を使用します。
- **Accounting Interim Update Interval(アカウンティング暫定更新間隔)**:システムは、間隔ごとにRADIUSサーバーへのアカウンティング情報を更新します。

OSEN:OSENとは、「The Online Signup (**O**SU) **S**erver-only authenticated layer 2 **E**ncryption **N**etwork(オンラインサインアップ(OSU)サーバーのみの認証済みレイヤー2暗号化ネットワーク)」の略で、「Hotspot 2.0 Release2」(HS2.0 R2)認証方式です。HS2.0 R2を設定する前に、各VAP、HS2.0 VAP(VAP1:WPA-Enterprise)またはOSEN VAP(VAP2:OSEN)のセキュリティを確認する必要があります。その他の構成の詳細については、*「セクション4 .8 Hotspot 2 .0」*を参照してください。

4.5 Repeater(リピーター)

APはWDSを利用して、無線ネットワークのカバレッジを拡張できます。無線ごとにピアAPへの最大8つのWDSリンクをサポートします。リモートピアのMACアドレスを入力し、***[SAVE(保存)]***をクリックして続行してください。

WDS:選択したWDSリンクプロファイルを*有効*または*無効にします*。

WDS Link Address(WDSリンクアドレス):選択したWDSリンクのAPインターフェイスのMACアドレス。

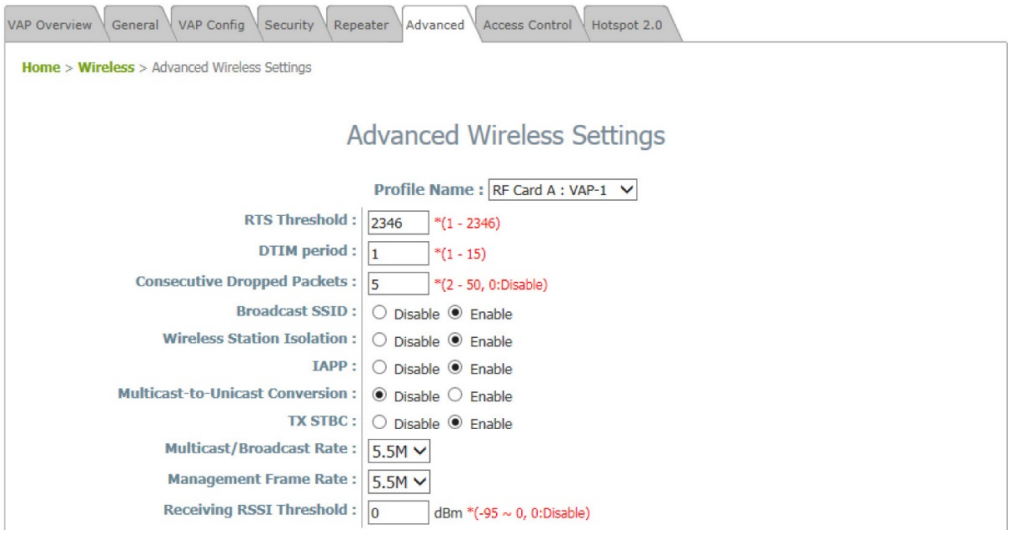
Remote AP MAC Address(リモートAP MACアドレス):リモートピアのMACアドレス。

Security Type(セキュリティタイプ):None(なし)、WEPまたはWPA-Personal(WPAパーソナル)。

CAPWAP Tunnel Interface(CAPWAPトンネルインターフェイス):このオプションをオンにして、APとコントローラーの間に確立されたCAPWAPトンネルを通過するようにWDSトラフィックを指定します。

4.6 Advanced(詳細)

管理者は次のパラメーターを調整して、接続不良が発生した場合のネットワーク通信パフォーマンスを向上させることができます。



RTS Threshold(RTSしきい値):1から2346までの値を入力しますRTS(Request to Send/信要求)しきい値は、システムがフラグメントを送信する前に送信要求(RTS)を発行して、隠しノードの問題を回避するパケットサイズを決定します。データサイズが指定された値を超えると、RTSメカニズムがアクティブになります。RTSしきい値を低く設定すると、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エリアや、クライアントが離れており、APのみを検出でき、お互いを検出できないエリアで役立ちます。

Fragmentation Threshold(フラグメンテーションしきい値)(802.11a、802.11b、および802.11gモード):256から2346までの値を入力しますこのしきい値より大きいパケットサイズは、送信前にフラグメント化されます(1つのチャンクではなく、いくつかのピースで送信されます)。値が小さいほどフレームは小さくなりますが、送信できるフレーム数が多くなります。Fragment Threshold(フラグメンテーションしきい値)設定を低くすると、通信が不十分であるか、深刻な量の無線干渉によって妨害されているエリアで役立ちます。

DTIM Period(DTIM期間):指定した頻度で定期的なビーコン内で生成されるDTIM間隔を入力します。DTIMが高いほど、無線クライアントはより多くのエネルギーを節約できますが、スループットは低下します。

Consecutive Dropped Packets(連続損失パケット):これは、クライアントが送信範囲外であると判断する前にパケット送信が失われたときにAPが試行する最大送信再試行回数です。送信の再試行が設定された回数失敗すると、アクセスポイントはクライアントをキックして、接続されている他のクライアントのパフォーマンスを最適化します。

Broadcast SSID(ブロードキャストSSID):この機能を無効にすると、システムはSSIDをブロードキャストしなくなります。SSIDのブロードキャストが無効になっている場合、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(無線ステーションの分離):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分離され、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ワイヤレスステーションの情報をピアアクセスポイントに自動的にブロードキャストします。これにより、ワイヤレスステーションは、同じワイヤレスLAN内のIAPP対応アクセスポイント間をスムーズにローミングできます。

Multicast-to-Unicast Conversion(マルチキャストからユニキャストへの変換)：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、アクセスポイントは、マルチキャストトラフィックを要求するポート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、ネットワークが非効率になります。

TX STBC：STBCとは、MIMOトランスミッターによって行われる送信前エンコーディングであり、単一RFレシーバー（非MIMO）でも信号対雑音比を向上させることができます。

Multicast/Broadcast Rate(マルチキャスト/ブロードキャストレート)：マルチキャスト/ブロードキャストパケットの帯域幅構成。無線クライアントがマルチキャスト/ブロードキャストパケットを送信するために、より大きなまたはより小さな帯域幅を必要とする場合、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。

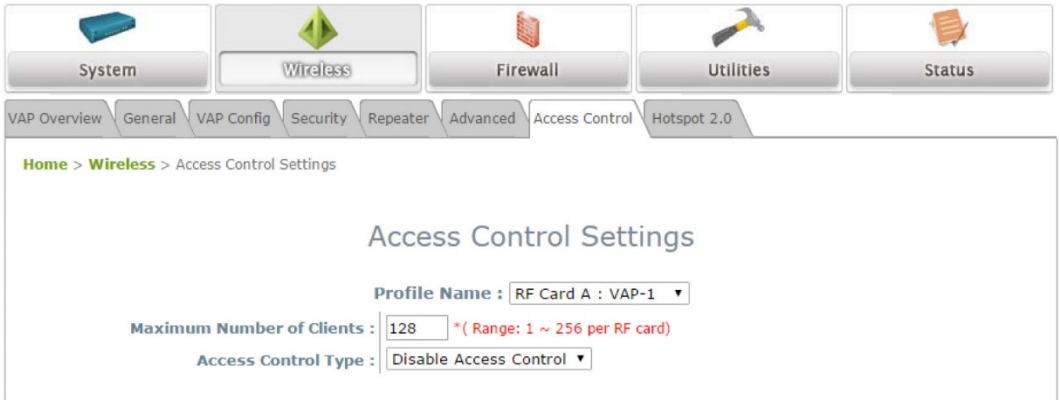
Management Frame Rate(管理フレームレート)：この機能は、管理フレームの帯域幅を制御します。

Receiving RSSI Threshold(受信RSSIしきい値)：接続されたステーションに高品質の接続速度があることを保証するため、ステーションは、その受信感度が構成されたしきい値を満たさない限り、ネットワークに関連付けることができません。

» 注：　一部のAPモデルでは、TX STBCが制限されている場合があります。

4.7 Access Control(アクセスコントロール)

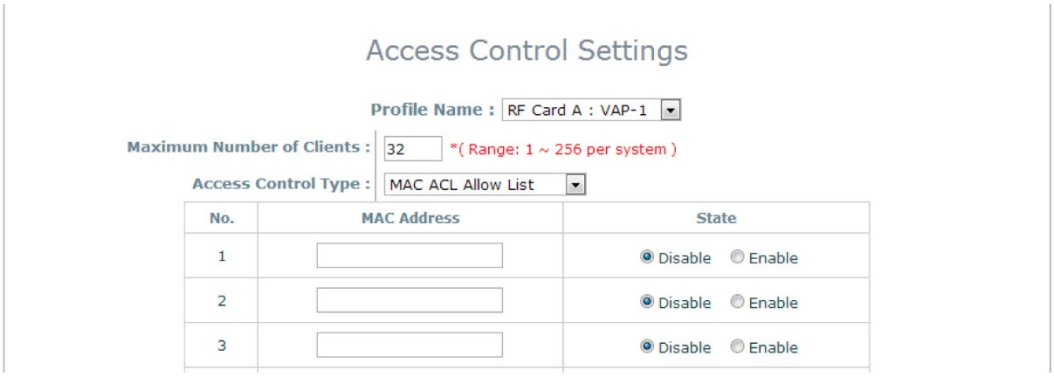
このページでは、ネットワーク管理者は、アクセスポイントに接続されているクライアントの総数を制限したり、デバイスにアクセスできる、またはアクセスできない特定のMACアドレスを指定したりできます。



Maximum Number of Clients(クライアントの最大数):デフォルトのポリシーは、認証を必要としない無制限のアクセスです。無線接続のステーション数を制限する場合は、値を目的の数に変更してください。たとえば、ステーション数が20に設定されている場合、指定されたVAPに接続できるのは20ステーションだけです。

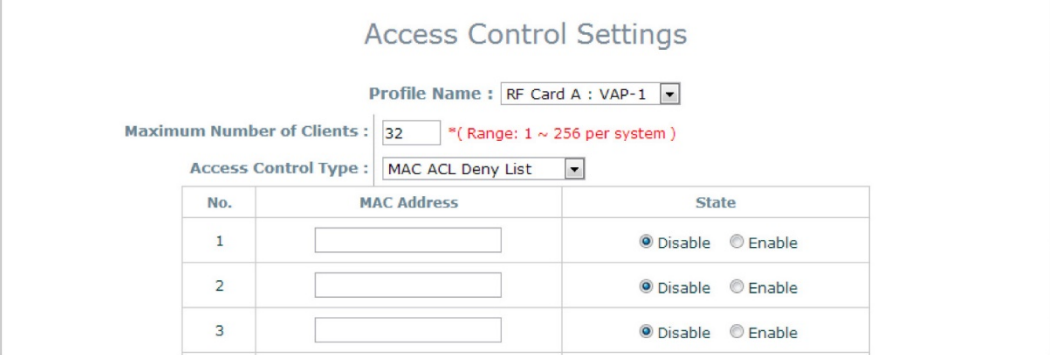
Access Control Type(アクセスコントロールタイプ) – Disable Access Control(アクセスコントロールの無効化):[Disable(無効化)]が選択されている場合、クライアントデバイスがシステムにアクセスするための制限はありません。

Access Control Type(アクセスコントロールタイプ) – MAC ACL Allow List(MAC ACL許可リスト):***[MAC ACL Allow List(MAC ACL許可リスト)]***を選択すると、Allow List(許可リスト)にリストされているクライアントデバイス(MACアドレスで識別される)(「許可されたMACアドレス」)にのみ、システムへのアクセスが許可されます。管理者は、管理者がリストされたMACを再度有効にするまで、***[Disable(無効化)]***をオンにすることで、許可されたMACアドレスを一時的にブロックできます。

