ユーザマニュアル

エンタープライズアクセスポイント

Version 3.45.0000

著作権

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ないです。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

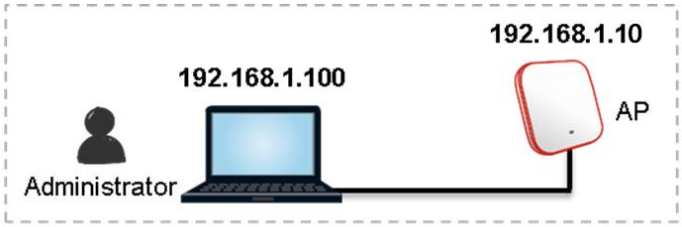
1. エンタープライズアクセスポイントクイック展開

AP を初めて設定するには、管理者は最初の設定を実行して、AP がローカルゲートウェイと通信し、Wi-Fi デバイスが有線ネットワークに接続できるようにするために必要な IP アドレスなどの情報を AP に割り当てる必要があります。

1.1 AP へのログイン

AP には、構成と管理のための Web ベースのインタフェースがあります。初めて Web 管理インタフェース(WMI)にアクセスするには、次の手順に従います。

1. **管理 PC が AP と同じサブネット(192.168.1.10/255.255.255.0)内のスタティック IP アドレスに手動で設定されていることを確認し、PC をイーサネットケーブルで AP の LAN ポートに接続します。**

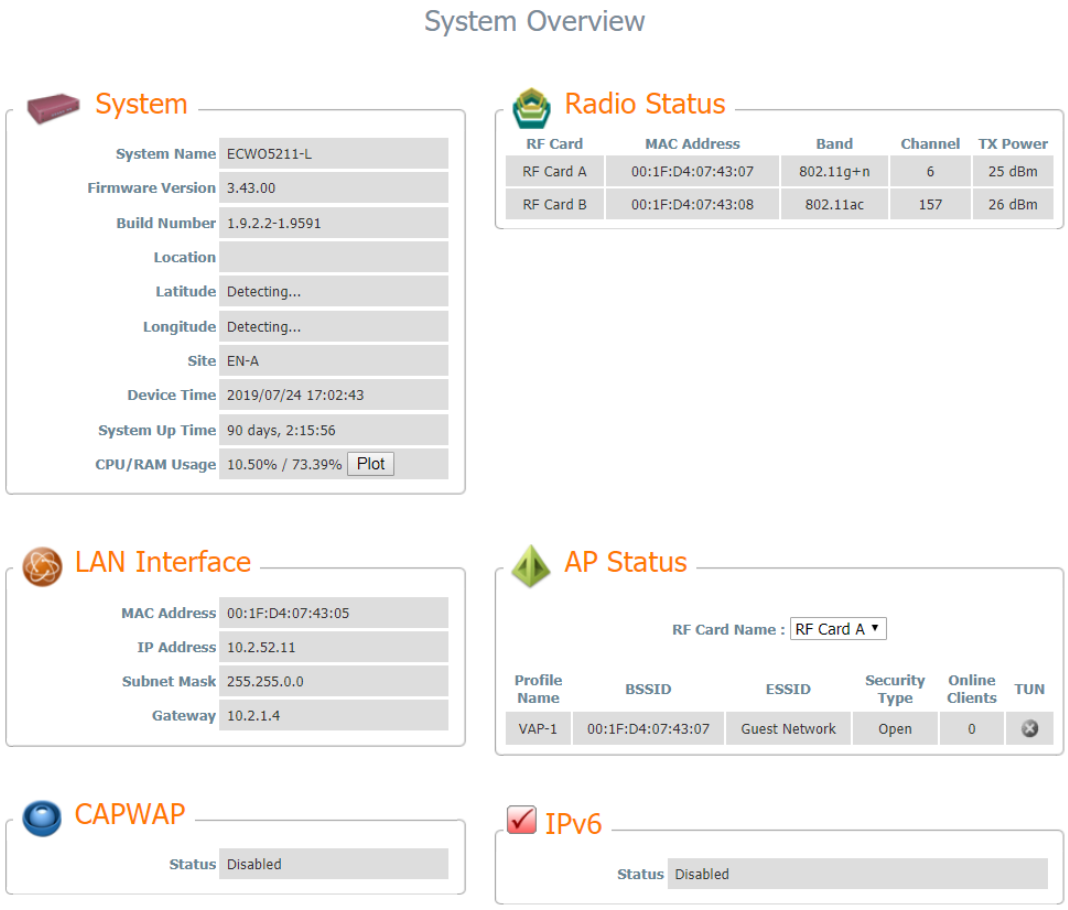


Same Subnet: 192.168.1.0/255.255.255.0 (**192.168.1.x**)

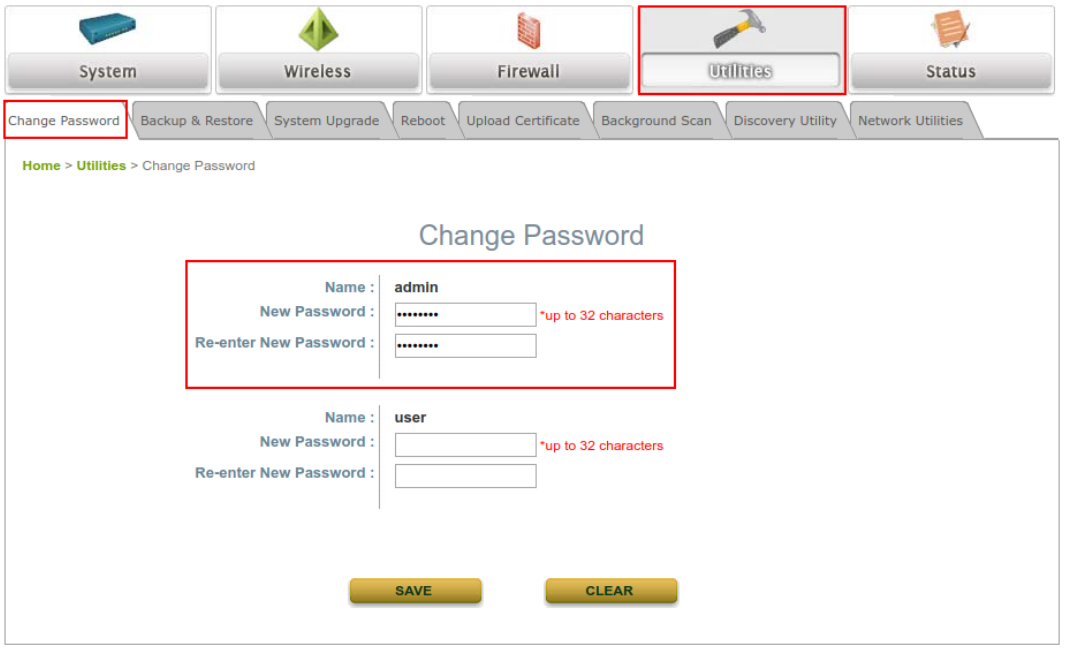
2. **Web ブラウザを起動し、AP(192.168.1.10)のデフォルト IP アドレスをアドレス欄に入力します。**

Administrator Login ページでデフォルトユーザ名(admin)とパスワード(admin)でログインします。

3. ログイン後、System Overview ページが表示されます。

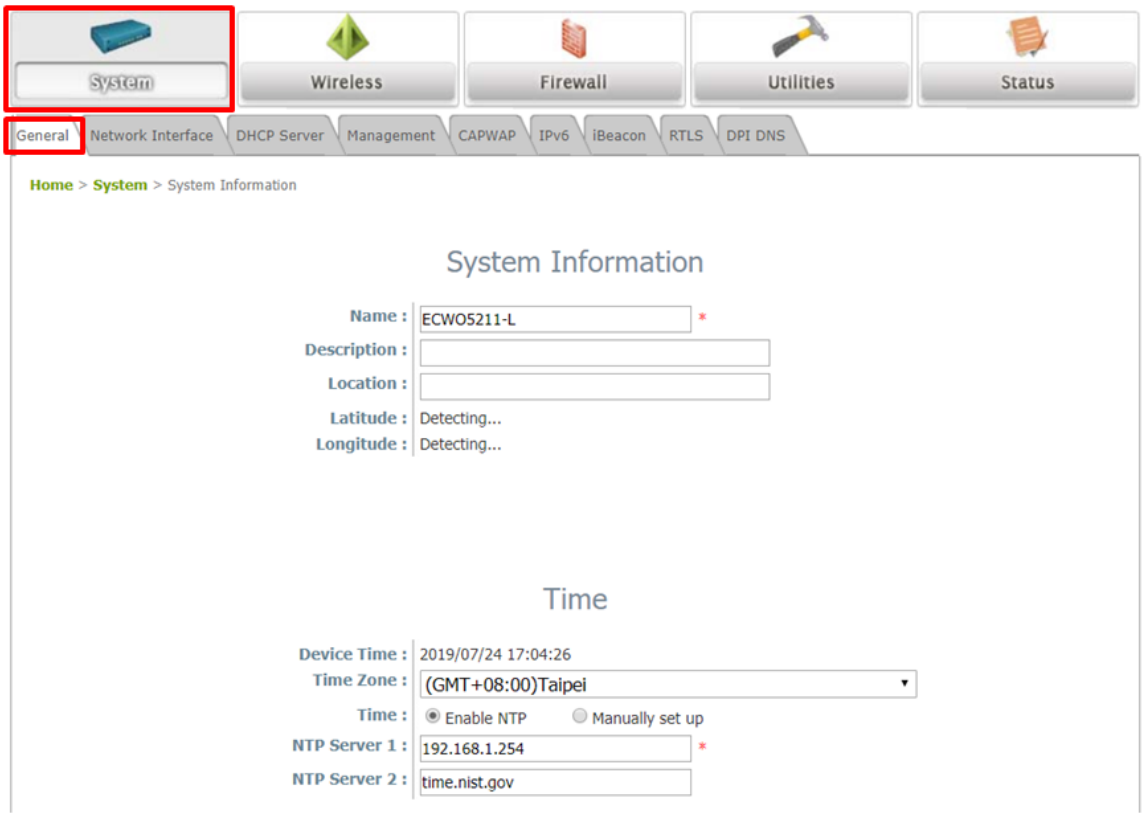


4. セキュリティ上の理由から、管理者のパスワードを変更します。
   - メインメニューの Utilities アイコンをクリックし、Change Password タブを選択します。
   - New Password を入力し、Re-enter New Password に再入力します。



1.2 全般情報の設定

System の General ページ(Home>System>General)に移動して、AP の全般情報を設定します。



1. **System Information**: システム関連の情報(Name、Description、および Location)を入力します。これにより、管理者はネットワーク内の AP を識別できます。

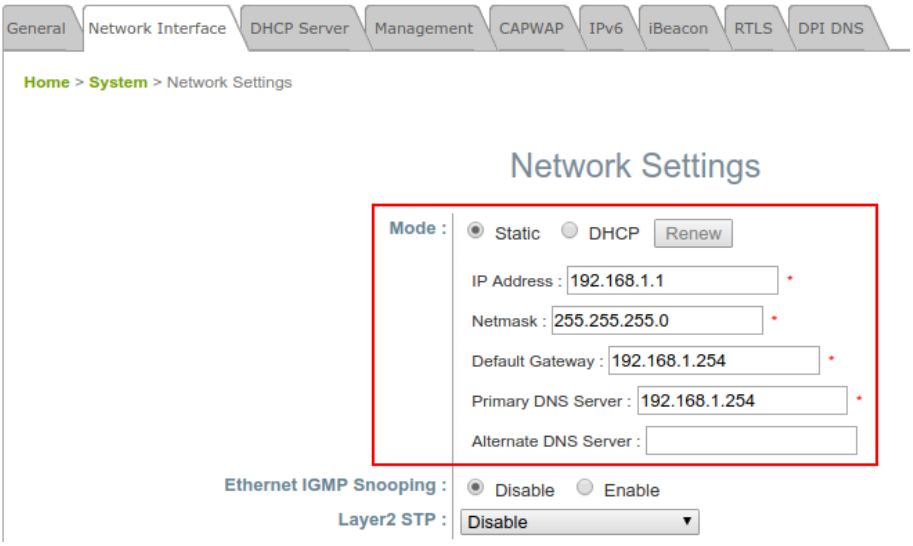
2. **Time**: この初期設定では、Enable NTP 方法(Network Time Protocol (NTP)サーバとシステム時刻を同期させる)を使用して、AP のシステム時刻を設定します。

1.3　ネットワークへの接続

以下の手順は、無線 LAN ネットワークを使えるようにするための基本的な手順です。AP は、LAN ポートを介して有線ネットワークに接続し、ネットワークへの無線アクセスを可能にします。

1.　AP の IP 設定の変更

Network Interface ページ(Home>System>Network Interface)に移動し、ネットワークの設定をします。



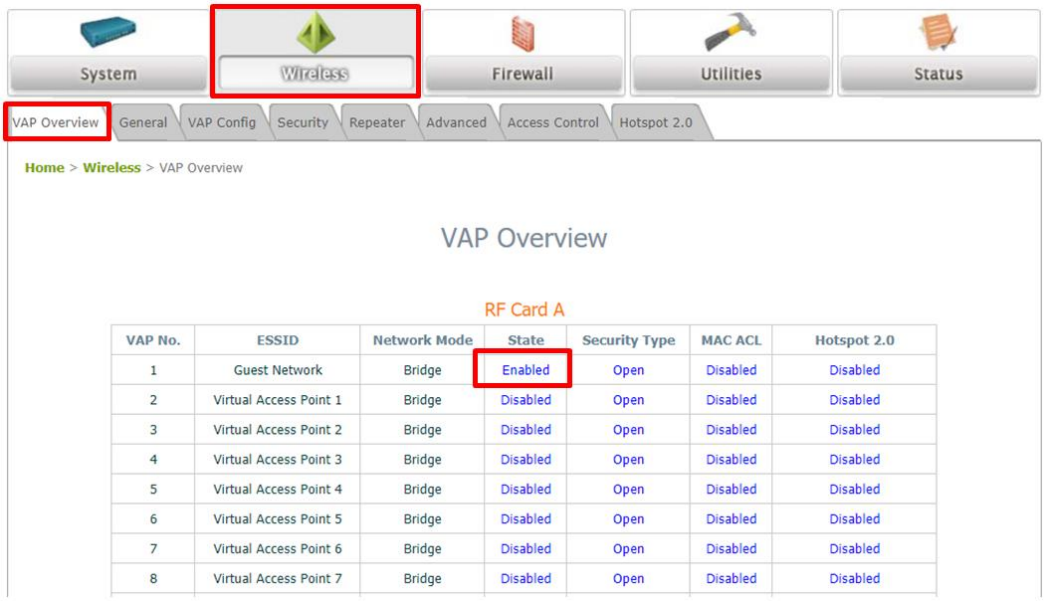
Mode:

Static: ネットワークインタフェース(IP Address、Netmask、Default Gateway、Primary DNS Server)の適切な値を手動で入力します。上記の例では、AP はまだデフォルト IP アドレス 192.168.1.10 を使用しています。

DHCP: AP が LAN からダイナミック IP アドレスを取得する必要がある場合は、モードを DHCP に設定し、SAVE をクリックして変更を送信します。

2.　Wi-Fi 接続用の最初の SSID の有効化

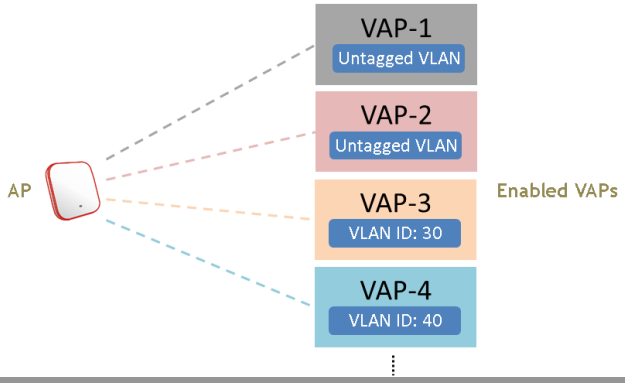
デフォルトでは、1 つの Service Set Identifier (SSID)が無線 A(RF Card A)で有効になり、1 つの SSID が無線 B(RF Card B)で有効になります。VAP Overview ページ(Home>Wireless>VAP Overview)に示すように、仮想アクセスポイント No.1(VAP-1)プロファイルは、使用可能な最初の SSID を表します。



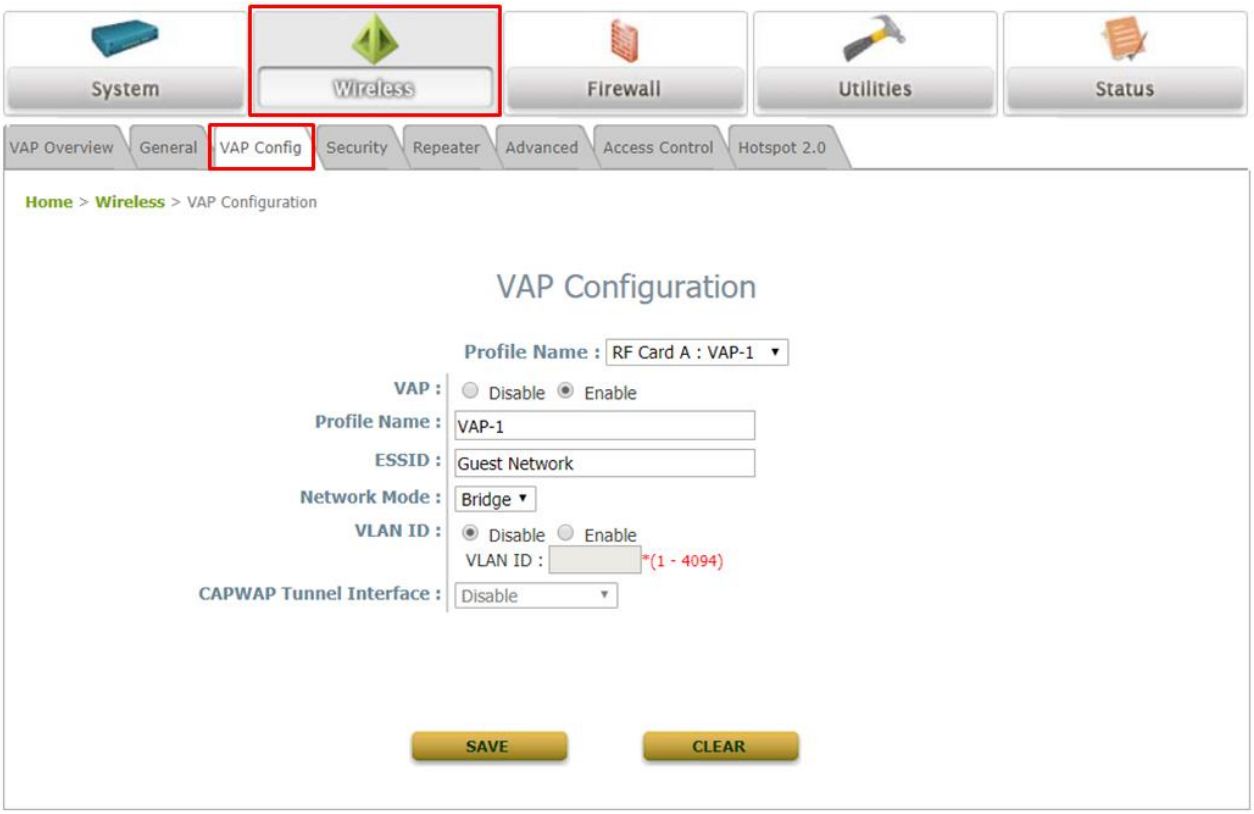
NOTE:

仮想 AP (VAP):

- VAP 機能を使用すると、以下の図の例に示すように、単一の物理 AP デバイス(一意の単一 BSSID)を複数の個別 AP として表示できます。
- それぞれの VAP は、独自の設定(SSID、Network Mode、VLAN ID、Security など)を使用して個別に有効または無効にでき、AP は複数の SSID を介してさまざまなクライアントをサポートできます。

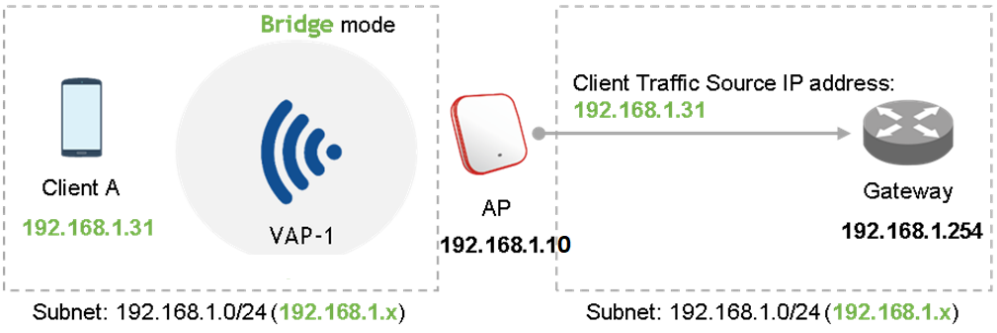


VAP-1 の状態(Enabled)をクリックしてプロファイルを設定します。これにより、次の VAP 設定ページが表示されます。

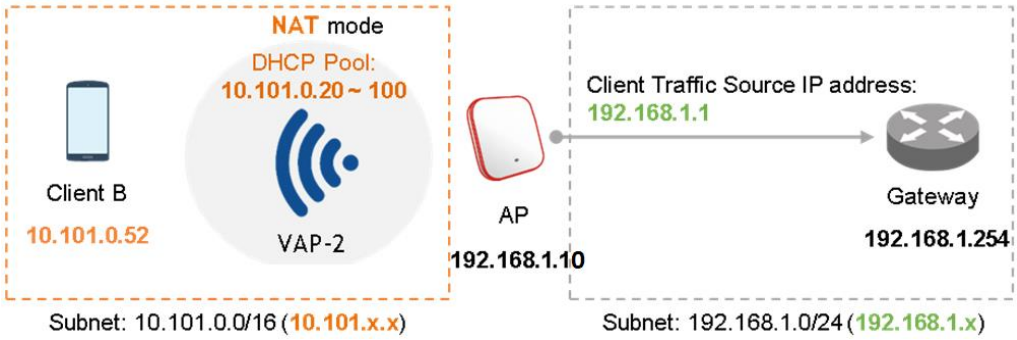


特定の VAP プロファイルを選択します(この場合、"RF Card A: VAP-1")。VAP の基本設定は、次のようにプロファイルに収集されます。

- **VAP**: この VAP を無効または有効にします。
- **Profile Name**: ID/管理を目的とした VAP プロファイルの名前。
- **ESSID**: Extended Service Set Identifier (ESSID)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。
- **Network Mode**:
  - **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/スイッチで確認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(この例では、下図に示すように 192.168.1.31)。



- **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/スイッチで確認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(この例では、下図に示すように 192.168.1.10)。

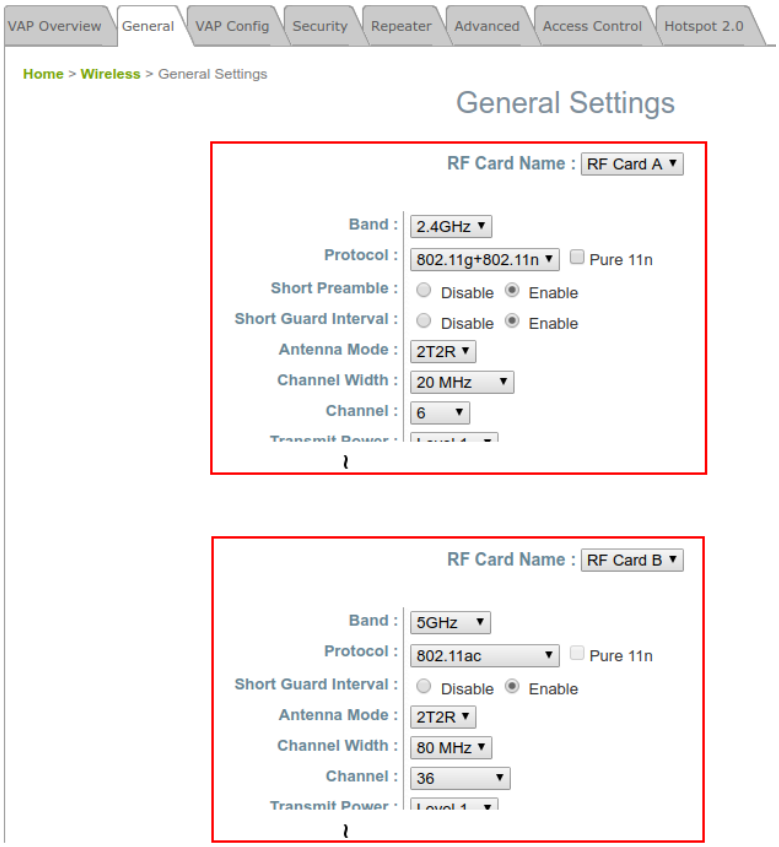


- **VLAN ID**: SSID ごとの VLAN タグ付け機能ー有効にすると、この SSID を介して AP に入るクライアントのトラフィックに、設定された VLAN ID がタグ付けされます。
- **DHCP Profile**: 内蔵 DHCP サーバプロファイル。DHCP サーバの IP 設定は Home>System>DHCP Server で確認可能です。
- **CAPWAP Tunnel Interface**: AP がコントローラによって管理されている場合、AP とコントローラ間の接続を示す 3 つの状態は次の通りです。
  - **Disable(トンネルなし)**: AP は、コントローラへの CAPWAP トンネル接続なしで動作しています。
  - **Split Tunnel**: AP は CAPWAP トンネルを介してコントローラに control トラフィックのみを渡します。つまり、data 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**: AP は、CAPWAP トンネルを介してコントローラに control トラフィックと data トラフィックの両方を渡します。

