User Manual

Enterprise Access Point

Verion 3.45.0000

Table of Content

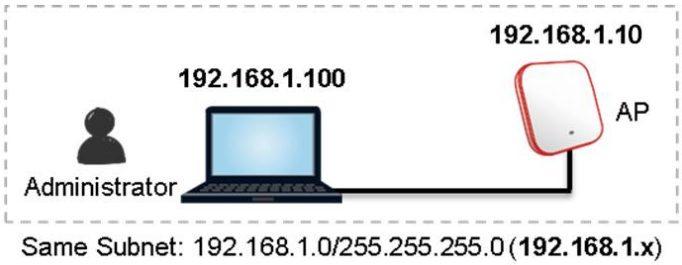
1. Edgecore Enterprise Access Point Quick Deployment

To set up The AP for the first time, administrators need to perform initial configuration to assign an IP address and other information necessary for the AP to communicate with the local gateways and for the AP to allow Wi-Fi devices to connect to the wired network.

1.1 Log in to the AP

The AP has a web-based interface for configuration and management. To access the Web Management Interface (WMI) for the first time, follow the steps below.

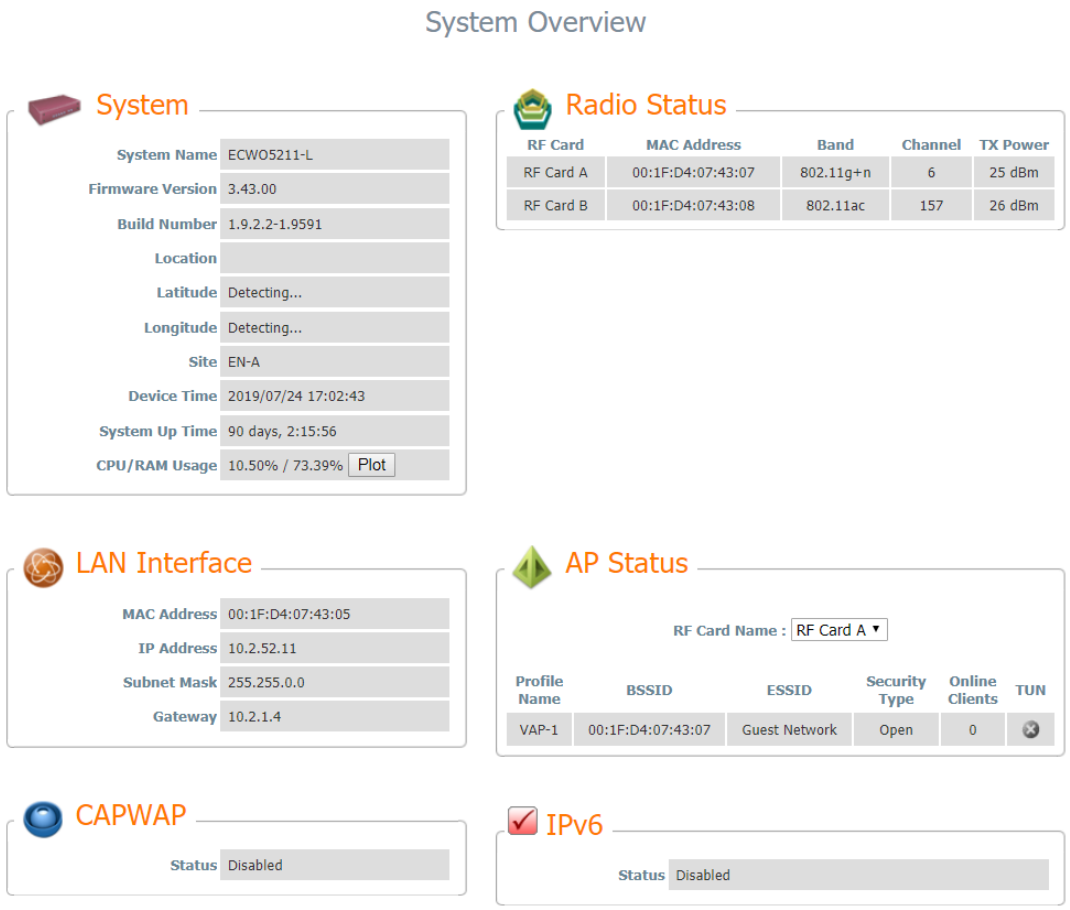
1. **Ensure that your administrative PC is manually set to a static IP Address in the same subnet as the AP's (192.168.1.10/255.255.255.0). Connect the PC directly to the LAN port of the AP via an Ethernet cable.**



2. **Launch the web browser and enter the default IP Address of the AP (192.168.1.10) in the address field.**