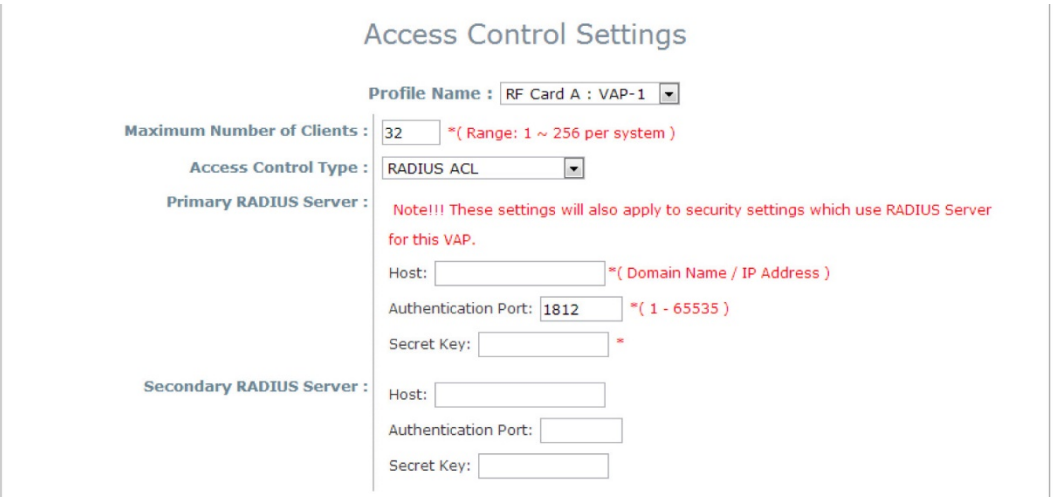


注: 空の許可リストは、許可されたMACアドレスがないことを意味します。少なくとも管理システムのMACが含まれていることを確認してください(例:ネットワーク管理者のコンピューター)

エンタープライズアクセスポイント **Access Control Type(アクセスコントロールタイプ) – MAC ACL Deny List(MAC ACL拒否リスト)**:***[MAC ACL Deny List,(MAC ACL拒否リスト)]***を選択すると、Deny List(拒否リスト)にリストされているもの(「拒否されたMACアドレス」)を除くすべてのクライアントデバイスにシステムへのアクセスが許可されます。管理者は、***[Disable(無効化)]***をオンにすることにより、拒否されたMACアドレスがシステムに一時的に接続することを許可できます。

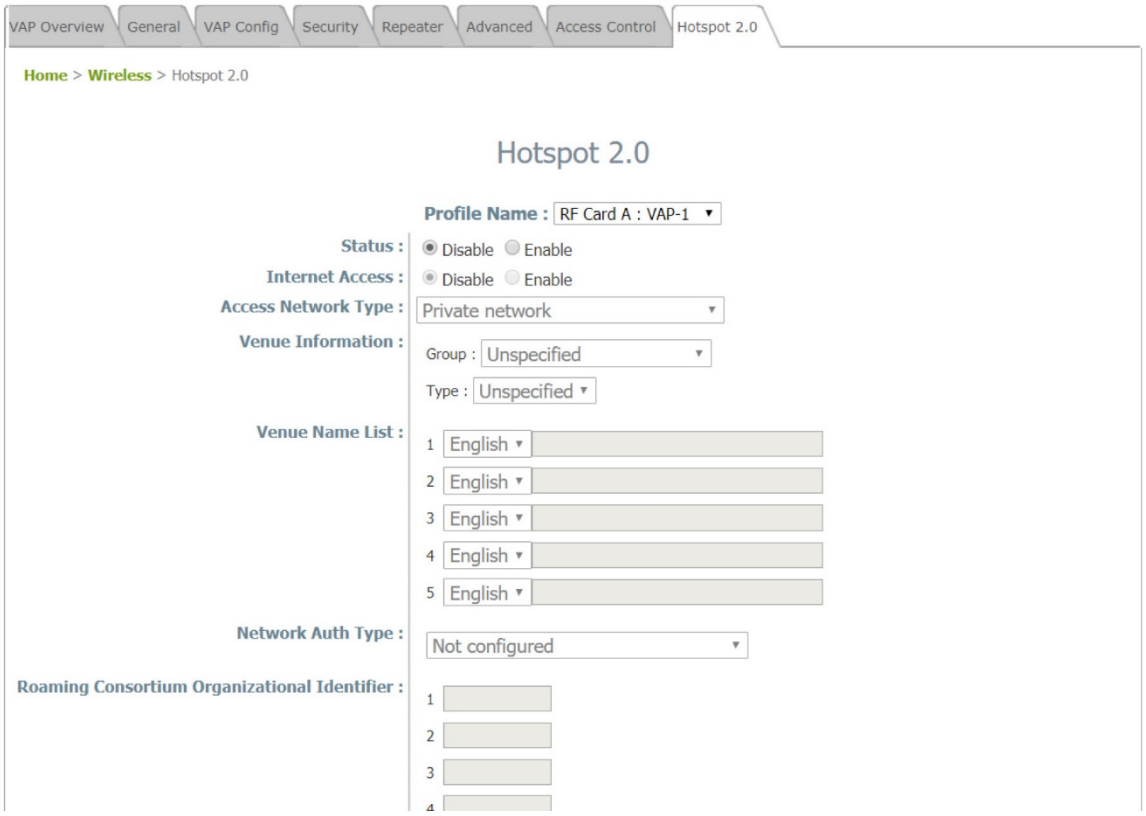


Access Control Type(アクセスコントロールタイプ) – RADIUS ACL:外部RADIUSによって着信MACアドレスを認証します。***[RADIUS ACL]***を選択すると、すべての着信MACアドレスが外部RADIUSによって認証されます。各VAPのMAC ACLとそのセキュリティタイプ(**[Security Settings(セキュリティ設定]**ページに表示)は、同じRADIUS構成を共有することに注意してください。



4.8 Hotspot 2.0(ホットスポット2.0)

ホットスポット2.0は、Wi-Fi Allianceが公衆Wi-Fiサブスクライバーにより良い帯域幅とサービスを提供するために開始したWi-Fi認定パスポイントとしても知られています。



Status(ステータス):ホットスポット2.0を有効または無効にします

Internet Access(インターネットアクセス):このネットワークがインターネットへのアクセスを提供する場合に有効にします

Access Network Type(アクセスネットワークタイプ)

- **Private(プライベート)**:自宅および企業ネットワーク
- **Private and Guest Access(プライベートおよびゲストアクセス)**:ゲスト接続を提供する企業
- **Chargeable Public Network(有料パブリックネットワーク)**:すべての人が利用可能ですが、料金が必要です
- **Free Public Network(無料パブリックネットワーク)**:無料ですべての人が利用可能です
- **Personal Device Network(パーソナルデバイスネットワーク)**:アドホックモードの周辺機器用
- **Emergency Services(緊急サービス)**
- **Test/Experimental/Wild Card(テスト/実験/ワイルドカード)**

Venue Information(会場情報):会場のGroup/Type(グループ/タイプ)はここで選択します。これは、会場の一般的なクラスと、各グループ内の会場の特定のタイプを識別します。

Venue Name List(会場名リスト):ネットワーク会場の名前、エンドユーザーがネットワークを選択するのに役立ちます。

Network Authentication Type(ネットワーク認証タイプ):安全でないネットワークへのアクセスを取得するための追加手順

- **Acceptance of terms and conditions(利用規約への同意)**
- **Online enrollment supported(オンライン登録対応)**:ユーザーアカウンティングが必要な場合があります
- **HTTP/HTTPS redirection(HTTP/HTTPSリダイレクト)**:ブラウザーのリダイレクト先のURLが示されます
- **DNS redirection(DNSリダイレクト)**:ホットスポット2.0仕様では、ネットワークオペレーターがDNSSECと相互運用できないプロトコルをサポートすることを禁止しています。キャプティブポータルのDNSリダイレトは、この要件に違反しています。
-

Roaming Consortium Organizational Identifier(ローミングコンソーシアムの組織識別子):ローミングコンソーシアムとは、ユーザーの資格情報を認証に使用できるサービスプロバイダー(SP)のグループです。ローミングコンソーシアムは、MACアドレスの前半と同様に、IEEEによって割り当てられる組織識別子(OI)によって識別されます。多くの場合、OIの長さは24ビットですが、36ビットにすることもできます(OUI-36など)。

IP Address Type(IPアドレスタイプ):IPv4またはIPv6

NAI Realm List(NAIレルムリスト):NAIレルムは、ユーザーの認証交換のための適切な認証サーバーまたはドメインを識別します。ネットワークでサポートされている認証レルムを検出することで、モバイルデバイスは優先ネットワークに対して選択的に認証できます。

- **EAP Type(EAPタイプ)**:NAIレルムリストは、各レルムでサポートされている拡張認証プロトコル(Extensible Authentication Protocol/EAP)タイプと、そのEAPタイプの認証パラメーターをオプションで示すこともできます。

Domain Name List(ドメイン名リスト):APを操作しているエンティティの1つ以上のドメイン名を一覧表示します。これはネットワークオペレーターを識別するため、ホットスポット2.0ネットワーク選択ポリシーにとって重要です。モバイルデバイスが自宅にあるか、ホットスポットにアクセスしたかを示します。

Cellular Network Information List(セルラーネットワーク情報リスト)(PLMN):APを介して使用可能な3GPPセルラーネットワークを識別します。具体的には、このフィールドは、モバイルオペレーターのモバイル国コード(Mobile Country Code/MCC)とモバイルネットワークコード(Mobile Network Code/MNC)で構成される公有地モバイルネットワーク(Public Land Mobile Network/PLMN)IDを識別します。

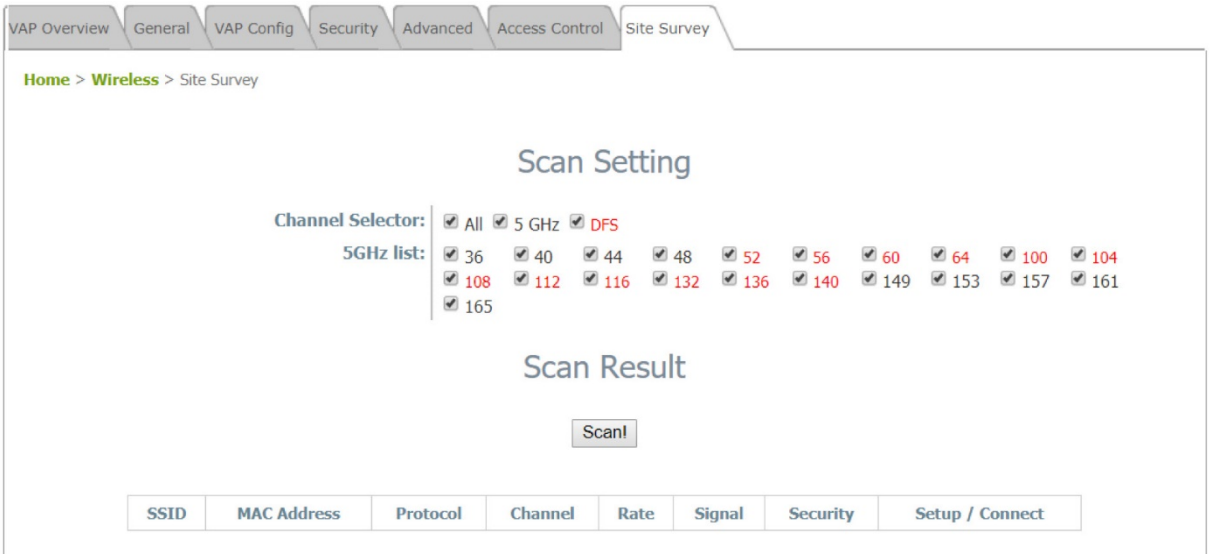
Hotspot 2.0 R2(ホットスポット2.0 R2)(ホットスポット2.0リリース2):ホットスポット2.0リリース1からの改善点が含まれています。

- **OSU SSID**:OSEN VAPのSSID名
- **OSU Server URI(OSUサーバーURI)**:OSUサーバーのURI
- **OSU Friendly Name(OSUフレンドリー名)**:人間の言語でのOSUプロバイダーの名前。これは、OSUサーバー証明書から取得した名前と正確に一致します。現在は英語のみに対応しています
- **OSU NAI**:OSUに対して認証します(OSEN用に構成されている場合)
- **OSU Service Description(OSUサービスの説明)**:OSUの説明。現在は英語のみに対応しています

4.9 Site Survey(サイト調査)(CPEモードのみ)

システムは、周囲の使用可能なアクセスポイント(AP)をスキャンして表示できます。管理者は、このページでシステムに関連付けるAPを選択できます。

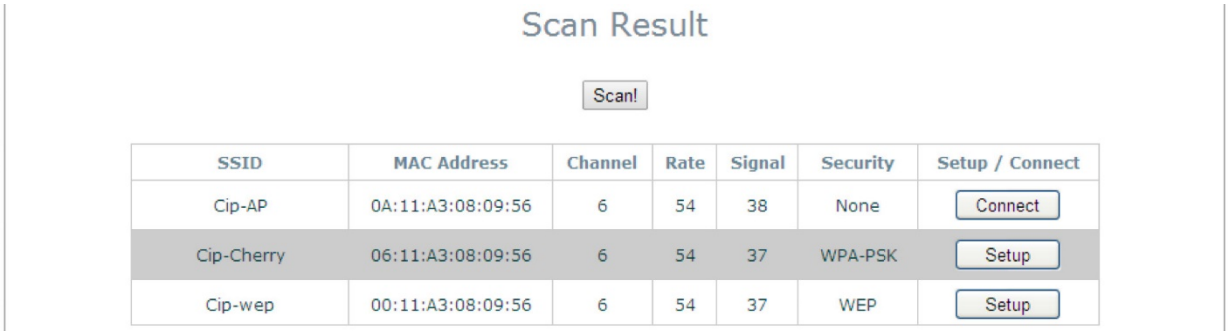
サイト調査は、周囲の無線環境に関する情報を提供するのに役立つツールです。利用可能なAPは、それぞれのSSID、MAC Address(MACアドレス)、Channel(チャンネル)、Rate setting(レート設定)、Signal reading(信号読み取り)、およびSecurity type(セキュリティタイプ)とともに表示されます。管理者は、[Setup(セットアップ)]または[Connect(接続)]をクリックして、上記の読み取りに従って無線接続を構成できます。