NOTE:
- VLAN ID は、VAP が Bridge モードにある場合にのみサポートされます。
- DHCP プロファイルおよび DHCP サーバは、VAP が NAT モードに設定されている場合にのみ有効になります。
- VAP が NAT モードの場合、CAPWAP トンネルインタフェースは Disable(トンネルなし)または Split Tunnel の 2 つの状態でのみ機能します。

3. 全般的な無線設定

Home>Wireless>General では、RF Card A と B のグローバル設定があります。RF Card A は 2.4GHz 帯で動作し、RF Card B は 5GHz 帯で動作しており、どちらもデフォルトで有効になっています。
最初の構成では、以下に示すデフォルトの基本設定を変更することができます。
RF Card A: 2.4GHz、802.11g+802.11n、Antenna Mode 2T2R、Channel Width 40MHz、Channel 6
RF Card B: 5GHz、802.11ac、Antenna Mode 2T2R、Channel Width 80MHz、Channel 36
他の設定は後から変更できます。



システムの再起動後、AP はこれらの設定で動作できる様になっています。

NOTE:

SSID、ESSID、および BSSID:

- Service Set Identifier (SSID)は、無線 LAN の名前を識別する鍵です。
- Extended Service Set Identifier (ESSID)=SSID。複数の物理 AP 間のローミングがサポートされるように、同じ SSID を使用するように複数の物理 AP を設定できます。
- 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内で)送信されます。

2. Web 管理インタフェースのナビゲーション

AP には、構成と管理のための Web ベースのインタフェースがあります。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ます。また、この 2 つのモードは互いに異なった Menu になります。次の表に、AP の Web 管理インタフェース(WMI)のメインメニューにあるすべての機能タブを示します。

AP Mode

System	Wireless	Firewall	Utilities	Status
General	VAP Overview	Firewall List	Change Password	Overview
Network Interface	General	Service	Backup & Restore	Interfaces
Port	VAP Config	Advanced	System Upgrade	Associated Clients
DHCP Server	Security		Reboot	DHCP Lease
Management	Repeater		Upload Certificate	Link Status
CAPWAP	Advanced		Background Scan	Event Log
IPv6	Access Control		Discovery Utility	Wireless Log
iBeacon	Hotspot 2.0		Network Utilities	Monitor
RTLS				
DPI DNS				

CPE Mode (ECWO5212-L のみ)

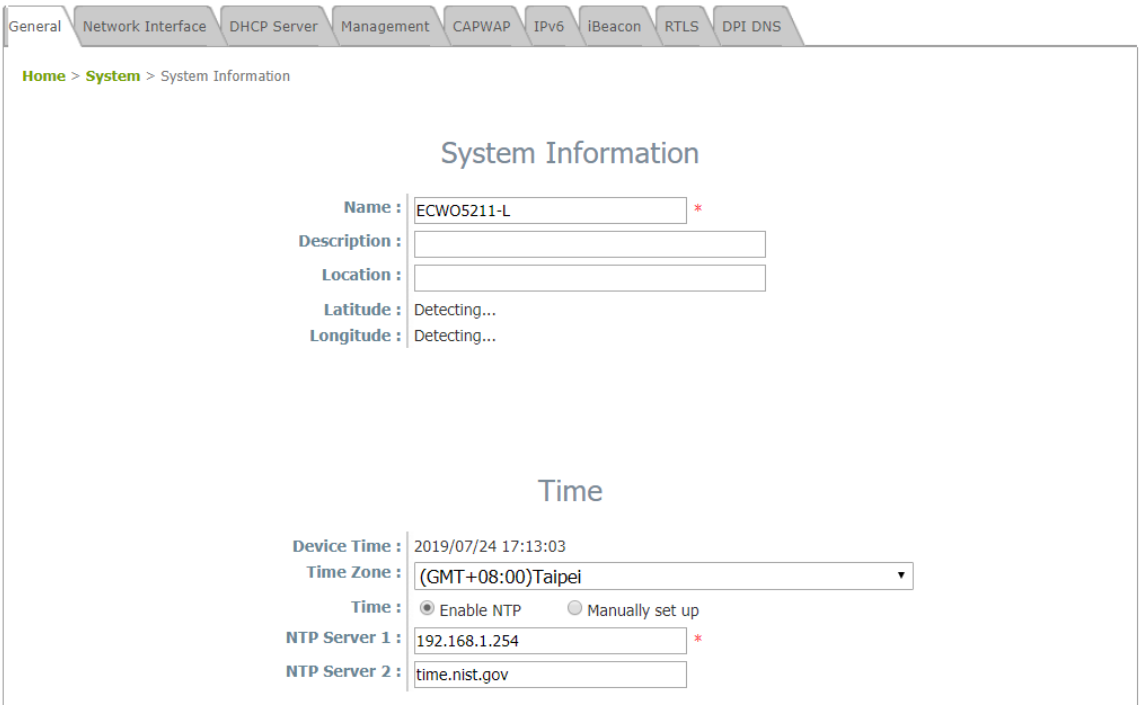
System	Wireless	Firewall	Utilities	Status
General	VAP Overview	IP/Port Forwarding	Change Password	Overview
Network Interface	General	DMZ	Backup & Restore	Interfaces
Port	VAP Config	Advanced	System Upgrade	Associated Clients
DHCP Server	Security		Reboot	Event Log
Management	Advanced		Upload Certificate	Monitor
	Access Control		Background Scan	DHCP Lease
	Site Survey		Discovery Utility	UPnP
			Network Utilities	

NOTE: 設定ページごとに SAVE をクリックして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 をクリックすると、**"Some modification has been saved and will take effect after Reboot."** というメッセージが表示されます。再起動中は、すべてのオンラインユーザが切断されます。

3. System

System をクリックすることにより、管理者は AP の全般的な設定を行うことができます。

3.1 General

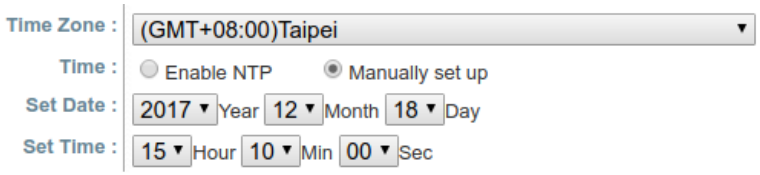


System Information
Name: このシステムを識別するために使用されるシステム名。
Description: システムの詳細(デバイスモデル、ファームウェアバージョン、アクティブ日など)。
Location: 管理者がシステムを簡単に見つけるための、システムの地理的な場所に関する情報。

Time
Device Time: 現在のシステム時刻を表示します。
Time Zone: 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ます。
Time: 時刻の設定には 2 つの方法があります。

- **Enable NTP**: システム時刻を Network Time Protocol (NTP)サーバと同期します。ローカル NTP サーバが使用可能ならばその IP アドレスまたはドメイン名を入力し、そうでなければ一番近い NTP サーバをオンラインで検索して入力し、SAVE をクリックします。

- **Manually set up**: システム時刻を手動で設定します。デフォルトの状態ではこの設定となっており、この方式を選択した場合、システムが起動するたびに設定が必要になります。タイムゾーンを選択し、それに応じて日付と時刻を入力し、SAVE をクリックします。

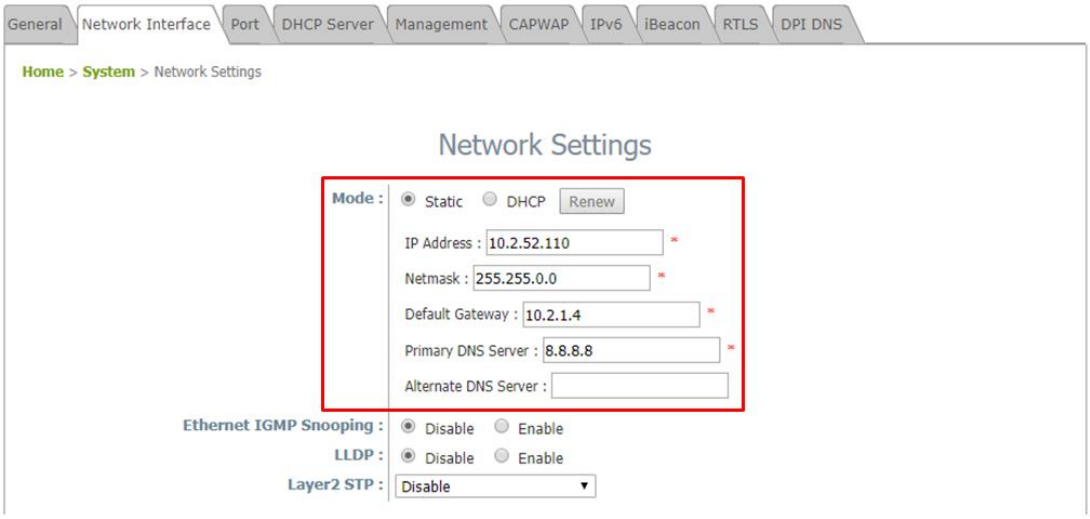


警告メッセージ “*Some modifications have been saved and will take effect after APPLY.” が WMI に表示されたら、APPLY をクリックします。

インターネット接続または NTP が使用できなくなった場合を除き、再起動時にシステム時刻を再設定する必要があるため、時刻同期に NTP サーバを使用することをお勧めします。

3.2 Network Interface

本機のネットワーク設定を行います。赤色のアスタリスク(IP Address、Netmask、Default Gateway、Primary DNS Server)が付いたフィールドは設定必須項目です。



Mode－Static: スタティック LAN IP アドレスを手動で設定できます。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**: LAN ポートの IP アドレス。
- **Netmask**: LAN ポートのサブネットマスク。
- **Default Gateway**: 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(ドメインネームシステム)サーバの IP アドレス。
- **Alternate DNS Server**: 代替 DNS サーバの IP アドレス。

Mode－DHCP: DHCP サーバが存在するネットワークに接続されている場合に設定します。必要なすべての関連 IP 情報は、DHCP サーバによって自動的に提供されます。

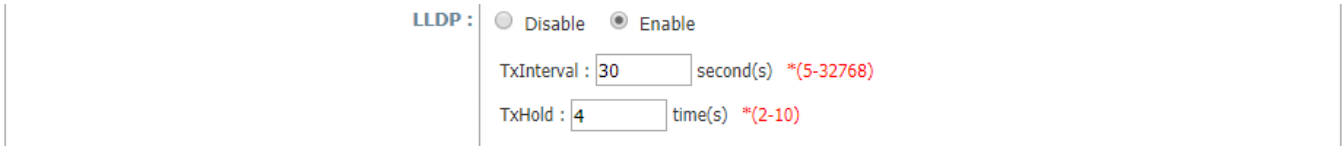
LTE (EAP100 Only): SIM カード付き LTE モジュールを USB ポートに接続した後、以下の 2 つのオプションが表示されます。

- **No LTE**: 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。

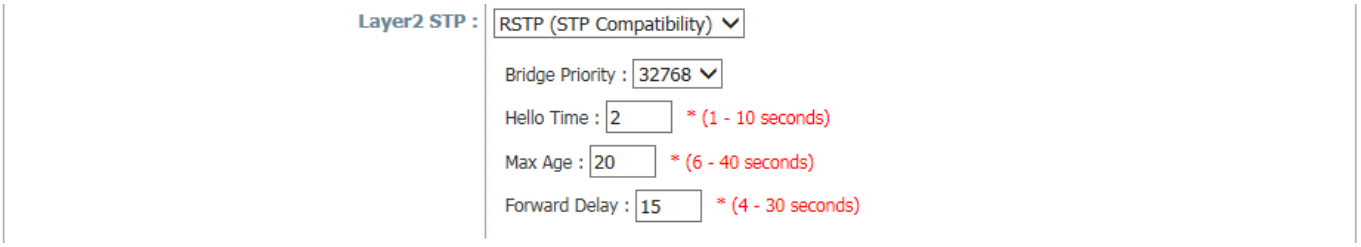
Ethernet IGMP Snooping: 有効にすると、スイッチはトラフィックを転送します。IGMP パケットは、アクセスポイントのネットワークインタフェースと IP マルチキャストホストを介して転送されます。レジストレーション情報は記録され、マルチキャストグループに分類されます。内部スイッチは、マルチキャストトラフィックを要求するポートにのみトラフィックを転送します。逆に、IGMP Snooping なしでは、マルチキャストトラフィックはブロードキャストトラフィックのように扱われ、パケットはすべてのポートに転送され、ネットワークの非効率性を引き起こします。

LLDP: LLDP(Link Layer Discovery Protocol)は、IEEE 標準プロトコル(IEEE802.1ab)であり、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します。これにより、デバイスは(TxInterval * TxHold)秒ごとに定期的に再送信して、基本的なデバイス情報を LAN(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ことができます。

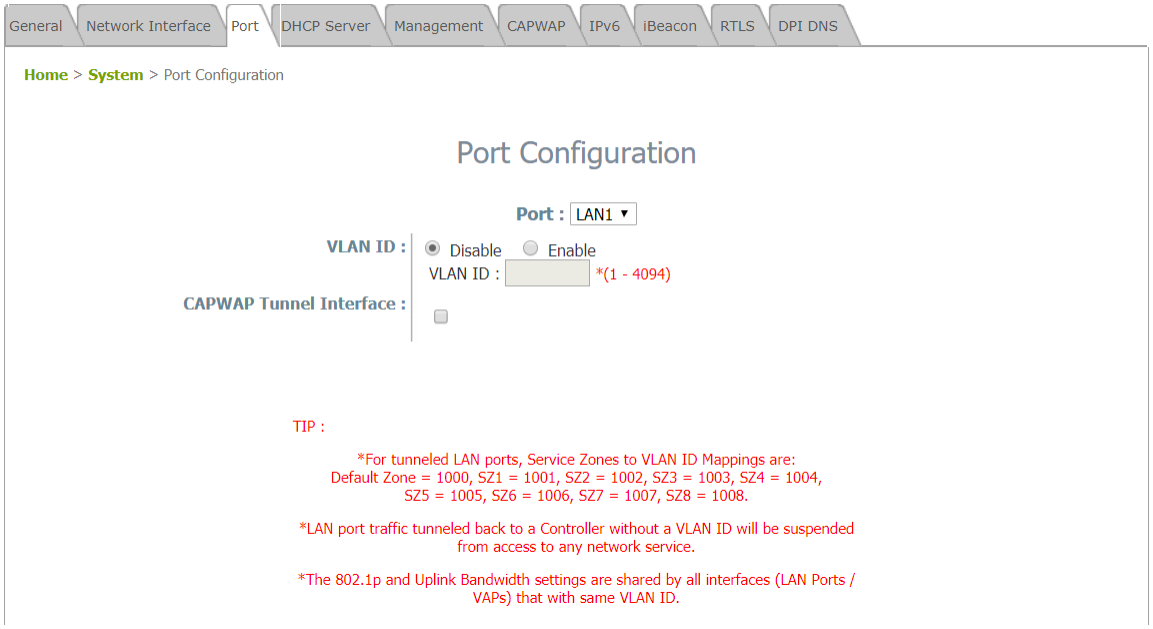
- **TxInterval**: パケットを送信する間隔を設定します。
- **TxHold**: パケットの送信間隔を設定します。



Layer 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、スイッチ間でブロードキャストパケットが無限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、望ましくないループを回避できます。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大部分を消費する可能性があります。従って、レイヤ 2 STP を有効にすることは、このような望ましくない事態を低減し、ネットワーク通信のために利用可能な最良のデータパスを導出することができます。AP は RSTP 動作もサポートしています。設定可能なパラメータには、Bridge Priority、Hello Time、Max Age、Forward Delay などがあります。推奨されるパラメータ値については、IEEE 規格を参照してください。



3.3 Port



Port: ポートの詳細設定を実施する場合は、該当する“Port”を選択します。

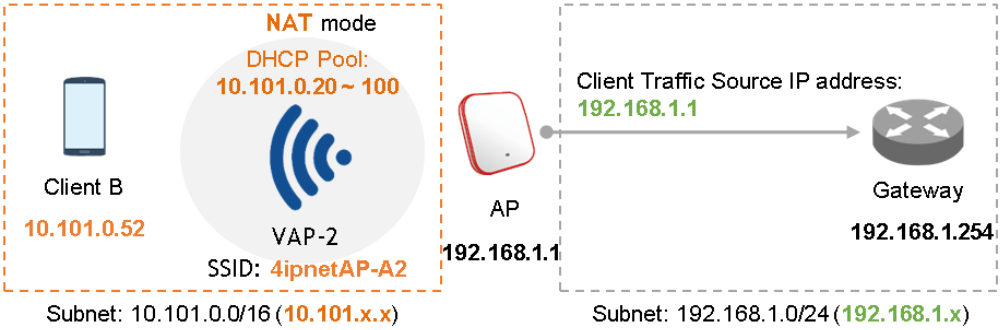
VLAN ID: Enable を選択すると、この LAN ポートからアップストリームに送信されるネットワークトラフィックに、下のフィールドで設定された VLAN ID がタグ付けされます。Disable を選択すると、この LAN ポートからのトラフィックには VLAN ID がタグ付けされません。

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トラフィックを指定するには、LAN、VAP、または WDS インタフェースを選択します。オフになっているネットワークインタフェースの場合、この AP がコントローラの WAN 側にリモートでデプロイされていると、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。

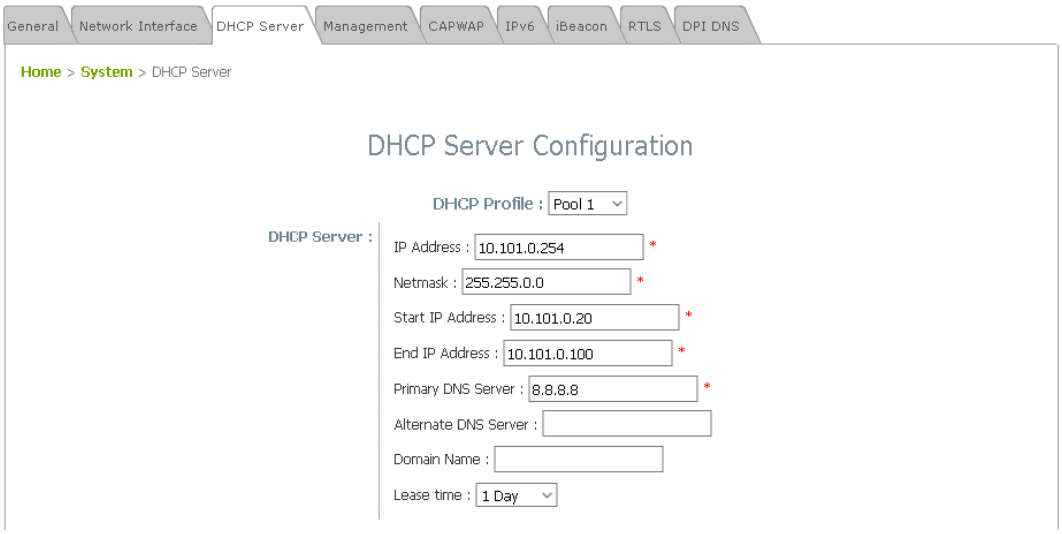
このページの下部にある赤色の TIP では、デフォルトからサービスゾーン 8 まで、CAPWAP を使用するときに、各サービスゾーンに固定の事前定義された VLAN ID 数が割り当てられていることが説明されています。管理者は、トラフィックを特定のサービスゾーンに戻すために、いずれかの数を入力する必要があります。

3.4 DHCP Server

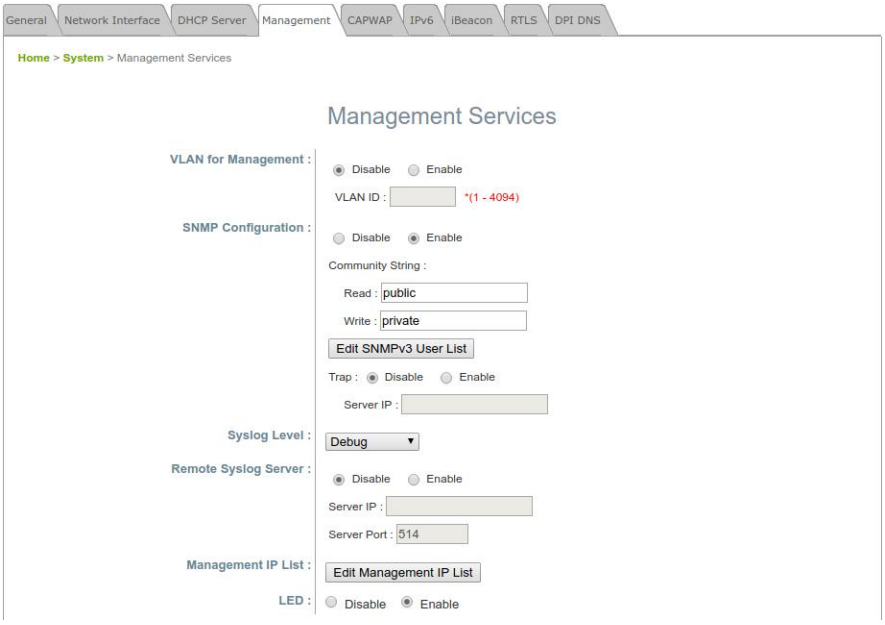
1 つの VAP が NAT モードで動作するように有効になっている場合、関連付けられたクライアント装置には、SSID で設定された DHCP プールから動的 DHCP IP アドレスが割り当てられます。NAT および DHCP モードは、トンネルなしで実行することも、スプリットトンネルを使用する WLAN コントローラで管理することもできます。



Pool1-Pool16 はすべて、A クラスの DHCP IP アドレスとしてデフォルト値として設定され、AP の Web マネジメントインタフェースでのみ設定可能であることに注意してください。16 個の DHCP プロファイルの場合、10.101.0.254/16 から 10.116.0.254/16 まで開始し、DHCP リース時間はデフォルト 1440 分です。



3.5 Management



VLAN for Management: 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 がタグ付けされます。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 Enable になっている場合は、VLAN ID に 1～4094 の値を入力します。

SNMP Configuration: 遠隔で情報を取得するための設定。

- **Enable/Disable**: この機能を有効または無効にします。
- **Community String**: システムの Management Information Base(MIB)にアクセスする場合、コミュニティストリングが必要です。
  Read: 読み取り権限を持つ MIB にアクセスするためのコミュニティストリングを入力します。
  Write: 書き込み権限を持つ MIB にアクセスするためのコミュニティストリングを入力します。
- **Edit SNMPv3 User List**: 読み取りまたは読み取り/書き込みアクセスで 5 つの SNMP ユーザが許可されます。SNMP アカウント一覧で名前と認証パスワードを確認します。
- **Trap**: Enable にすると、コールドスタート、インタフェースアップ&ダウン、アソシエーション&ディスアソシエーションのイベントを、割り当てられたサーバに報告できます。
- **Server IP Address**: トラップレポートを受信する割り当てられたサーバの IP アドレスを入力します。

Syslog Level: ドロップダウンメニューから、受信したいイベントのレベルを選択します。Debug レベルはデフォルト設定と同じです。

Remote Syslog Server: この機能を Enable にした場合、リモートから SYSLOG メッセージを受信する外部 SYSLOG サーバを指定します。

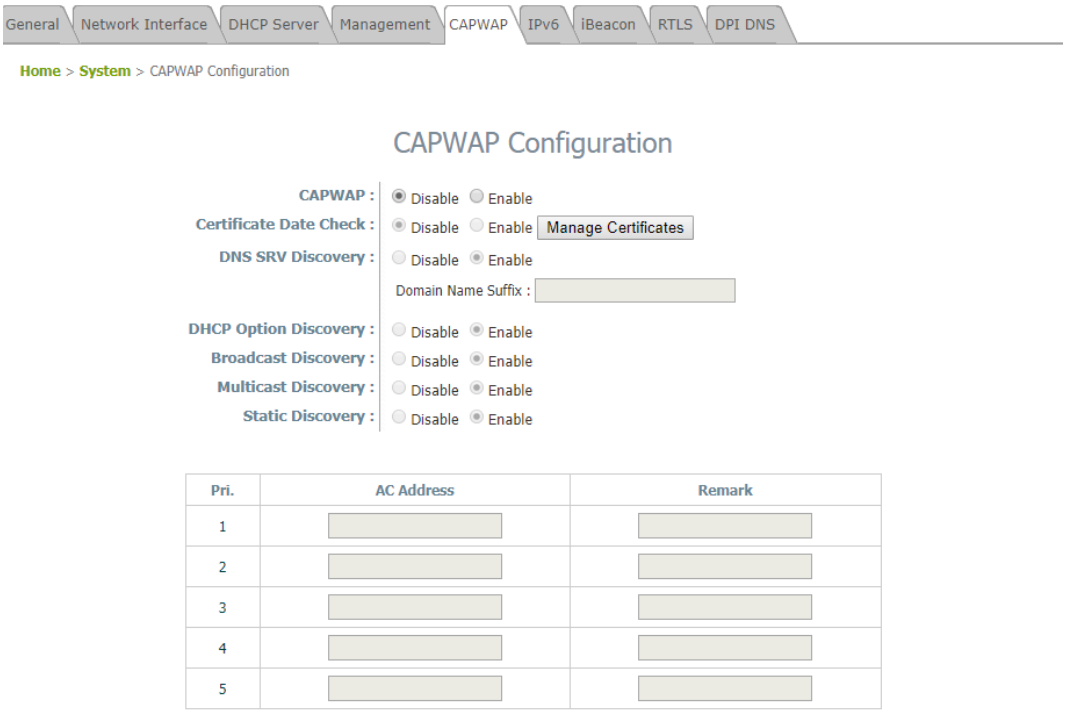
- **Enable/Disable**: この機能を有効または無効にします。
- **SYSLOG Server IP**: 報告されたイベントを受信する Syslog サーバの IP アドレス。
- **Server Port**: Syslog サーバのポート番号。