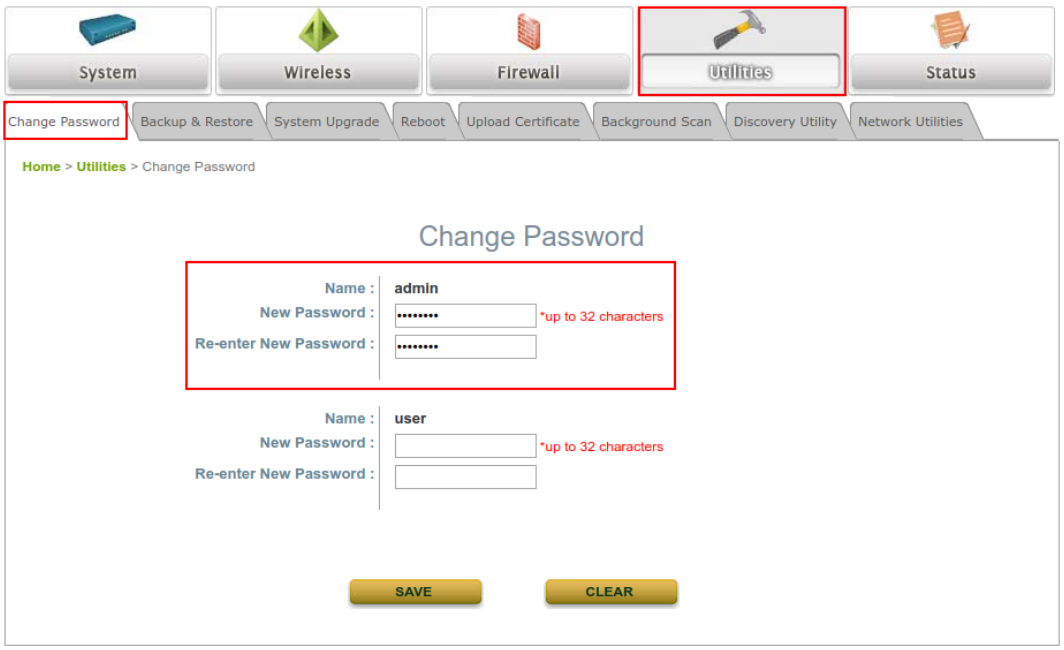
Log in using default Username (**admin**) and Password (**admin**) on the Administrator Login Page:

3. System Overview page of the WMI will appear after login.



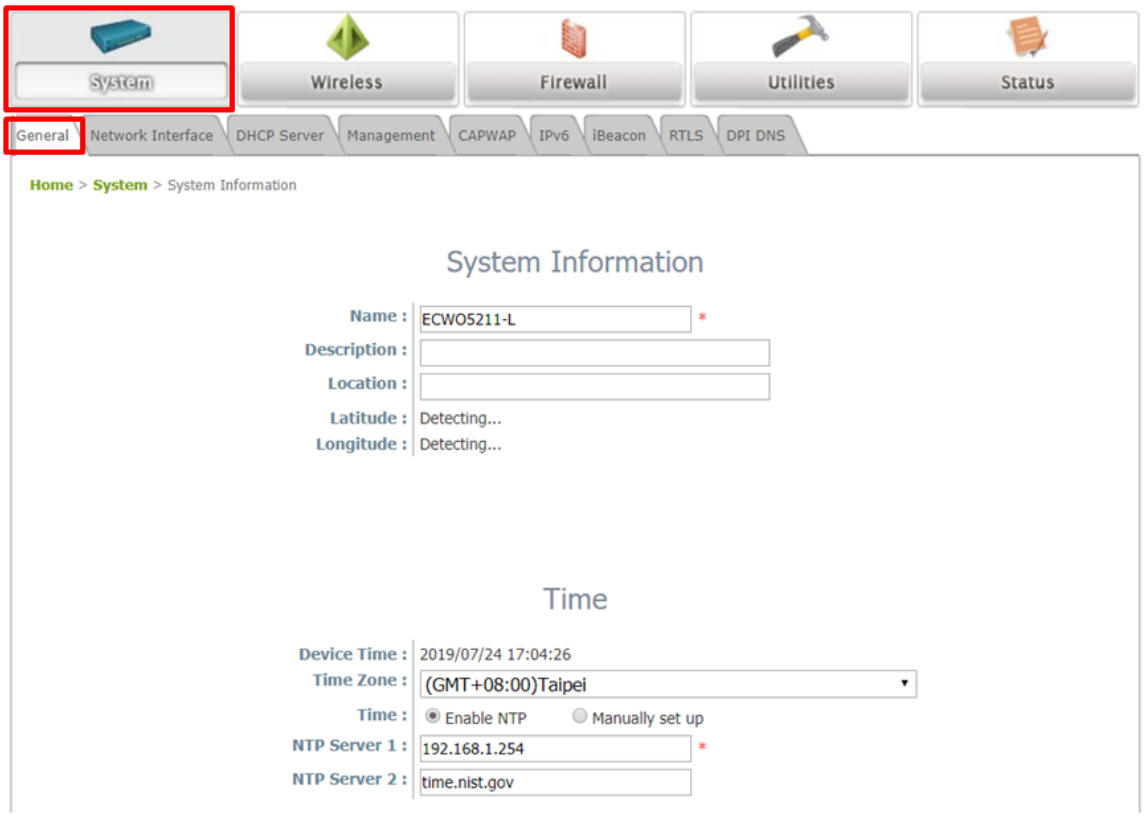
4. Change the administrator's password for security reasons

- Click on the **Utilities** icon on the main menu, and select the **Change Password** tab.
- Enter the **New Password** and retype it in the **Re-enter New Password** field.



1.2 General Information Configuration

Go to System **General** page (Home > System > General) to configure general information for the AP.



1. **System Information**: Enter appropriate system related information (**Name**, **Description**, and **Location**), by which administrators will be able to identify the AP in the network.