Channel Selector(チャンネルセレクター):スキャンするチャンネルタイプを選択します。

5GHz list(5GHzリスト):スキャンする特定のチャンネルを選択します。

Scan Result(スキャン結果):[Channel Selector(チャンネルセレクター)]と[5GHz list(5GHzリスト)]を選択し、[Scan!(スキャン!)]ボタンをクリックすると、スキャン結果が下に表示されます。



Setup/Connect(セットアップ/接続):

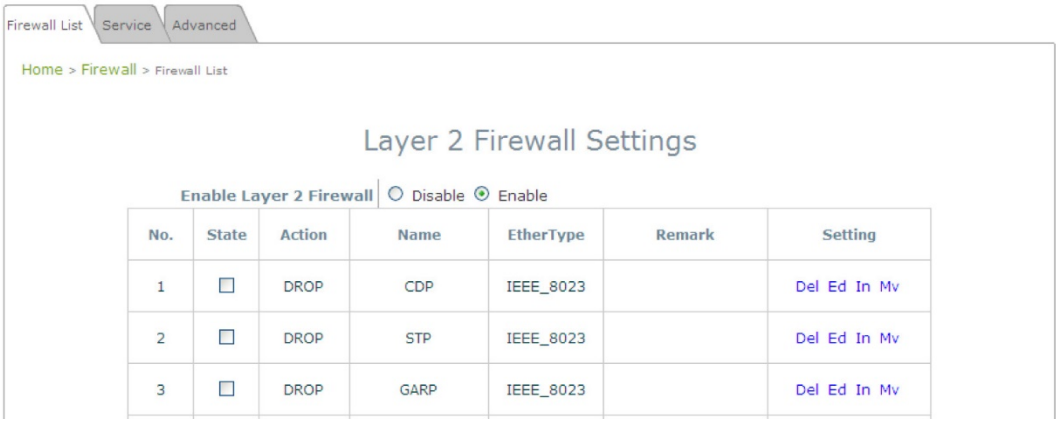
- **Connect(接続)**:[Connect(接続)]ボタンをクリックして、それぞれのAPに直接関連付けます。それ以上の構成は必要ありません。
- **Setup(セットアップ)**:[Setup(セットアップ)]ボタンをクリックして、それぞれのAPに関連付けるためのセキュリティ設定を構成します。

5. Firewall(ファイアウォール)

システムには、一般的なAPセキュリティに加えて、追加のセキュリティ機能であるLayer2 Firewall(レイヤー2ファイアウォール)が用意されています。レイヤー2ファイアウォールは、特にレイヤー2トラフィックに合わせて調整されたファイアウォール機能を提供し、WLAN（APインターフェイス）から/への起こり得るセキュリティ脅威に対するシールドの別の選択肢を提供します。したがって、ゲートウェイで構成されたファイアウォールポリシーに加えて、この追加のセキュリティ機能は、セキュリティ違反の可能性を軽減することができます。このセクションでは、以下の機能について説明します：**Firewall Lists(ファイアウォールリスト)**、**Service(サービス)**、および**Advanced Firewall Settings(ファイアウォールの詳細設定)**。

5.1 Firewall List(ファイアウォールリスト)

システムのファイアウォールルールの概要を示します。合計で最大20のファイアウォールルールを含む6つのデフォルトルールを設定できます。



概要表から、各ルールは次のフィールドで指定されます。
No.(番号)：番号は、システムが表内の使用可能なファイアウォールルールを実行するための優先順位を決定します。

State(状態)：チェックマークはそれぞれのルールを有効にします。

Action(操作)：***DROP(停止)***はブロックルールを示します。***ACCEPT(受入)***はパスルールを示します。

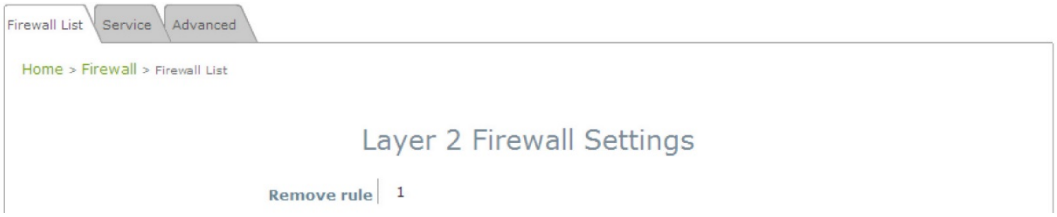
Name(名前)：ルールの名前を表示します。

EtherType(イーサタイプ)：このルールの対象となるトラフィックのタイプを示します。

Remark(備考)：このルールの注を表示します。

Setting(設定)：4つの操作が利用可能です。***Del***はルールを削除することを示し、***Ed***はルールを編集することを示し、***In***はルールを挿入することを示し、***Mv***はルールを移動することを示します。

特定のルールを削除する場合は、
ファイアウォールリストの[Setting(設定)]列で***[Del]***をクリックすると、削除の確認のために次のページが表示されます。***[SAVE保存)]***ボタンをクリックしてシステムを再起動すると、ルールは削除されます。



特定のルールを編集する場合は、
ファイアウォールリストの[Setting(設定)]列で***[Ed]***をクリックすると、詳細構成のために次のページが表示されます。このページから、ルールを最初から編集したり、既存のルールから編集したりできます。次のフィールドが表示されます:

Rule ID(ルールID):この特定のルールの番号によって、表内の使用可能なファイアウォールルール間の優先順位が決まります。

Rule name(ルール名):ルール名はここで指定できます。

EtherType(イーサタイプ):ドロップダウンリストには、このルールの対象となる利用可能なトラフィックのタイプが表示されます。

Interface(インターフェイス):これは、必要なインターフェイスを備えたインバウンド/アウトバウンド方向を示します。

Service(サービス)(EtherType(イーサタイプ)が**IPv4**の場合):ドロップダウンリストから使用可能な上位レイヤープロトコル/サービスを選択します。

DSAP/SSAP(EtherType(イーサタイプ)が**IEEE 802.3**の場合):802.2 LLCフレームヘッダーのフィールドに値をさらに指定できます。

Type(タイプ)(EtherType(イーサタイプ)が**IEEE 802.3**の場合):このフィールドは、カプセル化されたトラフィックのタイプを示すために使用できます。

VLAN ID(EtherType(イーサタイプ)が**802.1 Q**の場合):VLAN IDは、特定のVLANタグ付けトラフィックに関連付けるために提供されます。

Priority(優先度)(EtherType(イーサタイプ)が**802.1 Q**の場合):これは、関連するVLANトラフィックの優先度レベルを示します。

Encapsulated Type(カプセル化タイプ)(EtherType(イーサタイプ)が**802.1 Q**の場合):カプセル化されたトラフィックのタイプを示すために使用できます。

Opcode(EtherType(イーサタイプ)が**ARP/RARP**の場合):このリストは、ARPヘッダーでARP Opcodeを指定するために使用できます。

Source(送信元):MAC Address/Mask(MACアドレス/マスク)は送信元MACを示します。IP

Address/Mask(IPアドレス/マスク)は、送信元IPアドレスを示します（EtherType(イーサタイプ)が**IPv4**の場合）。ARP IP/MAC＆MASKは、ARPペイロードフィールドを示します。

Destination(送信先)：MAC Address/Mask(MACアドレス/マスク)は送信先MACを示します。IP Address/Mask(IPアドレス/マスク)は、送信先IPアドレスを示します（EtherType(イーサタイプ)が**IPv4**の場合）。ARP IP/MAC＆MASKは、ARPペイロードフィールドを示します。

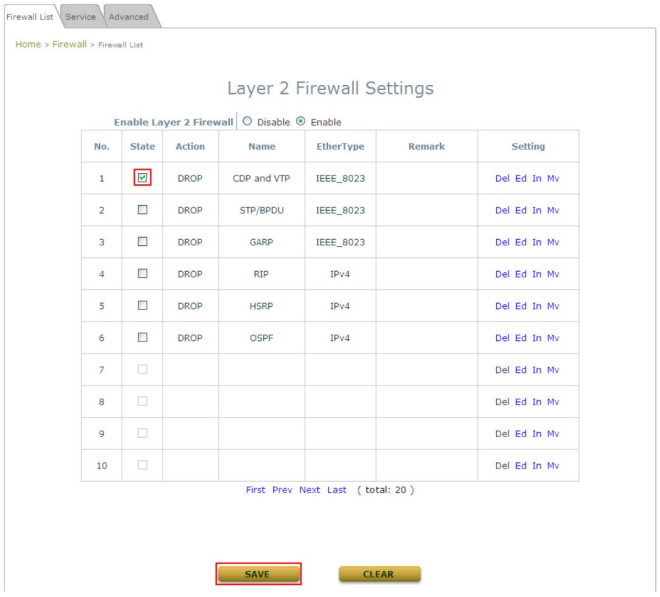
Action(操作)：ルールは、**Block(ブロック)**または**Pass(パス)**に選択できます。

Remark(備考)：このルールの注はここで指定できます。
ファイアウォールルールの構成が完了したら、***[SAVE and Reboot system(保存してシステムを再起動)]***をクリックして、ファイアウォールルールを有効にしてください。

特定のルールを挿入する場合は、
ファイアウォールリストの[Setting(設定)]列で***[In]***をクリックすると、現在挿入されているルールのルールIDを使用した詳細構成のために次のページが表示されます。

特定のルールを移動する場合は、
ファイアウォールリストの[Setting(設定)]列で***[Mv]***をクリックすると、順序変更の確認のために次のページが表示されます。***[SAVE保存)]***ボタンをクリックしてシステムを再起動すると、ルールの順序が更新されます。

必要なすべてのルール（ルールの状態）がオンにされ、概要ページに保存されていることを確認してください。ルールはシステムの再起動時に適用されます。



5.2 Service(サービス)

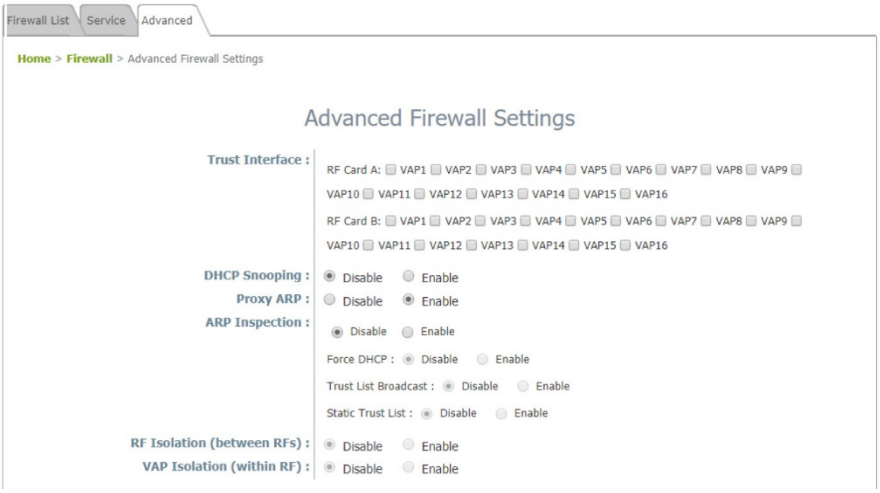
管理者はここでファイアウォールサービスを追加または削除できます。このリストのサービスは、ファイアウォールルールで選択するオプションになります（EtherType(イーサタイプ)がIPv4の場合）。

アクセスポイントは、レイヤー3以上のプロトコルのトラフィックをブロックまたは通過させるルールリストを提供します。これらのサービスは、EtherType(イーサタイプ) IPv4のレイヤー2ファイアウォールルール編集ページのドロップダウンリストから選択できます。最初の28エントリはデフォルトのサービスであり、管理者は追加の必要なサービスを追加/削除できます。

デフォルトの設定では28のファイアウォールサービスを利用できます。これらのデフォルトサービスは削除できませんが、無効にすることができます。変更を行った場合は、このページを閉じる前に、***[SAVE(保存)]***をクリックして設定を保存してください。