Management IP List: この AP の WMI へのアクセスを許可する管理者 PC の送信元 IP アドレス/サブネットを入力します。このリストにない他のユーザは、WMI アクセスを拒否されます。デフォルトエントリ 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 インジケータをオンまたはオフにします。

3.6 CAPWAP

CAPWAP は、コントローラが無線アクセスポイントの集合を管理できるようにする標準の相互運用可能なプロトコルです。自動 AP 探索には、DNS SRV、DHCP オプション、ブロードキャスト、マルチキャスト、スタティックの 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: この項目を有効にするには、Enable を選択し、Manage Certificates をクリックして証明書のアップロードページを開きます。「6.5 Upload Certificate」を参照してください。
DNS SRV Discovery: DNS SRV を使用してアクセスコントローラを検出します。

- **Domain Name Suffix**: アクセスコントローラの接尾辞(example.com など)を入力します。

DHCP Option Discovery: DHCP オプションを使用してアクセスコントローラを検出します。

Broadcast Discovery: ブロードキャストを使用してアクセスコントローラを検出します。

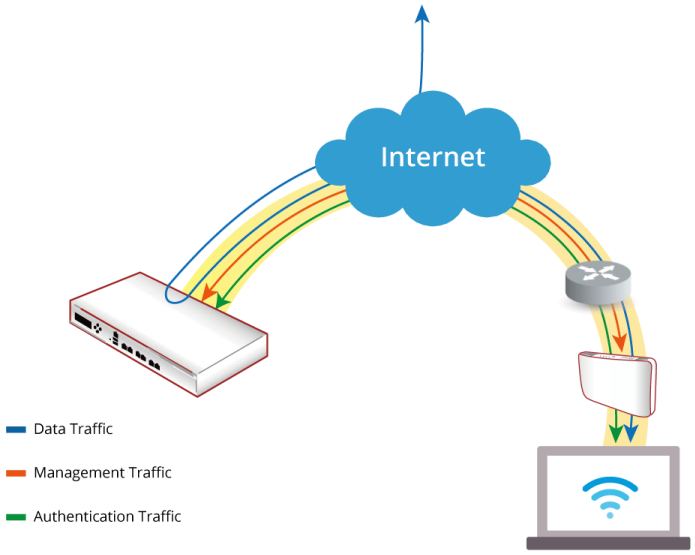
Multicast Discovery: マルチキャストを使用してアクセスコントローラを検出します。

Static Discovery: スタティックアプローチを使用してアクセスコントローラを検出します。

- **AC Address**: アクセスコントローラの 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。

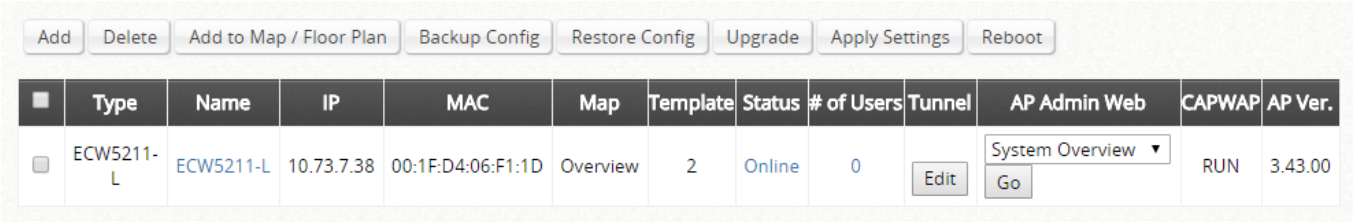
3.6.1 コンプリートトンネルを使用して無線 LAN コントローラで管理するには

コンプリートトンネルは CAPWAP プロトコルを使用してアクセスポイントと通信し、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。無線 LAN コントローラは、リモートサイトでユーザアクセス制御を使用できるように、レイヤ 3 ネットワーク経由でロールベースのポリシーを実装できます。この機能により、WLAN 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。

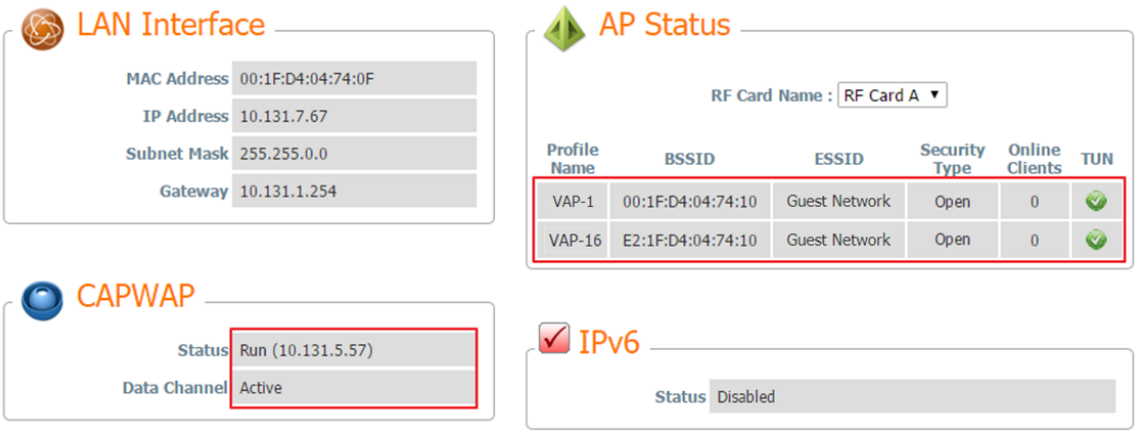


以下の手順が役立つ場合があります。

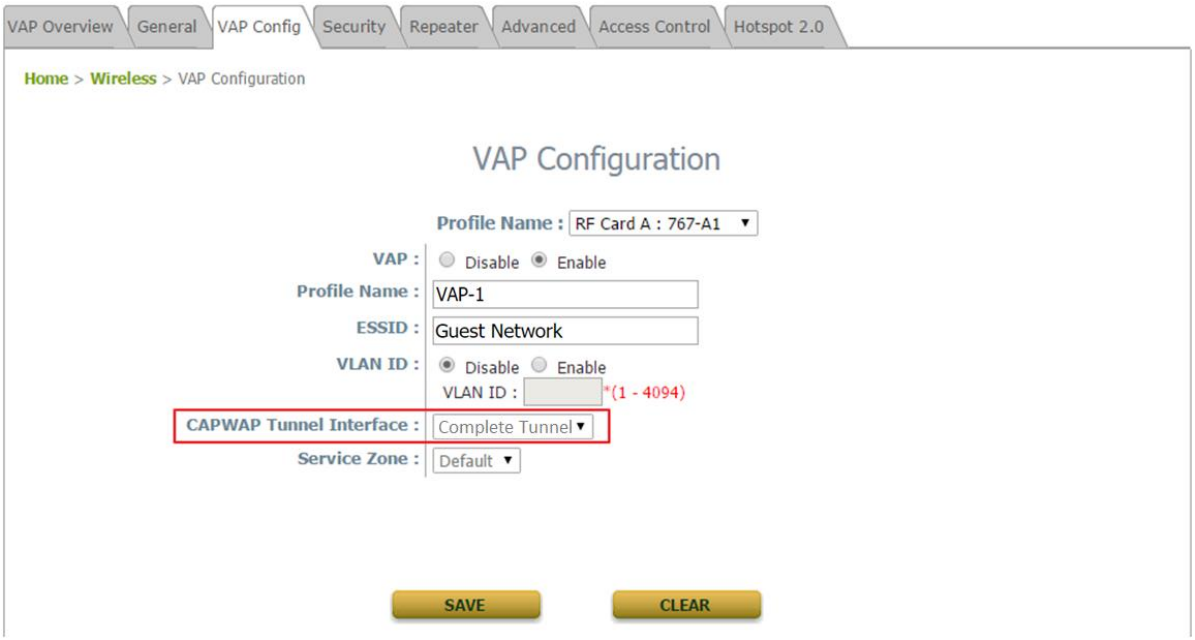
1. On AP: Static Discovery の IP アドレスを入力し、CAPWAP 列に RUN ステータスが表示されるまで待機します。
2. On EWS: CAPWAP Tunnel Interface－Complete Tunnel で VAP Configuration のテンプレートを準備します。
3. On EWS: テンプレートを CAPWAP に適用して AP との間のトンネルを確立すると、VAP がコントローラにトンネリングされるように設定されている場合、トンネルステータスにクリック可能な Edit ボタンが黒色で表示されます。



4. On AP: データチャネルを示す AP WMI がアクティブであることを確認するには、System Overview ページの VAP トンネルステータスが緑色ライトであることを確認します。

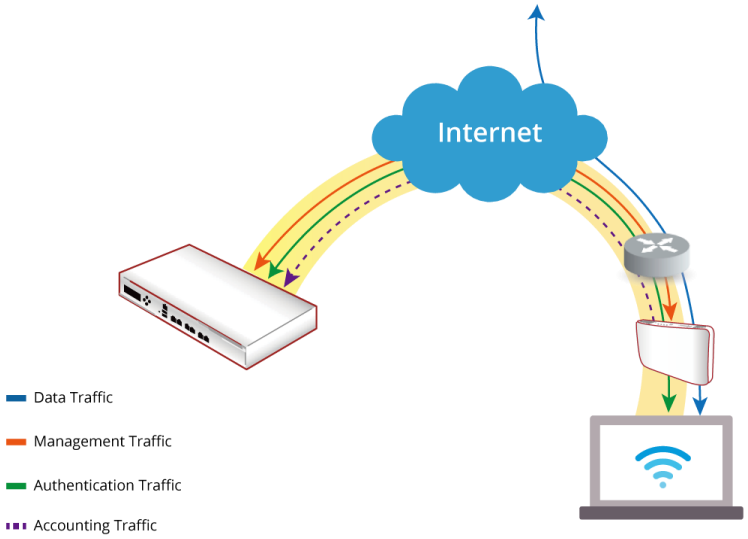


5. On AP: 特定の VAP 構成が Complete Tunnel であることを再確認します。



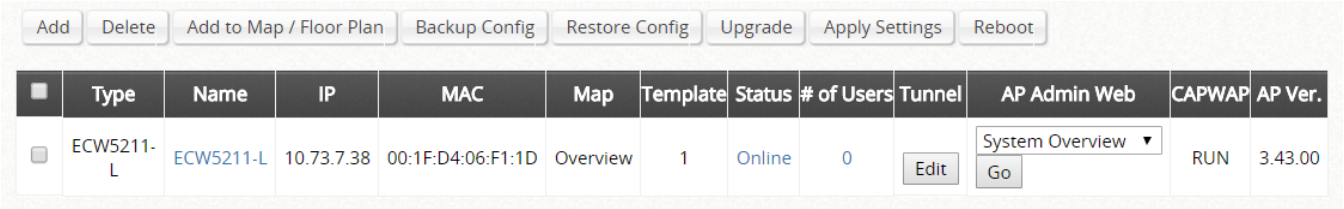
3.6.2　スプリットトンネルを使用して無線 LAN コントローラで管理するには

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を介して直接的にインターネットに送信されます。また、短経路でのユーザ伝送や、コントローラのネットワーク負荷を低減することができます。

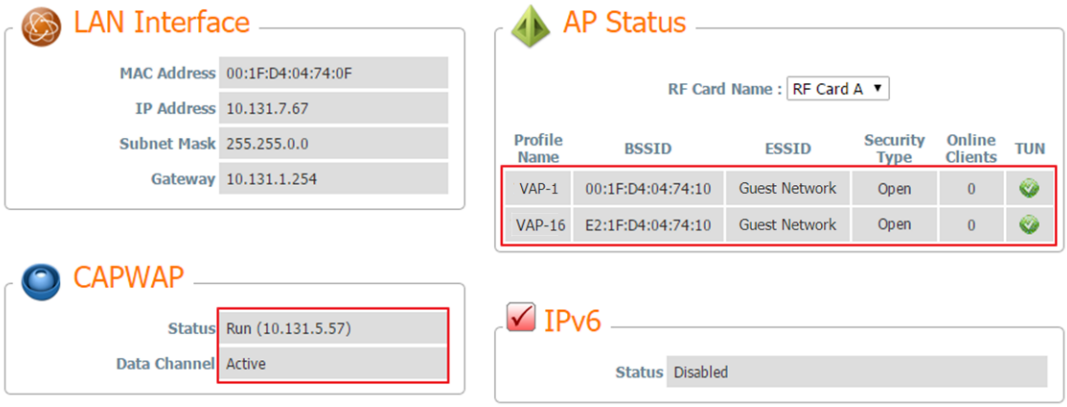


以下の手順が役立つ場合があります。

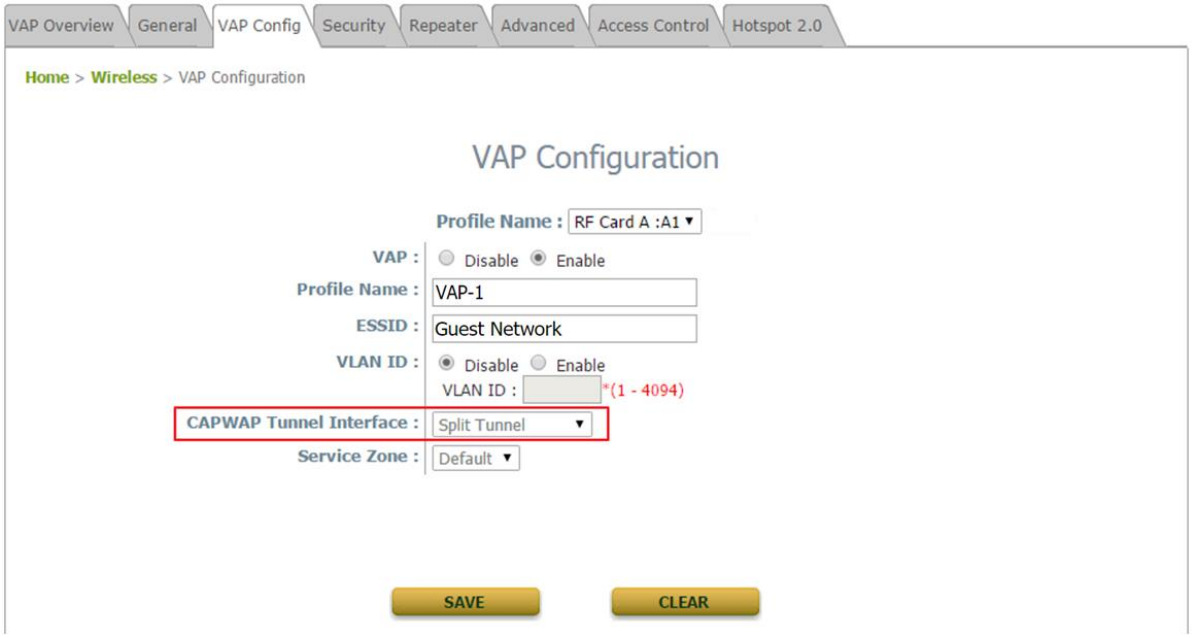
1. On AP: Static Discovery の IP アドレスを入力し、CAPWAP 列に RUN ステータスが表示されるまで待機します。
2. On EWS: CAPWAP Tunnel Interface－Split Tunnel を使用して VAP Configuration のテンプレートを準備します。
3. On EWS: テンプレートを CAPWAP に適用して AP との間のトンネルを確立すると、VAP がコントローラにトンネリングされるように設定されている場合、トンネルステータスにクリック可能な Edit ボタンが黒色で表示されます。



4. On AP: データチャネルを示す AP WMI がアクティブであることを確認するには、System Overview ページの VAP トンネルステータスが緑色ライトであることを確認します。

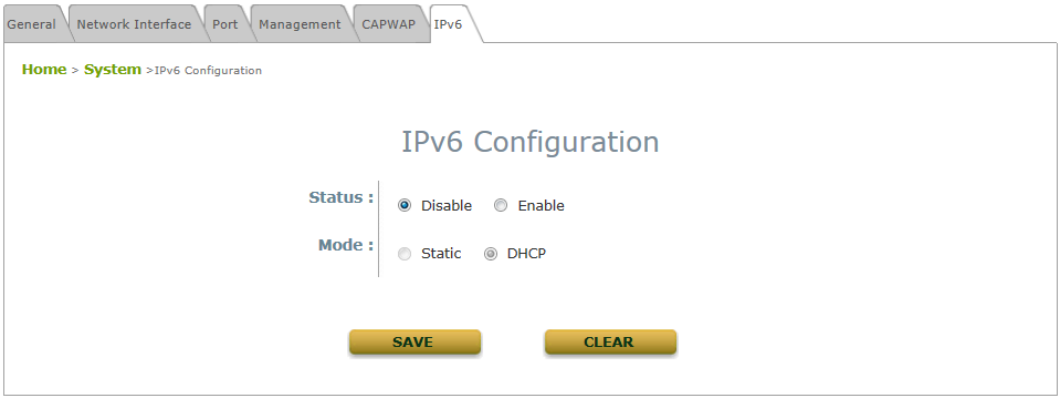


5. On AP: 特定の VAP 構成が Split Tunnel であることを再確認します。



3.7 IPv6

IPv6 および IPv4 のデュアルスタックアドレッシング機能がサポートされています。



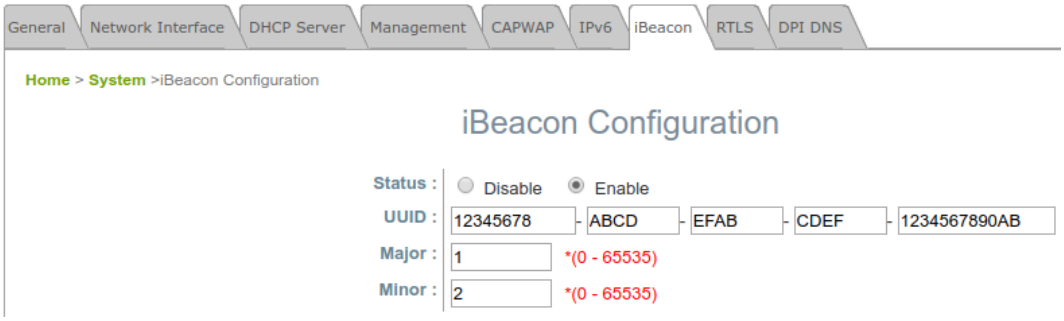
Status: IPv6 はデフォルトで無効になっていますが、このタブページで有効にすることができます。

Mode: この装置の 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**: 動作のために永続的な IPv6 アドレスをすでに取得している場合は、このオプションを使用して IPv6 アドレスを手動で設定します。
- **DHCP**: アップストリームサーバから IPv6 アドレスを自動的に取得します。

3.8 iBeacon

iBeacon は、2013 年にアップル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。正しく設定されると、AP は iBeacon 互換性のハードウェアトランスミッタになり、Bluetooth Low Energy(BLE)を介して近くのデバイスに情報をブロードキャストします。



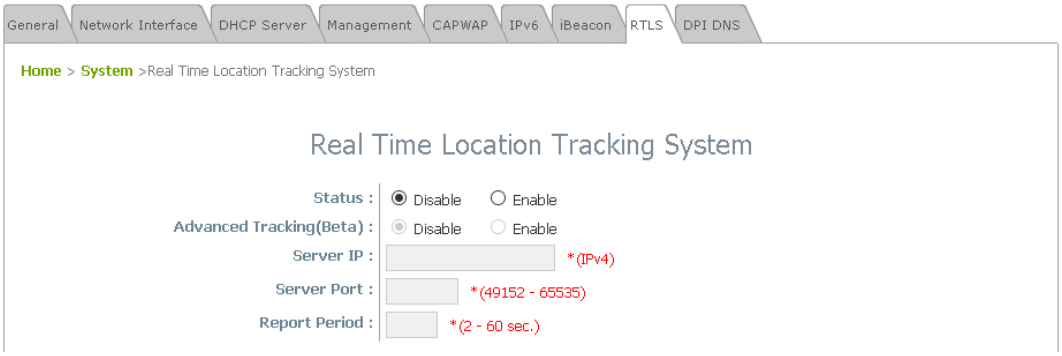
UUID、メジャー、マイナーは、AP によって継続的に送信される iBeacon の Advertising Packets の主要コンポーネントを構成するために使用される識別パラメータです。

UUID: ユニバーサルー意識別子。ネットワーク内の独自の AP と、制御外のネットワーク内の他のすべての iBeacon トランスミッタを区別するための番号です。これには 32 桁の 16 進数が含まれており、5 つのグループに分割されており、次のようになります。12345678-ABCD-EFAB-CDEF-1234567890AB

Major & Minor: AP を UUID 単独で識別するよりも正確に識別するために、独自の AP に割り当てられる数値(0～65535 の整数値)です。通常、メジャー値はグループの識別と区別を目的としていますが、マイナー値は個々の識別と区別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 で配置された iBeacon トランスミッタが多数あり、それらが別のフロア/店舗に配置されているとします。そして、これらの送信機は、異なるメジャー(例えば、1 階の場合は 1)とマイナー(例えば、2 番目の店舗の場合は 2)の値によって識別されます。

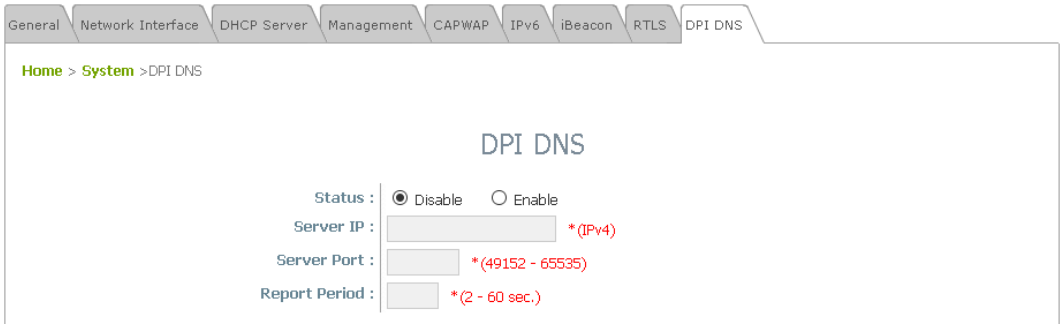
3.9 RTLS

Wi-Fi ベースのロケーションソリューションを実装するために、お客様は、この機能を Real Time Location System (RTLS)の専用 Linkyfi(技術パートナー)サーバと統合することができます。これは、あらゆる種類の設置場所における屋内位置および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である Linkyfi ロケーションエンジンの一部です。



3.10 DPI DNS

Wi-Fi マーケティング分析を実行するために、顧客はこの機能を有効にして、Deep Packet Inspection(DPI)技術を介して DNS トラフィックを分析する Linkyfi ロケーションエンジンの一部である Linkyfi の DNS サーバと AP を統合することができます。