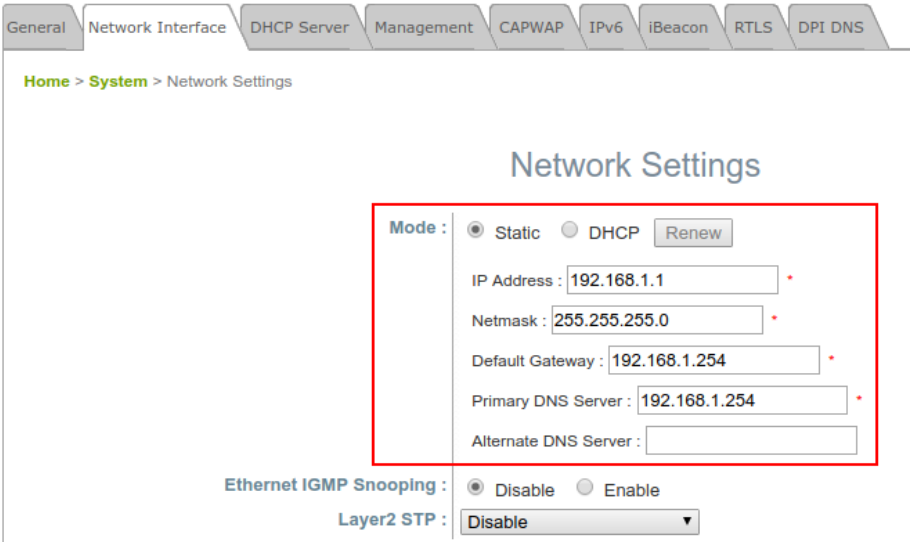
2. **Time**: For this initial configuration, set the system time for the AP using the method of **Enable NTP** (to sync the system clock with Network Time Protocol (NTP) server).

1.3 Connect the AP to the Network

The following instructions are the basic steps to establish the wireless coverage of your network. The AP will connect to the wired network through its LAN port and enable wireless access to your network.

1. Change IP Settings of the AP

Go to **Network Interface** page (Home > System > Network Interface) to perform configuration of the network settings.



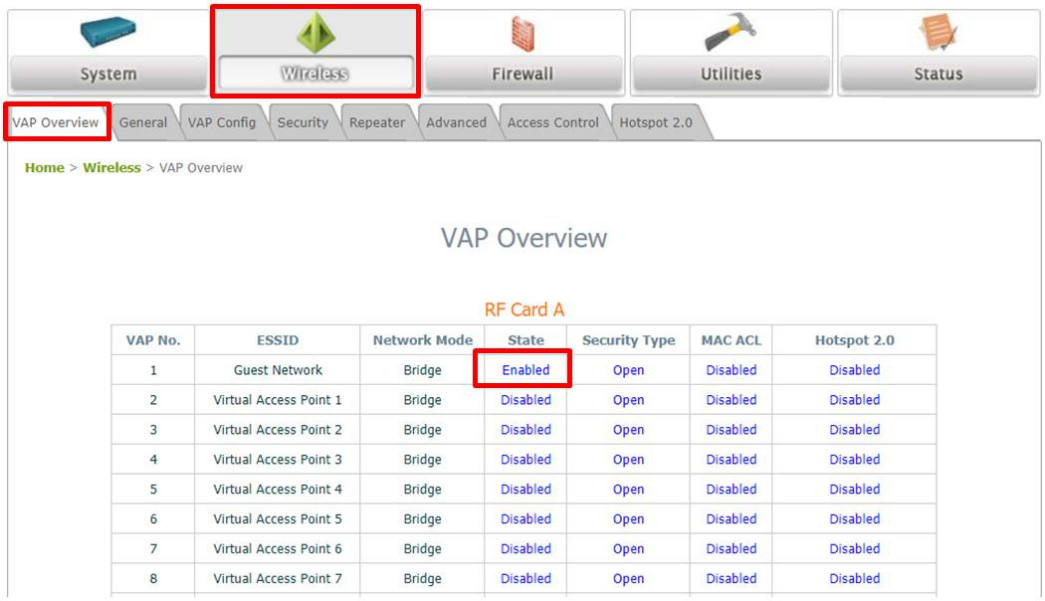
Mode:

Static: Manually fill in appropriate values for the network interface (**IP Address**, **Netmask**, **Default Gateway**, and **Primary DNS Server**) – in the example above, the AP is still using the default IP address 192.168.1.10.

DHCP: If the deployment requires that the AP get a dynamic IP Address from the LAN, set Mode to **DHCP**; Click ***SAVE*** to submit the changes.

2. Activate the first SSID for Wi-Fi access

By default, one Service Set Identifier (SSID) is enabled with the Radio A (**RF Card A**) and one SSID is enabled with the Radio B (**RF Card B**). As shown on the **VAP Overview** page (Home > Wireless > VAP Overview), Virtual Access Point No.1 (VAP-1) profile represents the first SSID available.