5.3 Advanced(詳細)

Firewall(ファイアウォール) >Advanced(詳細)では、ファイアウォールルールのより詳細な設定を構成でき、システムの使用可能なインターフェイスを通過するDHCPおよびARPトラフィックに対するセキュリティをさらに強化でます。



Trust Interface(信頼インターフェイス):各VAPインターフェイスを個別にオンにして、信頼できるインターフェイスとしてマークできます。DHCPスヌーピングやARPインスペクションなどのDHCP/ARPのセキュリティ強化は、信頼されていないインターフェイスで実行されます。

DHCP Snooping(DHCPスヌーピング):有効にすると、DHCPパケットはDHCP枯渇攻撃などの可能性のある脅威に対して検証されます。さらに、信頼できるDHCPサーバー(IP/MAC)を指定して、DHCPサーバーの不正使用を防ぐことができます。

ARP Inspection(ARPインスペクション):有効にすると、ARPパケットはARPスプーフィングに対して検証されます。

- **Proxy ARP option(プロキシARPオプション)**:有効にすると、APはダウンリンクステーションに代わってARP要求に応答します。APが保持するARPテーブルは、APアップリンクからのARP要求の受信時に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、ネットワークが非効率になります。
- **Force DHCP option(強制DHCPオプション)**:有効にすると、APはDHCPパケットを介してMAC/IPペア情報のみを学習します。静的IPアドレスで構成されたデバイスはDHCPトラフィックを送信しないため、静的IPアドレスを持つクライアントは、MAC/IPペアが**Static Trust List(静的信頼リスト)**にリストされ、有効にされていない限り、インターネットアクセスからブロックされます。
- **Trust List Broadcast(信頼リストブロードキャスト)**を有効にして、(L2ファイアウォール機能を備えた)他のAPが信頼できるMAC/IPペアを学習して、ARP要求を発行できるようにすることができます。
- **Static Trust List(静的信頼リスト)**を使用して、ARP要求の発行が信頼されているデバイスのMACまたはMAC/IPペアを追加できます。他のネットワークノードは引き続きARP要求を送信できます。ただし、それらのIPが静的リストに(異なるMACで)表示されている場合、盗聴を防止するためにそれらのARP要求はドロップされます。

RF Isolation(RF分離)(RF間):クライアントは、RF Card A(RFカードA)とRF Card B(RFカードB)の間で分離されています。

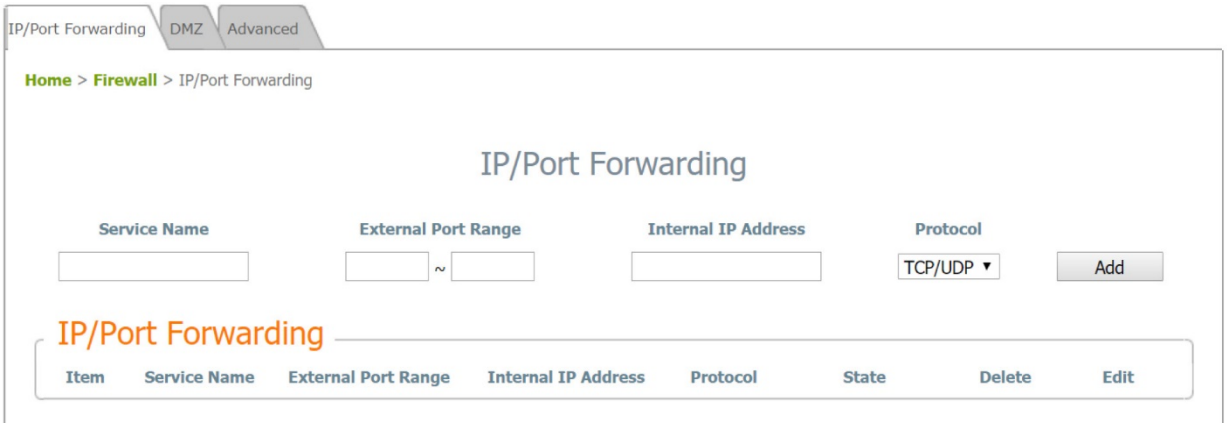
VAP Isolation(VAP分離)（RF内）：同じRF Card(RFカード)上の異なるVAP上のクライアントは分離されます。

設定を変更した場合は、このページを閉じる前に、***[SAVE(保存)]***をクリックして構成を保存してください。

注：
- 一部のAPモデルでは、RF Isolation(RF分離)（RF間）が制限されている場合があります。
- 一部のAPモデルでは、VAP Isolation(VAP分離)（RF内）が制限されている場合があります。

5.4 IP/Port Forwarding(IP/ポート転送)（CPEモードのみ）

このページのオンラインゲームやビデオ会議などの特別な目的のインターネットサービスのために、ネットワークの特定の部分を制限かつ制御された方法でインターネットに公開することができます。使用する内部ポートが他のアプリケーションによって使用されていないことを確認してください。



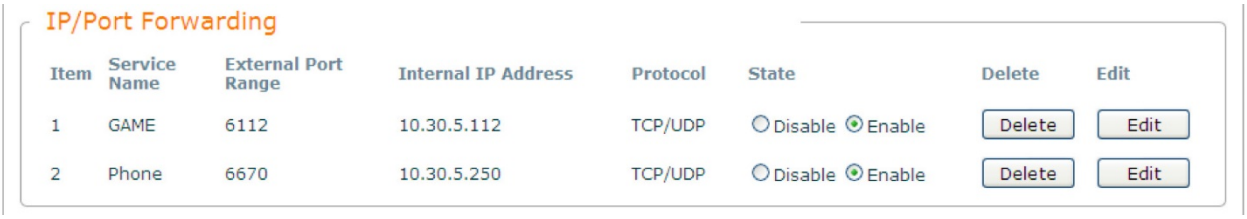
Service Name(サービス名)：管理者は、特定の転送に覚えやすい別名を付けることができます。

External Port Range(外部ポート範囲)：トラフィックを転送するための外部ポートの範囲は、管理者が手動で定義できます。

Internal IP Address(内部IPアドレス)：LAN IPアドレスを入力して、転送トラフィックを受信します。

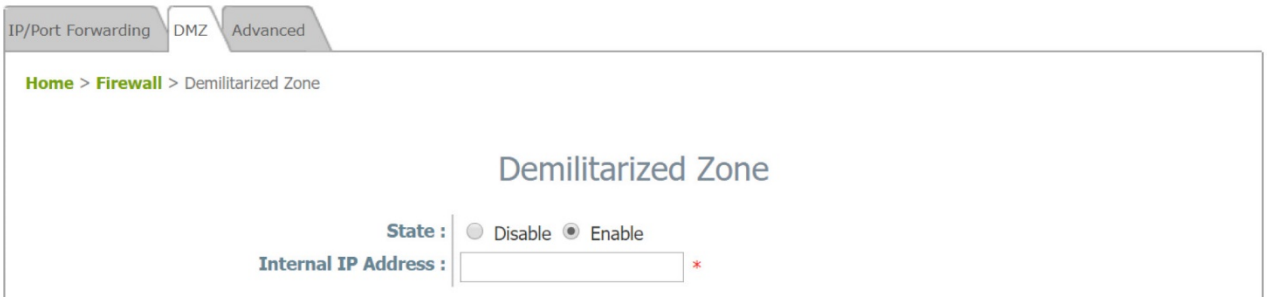
Protocol(プロトコル)：転送トラフィックプロトコルをドロップダウンリストから選択して、TCP/UDP、TCPまたはUDPにすることができます。Add(追加)：[Add(追加)]をクリックして、新しいサービスをアクティブにします。

IP/ Port Forwarding(IP/ポート転送)：現在利用可能なサービスの詳細。[Delete(削除)]をクリックして、指定したサービスを削除します。[Edit(編集)]をクリックして、現在の設定を構成します。



5.5 DMZ（CPEモードのみ）

DMZ（Demilitarized Zone/非武装地帯）を使用すると、1台のローカルコンピューターまたはサーバー（DMZホストとして使用）をインターネットに公開して、Webサーバーとして機能するなどの特別な目的のインターネットサービスを利用できます。外部ユーザーは認証なしでDMZホストにアクセスできます。



Enable(有効化)：[Enable(有効化)]を選択して、この機能を有効にします。[Disable(無効化)]を選択して、この機能を無効にします。

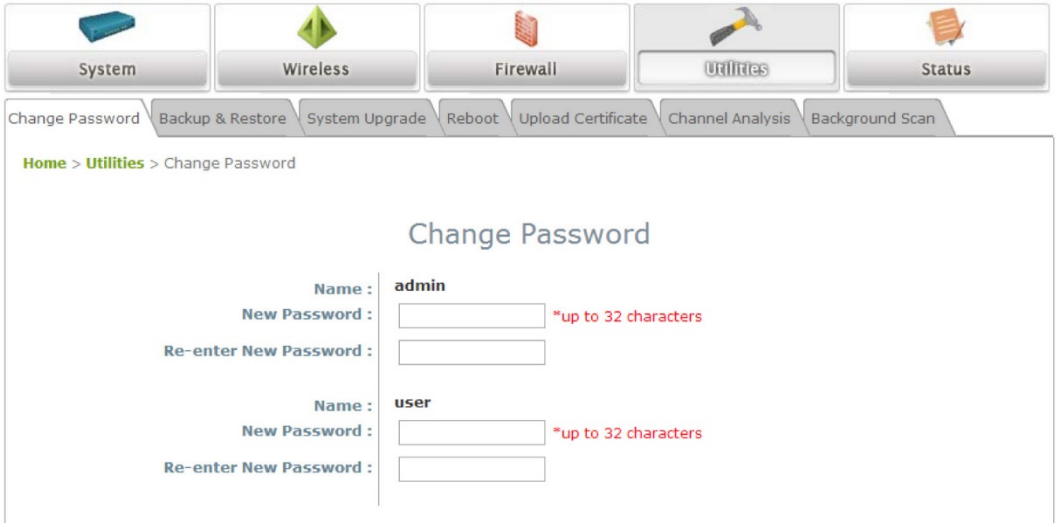
Internal IP Address(内部IPアドレス)：内部IPアドレスを入力して、IP/ポート転送に具体的にリストされているトラフィック以外のシステム転送トラフィックを許可します。

6. Utilities(ユーティリティ)

このページの次のユーティリティ機能により、管理者はシステムを保守できます：Change Password(パスワードの変更)、Backup & Restore(バックアップおよび復元)、System Upgrade(システムアップグレード)、Reboot(再起動)、Upload Certificate(証明書のアップロード)、Channel Analysis(チャンネル分析)、Background Scan(バックグラウンドスキャン)。

6.1 Change Password(パスワードの変更)

不正アクセスからWeb管理インターフェイスを保護するために、管理者のパスワードを安全なパスワードに変更することを強くお勧めします。使用できるのは英数字のみです。また、数字とアルファベットの両方を組み合わせて使用することをお勧めします。

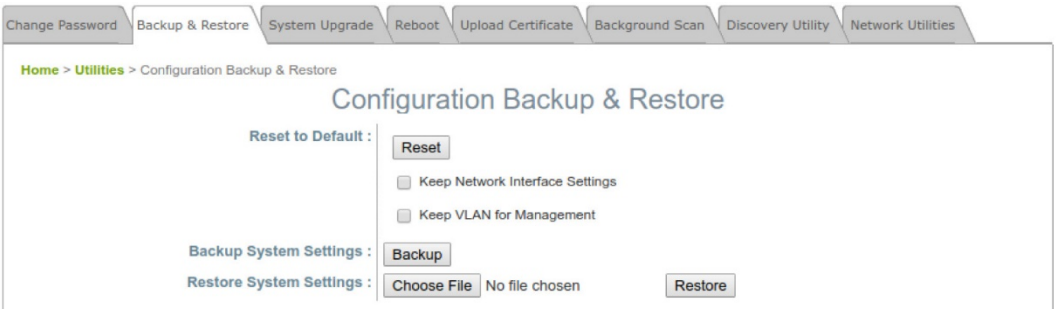


管理者はこのページでパスワードを変更できます。元のパスワード(「**admin**」)と新しいパスワードを入力し、[***Re-enter New Password(新しいパスワードの再入力)***]フィールドに新しいパスワードを再入力します。***[SAVE(保存)]***をクリックして、新しいパスワードを保存します。

管理者アカウントに加えて、構成制限付きでWeb管理インターフェイスにアクセスできる「**user(ユーザー)**」アカウントがあります。「user(ユーザー)」アカウントは、APを再起動したり、ワイヤレス設定を変更したり、チャンネル分析機能を有効にしたりできません。このアカウントは通常、従業員がAPステータスを監視するためにITスタッフによって発行されます。