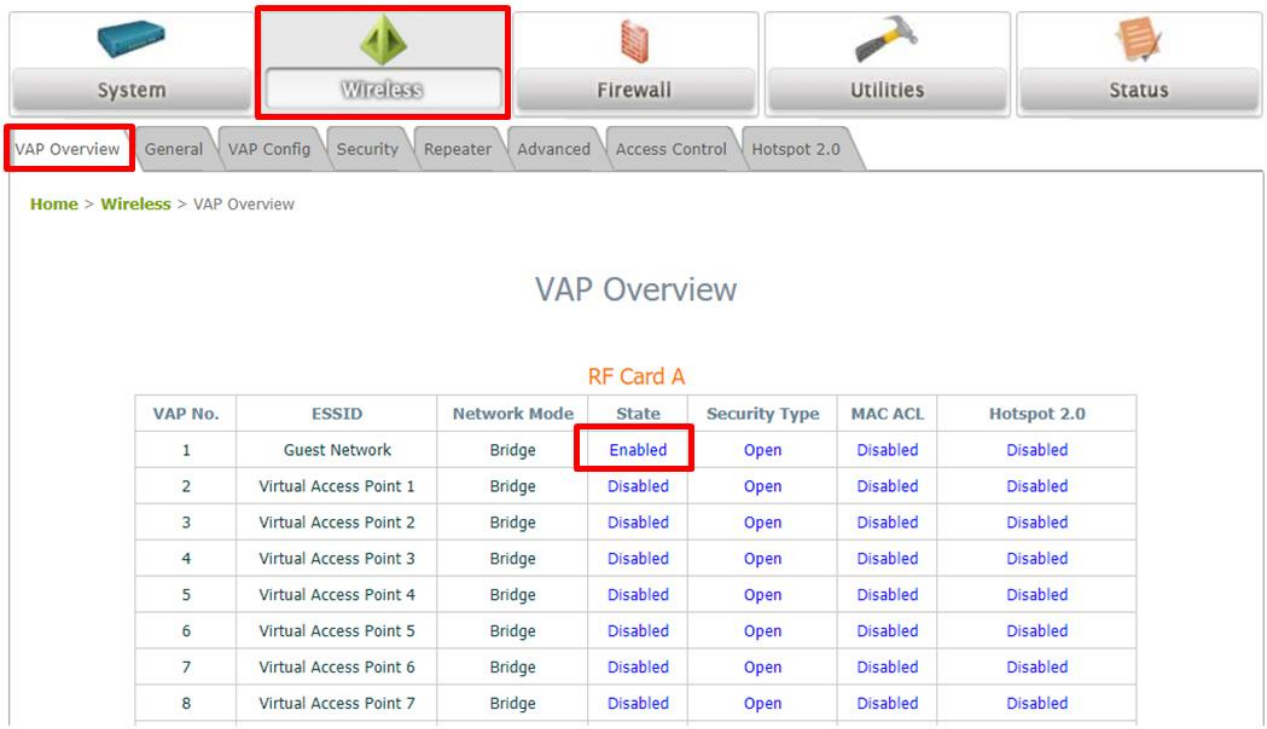


4. Wireless

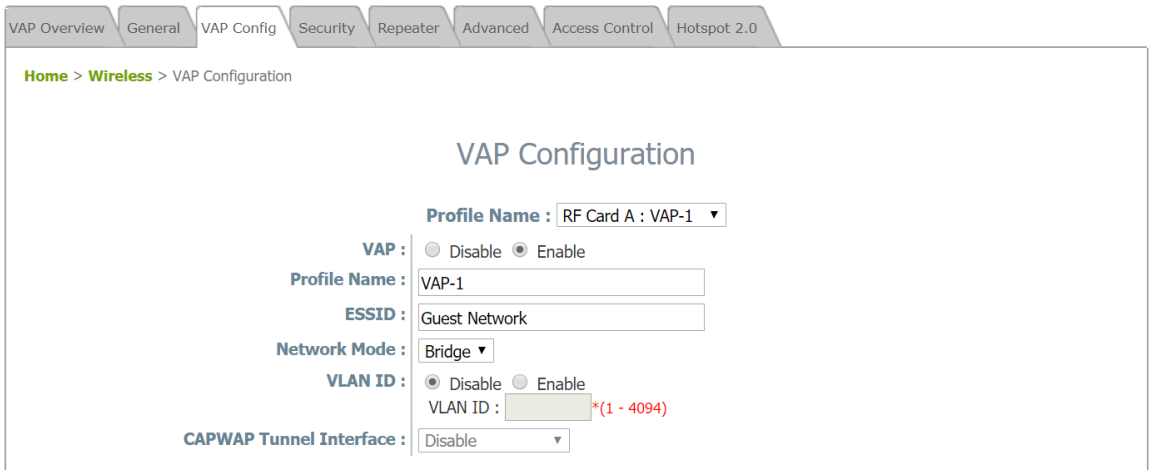
ここでは、VAP Overview、General、VAP Configuration、Security、Repeater、Advanced、Access Control と Hotspot 2.0 の機能について説明します。本アクセスポイントは、RF Card あたり最大 16 個の仮想アクセスポイント(VAP)をサポートします。VAP ごとに独自の設定(ESSID、VLAN ID、セキュリティ設定など)を設定できます。このような VAP 機能を使用すると、ネットワーク要件を満たすように異なるレベルのサービスを設定できます。

4.1 VAP Overview

このページでは、ESSID、Network Mode、State、Security Type、MAC ACL、および Hotspot 2.0 などの全体的な状態が収集されます。これらの AP では、無線ごとに 16 個の VAP が設定されています。この表では、ハイパーリンクをクリックして、個々の VAP をさらに設定してください。

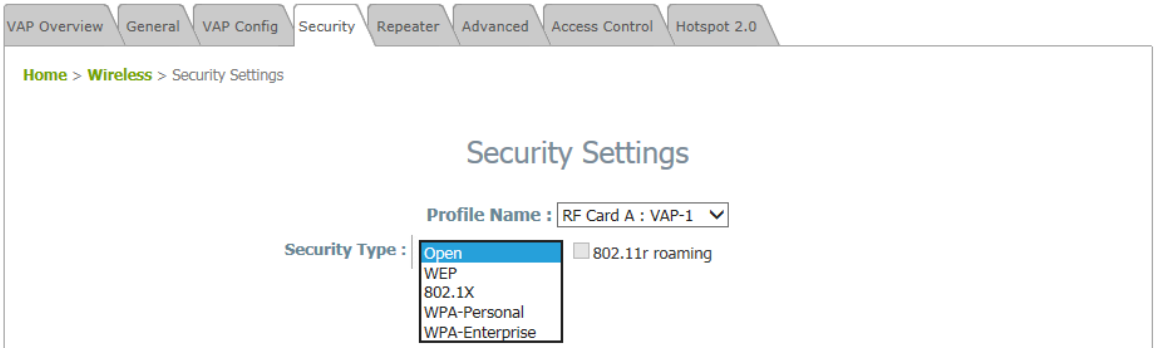


State: Enable または Disable と表示されているハイパーリンクは、VAP Configuration ページへのリンクになっています。



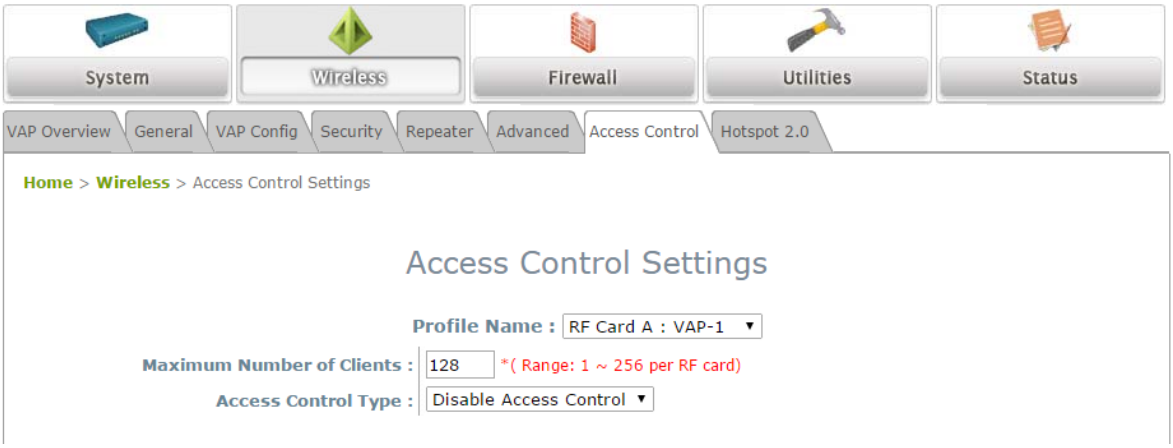
VAP－State ページ

Security Type: Security Type 欄に表示されているハイパーリンクは、Security Settings ページへのリンクになっています。



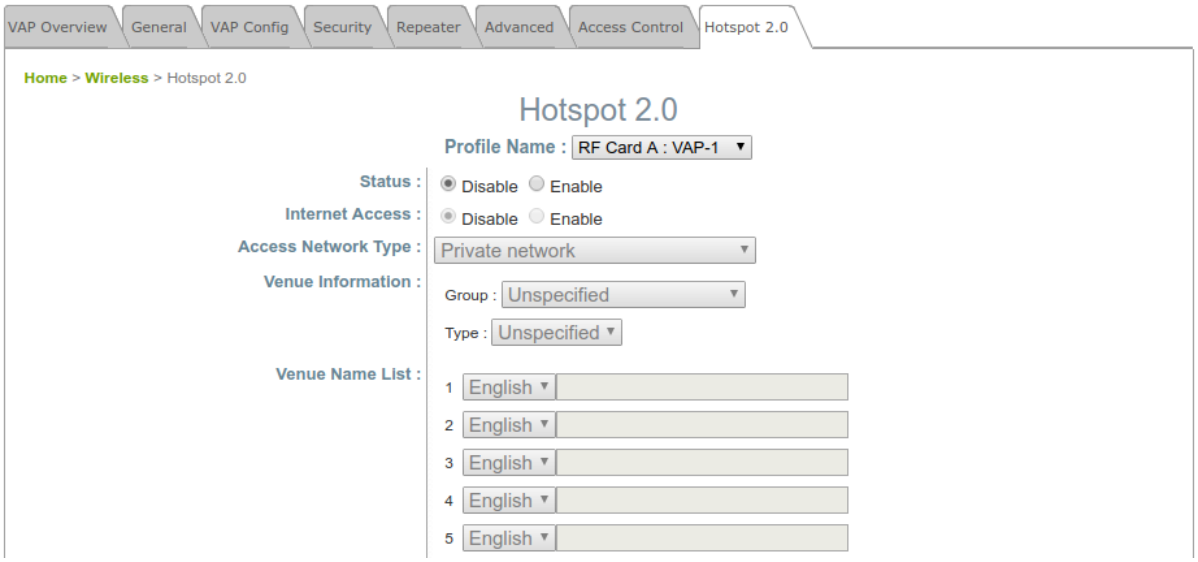
VAP－Security Type ページ

MAC ACL: Allow または Disable と表示されているハイパーリンクは、Access Control Settings ページへのリンクになっています。



VAP－MAC ACL ページ

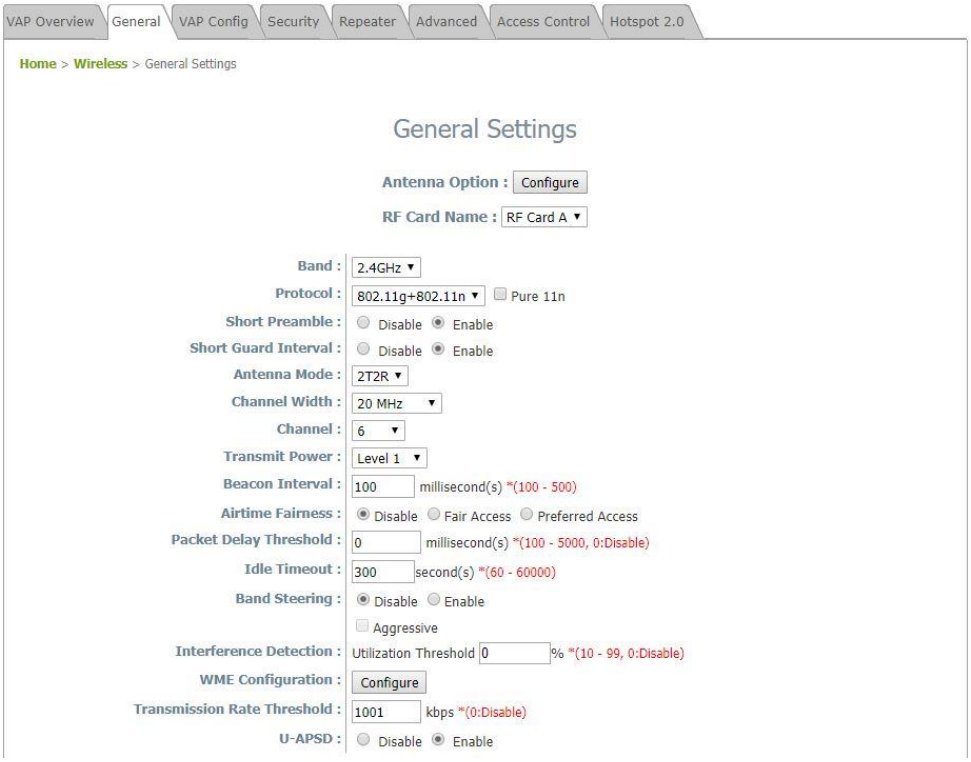
Hotspot 2.0: Hotspot 2.0 欄に表示されているハイパーリンクは、Hotspot 2.0 ページへのリンクになっています。



VAP－Hotspot 2.0 ページ

4.2 General

AP のシステム全般の無線の設定をします。



Antenna Option(OAP100 のみ): 装置は 4 つのアンテナで構成され、2 つは 2.4GHz 用、2 つは 5GHz 用です。サービスごとに 2 つのオプションがあります。

- **Hotspot**: ホットスポットの目的に使用します。2.4GHz では、クライアントにサービスを提供するために使用されるオムニアンテナを採用しています。2 つの 5GHz では、ポイントツーポイント接続に使用される、方位および高度が 30 度の指向性アンテナを採用しています。
- **Point to Point**: ポイントツーポイントの目的に使用します。2 つの 2.4GHz と 2 つの 5GHz には、90 度の方位角と 30 度の高度を持つ指向性アンテナを採用しています。

RF Card Name: さらに設定を行うには、1 つの RF Card を選択します。

Band: 無線機能が不要な場合は Disable を選択します。

Protocol: 適切な無線プロトコル(802.11a、802.11a+802.11n、802.11ac または 802.11b、802.11g、802.11b+802.11g、802.11g+802.11n)を選択します。プロトコルは、RF Card の Band に依存します。

- **Pure 11n**: このチェックボックスをチェックすると、802.11n のみを有効にします。

Short Preamble: 56 ビットの同期フィールドを持つ短いプリアンブルを使用すると、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、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、符号間干渉を排除するために送信されるシンボル(文字)間の空間です。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です。ショートガードインターバルを使用するには Enable を選択し、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。

Antenna Mode: RF Cardの空間ストリームの数を選択します。1つの空間に対して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(帯域が802.11g+802.11n、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に、40MHzまたは80MHzのダブルチャネル帯域幅を使用します。

Channel: ドロップダウンメニューから適切なチャネルを選択して、規則性を満たします。
- RF card B で Auto に設定されている場合、選択されたチャネルが干渉するか、DFS チャネル信号が検出された時に使う、チャネルを切替えるためのセレクタテーブルがあります。
- 屋外 AP モデルの場合、Outdoor mode はチャネル選択に影響します。

Channel Selector: このオプションは、Band が 5GHz に設定され、Channel が Auto または DFS チャネルに設定されている場合に、RF Card B に表示されます。
- システム起動時にチャネルが Auto に設定されている場合、チャネルの空き状況に応じてシステムがチャネルを選択します。
- DFS チャネルでレーダー信号が検出された場合、または干渉しきい値(設定されている場合)に達した場合などの理由により、システムが別のチャネルに切り替えると判断すると、どのチャネルがクリアであるかに基づいて、選択されたチャネルの 1 つにのみ切り替えられます。

Transmit Power: 本機から送信する電波の強さをレベルで選択できます。
- 各レベルは、最大電力から 1dBm 減少することを意味します。
- レベル 1 は実際の最大電力、レベル 2 は最大電力から 1dBm を引いた値、というように続きます。

Distance: WDS で接続されている場合、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への距離を指します。Distance を入力すると、以下の ACK Timeout の値が自動調整されます。

ACK Timeout: 再送なしに局から送り返された肯定応答フレームを待つ時間を示します。言い換えると、本項で設定した時間内に、確認応答フレームがまだ受信されない場合、フレームは再送されます。このオプションを使用して、ネットワークパフォーマンスを調整し、カバレッジを拡張することができます。通常の室内設置の場合は、デフォルト設定を維持してください。

Beacon Interval (ms): 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。
- 7VAP を超える VAP が有効になっている場合、ビーコン間隔は 500 ミリ秒より大き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、ビーコン間隔は 250 ミリ秒より大きくする必要があります。

Airtime Fairness: 802.11a/b/g/n レガシーデバイスがエアタイムを占有する場合、802.11ac デバイスのスループットは影響を受けます。
- **Enable**: 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します。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。
- **Preferred Access**: N バンド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): アクセスポイントは、ビジー状態のクライアントまたは通信圏外のクライアントにパケットを送信しようとするため、接続されている他のクライアントへの送信を遅延させる可能性があります。有効にすると、この送信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、すぐに他のパケットの処理を開始します(デフォルト=0(無効))。この機能は複雑な無線ネットワークのパフォーマンスを向上させますが、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): 非アクティブが設定された秒数(デフォルト=300)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 帯域の輻輳を低減します。これは、AP が 2 つの RF Card 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**: 5GHz 接続があるクライアントは、5GHz 帯に強制的に接続されます。
- これはアクセスポイントの一般的な設定であり、RF Card ごとに設定されないことに注意してください。

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(および不正なパケットレート)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。

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

Transmission Rate Threshold: 伝送速度が設定したしきい値を下回ると、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。

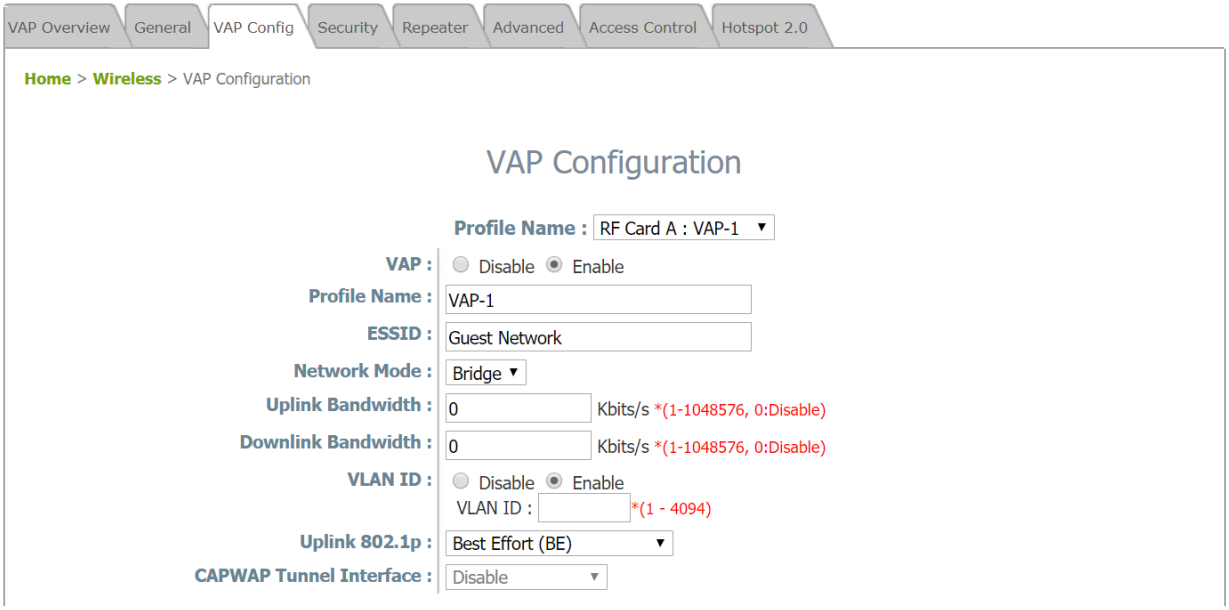
CCA Minimum Power: Clear Channel Assessment(CCA)は、無線周波数が使用されているかどうかを確認する方法です。CCA Minimum Power は、システムが解決可能とみなす最小信号強度です。つまり、電力レベルが CCA Minimum Power より低い場合、受信信号はノイズとして扱われます。

U-APSD: 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ない)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。

NOTE: Short Preamble、ACK Timeout などの機能は、RF Card B で制限される場合があります。

4.3 VAP Config

ここでは、Profile Name、ESSID、VLAN ID などの設定を使用した仮想アクセスポイントの設定について説明します。特定の VAP を有効にするには、Profile Name のドロップダウンリストから VAP を選択します。

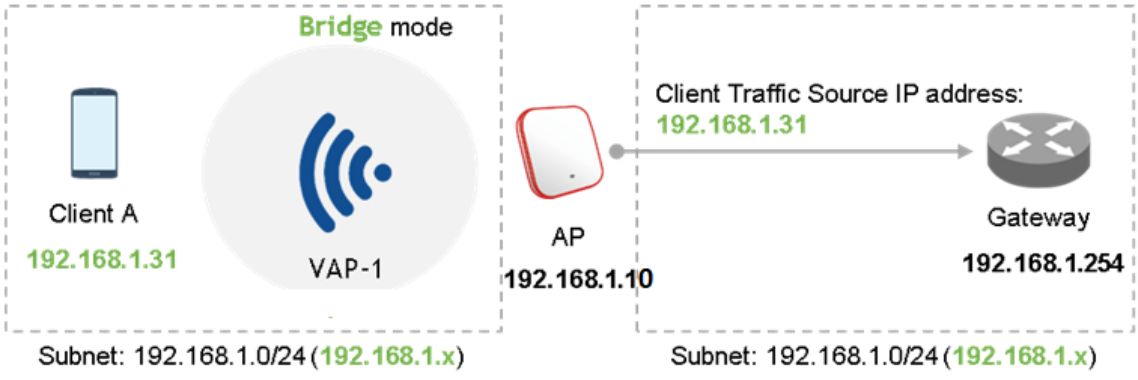


VAP: この VAP を無効または有効にします。

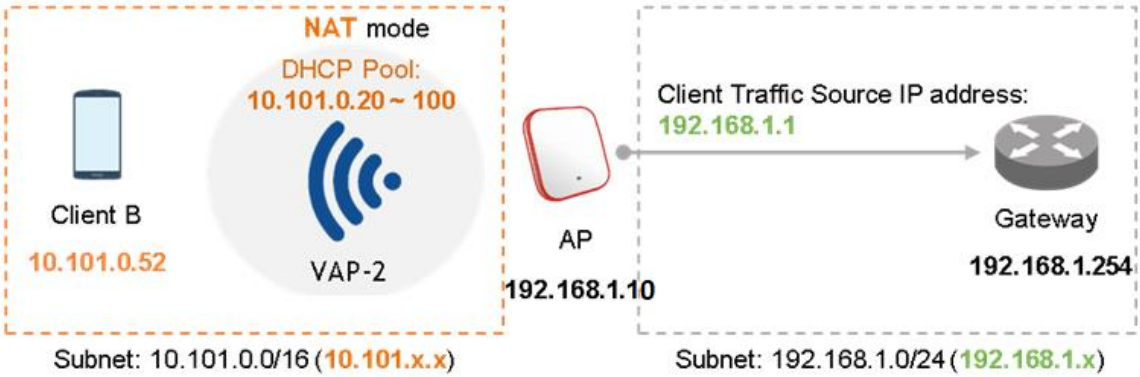
Profile Name: ID/管理を目的とした VAP プロファイルの名前。

ESSID: Extended Service Set Identifier (ESSID)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。

Network Mode－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/スイッチで確認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(この例では、下図に示すように 192.168.1.31)。



Network Mode－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 に設定された 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/スイッチで確認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(この例では、下図に示すように 192.168.1.10)。



Uplink/Downlink Bandwidth: 帯域幅制御は、Kbps で VAP 上で構成可能です。帯域幅を無制限に制御するには、0 を設定します。

VLAN ID: SSID ごとの VLAN タグ付け機能－有効にすると、この SSID を介して AP に入るクライアントのトラフィックに、設定された VLAN ID がタグ付けされます。

Uplink 802.1P per VAP: ここでは、アップリンクトラフィックの優先順位レベルを選択できます。利用可能なオプションは、背景、ベストエフォート、エクセレントエフォート、クリティカルアプリケーション、映像、音声、ネットワーク間制御、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(NAT モード): 内蔵 DHCP サーバプロファイル。DHCP サーバの IP 設定は Home>System>DHCP Server で確認可能です。

CAPWAP Tunnel Interface: AP がコントローラによって管理されている場合、AP とコントローラ間の接続を示す 3 つの状態は次の通りです。

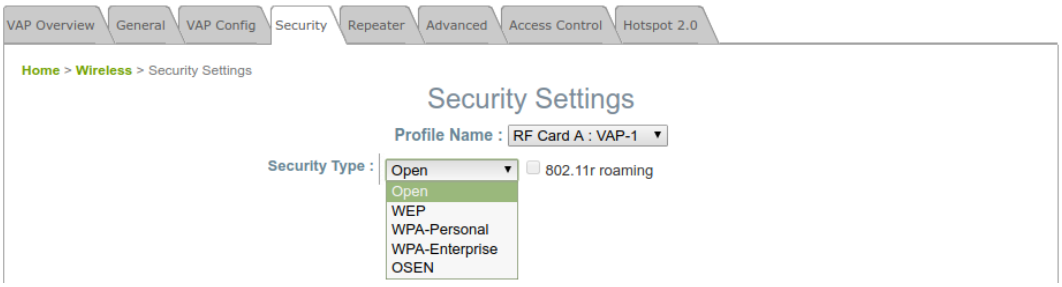
- **Disable(トンネルなし)**: AP は、コントローラへの CAPWAP トンネル接続なしで動作しています。
- **Split Tunnel**: AP は CAPWAP トンネルを介してコントローラに control トラフィックのみを渡します。つまり、data トラフィックはトンネルを通過せずにローカルに送信されます。
- **Complete Tunnel**: AP は、CAPWAP トンネルを介してコントローラに control トラフィックと data トラフィックの両方を渡します。