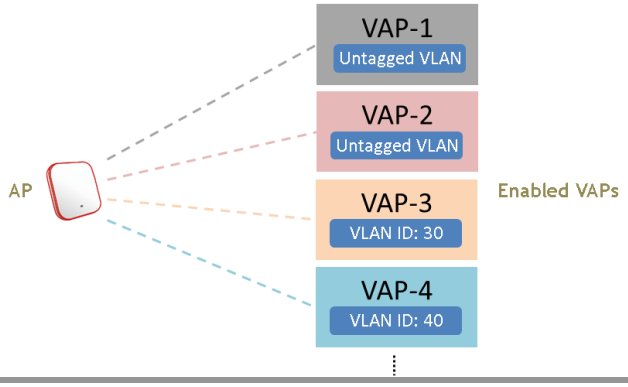


VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled
4	Virtual Access Point 3	Bridge	Disabled	Open	Disabled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

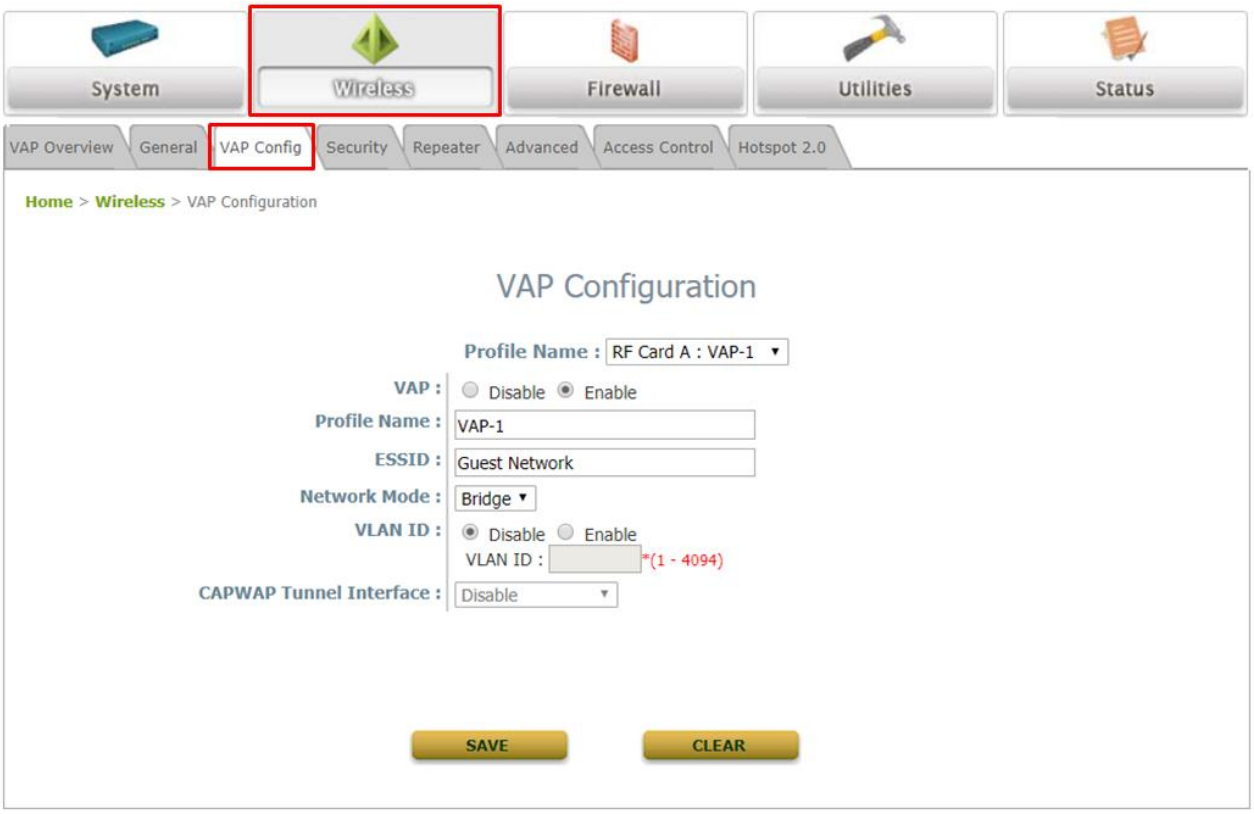
Virtual Access Point (VAP):

- VAP feature allows a single physical AP device (with a unique, single BSSID) to present itself as multiple discrete APs, as shown in the example diagram below;
- Each VAP can be independently enabled or disabled, with its own settings (e.g. SSID, Network Mode, VLAN ID, Security, etc.), such that the AP is able to support different clients through multiple SSIDs.

Note:

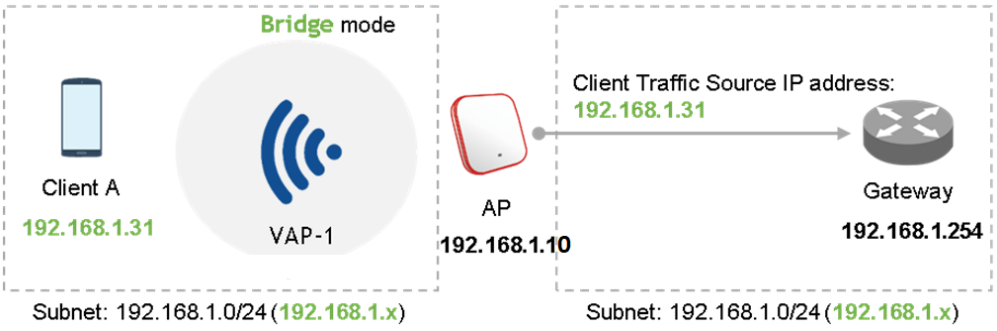


Click on the State (**Enabled**) of VAP-1 to configure the profile. This will bring up the following VAP Configuration page.