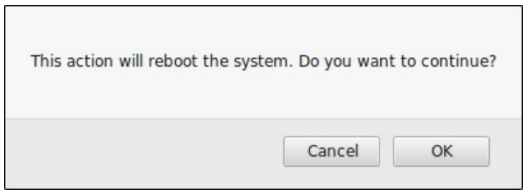
6.2 Backup & Restore(バックアップおよび復旧)

この機能は、アクセスポイントの設定をバックアップおよび復元するために使用されます。この機能を使用して、APを工場出荷時デフォルトに復元することもできます。他のアクセスポイントに設定を複製するために使用できます（このシステムの設定をバックアップしてから、別のAPで復元します）。

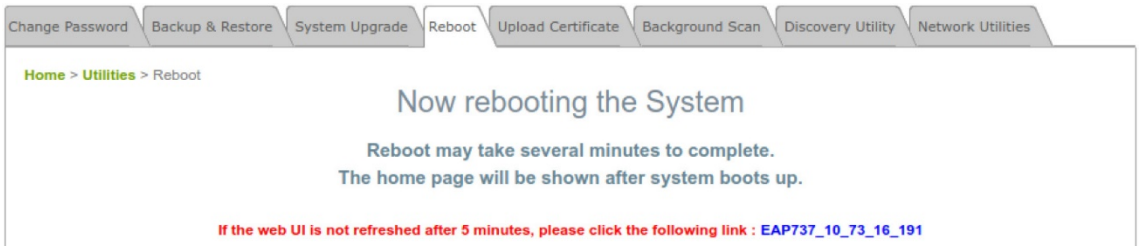


Reset to Default(デフォルトにリセット)
通常、管理者は、以下の説明のように、Web管理インターフェイスからシステムを工場出荷時デフォルトにリセットできます。さらに、コンソールインターフェイから行う別の方法があります。「*セクション8.2 SSHインターフェイスによるリモート接続*」を参照してください。

- **Keep Network Interface Settings(ネットワークインターフェイス設定を保持する)**：場合によっては、このオプションをオンにして、システムをデフォルトにリセットした後でも元のネットワークインターフェイス設定が確実に残るようにすることが有用となります。
- **Keep VLAN for Management(管理用VLANを維持する)**：場合によっては、このオプションをオンにして、システムをデフォルトにリセットした後でも、元の管理用VLANが確実に残るようにすることが有用となります。
- ***[Reset(リセット)]***をクリックして、工場出荷時デフォルト設定をロードします。ポップアップメッセージが表示されますので、システムを再起動する要求を再確認してください。***[OK]***をクリックして続行するか、***[Cancel(キャンセル)]***をクリックして操作をキャンセルします。



- 再起動中は、以下のようなメッセージが表示されます。再起動プロセスが完了する前に、システム電源をオンにしておく必要があります。再起動が完了すると、**[System Overview(システム概要)]**ページが表示されます。



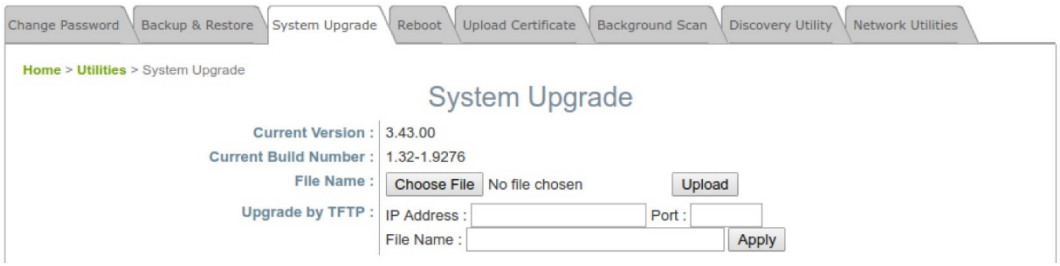
Backup System Settings(システム設定のバックアップ)：現在のシステム構成を管理コンソールのローカルディスク上のバックアップファイルに保存します。***[Choose File(ファイルの選択)]***ボタンをクリック

してバックアップファイルを選択し、***[Restore(復元)]***ボタンをクリックしてプロセスを実行すると、バックアップファイルをシステムに復元できます。

Restore System Settings(システム設定の復元):***[Choose File(ファイルの選択)]***をクリックして、コントローラーによって作成された.dbデータベースバックアップファイルを検索し、***[Restore(復元)]***をクリックして、バックアップファイルが保存されたときと同じ設定に復元します。

6.3 System Upgrade(システムアップグレード)

ファームウェアのアップグレードには、WMI経由またはTFTPサーバー経由の2つの方法があります。管理者は、Edgecoreサポートチームから最新のファームウェアを入手できます。ファームウェアをアップグレードする場合は、[Choose File(ファイルの選択)]をクリックしてPCにダウンロードした新しいファームウェアファイルを選択し、[Upload(アップロード]をクリックしてプロセスを実行します。TFTPでアップグレードするには、designated IP address(指定したIPアドレス)、Port(ポート)、File Name(ファイル名)を入力し、[Apply(適用)]をクリックします。ファームウェアをアップグレードした後、システムを再起動してください。

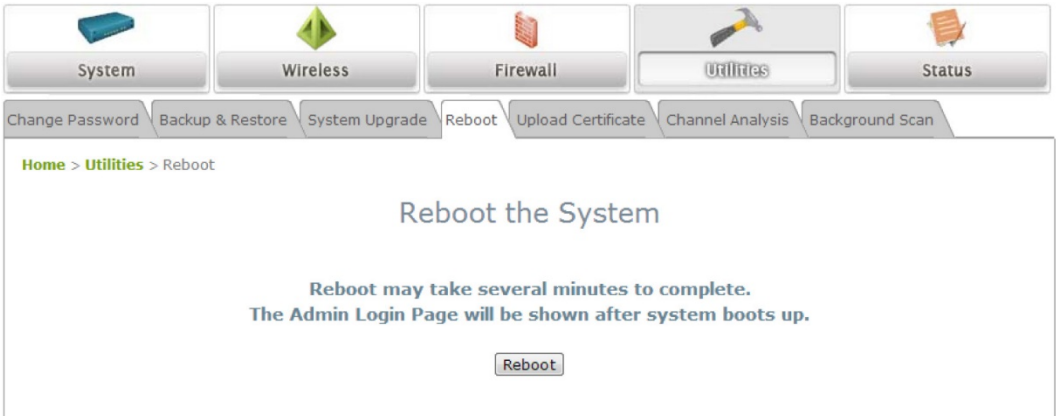


注:

- 先に進む前に、ファームウェアのバージョン番号を確認することをお勧めします。正しいファームウェアファイルがあることを確認してください。
- ファームウェアのアップグレードにより、データが失われることがあります。ファームウェアをアップグレードする前に、必要な設定がすべて書き留められていることを確認してください。
- ファームウェアのアップグレード中は、電源を切らないでください。これにより、システムが恒久的に損傷する可能性があります。
- 一部のAPモデルでは、TFTPによるアップグレードが制限されている場合があります。

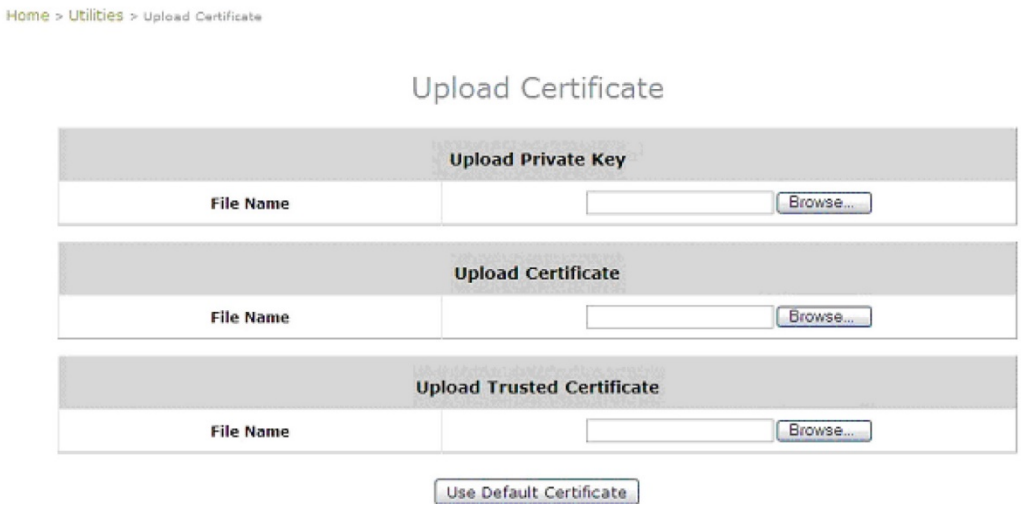
6.4 Reboot(再起動)

[Reboot(再起動)]をクリックして、APを安全に再起動します。このプロセスには約3分かかります。再起動が成功すると、System Overview(システム概要)ページが表示されます。注:場合によっては、パラメーターの変更が送信されたことを確認するためにAPを再起動する必要があります。



6.5 Upload Certificate(証明書のアップロード)

この機能は、CAPWAPで必要なセキュリティ検証のための有効な証明書を構成するために使用されます。

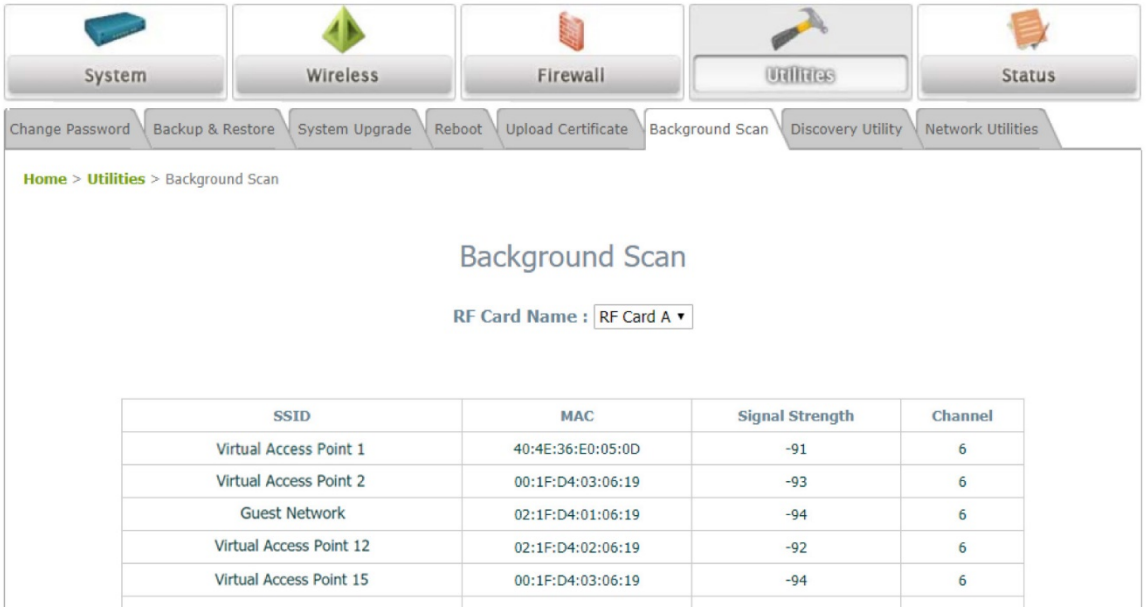


Upload Certificate(証明書のアップロード):CAPWAPまたは他のセキュリティニーズのセキュリティ検証の手段として、顧客自身の証明書、秘密鍵、または信頼できる証明書をサポートする柔軟性を提供し、他のネットワークエンティティに対するこのAPの信頼性を保証します。

Use Default Certificate(デフォルト証明書の使用):***[Use Default Certificate(デフォルト証明書の使用)]***をクリックして、デフォルトの証明書とキーを使用します。

6.6 Background Scan(バックグランドスキャン)

アクセスポイントは、サービスに影響を与えずにバックグラウンドスキャンを実行できます。これは Channel Analysis(チャンネル分析)を補完する形で機能するため、管理者は無線環境の完全な概要を把握できます。