NOTE:

- VLAN ID は、VAP が Bridge モードにある場合にのみサポートされます。
- DHCP プロファイルおよび DHCP サーバは、VAP が NAT モードに設定されている場合にのみ有効になります。
- VAP が NAT モードの場合、CAPWAP トンネルインタフェースは Disable(トンネルなし)または Split Tunnel の 2 つの状態でのみ機能します。

4.4 Security

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異なるサービスレベルを提供できます。セキュリティタイプには、Open、WEP、WPA-Personal、WPA-Enterprise、および OSEN が含まれます。



Open: 認証は不要で、送信中に暗号化されません。

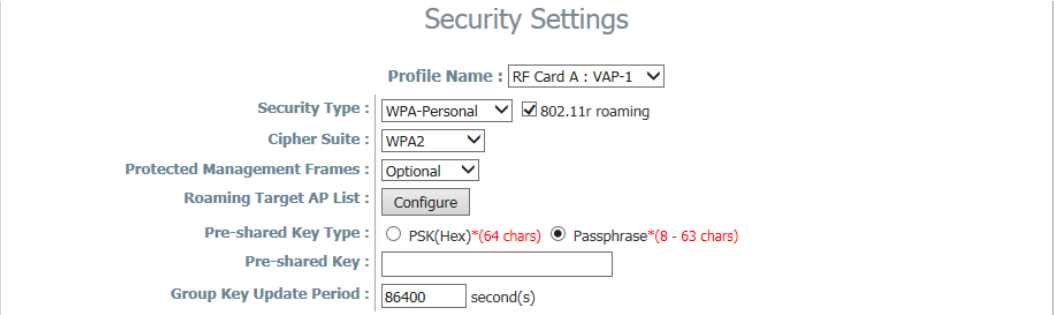
WEP: Wired Equivalent Privacy は、64 ビット、128 ビット、または 152 ビットの共有キーアルゴリズムに基づくデータ暗号化メカニズムです。

- **802.11 Authentication**: Open System、Shared Key、Auto から選択します。
- **WEP Key Length**: 64 ビット、128 ビット、または 152 ビットからキー長を選択します。
- **WEP Key Format**: ASCII または Hex から WEP キーフォーマットを選択します。
- **WEP Key Index**: 1～4 からキーインデックスを選択します。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**: 事前定義された WEP キー値を指定します。最大 4 セットの WEP キーがサポートされます。

NOTE: 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。

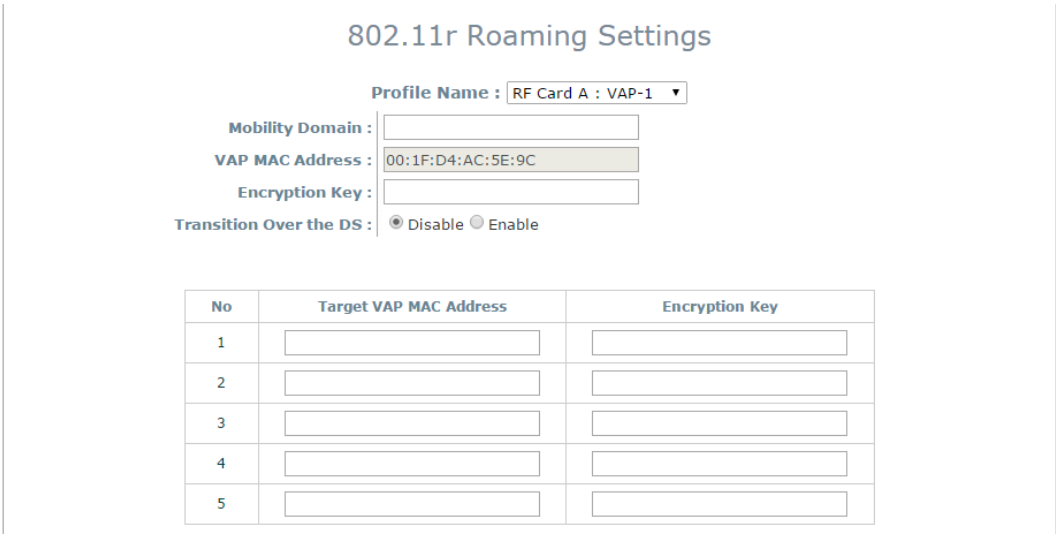
WPA-Personal: WPA-Personal は事前共有キー(PSK)認証方法です。

- **802.11r Roaming**: ローミングは、同じ暗号化キーを持つ別の AP 上の同じモビリティドメイン内のクライアントに対して実行できます。



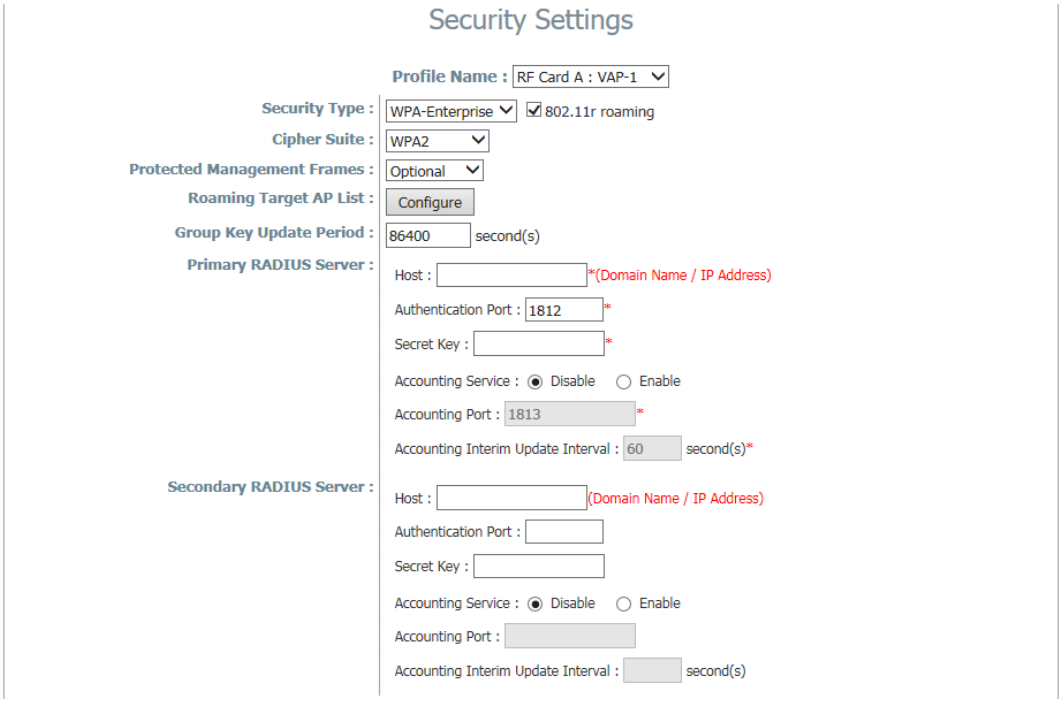
Security Settings: WPA-Personal

- **Cipher Suite**: WPA2 または WPA2/WPA から暗号化方式を選択します。
- **Protected Management Frames**: Disable、Optional、または Mandatory を選択します。
- **Roaming Target AP List**(802.11r が有効な場合)



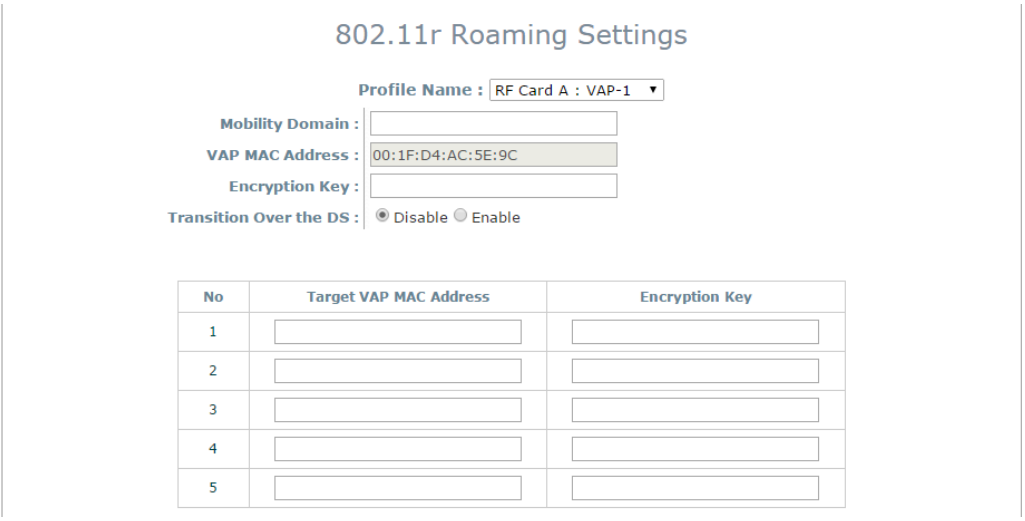
- **Pre-shared Key Type**: 事前共有キーの種類(PSK(Hex)またはパスフレーズ)を選択します。
- **Pre-shared Key**: 事前共有キーのキー値を入力します。キー値のフォーマットは、選択したキーの種類によって異なります。
- **Group Key Update Period**: グループキーを更新する時間間隔。時間単位は秒です。

WPA-Enterprise: 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: WPA-Enterprise

- **Cipher Suite**: WPA2 または WPA2/WPA から暗号化方式を選択します。
- **Protected Management Frames**: Disable、Optional、または Mandatory を選択します。
- **Roaming Target AP List**(802.11r が有効な場合)



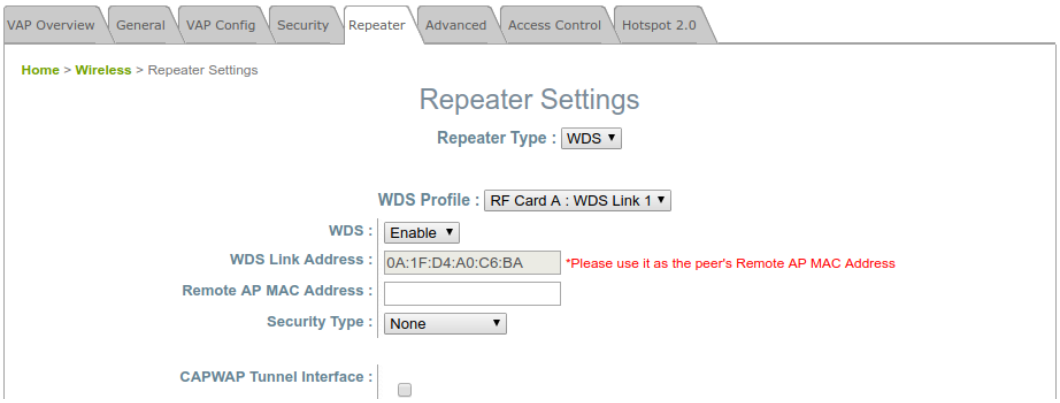
- **Group Key Update Period**: グループキーを更新する時間間隔。時間単位は秒です。
- **RADIUS Server Settings (Primary/Secondary)**:
  - **Host**: RADIUS サーバの IP アドレスまたはドメイン名を入力します。
  - **Authentication Port**: RADIUS サーバで使用されるポート番号。ポート番号を指定するか、デフォルト 1812 を使用します。
  - **Secret Key**: RADIUS サーバと通信するための秘密鍵。
  - **Accounting Service**: このオプションを有効にすると、RADIUS サーバを介したログインとログアウトのアカウンティングが可能になります。
  - **Accounting Port**: RADIUS サーバ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 1813 を使用します。

- **Accounting Interim Update Interval**: アカウンティング情報は、インターバルごとに RADIUS サーバにアップデートされます。

OSEN: OSEN は The Online Signup(OSU) Server-only authenticated layer 2 Encryption Network の意味で、"Hotspot 2.0 Release2"(HS2.0 R2)の認証方法です。HS2.0 R2 を設定する前に、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。詳細な設定は、「session 4.8 Hotspot 2.0」を確認してください。

4.5 Repeater

AP は WDS を使用して無線 LAN ネットワークの範囲を広げることができます。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 をクリックして続行します。



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: 選択した WDS リンクの AP インタフェースの MAC アドレス。

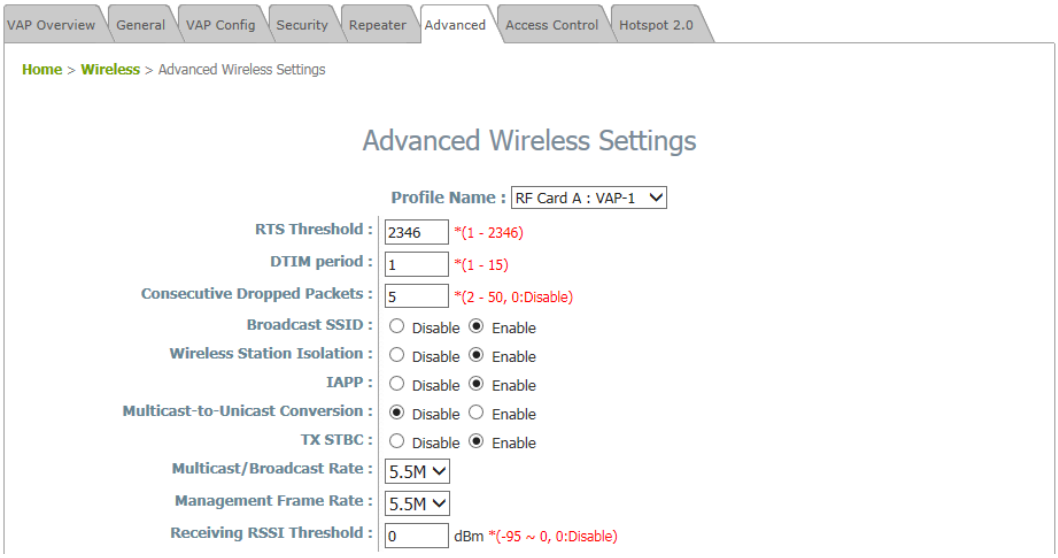
Remote AP MAC Address: リモートピアの MAC アドレス。

Security Type: None、WEP、または WPA-Personal。

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 WDS トラフィックを指定するには、このオプションをオンにします。

4.6 Advanced

管理者は、接続不良が発生した場合にネットワーク通信のパフォーマンスを向上させるために、次のパラメータを調整できます。



RTS Threshold: 1～2346 の値を入力します。RTS(送信要求)しきい値では、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 に接続している領域、またはクライアントが遠く離れていてこの AP だけを検出できたが相互には検出できてい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。フラグメントしきい値(Fragment 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、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: 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。

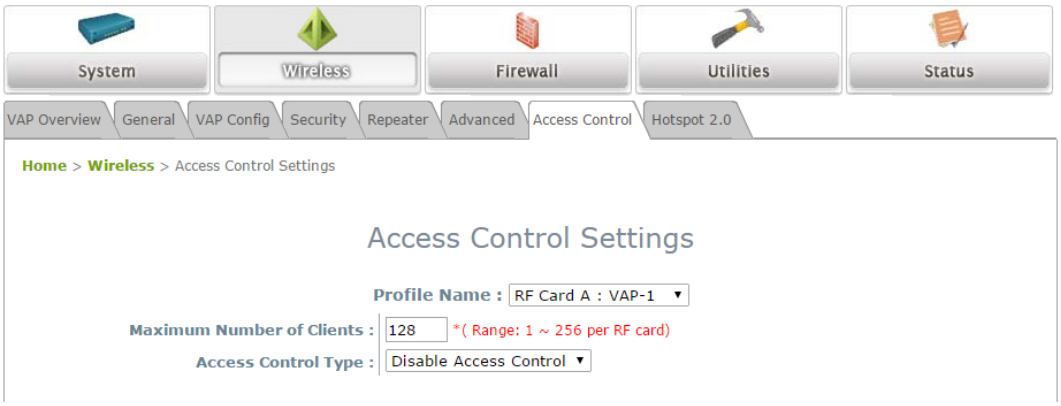
Management Frame Rate: この機能は、マネジメントフレームの帯域幅を制御します。

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。

NOTE: TX STBC は、選択した AP モデルに制限される場合があります。

4.7 Access Control

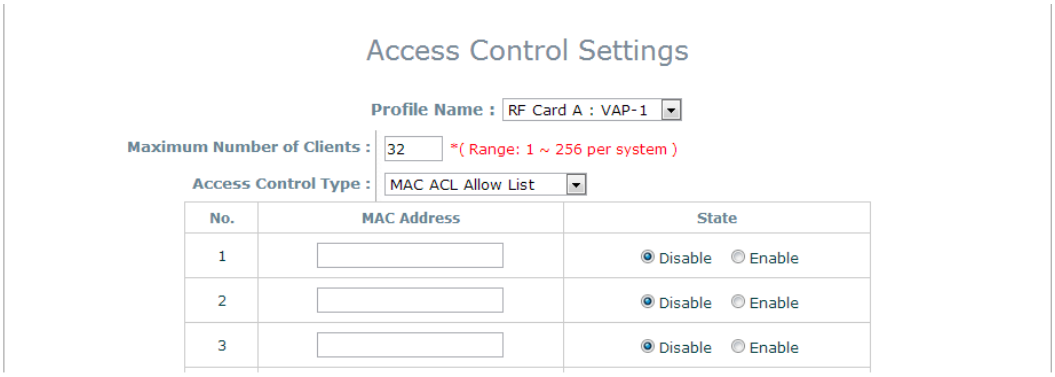
このページで、ネットワーク管理者は、アクセスポイントに接続されたクライアントの総数を制限することができ、また、デバイスにアクセスすることができる、またはアクセスすることができない特定の MAC アドレスを指定することができます。



Maximum Number of Clients: デフォルトポリシーは、認証なしで無制限にアクセスできます。無線接続の局数を制限するには、値を目的の番号に変更します。たとえば、ステーション数を 20 に設定した場合、指定した VAP への接続は 20 局のみ許可されます。

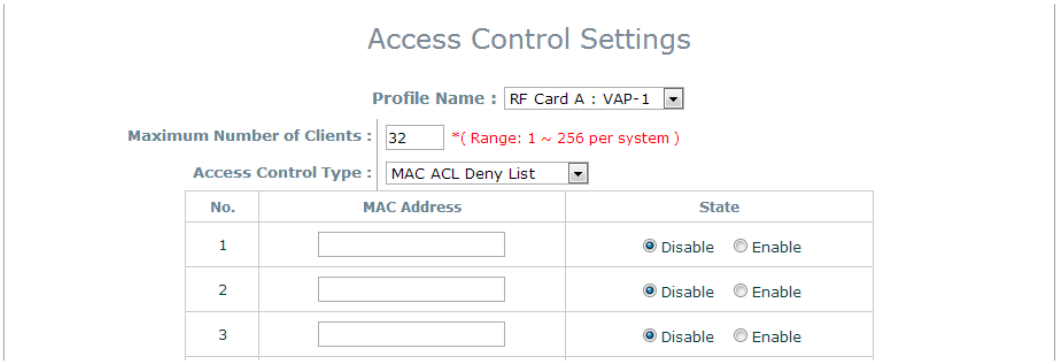
Access Control Type－Disable Access Control: 無効を選択した場合、クライアント装置からのアクセスは制限されません。

Access Control Type－MAC ACL Allow List: MAC ACL Allow List を選択した場合、許可リスト(許可された MAC アドレス)にリストされているクライアント装置(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許可された MAC アドレスを一時的にブロックできます。

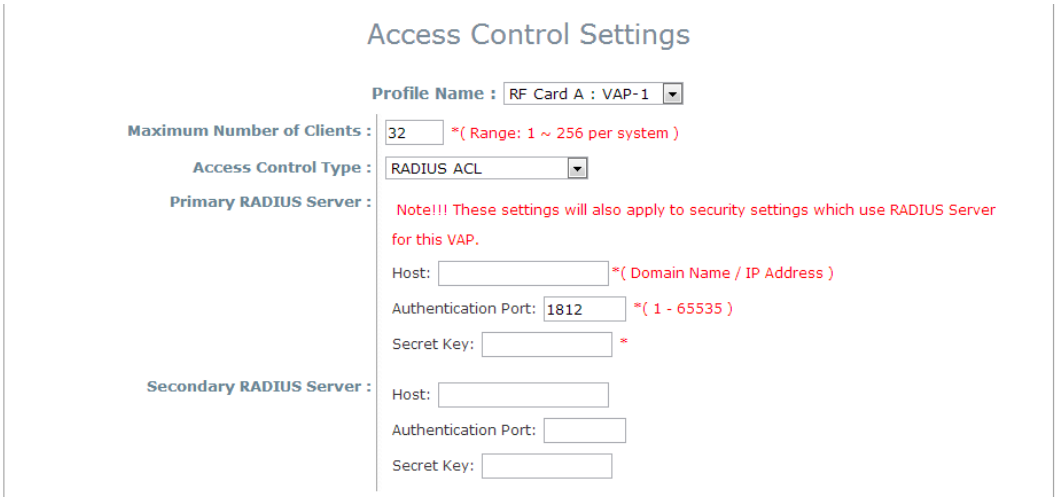


NOTE: 空の許可リストは、許可された MAC アドレスがないことを意味します。少なくとも管理システムの MAC が含まれていることを確認します(ネットワーク管理者のコンピュータなど)。

Access Control Type－MAC ACL Deny List: MAC ACL Deny List を選択すると、拒否リスト(拒否された 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が許可されます。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。

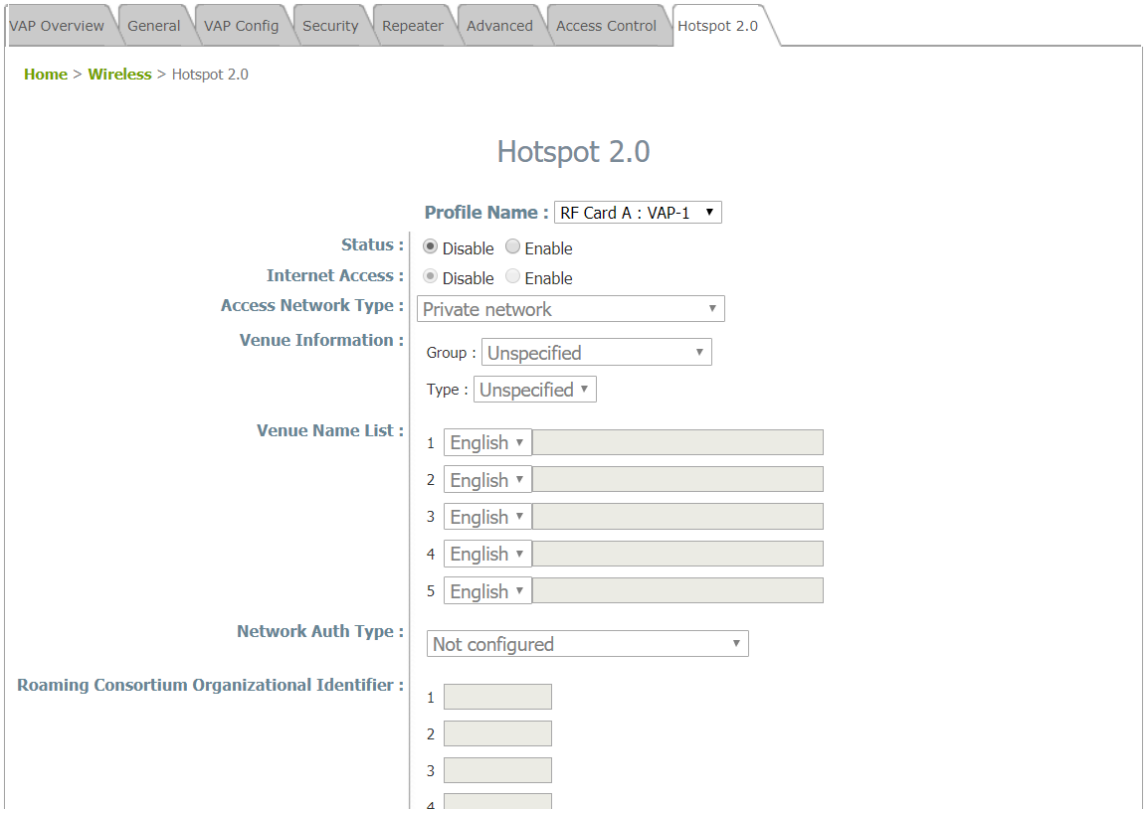


Access Control Type－RADIUS ACL: 外部 RADIUS で受信 MAC アドレスを認証します。RADIUS ACL を選択すると、すべての受信 MAC アドレスが外部 RADIUS によって認証されます。各 VAP の MAC ACL とそのセキュリティタイプ(Security Settings ページに表示)は、同じ RADIUS 構成を共有していることに注意してください。



4.8 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 アライアンスによって開始された Wi-Fi 認定パスポイントとしても知られています。



Status: Hotspot 2.0 を有効化または無効化します。

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

Access Network Type

- **Private**: ホームネットワークと企業ネットワーク。
- **Private and Guest Access**: ゲスト接続を提供するエンタープライズ。
- **Chargeable Public Network**: 有料を除くすべてのユーザが利用できます。
- **Free Public Network**: 料金無料で利用できます。
- **Personal Device Network**: アドホックモードの周辺装置のための設定。
- **Emergency Services**
- **Test/Experimental/Wild Card**