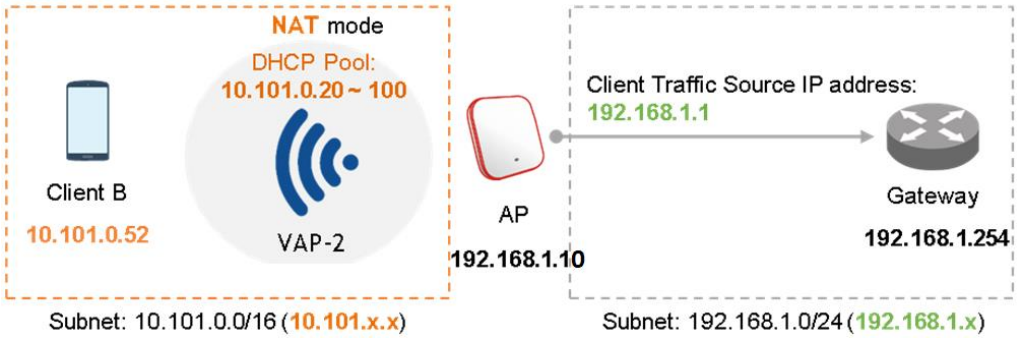


Select the specific VAP profile (in this case, "RF Card A: VAP-1"). The basic settings of the VAP are collected in the profile as follows:

- **VAP:** Disable or Enable this VAP.
- **Profile Name:** Name of the VAP profile for identity / management purposes.
- **ESSID:** Extended Service Set Identifier (ESSID) serves as an identifier for clients to associate with the specific VAP.
- **Network Mode:**
  - **Bridge** mode: the VAP operates transparently (i.e. no NAT, no DHCP) such that client devices will be assigned a dynamic IP address from a DHCP server on the LAN side. The source IP address of client traffic seen by the uplink gateway/switch will remain the original IP address of the client (in this case, 192.168.1.31, as shown in the diagram below).



- **NAT mode:** the VAP operates like a Network Address Translation (NAT) device with a built-in DHCP server on this SSID such that client devices will be assigned a dynamic IP address from the configured DHCP pool on this SSID. After NAT conversion, the source IP address of client traffic seen by the uplink gateway/switch will be the IP address of the AP (in this case, 192.168.1.10, as shown in the diagram below).



- **VLAN ID:** Per-SSID VLAN tagging function – when enabled, clients' traffic which enters the AP through this SSID will be tagged with the configured VLAN ID.
- **DHCP Profile:** Built-in DHCP Server profile; IP settings of DHCP Server are under Home > System > DHCP Server.
- **CAPWAP Tunnel Interface:** Three states indicating the connectivity between AP and Controller, when AP is managed by Controller
  - **Disable** (No Tunnel)**:** the AP is operating with no CAPWAP Tunnel connection to the Controller
  - **Split Tunnel:** the AP passes only "control" traffic to the Controller via the CAPWAP Tunnel; i.e. "data" traffic will go out locally without passing through the Tunnel
  - **Complete Tunnel:** the AP passes both "control" and "data" traffic to the Controller via the CAPWAP Tunnel

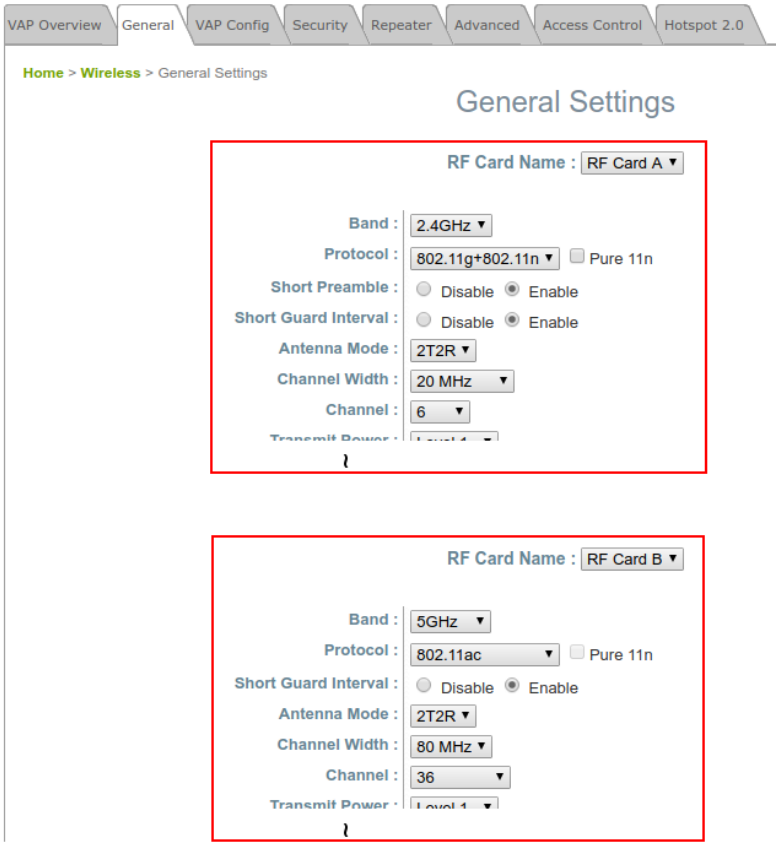
Note:

- VLAN ID is supported only when the VAP is in Bridge mode.
- DHCP Profile and DHCP Server are activated only when the VAP is set to NAT mode.
- If the VAP is in NAT mode, the CAPWAP Tunnel Interface will only work in two states:

Disable (No Tunnel) or Split Tunnel.