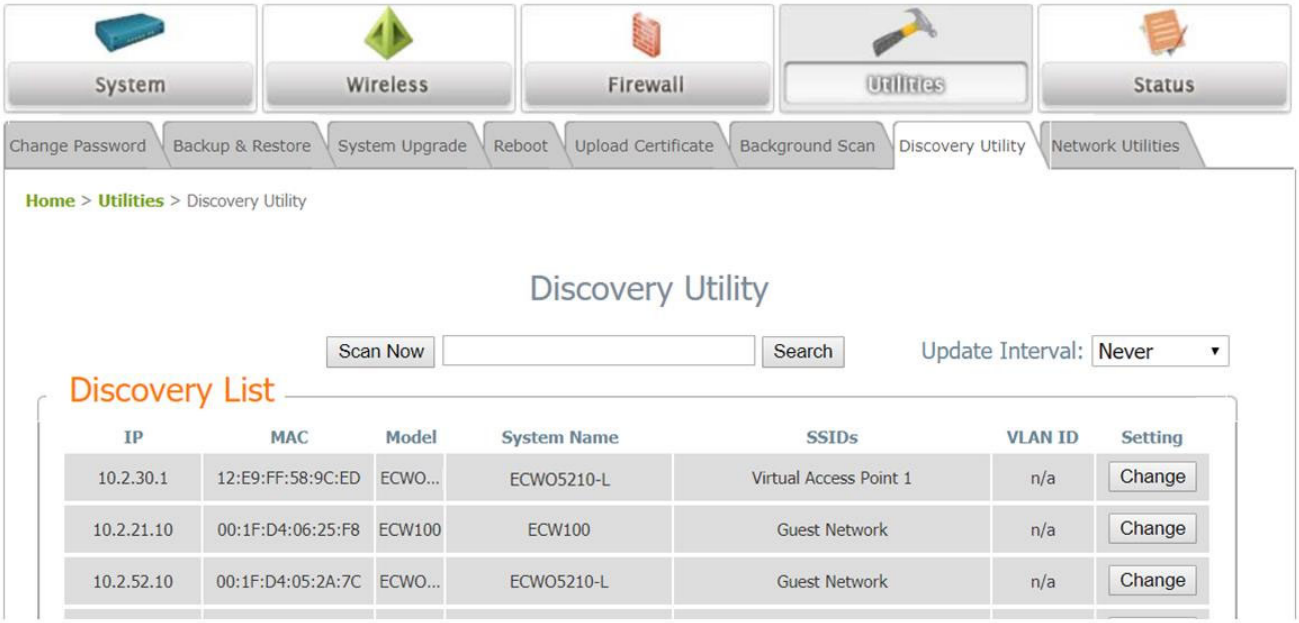
SSID	MAC	Signal Strength	Channel
Virtual Access Point 1	40:4E:36:E0:05:0D	-91	6
Virtual Access Point 2	00:1F:D4:03:06:19	-93	6
Guest Network	02:1F:D4:01:06:19	-94	6
Virtual Access Point 12	02:1F:D4:02:06:19	-92	6
Virtual Access Point 15	00:1F:D4:03:06:19	-94	6

[Scan Whole Channel(全チャンネルのスキャン)]ボタンをクリックすると、APがトリガーされ、構成されたバンド内のすべてのチャンネルがスキャンされます。Radio(無線)は、構成されたバンド内のみをスキャンできることに注意してください。

6.7 Discovery Utility(検出ユーティリティ)

ネットワーク管理者は、APのIPアドレスを忘れたり、管理者のパスワードを忘れたり、APのIPアドレスを構成したりするなど、APインターフェイスにアクセスせずに情報にアクセスまたは変更する必要があります。

ネットワーク管理者が行う必要があることは、現在のシステムのポートから同じレイヤー2内のEdgecore APを接続し、[Search(検索)]ボタンを押して、IP検出ユーティリティを実行することです。スキャン結果は、デバイスの対応するIP address(IPアドレス)、MAC address(MACアドレス)、Model(モデル)、System Name(システム名)、SSID（各VAP）、VLAN IDになります。デバイスのLANポートは、スイッチを介して他のデバイス（AP）に接続できます。

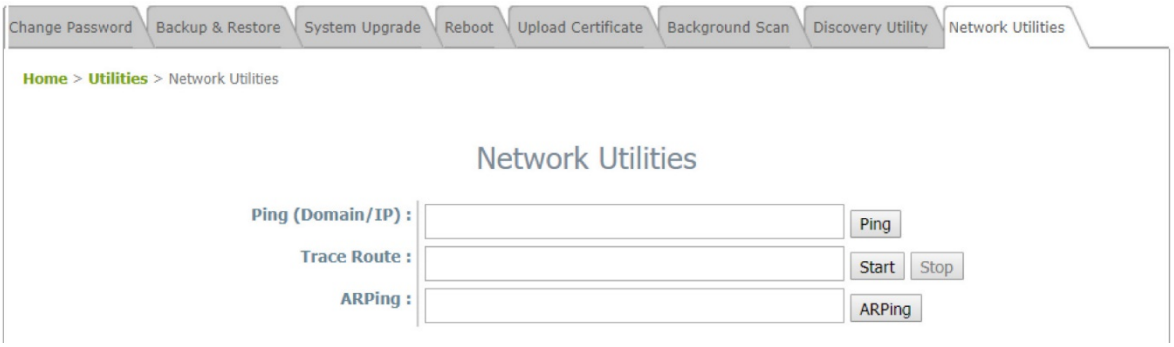


Scan Now(今すぐスキャン):このボタンをクリックして検出プロセスを開始すると、結果が[Discovery List(検出リスト)]テーブルに表示されます。

Search(検索):特定のAPを検索するためのキーワードを入力します。

Change(変更):これにより、管理者は、IP address(IPアドレス)、Netmask(ネットマスク)、Gateway(ゲートウェイ)、Primary DNS Server(プライマリDNSサーバー)、Username(ユーザー名)、Password(パスワード)など、特定のAPの設定を変更できます。

6.8 Network Utilities(ネットワークユーティリティ)

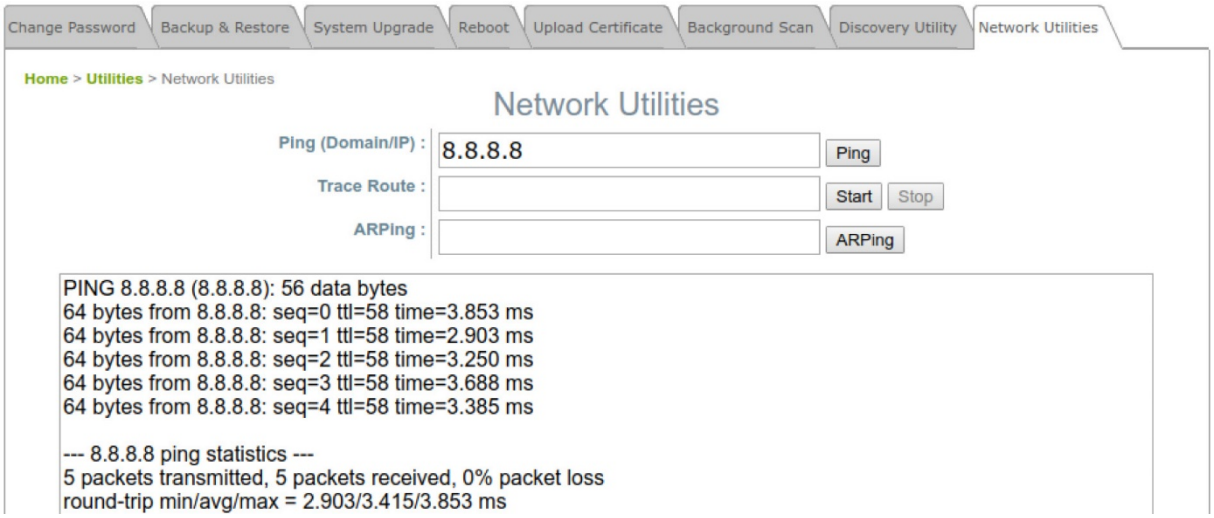


Ping:これにより、管理者は、IPアドレスまたはホストドメイン名を使用してデバイスを検出し、デバイスが動作しているかどうかを確認できます。

Trace Route(トレースルート):管理者は、IPアドレスまたはホストドメイン名を使用して、ゲートウェイから送信先へのパケットの実際のパスを回復できます。

ARPing:管理者が特定のIPアドレスまたはドメイン名のARP要求を送信できるようにします。

Result(結果):操作結果がここに表示されます。

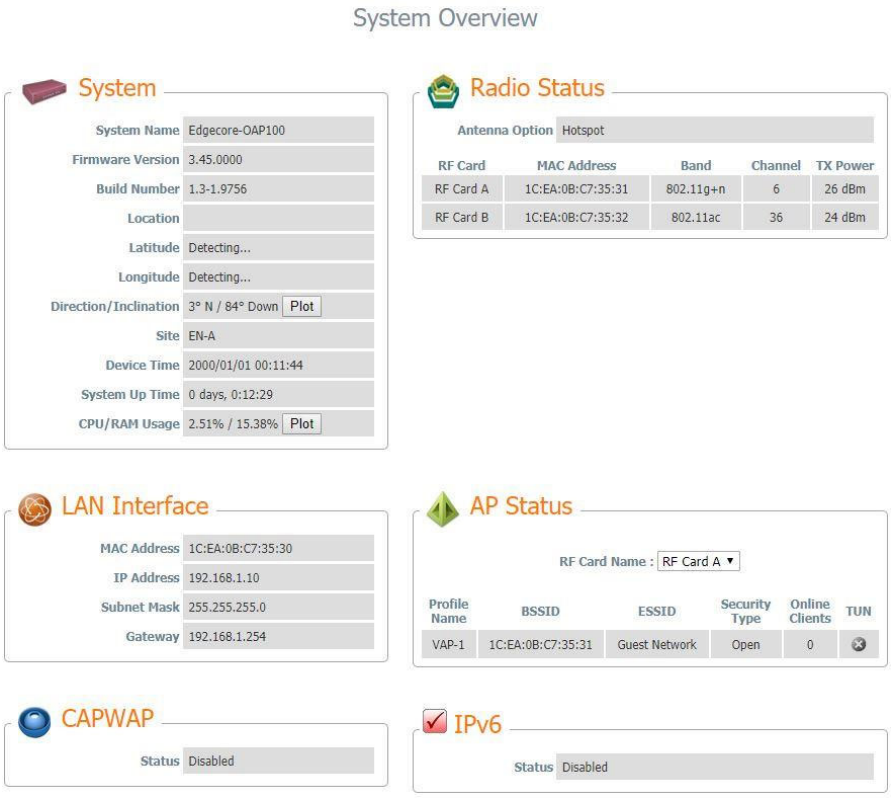


7. Status(ステータス)

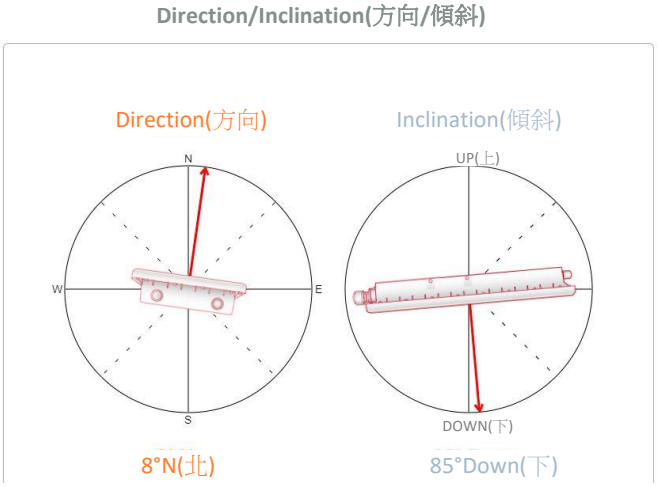
次の機能タブには、システムの現在の条件と状態が表示されます：Overview(概要)、Interfaces(インターフェイス、Associated Clients(関連クライアント)、DHCP Lease(DHCPリース)、Link Status(リンクステータス)、Event Log(イベントログ)、Wireless Log(無線ログ)、およびMonitor(モニター)。

7.1 Overview(概要)

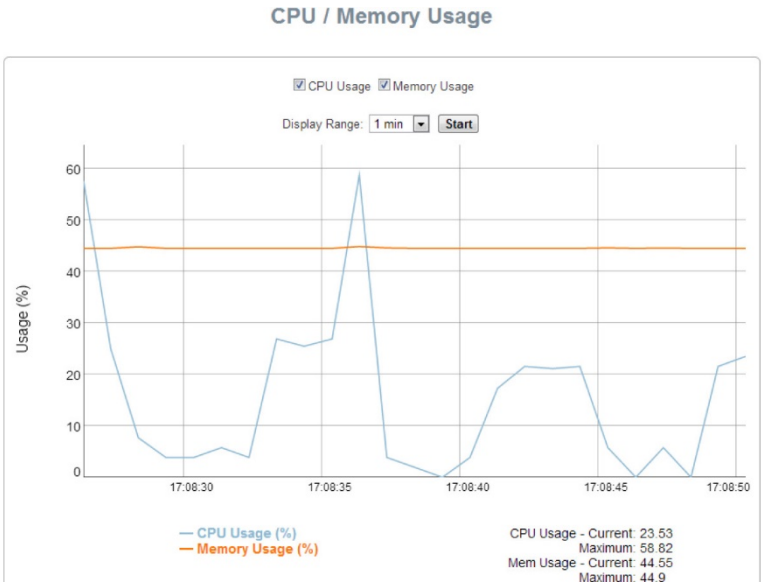
[System Overview(システム概要)]ページには、管理者のシステムステータスの概要が表示されます。