Venue Information: 設置場所のグループ/タイプがここで選択されます。これにより、設置場所の一般的なクラスと、各グループ内の設置場所の特定のタイプが識別されます。

Venue Name List: エンドユーザがネットワークを選択するために役立つネットワーク設置場所の名前。

Network Authentication Type: 安全でないネットワークへのアクセス権を取得するための追加手順。

- **Acceptance of terms and conditions**
- **Online enrollment supported**: ユーザアカウンティングが必要な場合があります。
- **HTTP/HTTPS redirection**: ブラウザがリダイレクトされる URL が示されます。
- **DNS redirection**: Hotspot 2.0 仕様では、ネットワークオペレータが DNSSEC と相互運用できないプロトコルをサポートすることは禁止されています。キャプティブポータルの DNS リダイレクトは、この要件に違反します。

Roaming Consortium Organizational Identifier: ローミングコンソーシアムは、ユーザの資格情報を認証に使用できるサービスプロバイダ(SP)のグループです。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 ID(OI)によって識別されます。OI の長さは多くの場合 24 ビットですが、36 ビット(OUI-36)でもかまいません。

IP Address Type: IPv4 または IPv6。

NAI Realm List: NAI レルムは、ユーザの認証交換に適した認証サーバ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により、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を行うことができます。

- **EAP Type**: NAI レルムリストには、各レルムでサポートされる拡張認証プロトコル(EAP)タイプと、その EAP タイプの認証パラメータをオプションで指定することもできます。

Domain Name List: AP を操作するエンティティの 1 つ以上のドメイン名を一覧表示します。これは、ネットワークのオペレータを識別するため、Hotspot 2.0 ネットワーク選択ポリシーにとって重要です。これは、モバイルデバイスが自宅からのアクセスか、ホットスポットにアクセスしたかを示します。

Cellular Network Information List(PLMN): AP を介して利用可能な 3GPP セルラーネットワークを識別します。具体的には、このフィールドは、移動体通信事業者の移動国コード(MCC)および移動体ネットワークコード(MNC)から成る公衆地上移動体ネットワーク(PLMN)ID を識別します。

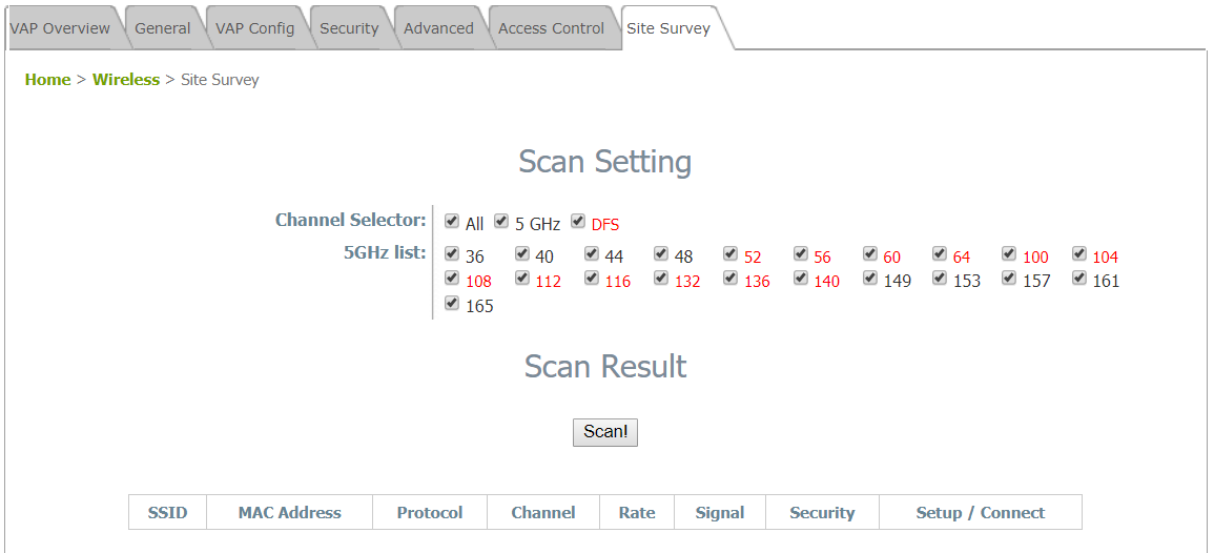
Hotspot 2.0 R2(Hotspot 2.0 Release 2): Hotspot 2.0 Release 1 よりも改善されました。

- **OSU SSID**: OSEN VAP の SSID 名称。
- **OSU Server URI**: OSU サーバの URI。
- **OSU Friendly Name**: OSU サーバ証明書から取得した名前と完全に一致する、人間の言語での OSU プロバイダの名前。現在は英語のみをサポートしています。
- **OSU NAI**: OSU への認証(OSEN 用に設定されている場合)。
- **OSU Service Description**: OSU の説明。現在は英語のみをサポートしています。

4.9 Site Survey(CPE モードのみ)

システムは、周辺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。

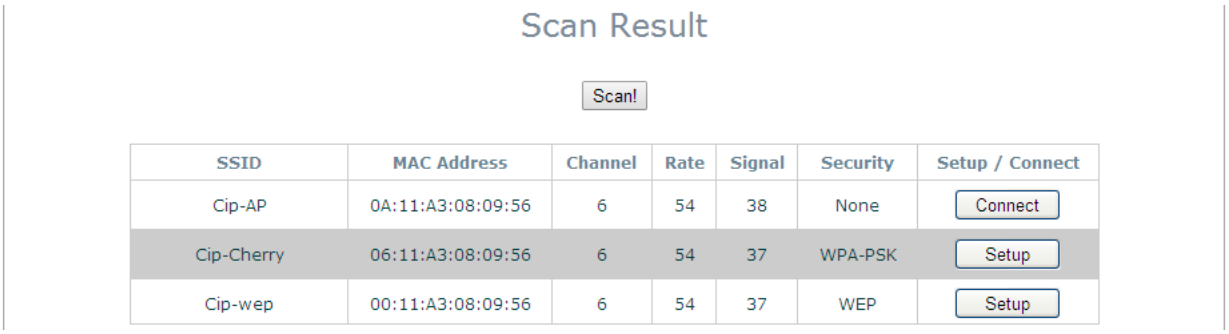
サイトサーベイは、利用可能な AP をそれぞれの SSID、MAC アドレス、チャネル、レート設定、信号読み取り、およびセキュリティの種類とともに表示することで、周囲の無線環境に関する情報を提供するのに役立ちます。管理者は、Setup または Connect をクリックして、前述の指示に従って無線接続を設定できます。



Channel Selector: スキャンするチャネルタイプを選択します。

5GHz list: スキャンするチャネルを選択します。

Scan Result: チャネルセレクターと 5GHz の一覧を選択し、Scan! をクリックすると、スキャン結果が下図のようになります。



Setup/Connect:

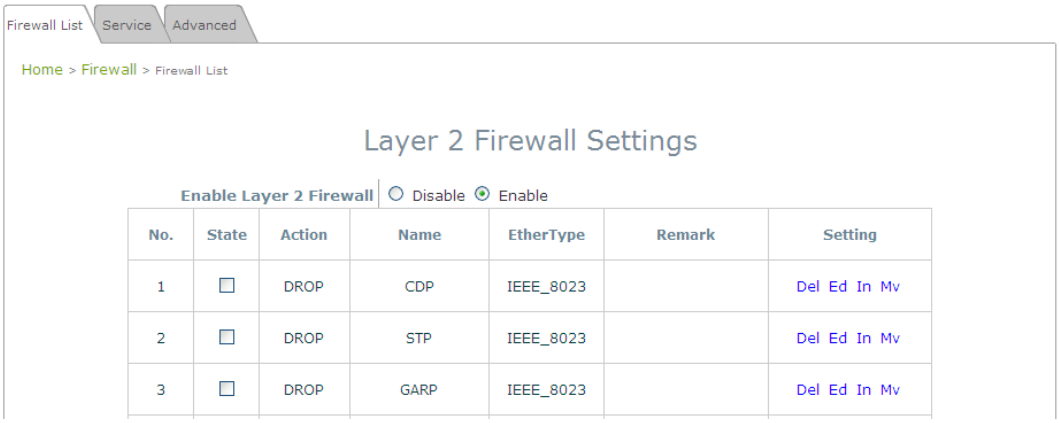
- **Connect**: Connect をクリックして、それぞれの AP を直接関連付けます。これ以上の構成は必要ありません。
- **Setup**: Setup をクリックすると、それぞれの AP に関連付けるセキュリティ設定を行うことができます。

5. Firewall

一般的な AP セキュリティに加えて、レイヤ 2 ファイアウォールというシステムのセキュリティ機能が提供されます。レイヤ 2 ファイアウォールは、レイヤ 2 トラフィック専用にカスタマイズされたファイアウォール機能を提供し、WLAN(AP インタフェース)から送受信される可能性のあるセキュリティ脅威に対する別のシールドを提供します。したがって、ゲートウェイに設定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、セキュリティ侵害の可能性を軽減するのに役立ちます。ここでは、Firewall Lists、Service および Advanced Firewall Settings の機能について説明します。

5.1 Firewall List

システム内のファイアウォールルールの概要を示します。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。



各ルールは、概要テーブルから次のフィールドで指定されます。

No.: この番号によって、テーブルで利用可能なファイアウォールルールを実行する優先順位が決まります。

State: チェックマークを付けると、それぞれのルールが有効になります。

Action: DROP はブロックルールを示し、ACCEPT はパスルールを示します。

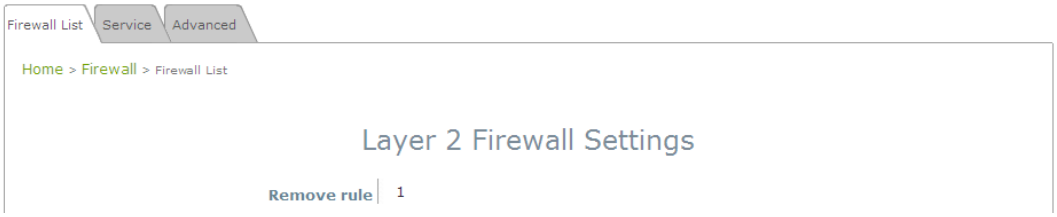
Name: ルールの名前が表示されます。

EtherType: 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: このルールの備考を表示します。

Setting: 4 つのアクションがあります。Del はルールの削除、Ed はルールの編集、In はルールを挿入、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には、
ファイアウォールリストの Setting 列で Del をクリックすると、削除を確認するための次のページが表示されます。
SAVE をクリックし、システムを再起動すると、ルールが削除されます。



特定のルールを編集するには、
ファイアウォールリストの Setting 列で Ed をクリックすると、詳細設定のための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することも、既存のルールからリビジョンを編集することもできます。以下のフィールドが表示されます。

Rule ID: 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: ルール名称を指定します。。

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

Interface: 目的のインタフェースのインバウンド/アウトバウンドの方向を示します。

Service(EtherType が IPv4 の場合): ドロップダウンリストから利用可能な上位レイヤプロトコル/サービスを選択します。

DSAP/SSAP(EtherType 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(EtherType が IEEE 802.3 の場合): カプセル化されたトラフィックの種類を示すために使用します。

VLAN ID(EtherType 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(EtherType が 802.1 Q の場合): 関連付けられた VLAN トラフィックの優先順位レベルを示します。

Encapsulated Type(EtherType が 802.1 Q 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。

Opcode(EtherType が ARP/RARP の場合): ARP ヘッダーの ARP オペコードを指定します。

Source: MAC アドレス/マスクは送信元 MAC を示し、IP アドレス/マスクは送信元 IP アドレスを示し(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 を示し、IP アドレス/マスクは宛先 IP アドレスを示し(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。

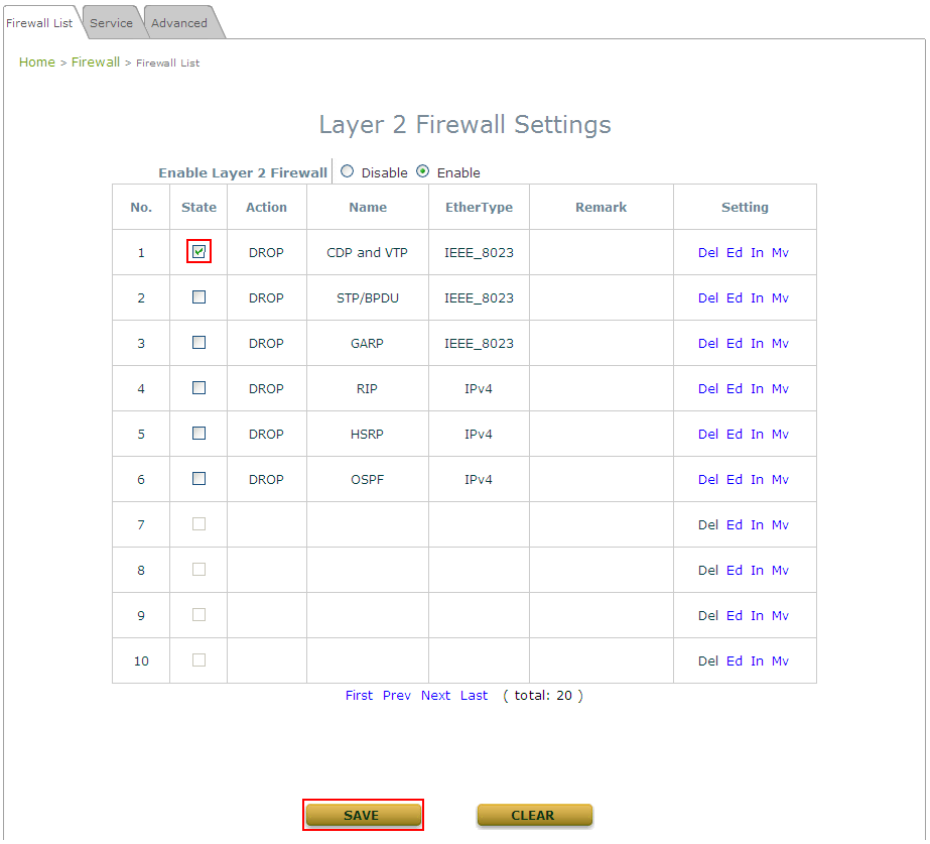
Remark: このルールの備考を指定します。

ファイアウォールルールの設定が完了したら、SAVE and Reboot system をクリックして、ファイアウォールルールを有効にします。

特定のルールを挿入するには、
ファイアウォールリストの Setting 列の 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 を持つ詳細設定のページが表示されます。

特定のルールを移動するには、
ファイアウォールリストの Setting 列の Mv をクリックすると、確認の順序を変更するための次のページが表示されます。SAVE をクリックすると、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)がチェックされ、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

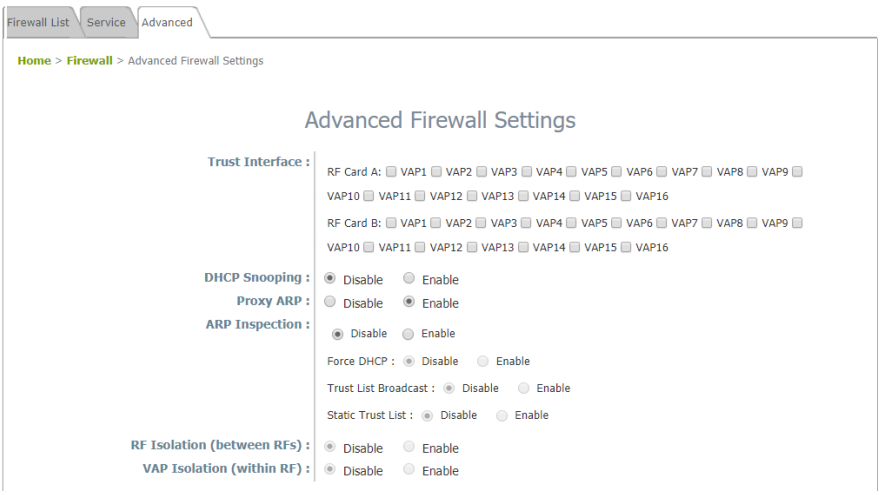
管理者は、ここでファイアウォールサービスを追加または削除できます。このリストのサービスは、ファイアウォールルール(EtherType が IPv4 の場合)で選択オプションになります。

アクセスポイントは、レイヤ 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のリストを提供します。これらのサービスは、Ether Type IPv4 のレイヤ 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サービスで、管理者は必要なサービスを追加/削除できます。

デフォルト設定には 28 のファイアウォールサービスがあります。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。変更が行われた場合は、SAVE をクリックして設定を保存してからこのページを終了してください。

5.3 Advanced

Firewall>Advanced では、ファイアウォールルールの詳細設定を行うことができます。これにより、利用可能なインタフェースを通過する DHCP および ARP トラフィックに対する追加のセキュリティ拡張が可能になります。



Trust Interface: 各 VAP インタフェースを個別にチェックして、信頼されたインタフェースとしてマークできます。DHCP snooping 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フェースで実行されるようにすることができます。

DHCP Snooping: 有効にすると、DHCP パケットは DHCP 資源枯渇攻撃などの潜在的な脅威に対して検証されます。さらに、信頼できる DHCP サーバ(IP/MAC)を指定して、不正な DHCP サーバを防止できます。

ARP Inspection: 有効にすると、ARP パケットは ARP スプーフィングに対して検証されます。

- **Proxy ARP** オプションを有効にすると、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。
- **Force 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。スタティック IP アドレスが設定されたデバイスは DHCP トラフィックを送信しないため、スタティック IP アドレスを持つクライアントは、その MAC/IP ペアが Static Trust List にリストされ、有効になっていない限り、インターネットアクセスからブロックされます。
- **Trust List Broadcast** を有効にすると、他の AP(L2 ファイアウォール機能付き)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なります。
- **Static Trust List** を使用して、ARP 要求を発行するために信頼されている機器の 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 ARP 要求を送信できますが、IP がスタティックリスト(別の MAC)に表示されている場合は、盗聴を防ぐために ARP 要求が破棄されます。

RF Isolation(RF 間): クライアントは RF Card A と RF Card B の間で隔離されます。

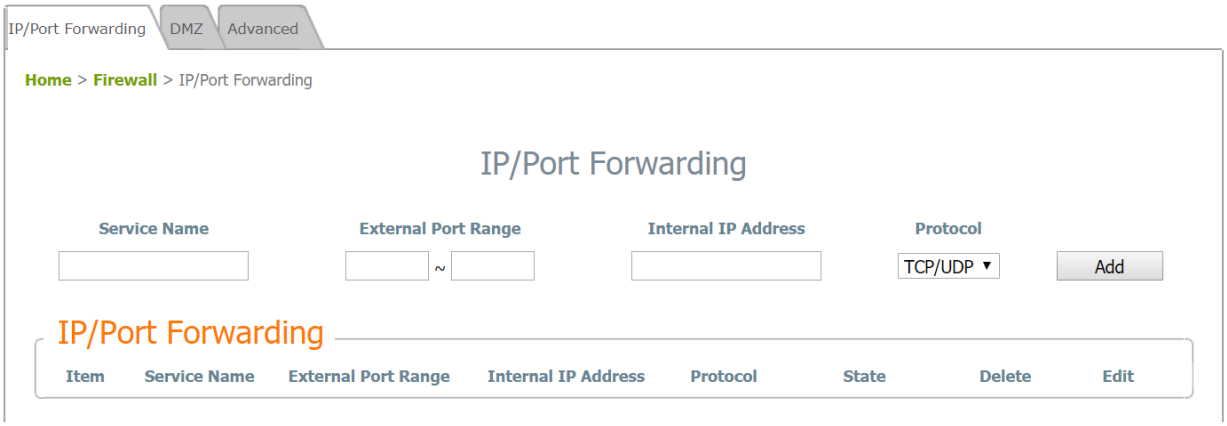
VAP Isolation(RF 内): 同じ RF Card 上の異なる VAP 上のクライアントは隔離されます。

設定が変更された場合は、SAVE をクリックして設定を保存してからこのページを終了してください。

NOTE:
- RF の隔離(RF 間)は、選択した AP モデルで制限される場合があります。
- VAP の分離(RF 内)は、選択した AP モデルで制限される場合があります。

5.4 IP/Port Forwarding(CPE モードのみ)

このページのオンラインゲームやテレビ会議のような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占有されていないことを確認してください。



Service Name: 管理者は、特定の転送のために、覚えやすい別名を指定できます。

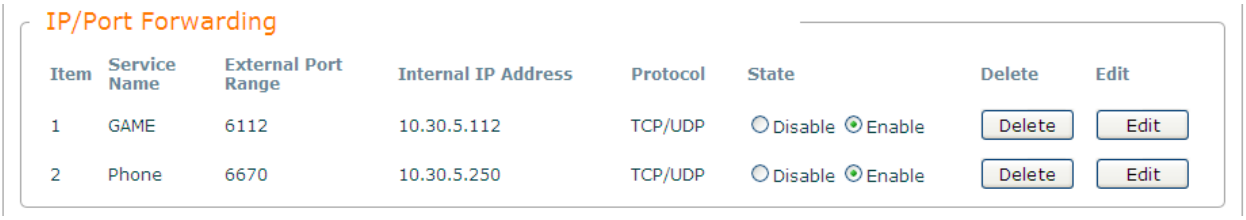
External Port Range: トラフィックを転送する外部ポートの範囲は、管理者が手動で定義できます。

Internal IP Address: 転送トラフィックを受信するための LAN IP アドレスを入力します。

Protocol: 転送トラフィックプロトコルは、ドロップダウンリストから TCP/UCP、TCP、または UDP を選択できます。

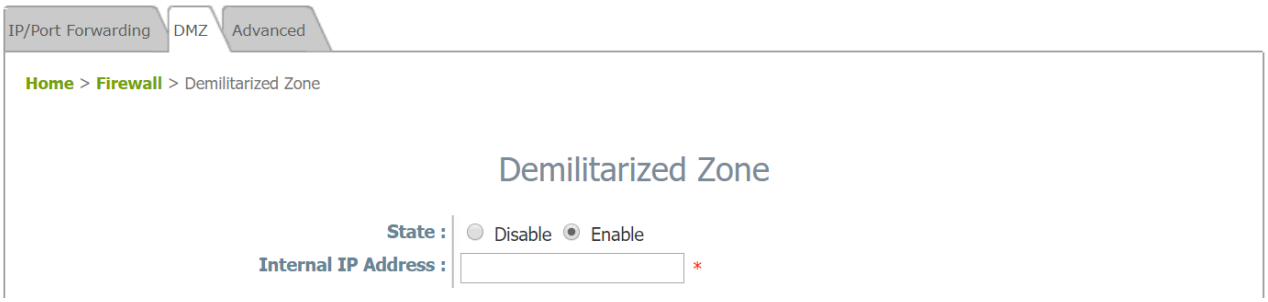
Add: Add をクリックして、新しいサービスを有効にします。

IP/Port Forwarding: 利用可能な現行サービスの詳細。Delete をクリックして、指定したサービスを削除します。Edit 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 を使用すると、1 台のローカルコンピュータまたはサーバ(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。外部ユーザは、認証なしで DMZ ホストにアクセスできます。



Enable: この機能を有効にする場合は Enable、無効にする場合は Disable を選択します。

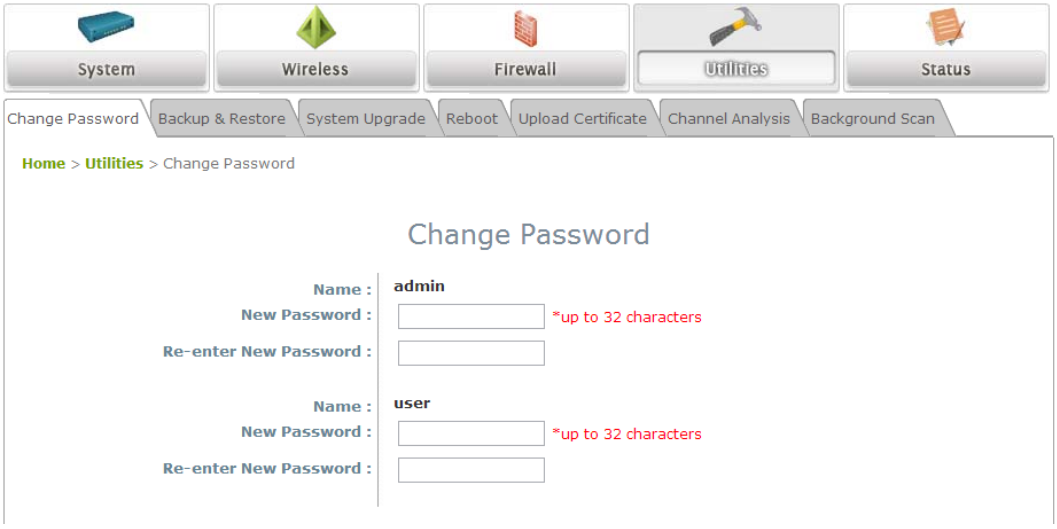
Internal IP Address: IP/ポートフォワーディングにリストされているトラフィック以外のシステム転送トラフィックを許可する内部 IP アドレスを入力します。