3. Configure General Wireless Settings

Under Home > Wireless > General, there are global settings for RF Card A and B. RF Card A is operating in 2.4 GHz band and RF Card B is operating in 5 GHz band, both of which are enabled by default.
For initial configuration, you might want to change the default basic settings shown below:
RF Card A: 2.4 GHZ, 802.11g+802.11n, Antenna Mode 2T2R, Channel Width 40 MHz, Channel 6
RF Card B: 5 GHz, 802.11ac, Antenna Mode 2T2R, Channel Width 80 MHz, Channel 36
You can make changes to other settings at a later time.



Congratulations! After a system restart, the AP should be able to operate with these settings.

Note:

SSID, ESSID, and BSSID:

- Service Set Identifier (**SSID**) is a key identifying the Name of a Wireless LAN.
- Extended Service Set Identifier (**ESSID**) = SSID; multiple physical APs can be configured to use the same SSID such that roaming across multiple physical APs is supported.
- Basic Service Set Identifier (**BSSID**) = MAC address of AP; unique BSSID will be transmitted (in the Beacon management frame) when multiple physical APs broadcast the same ESSID.

2. Navigating the Web Management Interface

The APs have a web-based interface for configuration and management. This chapter will guide users through the AP's detailed settings. The AP can be set as AP mode or CPE mode, and the two modes will have different Menu for each other. The following table shows all the function tabs under the **Main Menu** of Web Management Interface (WMI) of the AP.

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 only)

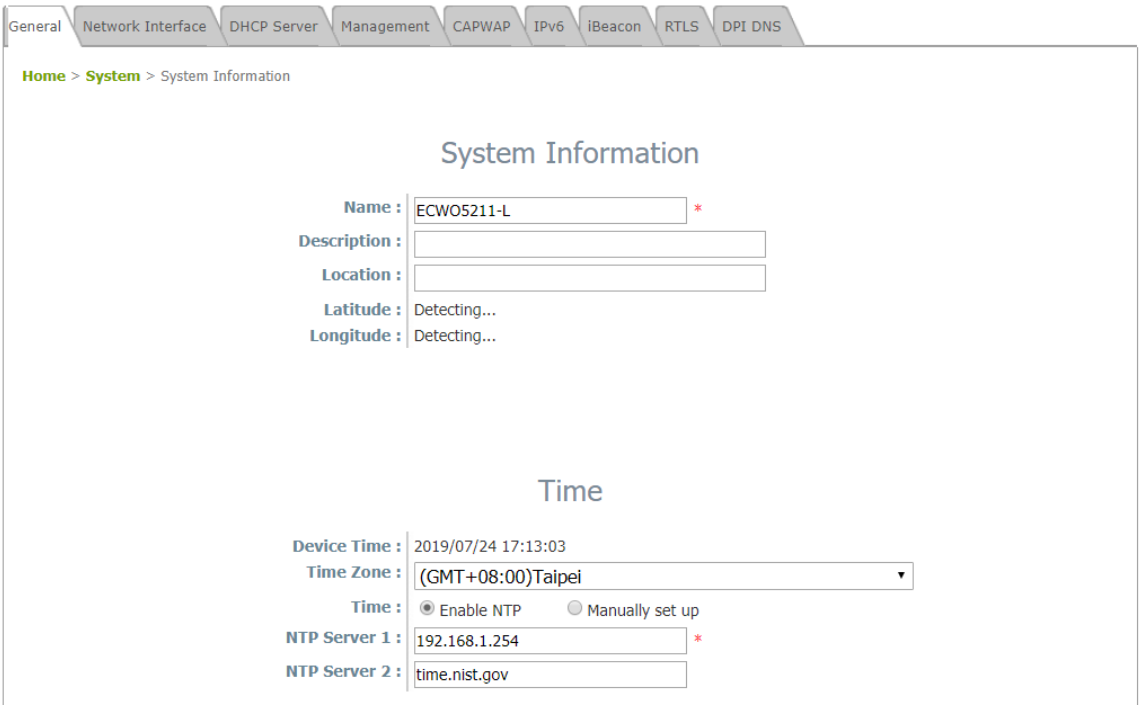
System	Wireless	Firewall	Utilities	Status
General	VAP Overview	IP/Port Forwarding	Change Password	Overview
Network Interface	General	DMZ	Backup & Restore	Interfaces
Port	VAP Config	Advanced	System Upgrade	Associated Clients
DHCP Server	Security		Reboot	Event Log
Management	Advanced		Upload Certificate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

» Note: On each configuration page, you may click ***SAVE*** to save the changes of your configured settings, but you must reboot the system for the changes to take effect. After clicking ***SAVE***, the following message will appear: **"Some modification has been saved and will take effect after Reboot."** All online users will be disconnected during reboot or restart.

3. System

Upon clicking the **System** icon, administrators can utilize this section for general configurations of the AP.

3.1 General

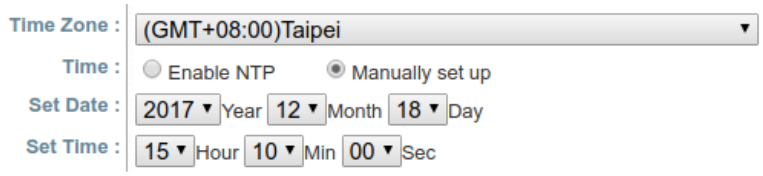


System Information
Name: The system name used to identify this system.
Description: Further information about the system (e.g. device model, firmware version, and active date).
Location: The information on geographical location of the system for the administrator to locate the system easily.