[Plot(プロット)]ボタンをクリックすると（OAP100のみ）、方向/傾斜のプロットが表示されます。左側はデバイスの水平角度を示します。右側は、デバイスの垂直傾斜角度を示しています。



エンタープライズアクセスポイント ***[Plot(プロット)]***ボタンをクリックすると、CPU/RAM使用量のリアルタイムプロットが表示されます。マウスを左クリックしてドラッグし、目的の領域を拡大します。グラフをダブルクリックして、プロットを元のスケールに戻します。



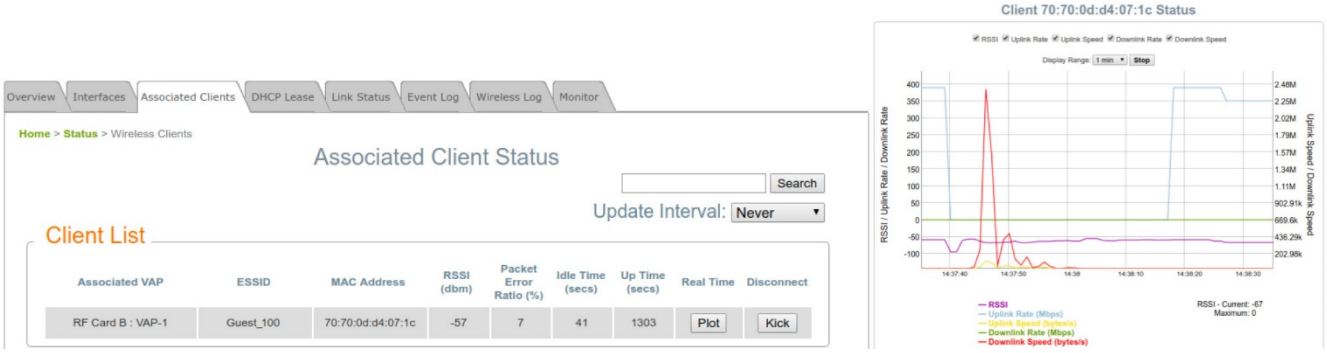
7.2 Interfaces(インターフェイス)

トラフィック情報はインターフェイスごとに利用できます。記録されるデータには、**Packets In(パケットイン)**、**Packets Out(パケットアウト)**、**Traffic In(トラフィックイン)**（**kb**）、および**Traffic Out(トラフィックアウト)**（**kb**）が含まれます。

リアルタイムプロットも各インターフェイスで使用できます。その時間軸は次のオプションで構成できます：1 minute(1分)、2 minutes(2分)、5 minutes(5分)、または10 minutes(10分)。マウスを左クリックして、目的の領域を拡大します。ダブルクリックして、プロットを元のスケールに戻します。

7.3 Associated Clients(関連クライアント)

管理者は、このページで関連するすべてのクライアントのステータスをリモートで監視できます。ここで低いSNRが見つかった場合、管理者は対応するパラメーターを調整するか、関連するクライアントの設定を調査して、ネットワーク通信のパフォーマンスを向上させることができます。



リアルタイムプロットも各インターフェイスで使用できます。その時間軸は次のオプションで構成できます:1 minute(1分)、2 minutes(2分)、5 minutes(5分)、または10 minutes(10分)。マウスを左クリックして、目的の領域を拡大します。ダブルクリックして、プロットを元のスケールに戻します。

Associated VAP(関連VAP):クライアントが関連付けられているVAPの名前。

ESSID:クライアントが関連付けられているExtended Service Set ID(拡張サービスセットID)。

MAC Address(MACアドレス):関連するクライアントのMACアドレス。

RSSI:各クライアントのアソシエーションのReceived Signal Sensitivity Index(受信信号感度指数)。

Packet Error Ratio(パケットエラー率):パケットが受信されていないかどうかを確認するための、関連するクライアントのサービス品質の指標。

Idle Time(アイドルタイム):関連するクライアントが非アクティブである期間。時間の単位は秒です。

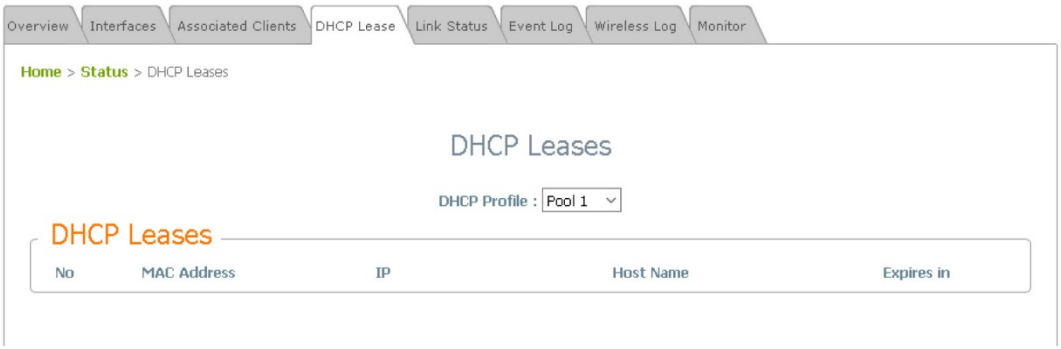
Up time(アップタイム):クライアントが関連付けられている期間。時間の単位は秒です。

Real Time(リアルタイム)(プロット):Packets In/Out(パケットイン/アウト)、In/Out in Kb(キロバイト単位のトラフィックイン/アウト)、RSSI、Uplink/Downlink Rates(アップリンク/ダウンリンクレート)など、関連する各クライアントのトラフィック情報のリアルタイムプロット。

Disconnect(切断):***[Kick(キック)]***をクリックすると、クライアントはシステムから切断されます。

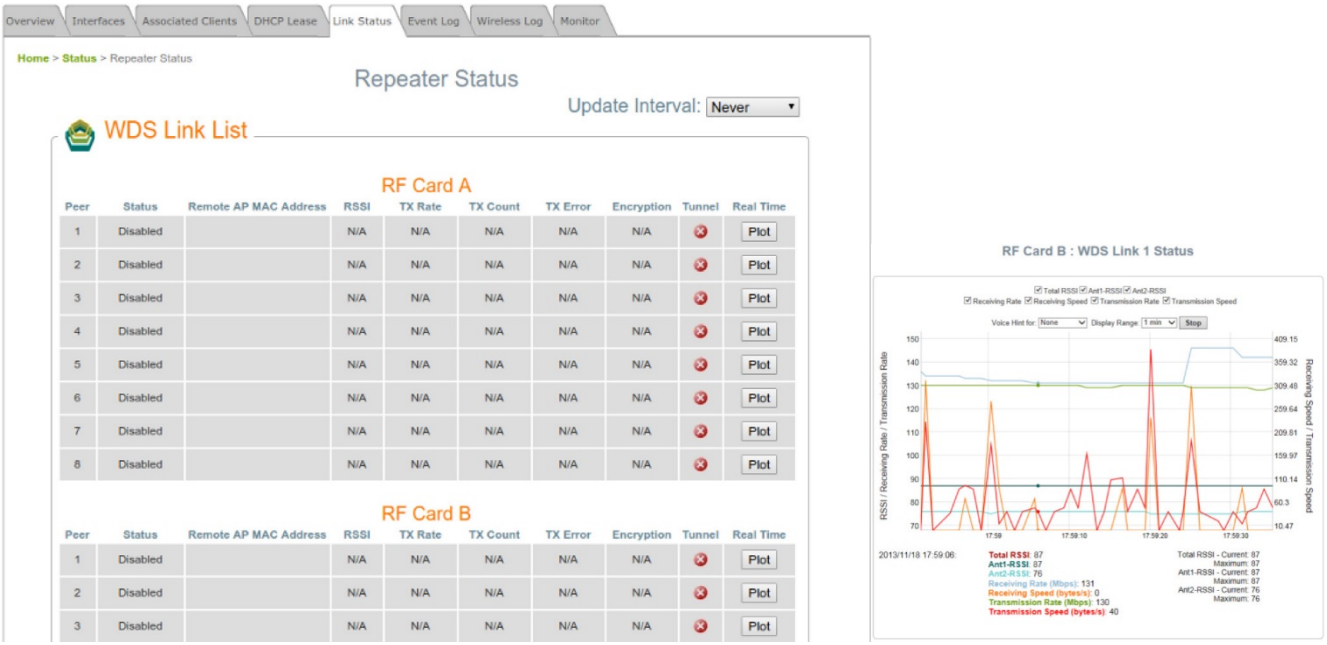
7.4 DHCP Lease(DHCPリース)

VAPがNATモードで動作している場合、DHCP Lease(DHCPリース)情報がこのテーブルに表示されます。



7.5 Link Status(リンクステータス)

管理者は、**Status(ステータス) > Link Status(リンクステータス)**で、リピーター機能の詳細情報を確認できます。WDSステータス、トラフィック統計、暗号化などの詳細情報が提供されます。

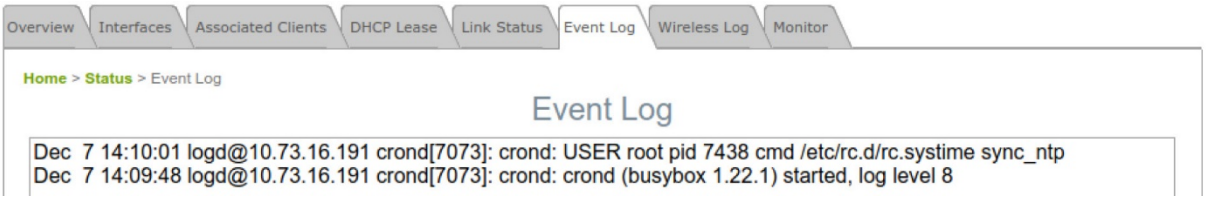


プロットをクリックすると、WDSリンクステータスの動的グラフが表示されます。プロットに関する情報には、Total RSSI(合計RSSI)、Ant1 RSSI、Ant2 RSSI、Transmission Rate(送信レート)、Receiving Rate(受信レート)、Transmission Speed(送信速度)、およびReceiving Speed(受信速度)が含まれます。

リアルタイムプロットも各インターフェイスで使用できます。その時間軸は次のオプションで構成できます:1 minute(1分)、2 minutes(2分)、5 minutes(5分)、または10 minutes(10分)。ダブルクリックして、プロットを元のスケールに戻します。
アンテナの調整時に、音声ヒントを有効にすることもできます。

7.6 Event Log(イベントログ)

Event Log(イベントログ)は、システムイベントの記録を提供します。管理者は、このログを確認することでシステムのステータスを監視できます。内部ストレージは限られているため、外部Syslogサーバーを介してすべてのログをバックアップすることをお勧めします。



Event Log(イベントログ)の各エントリはイベントレコードを表します。 各行には4つのフィールドがあります:

Date and Time(日時):イベントが発生した日時。

IP Address(IPアドレス):このイベントを記録したシステムのLAN IPアドレスを示します。このページのすべてのイベントはローカルイベントであるため、このフィールドのIPアドレスは常に同じであることに注意してください。ただし、リモートSYSLOGサービスでは、このフィールドは管理者がこのアクセスポイントからのイベントを識別するのに役立ちます。

Process name(プロセス名):実行中のインスタンスによって生成されたイベントを示します

Description(説明):各イベントのメッセージを表示します

SAVE LOG(ログの保存):ファイルをローカルディスクに.txtファイルとして保存します

CLEAR(消去):すべてのレコードを消去します

7.7 Wireless Log(無線ログ)

このWireless Log(無線ログ)は、クライアントの関連付けとWDS接続に関連するアクティビティを追跡します。管理者は、このログを確認することでシステムのステータスを監視できます。内部ストレージは限られているため、外部Syslogサーバーを介してすべてのログをバックアップすることをお勧めします。

Wireless Log(無線ログ)の各エントリはイベントレコードを表します。各行には4つのフィールドがあります:

Date and Time(日時):イベントが発生した日時。

IP Address(IPアドレス):このイベントを記録したシステムのLAN IPアドレスを示します。このページのすべてのイベントはローカルイベントであるため、このフィールドのIPアドレスは常に同じであることに注意してください。ただし、リモートSYSLOGサービスでは、このフィールドは管理者がこのアクセスポイントからのイベントを識別するのに役立ちます。