6. Utilities

管理者は、次のユーティリティ機能を使用して、Change Password、Backup & Restore、System Upgrade、Reboot、Upload Certificate、Channel Analysis、Background Scan を保守できます。

6.1 Change Password

Web 管理インタフェースを不正アクセスから保護するために、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。英数字のみを使用できます。また、数字と英字の両方を使用することをお勧めします。

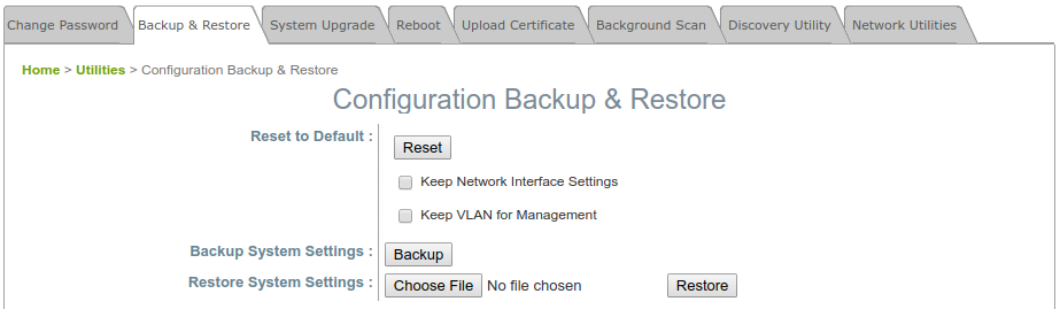


管理者はこのページでパスワードを変更できます。元のパスワード(admin)と新しいパスワードを入力し、Re-enter New Password フィールドに新しいパスワードを再入力します。SAVE をクリックして新しいパスワードを保存します。

管理者アカウントに加え、構成に制限のある Web 管理インタフェースにアクセスできる user アカウントがあります。user アカウントは、AP の再起動、無線構成の変更、またはチャネル解析機能の有効化を行うことができません。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 担当者によって発行されます。

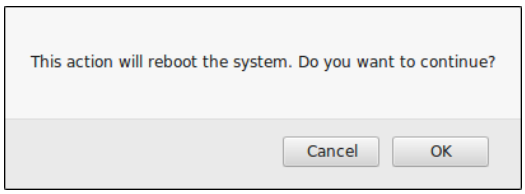
6.2 Backup & Restore

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します。この機能を使用して、AP をエ場出荷時のデフォルトに復元することができます。他のアクセスポイントに設定を複製するために使用することもできます(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)。

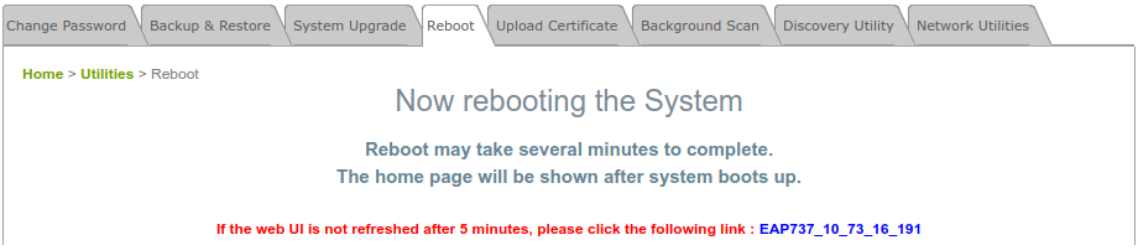


Reset to Default
通常、管理者は、以下の説明に従って、管理インタフェースからシステムを工場出荷時のデフォルトに戻すことができます。また、コンソールインタフェースから別の方法もあります。「8.2 SSH インタフェースによるリモートコネクション」を参照してください。

- **Keep Network Interface Settings**: 場合によっては、このオプションのチェックボックスをチェックして、システムがデフォルトにリセットされても元のネットワークインタフェース設定が維持されるようにすることをお勧めします。
- **Keep VLAN for Management**: 場合によっては、このオプションのチェックボックスをチェックして、システムがデフォルトにリセットされた後も、管理設定の元の VLAN が維持されるようにすると便利です。
- Reset をクリックして、工場出荷時のデフォルト設定を読み込みます。再起動の要求を確認するポップアップメッセージが表示されます。OK をクリックして続行するか、Cancel をクリックしてアクションを取り消します。



- 再起動中に次のようなメッセージが表示されます。再起動処理が完了する前に、システムの電源を入れておく必要があります。再起動完了後、System Overview ページが表示されます。

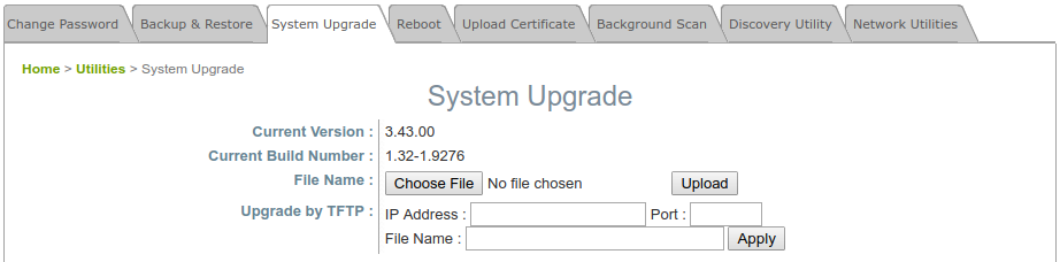


Backup System Settings: 現在のシステム構成を管理コンソールのローカルディスク上のバックアップファイルに保存します。Choose File をクリックしてバックアップファイルを選択し、Restore をクリックすると、バックアップファイルをシステムに復元することができます。

Restore System Settings: Choose File をクリックして、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検索し、Restore をクリックして、バックアップファイルの保存時と同じ設定に復元します。

6.3 System Upgrade

ファームウェアアップグレードには、WMI 経由と TFTP サーバ経由の 2 つの方法があります。管理者は、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には、Choose File をクリックし、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て Upload をクリックします。TFTP でアップグレードするには、指定された IP アドレス、ポート、およびファイル名を入力し、Apply をクリックします。ファームウェアのアップグレード後、システムを再起動してください。

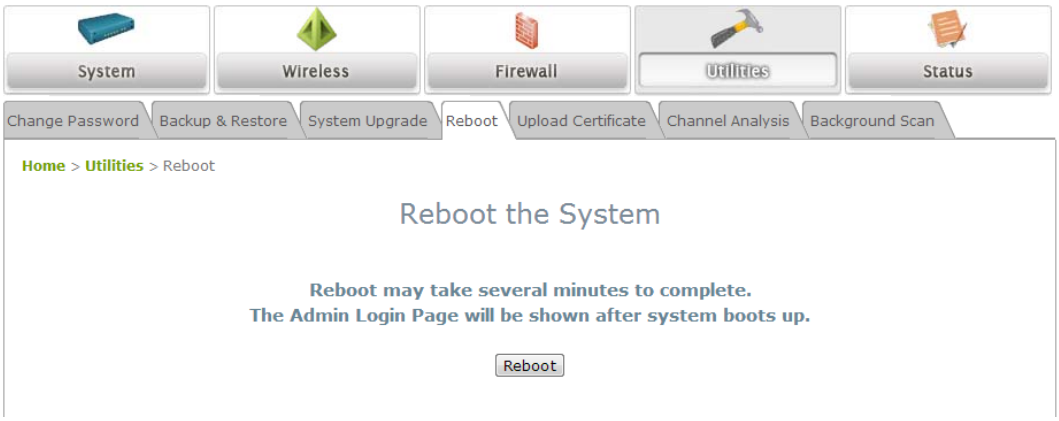


NOTE:

- 続行する前に、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。
- ファームウェアをアップグレードすると、データが失われる場合があります。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。
- ファームウェアアップグレード中は、電源を切らないでください。システムに永久的な損傷を与える可能性があります。
- TFTP によるアップグレードは、選択した AP モデルで制限される場合があります。

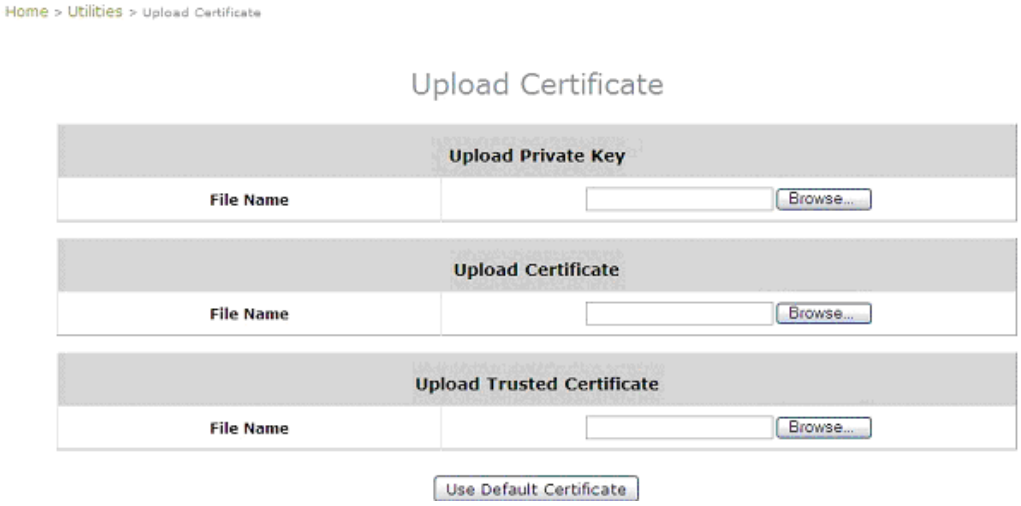
6.4 Reboot

Reboot 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 ページが表示されます。場合によっては、パラメータの変更が確実に送信されるように AP を再起動する必要があります。



6.5 Upload Certificate

この関数は、CAPWAP で必要なセキュリティ検証用の有効な証明書を設定するために使用されます。

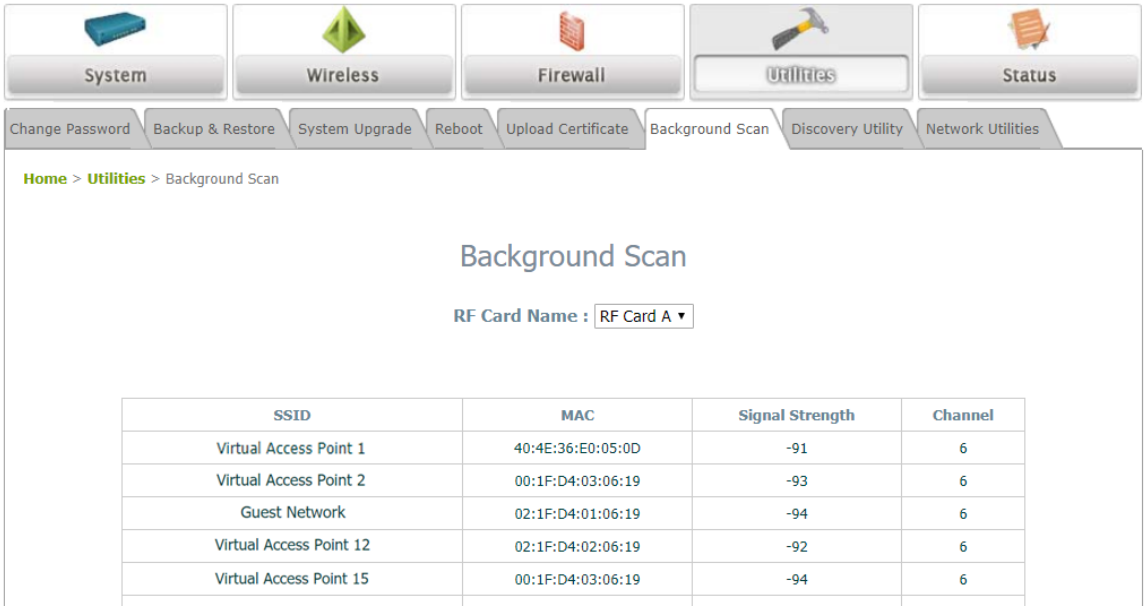


Upload Certificate: CAPWAP または他のセキュリティのセキュリティ検証の手段として、顧客自身の証明書、秘密鍵、または信頼された証明書を柔軟にサポートし、他のネットワークエンティティへのこの AP の信頼性を確保する必要があります。

Use Default Certificate: デフォルト証明書と鍵を使用するには、Use Default Certificate をクリックします。

6.6 Background Scan

アクセスポイントは、サービスに影響を与えることなくバックグラウンドスキャンを実行できます。これはチャネル分析を補完的に機能するため、管理者は無線環境の完全な概要を把握できます。



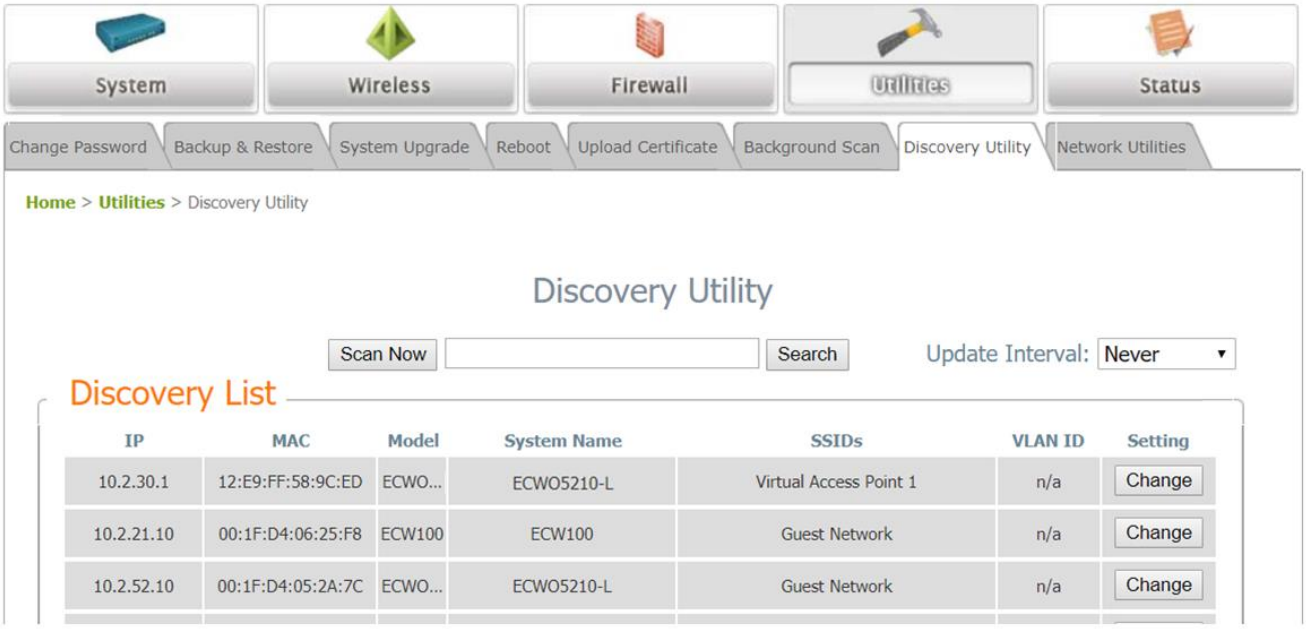
SSID	MAC	Signal Strength	Channel
Virtual Access Point 1	40:4E:36:E0:05:0D	-91	6
Virtual Access Point 2	00:1F:D4:03:06:19	-93	6
Guest Network	02:1F:D4:01:06:19	-94	6
Virtual Access Point 12	02:1F:D4:02:06:19	-92	6
Virtual Access Point 15	00:1F:D4:03:06:19	-94	6

Scan Whole Channel ボタンで、設定された帯域内のすべてのチャネルのスキャンを開始します。無線は、設定された帯域でのみスキャン可能であることに注意してください。

6.7 Discovery Utility

ネットワーク管理者は、AP インタフェースに入らずにいくつかの情報を見たり変更したりする必要に迫られることがあります。例えば、AP の IP アドレスを忘れた、管理者のパスワードを忘れた、AP の IP アドレスを変更したい、などの場合です。

必要な操作は、同じレイヤ 2 内の AP を現行のポートから接続し、Search をクリックして IP 検出ユーティリティを実行することだけです。検索結果は、デバイスの対応する IP アドレス、MAC アドレス、モデル、システム名、SSID(各 VAP)、VLAN ID です。機器の 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。

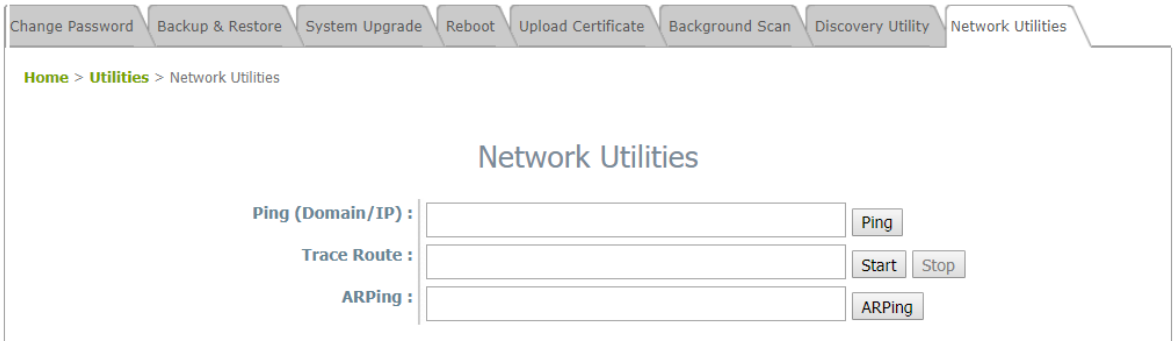


Scan Now: このボタンをクリックすると、検出処理が開始され、結果が Discovery List テーブルに表示されます。

Search: 特定の AP を検索するためのキーワードを入力します。

Change: これにより、管理者は、IP アドレス、ネットマスク、ゲートウェイ、プライマリ DNS サーバ、ユーザ名、パスワードなどの特定の AP の設定を変更できます。

6.8 Network Utilities

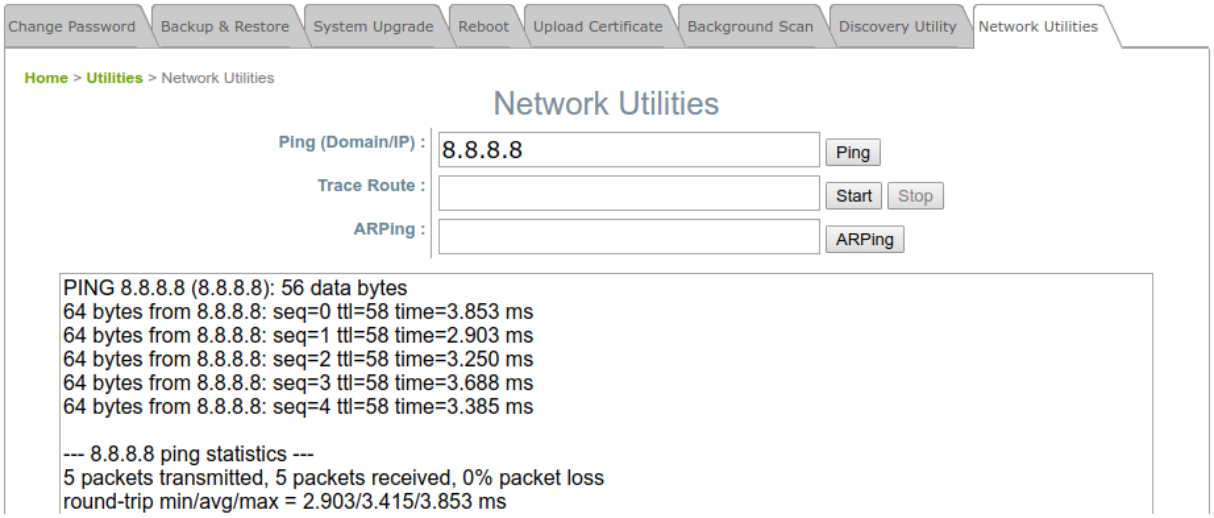


Ping: 管理者は、IP アドレスまたはホストドメインネームを使用してデバイスを検出し、デバイスが稼働しているかどうかを確認できます。

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。

Result: 演算結果が表示されます。

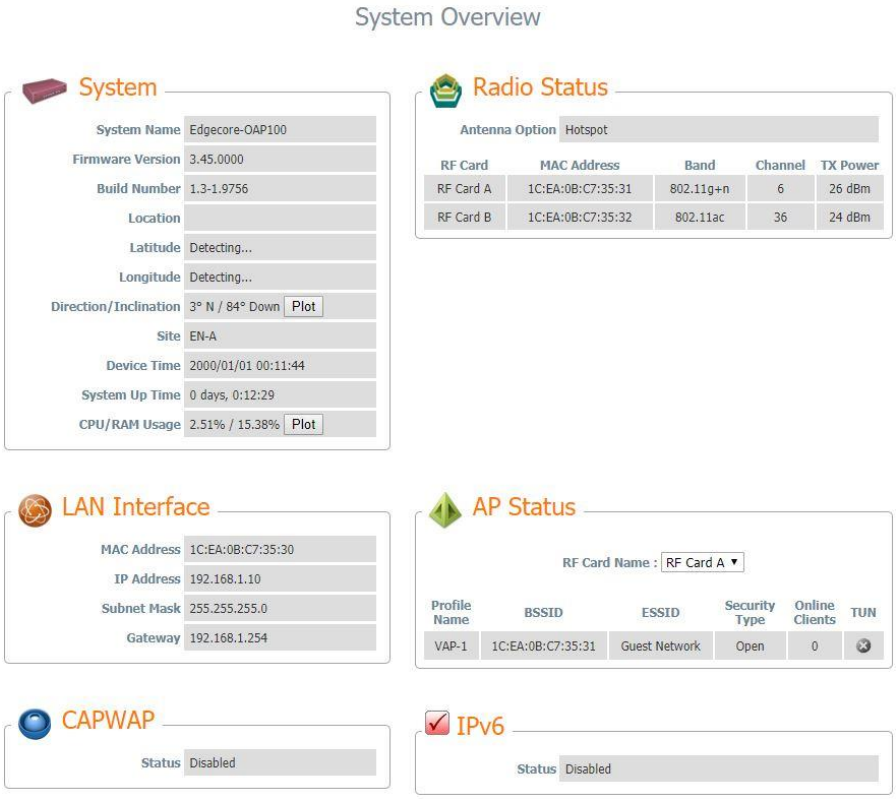


7. Status

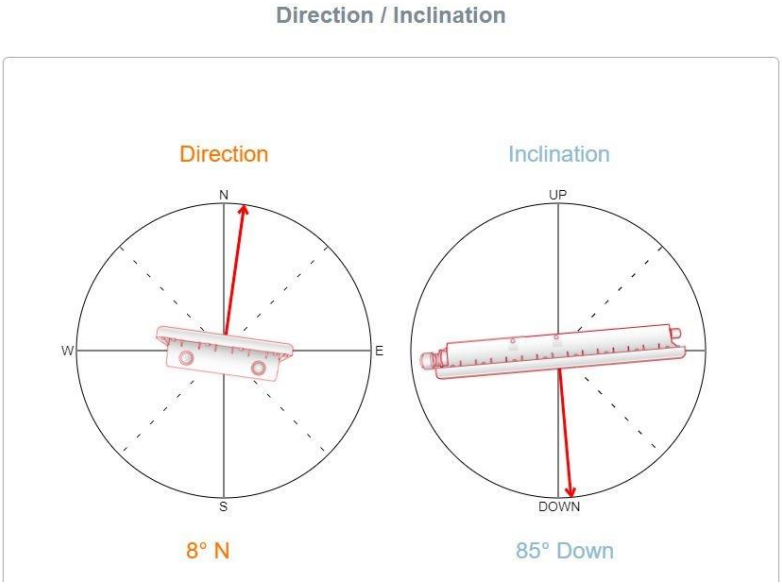
次のファンクションタブには、システムの現状と状態が表示されます。Overview、Interfaces、Associated Clients、DHCP Lease、Link Status、Event Log、Wireless Log、Monitor。

7.1 Overview

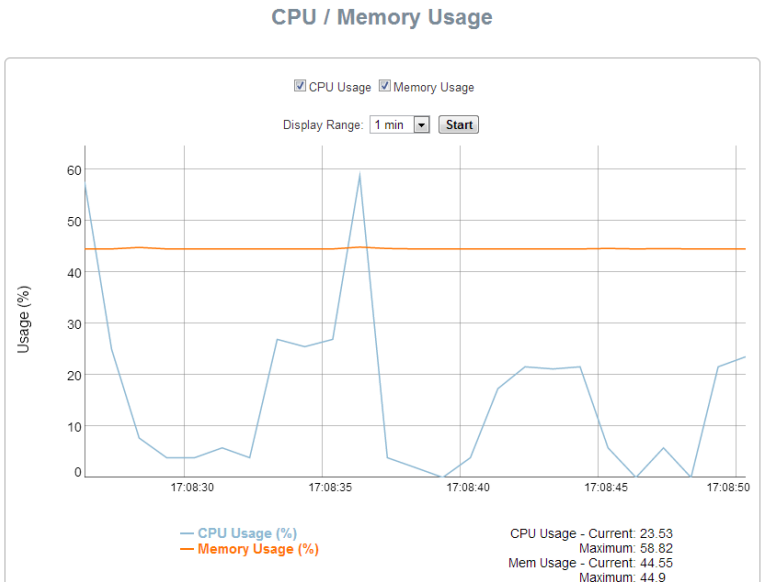
System Overview ページには、管理者向けにシステム状態の概要が表示されます。