Time
Device Time: Display the current system time.
Time Zone: Select an appropriate time zone from the drop-down list box.
Time: There are two methods of setting up the time –

- **Enable NTP:** Synchronize the system clock with Network Time Protocol (NTP) server. Simply enter the IP Address or domain name of a local NTP server (if available, or search online for a NTP server nearest to you) and click *SAVE*.

- **Manually set up:** Set the system clock manually. This is the default method and requires setup every time when the system starts up. Simply choose a time zone, enter the date and the time accordingly, and click *SAVE*.

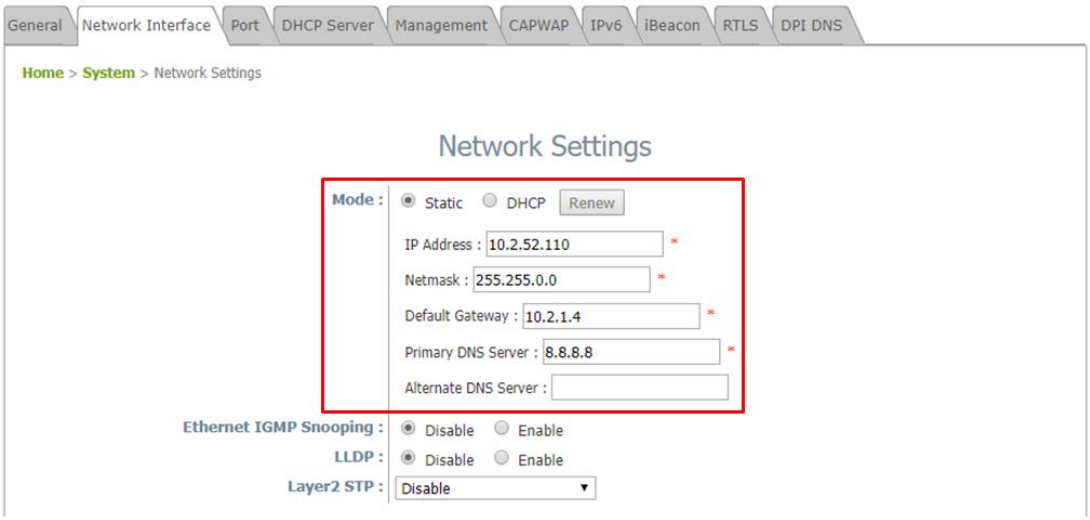


Click APPLY after an alert message "*Some modifications have been saved and will take effect after APPLY." appears on the WMI.

Unless Internet connection or NTP becomes unavailable, it is recommended to use NTP server for time synchronization because the system time needs to be reconfigured upon reboot.

3.2 Network Interface

On this page, the network settings of the device can be configured; fields with a red asterisk (i.e. **IP Address**, **Netmask**, **Default Gateway**, and **Primary DNS Server**) are mandatory.



Mode – Static: The administrator can manually set up the static LAN IP address. All required fields are marked with a red asterisk.

- **IP Address:** The IP address of the LAN port.
- **Netmask:** The Subnet mask of the LAN port.
- **Default Gateway:** The Gateway IP address of the LAN port.
- **Primary DNS Server:** The IP address of the primary DNS (Domain Name System) server.
- **Alternate DNS Server:** The IP address of the substitute DNS server.

Mode – DHCP: This configuration type is applicable when the system is connected to a network with the presence of a DHCP server; all related IP information required will be provided by the DHCP server automatically.

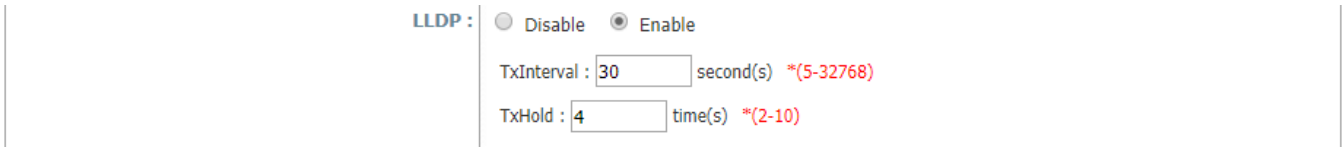
LTE (EAP100 Only): After plugging the LTE module with the SIM card into the USB port, the following two options will appear.

- **No LTE:** Choose the LAN port as the uplink.
- **LTE:** Choose the LTE as the uplink.

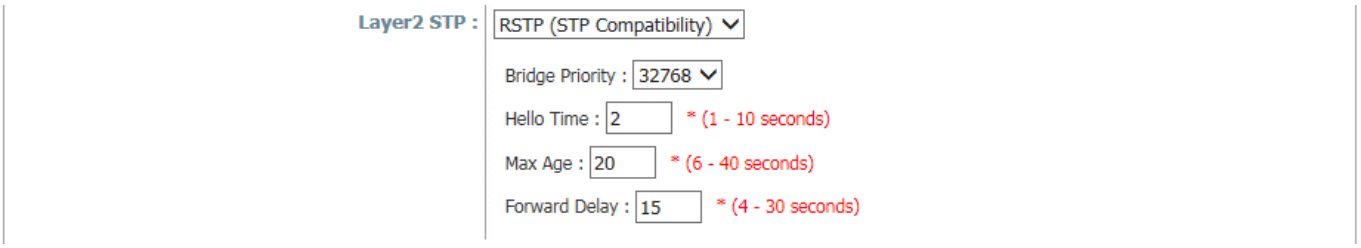
Ethernet IGMP Snooping: When Enabled, the switch forwards traffic IGMP packets are transferred via the Access Point's network interface and the IP multicast host. Registration information is recorded and sorted into multicast groups. The internal switch forwards traffic only to those ports that request multicast traffic. Adversely, without IGMP snooping, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.