Process name(プロセス名):実行中のインスタンスによって生成されたイベントを示します

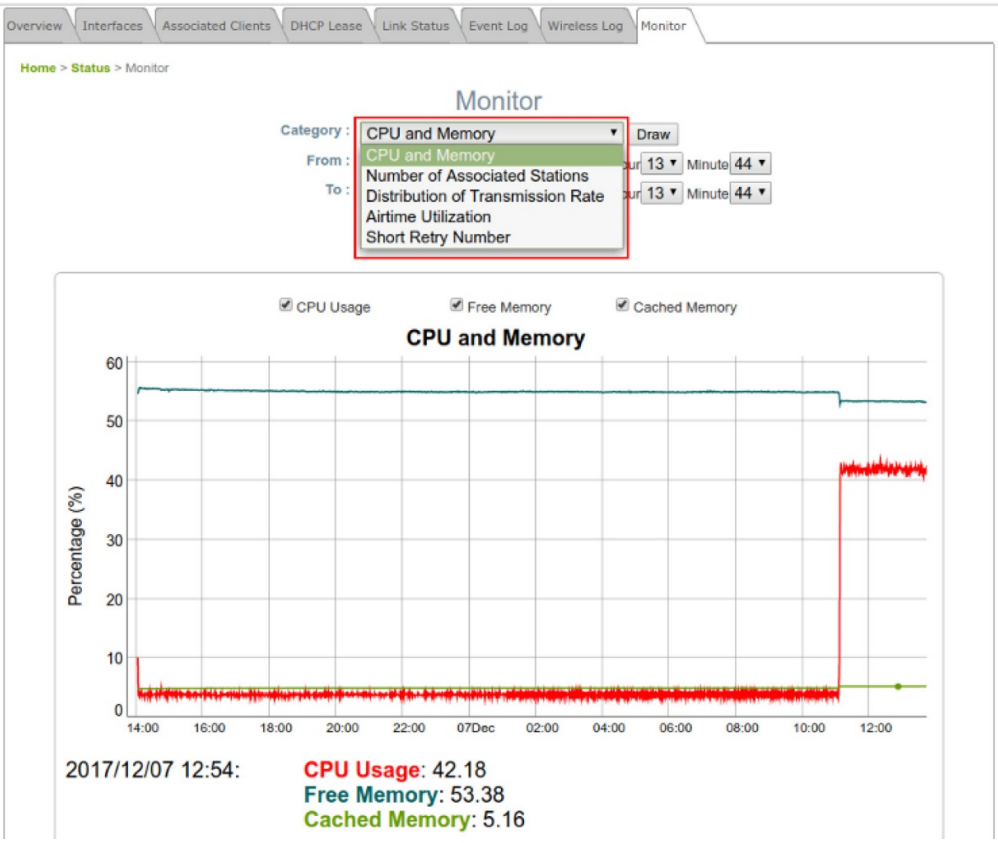
Description(説明):各イベントのメッセージを表示します

SAVE LOG(ログの保存):ファイルをローカルディスクに.txtファイルとして保存します

CLEAR(消去):すべてのレコードを消去します

7.8 Monitor(モニター)

複数のモニターチャートは、時間ディメンションにおけるAPのパフォーマンスの概要をすばやく提供します。データをフィルタリングするために、各チャートの[Begin time(開始時間)]と[End time(終了時間)]を選択できます。マウスを左クリックして、目的の領域を拡大します。ダブルクリックして、プロットを元のスケールに戻します。



CPU and Memory(CPUとメモリ):デバイスの使用状況を表示します。CPU < 90 %およびRAM < 90 %は許容範囲です

Number of Associated Station(関連付けられたステーションの数):選択した無線(RF Card A(RFカードA)またはRF Card B(RFカードB))に接続されているデバイスの数を表示します。

Distribution of Transmission Rate(送信レートの分布):送信レートで分類された送信パケット数を表示します。

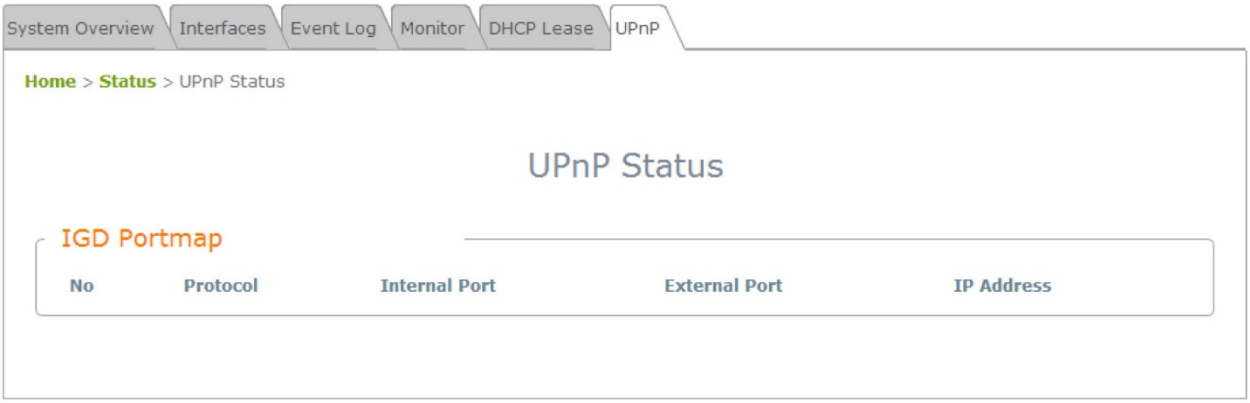
Airtime Utilization(エアタイム使用率):無線環境の信号対ノイズを表示します。Airtime Utilization(エアタイム使用率) < 70%が最適です

- **RX Clear Rate(RXクリアレート)**:現在のチャネルが使用するエアタイムの割合。
- **RX Frame Rate(RXフレームレート)**:APが受信して復号するエアタイムの割合。
- **TX Frame Rate(TXフレームレート)**:APがデータを送信しているエアタイムの割合。

Short Retries Number(短い再試行回数):再送信されたパケットの数を表示します。Short Retries(短い再試行) < 200が最適です

7.9 UPnP（CPEモードのみ）

このテーブルは、Protocol(プロトコル)、Internal Port(内部ポート)、External Port(外部ポート)、IP Address(IPアドレス)などのUPnPの概要に関する情報を提供します。



IGD Portmap(IGDポートマップ):

- **No.(番号)**:UPnPデバイスの項目番号。
- **Protocol(プロトコル)**:UPnPデバイスが使用するプロトコル。
- **Internal Port(内部ポート)**:UPnPデバイスの内部ポート番号。
- **External Port(外部ポート)**:システムのマップされた外部ポート番号。
- **IP Address(IPアドレス)**:UPnPデバイスのIPアドレス。

8. Console Interface(コンソールインターフェイス)

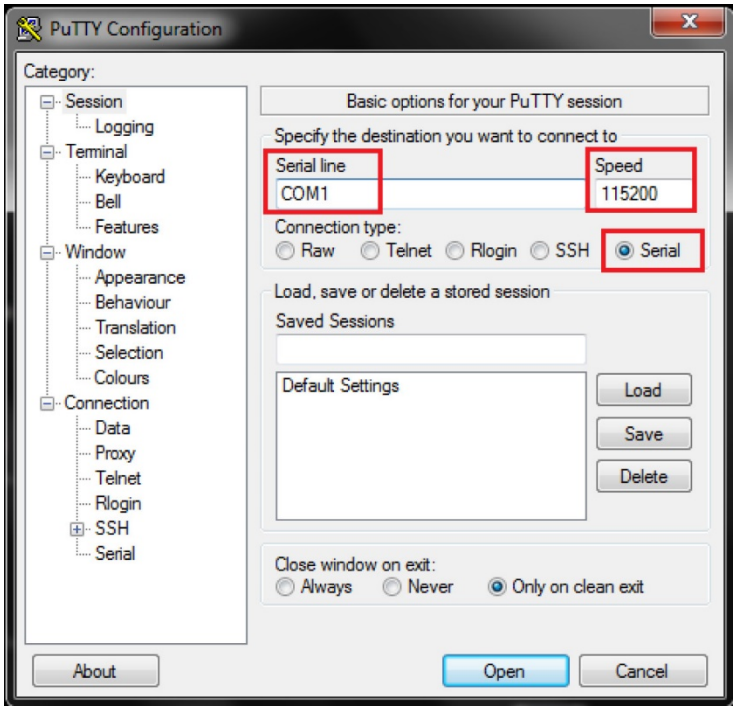
管理者は、コンソールポートを経由して、コンソールインターフェイスに入り、APを工場出荷時デフォルト設定にリセットできます。APのコンソールポートに接続する場合は、コンソールケーブル、およびターミナルシミュレーションプログラム（PuTTyなど）が必要です。コンソールインターフェイスにアクセスするには2つの方法があります

8.1 コンソールケーブルによる直接接続

PC > USB to RS-232 DB9 Serial Converter Cable(USB-RS-232 DB9シリアルコンバータケーブル) > Console Cable(コンソールケーブル)（DB9-to-RJ45） > Console Port(コンソールポート)
USB-to-RS232ケーブルは、標準パッケージには付属していません。パッケージに付属のコンソールケーブルのみを使用することをお勧めします。

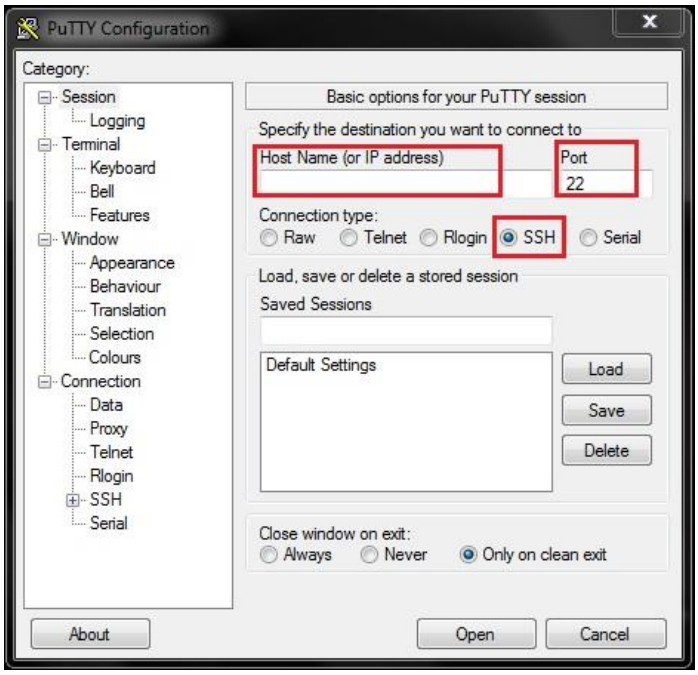
ケーブル	説明
	USB-RS-232シリアル変換ケーブル（USB-DB9オス）
	コンソールケーブル（DB9メス-RJ45オス）

速度（ボーレート）は115200です。

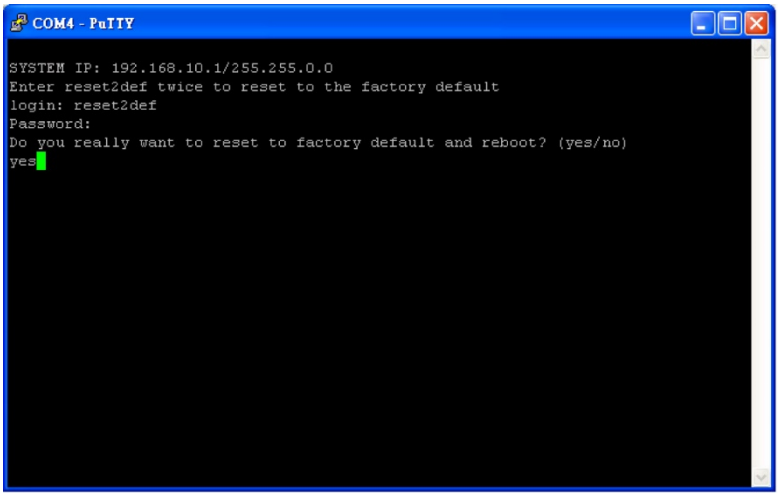

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Serial line
COM1
Speed
115200
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

8.2 Remote Connection by SSH Interface(SSHインターフェイスによるリモート接続)

システムは、SSHを経由するコンソールインターフェイスへのアクセスをサポートしています。通常、SSHはポート22を使用し、アクセスにはWAN IPアドレスが必要です。



コンソールインターフェイスからシステムを工場出荷時デフォルトにリセットするには、「reset2def」としてログインし、パスワードとして「reset2def」を入力します。



コンソール接続がすぐに利用できない場合、APのIPアドレスは、別のAPの検出ユーティリティ(Home(ホーム) > Utilities(ユーティリティ) > Discovery Utility(検出ユーティリティ))で取得できます。イーサネットケーブルで接続し、Discovery Utility(検出ユーティリティ)を実行するだけです。