Direction/Inclination 内にある Plot ボタン(OAP100 のみ)をクリックすると、方向/傾きのプロットが表示されます。左側には、デバイスの水平角度が表示されます。右側には、デバイスの垂直方向の傾斜角度が表示されます。

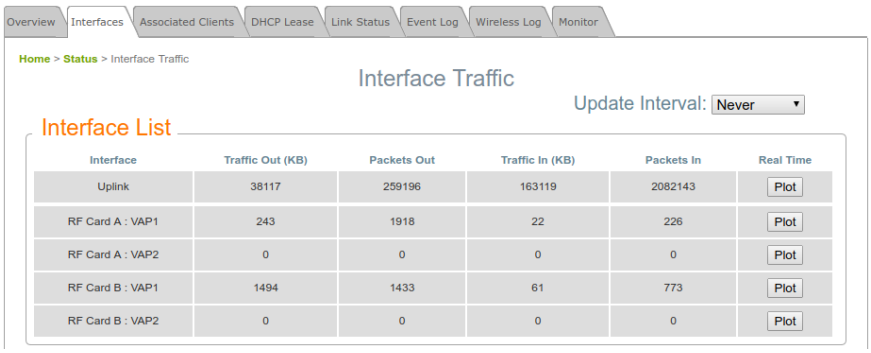


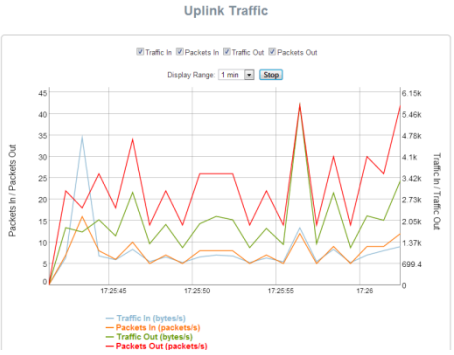
CPU/RAM Usage 内にある Plot ボタンをクリックすると、CPU/RAM 使用量のリアルタイムプロットが表示されます。マウスを左クリックしてドラッグし、目的の領域をズームインします。グラフをダブルクリックすると、プロットが元のスケールに戻ります。



7.2 Interfaces

1 インタフェースあたりのトラフィック量が表示されます。記録されるデータには、Packets In、Packets Out、Traffic In(kb)、Traffic Out(kb)が含まれます。

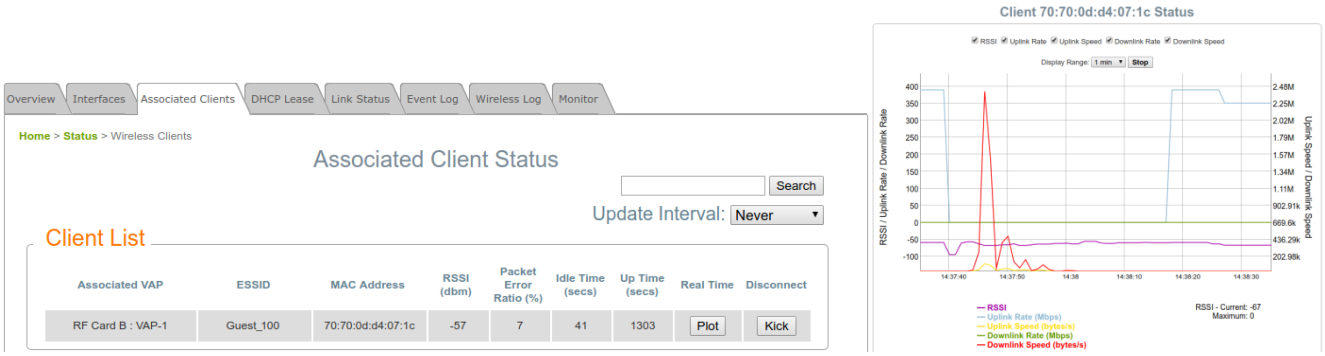




1 分、2 分、5 分、または 10 分のオプションで時間軸を設定できるインタフェースごとにリアルタイムプロットを使用することもできます。マウスを左クリックすると、希望する領域にズームインします。ダブルクリックすると、プロットが元のスケールに戻ります。

7.3 Associated Clients

管理者は、このページに関連付けられてい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。



1 分、2 分、5 分、または 10 分のオプションで時間軸を設定できるインタフェースごとにリアルタイムプロットを使用することもできます。マウスを左クリックすると、希望する領域にズームインします。ダブルクリックすると、プロットが元のスケールに戻ります。

Associated 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拡張サービスセット ID。

MAC Address: 関連付けられたクライアントの 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。

Packet Error Ratio: パケットが受信されていないかどうかを確認するために、関連付けられたクライアントのサービスクオリティを示します。

Idle Time: 関連付けられたクライアントが非アクティブである期間。時間単位は秒です。

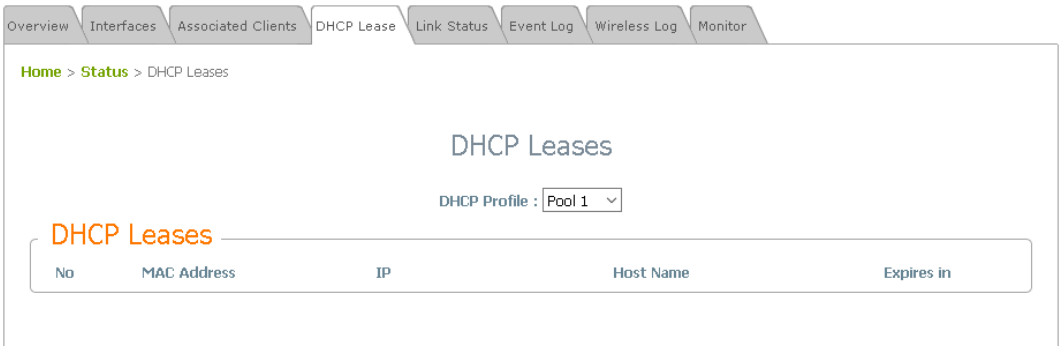
Up time: クライアントが関連付けられている期間。時間単位は秒です。

Real Time (Plot): パケット入出力、トラフィック入出力(KB)、RSSI、アップリンク/ダウンリンク速度など、関連付けられた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: Kick をクリックすると、本機との接続が切断されます。

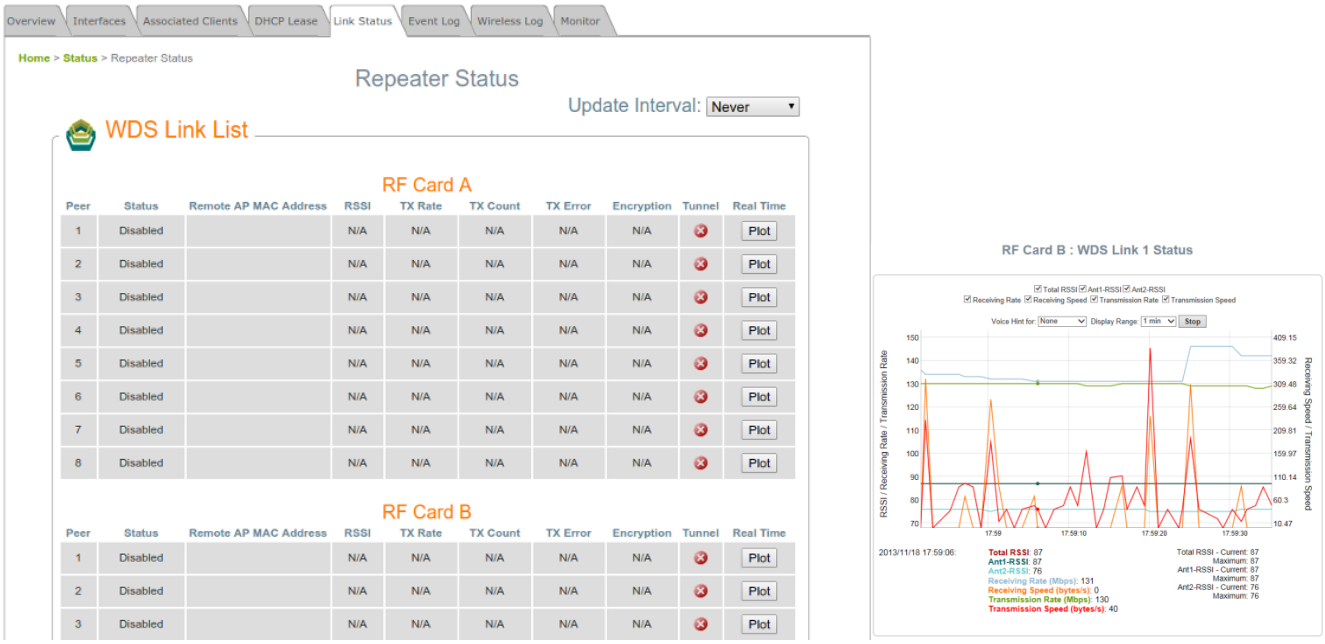
7.4 DHCP Lease

いずれかの VAP が NAT モードで動作する場合、DHCP リースインフォメーションがこのテーブルに表示されます。



7.5 Link Status

管理者は、Status>Link Status 画面表示時にリピータ機能の詳細を確認することができます。WDS の状態、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。

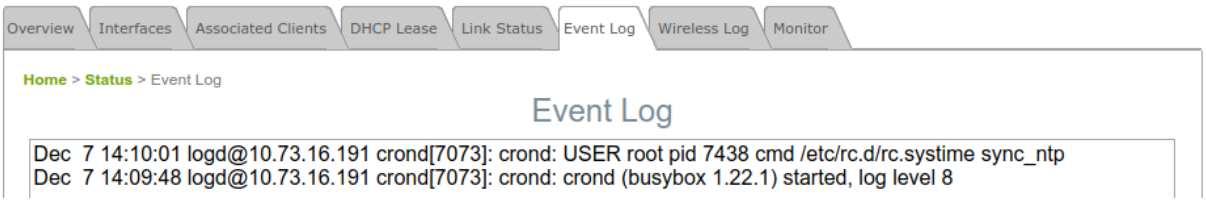


Plot をクリックすると、WDS リンクステータスの動的グラフが表示されます。プロットの情報には、Total RSSI、Ant1RSSI、Ant2RSSI、Transmission Rate、Receiving Rate、Transmission Speed、および Receiving Speed が含まれます。

1 分、2 分、5 分、または 10 分のオプションで時間軸を設定できるインタフェースごとにリアルタイムプロットを使用することもできます。ダブルクリックすると、プロットが元のスケールに戻ります。
また、アンテナ調整時にも音声ヒントを有効にすることができます。

7.6 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、システムの状態を監視できます。内部記憶域は制限されているため、外部の Syslog サーバ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。



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: イベントが発生した日時。

IP Address: このイベントが記録された 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。しかしながら、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: 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。

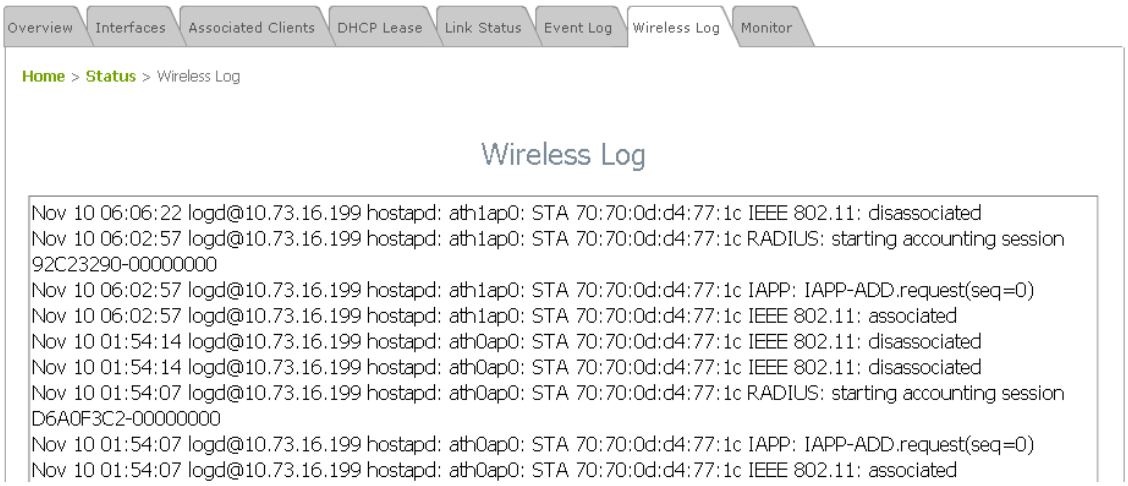
Description: イベントごとのメッセージを表示します。

SAVE LOG: txt ファイルとしてローカルディスクに保存します。

CLEAR: すべてのレコードを消去します。

7.7 Wireless Log

この無線ログは、クライアントの関連付けと WDS 接続関連の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、システムの状態を監視できます。内部記憶域は制限されているため、外部の Syslog サーバ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。



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。
g
Date and Time: イベントが発生した日時。

IP Address: このイベントが記録された 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。しかしながら、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: 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。

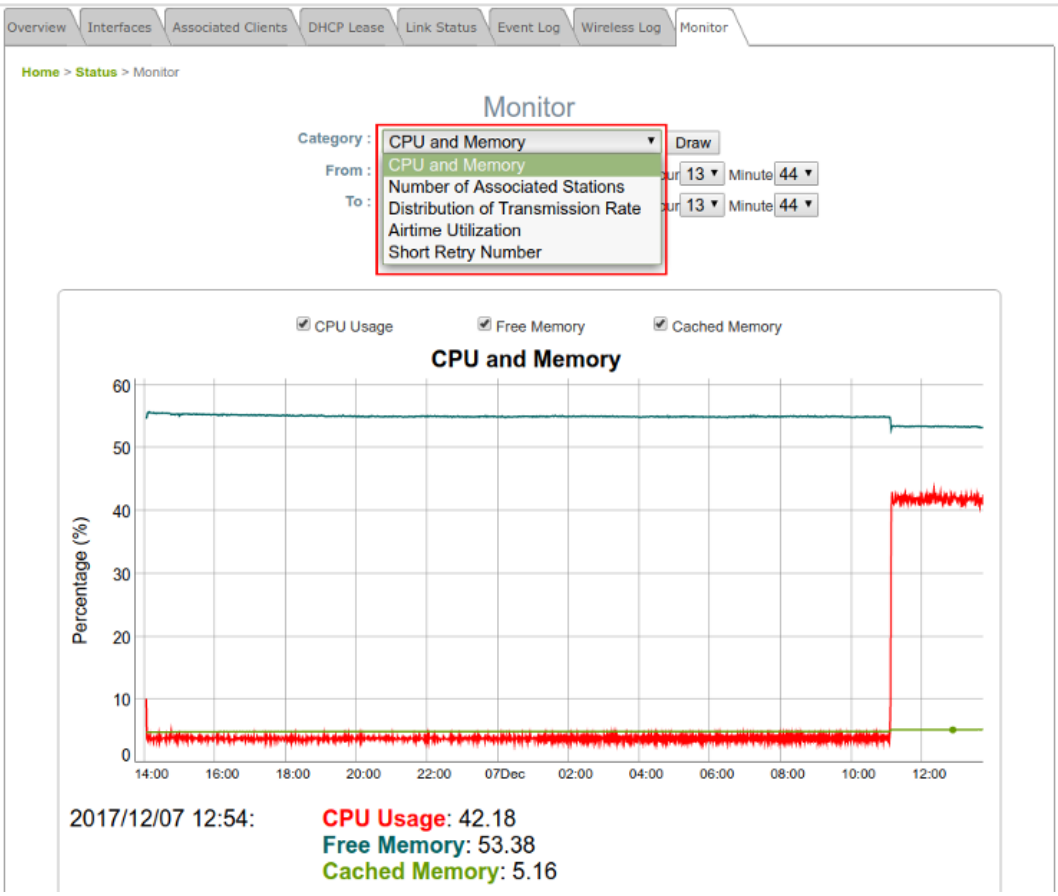
Description: イベントごとのメッセージを表示します。

SAVE LOG: txt ファイルとしてローカルディスクに保存します。

CLEAR: すべてのレコードを消去します。

7.8 Monitor

複数のモニタチャートを使用すると、時間軸における AP のパフォーマンスの概要をすばやく確認できます。各チャートの開始時間と終了時間は、データのフィルタリングのために選択できます。マウスを左クリックすると、希望する領域にズームインします。ダブルクリックすると、プロットが元のスケールに戻ります。



CPU and Memory: デバイスの使用状況を表示します。CPU < 90%、RAM < 90%が許容範囲です。

Number of Associated Station: 選択した無線(RF Card A または RF Card 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: 伝送速度で分類されたパケットの個数を表示します。

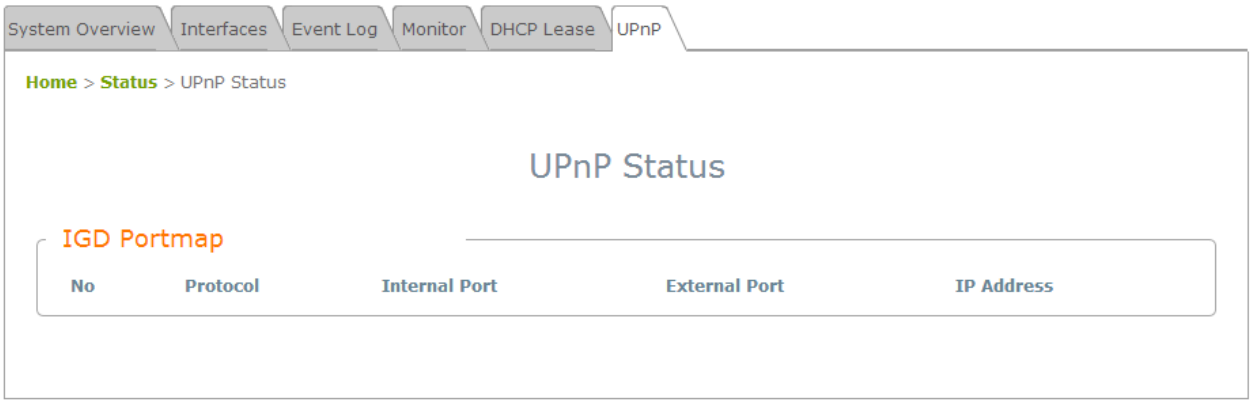
Airtime Utilization: 無線環境の信号とノイズを表示します。エアタイム使用率 < 70%が最適です。

- **RX Clear Rate**: 現在のチャネルで使用されているエアタイムの割合。
- **RX Frame Rate**: AP が受信および復号するエアタイムの割合。
- **TX Frame Rate**: AP がデータを送信してからのエアタイムの割合。

Short Retries Number: 再送信されたパケットの個数を表示します。Short Retry < 200 が最適です。

7.9 UPnP(CPE モードのみ)

このテーブルには、Protocol、Internal Port、External Port、IP Address などの UPnP の概要が表示されます。



IGD Portmap:

- **No**: UPnP 機器の項目番号です。
- **Protocol**: UPnP デバイスが使用するプロトコル。
- **Internal Port**: UPnP 機器の内蔵ポート No。
- **External Port**: マップされた外部ポート番号。
- **IP Address**: UPnP 機器の IP アドレス。

8. コンソールインタフェース

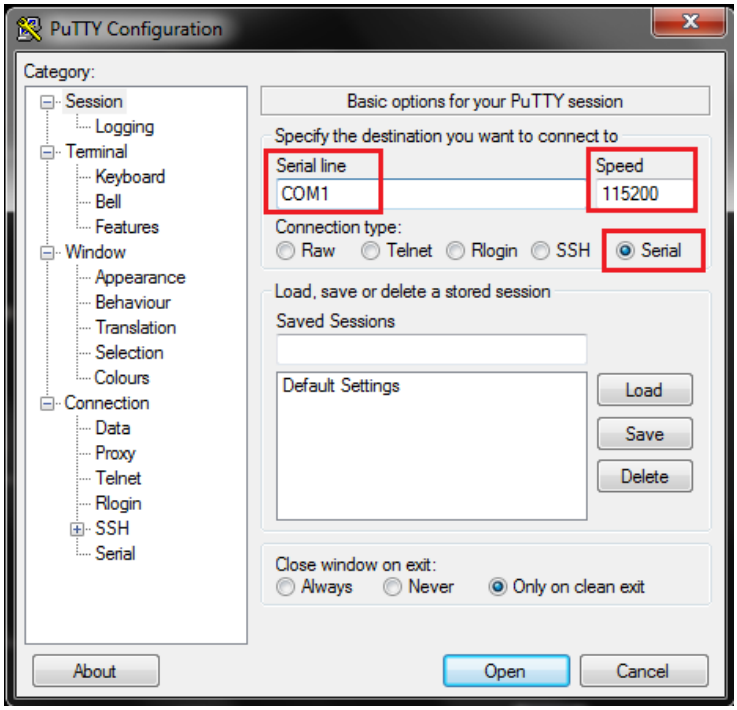
管理者は、コンソールポートを介してコンソールインタフェースに入り、AP を出荷時のデフォルト設定に戻すことができます。AP のコンソールポートに接続するには、AP、コンソールケーブル、およびターミナルシミュレーションプログラム(PuTTy など)が必要です。本体インタフェースには、次の 2 つの方法があります。

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>Console Cable(DB9-to-RJ45)>Console Port
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。同梱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。

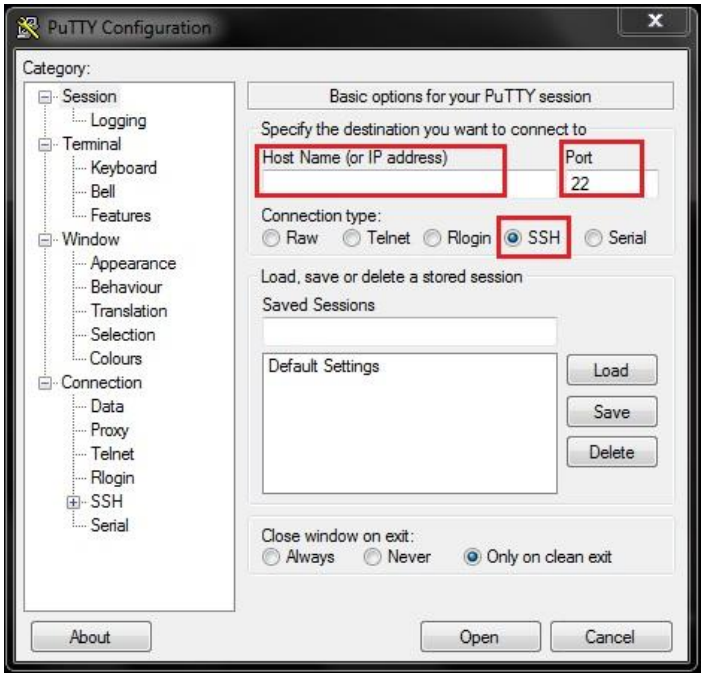
ケーブル	説明
	USB-RS-232 シリアルコンバータケーブル(USB-DB9 オス)
	コンソールケーブル(DB9 メス-RJ45 オス)

速度(ボーレート)は 115200 です。

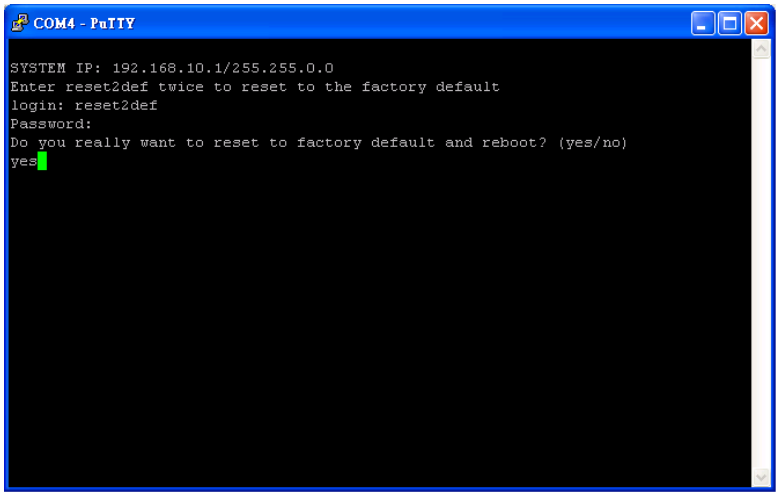


8.2 SSH インタフェースによるリモートコネクション

SSH を介したコンソールインタフェースへのアクセスがサポートされています。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。



コンソールインタフェースから出荷時のデフォルトにリセットするには、「reset2def」としてログインし、パスワードは「reset2def」と入力します。



コンソール接続がすぐに使用できない場合は、別の AP(Home>Utilities>Discovery Utility)の検出ユーティリティを使用して AP の IP アドレスを取得できます。イーサネットケーブルを使用して接続し、検出ユーティリティを実行します。