LLDP: LLDP (Link Layer Discovery Protocol) is an IEEE standard protocol (IEEE 802.1ab) that defines messages, encapsulated in Ethernet frames for the purpose of giving devices a means of announcing basic device information to other devices on the LAN (Local Area Network) through periodic retransmissions out every (**TxInterval * TxHold**) seconds.

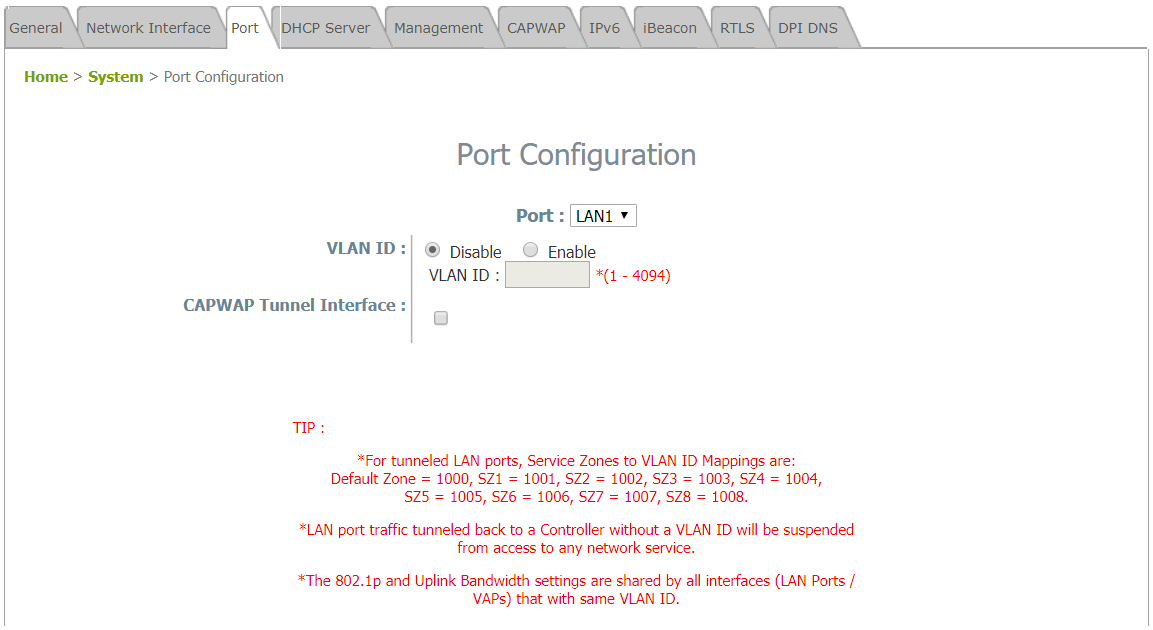
- **TxInterval:** Setting the interval for sending the packets.
- **TxHold:** Setting the times of interval for sending the packets.



Layer 2 STP: If the AP is set up to bridge other network components, this option can be enabled to prevent undesired loops because a broadcasting storm may occur in a multi-switch environment where broadcast packets are forwarded in an endless loop between switches. Moreover, a broadcast storm may consume most of the available system resources in addition to available bandwidth. Thus, enabling the Layer 2 STP can lower such undesired occurrence and derive the best available data path for network communication. The AP also supports RSTP Operation. Configurable parameters include **Bridge Priority**, **Hello Time**, **Max Age**, and **Forward Delay**. Please refer to IEEE standards for recommended parameter values.



3.3 Port



Port: Select one Port for further configuration.

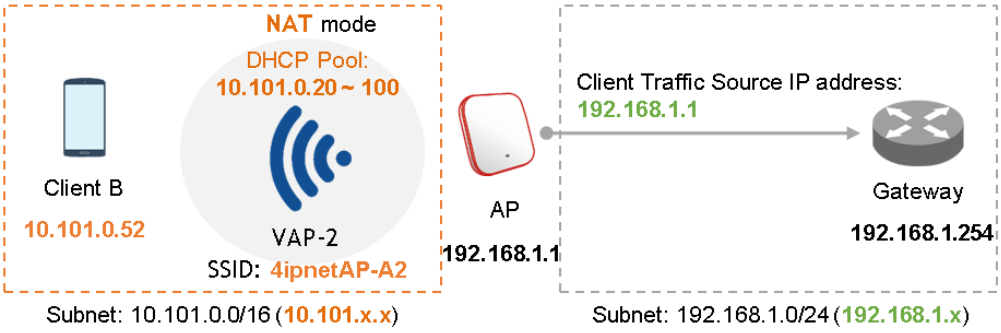
VLAN ID: Enable selected implies that network traffic sent upstream from this LAN port will be tagged with the VLAN ID configured in the field below. Disable selected implies that traffic from this LAN port will not be tagged with a VLAN ID.

CAPWAP Tunnel Interface: Select a LAN, VAP or WDS interface to designate its traffic to pass through the CAPWAP Tunnel established between the AP and the controller. For network interfaces that are unchecked, their traffic will be forwarded locally into the internet if this AP is deployed remotely on the WAN side of a controller.

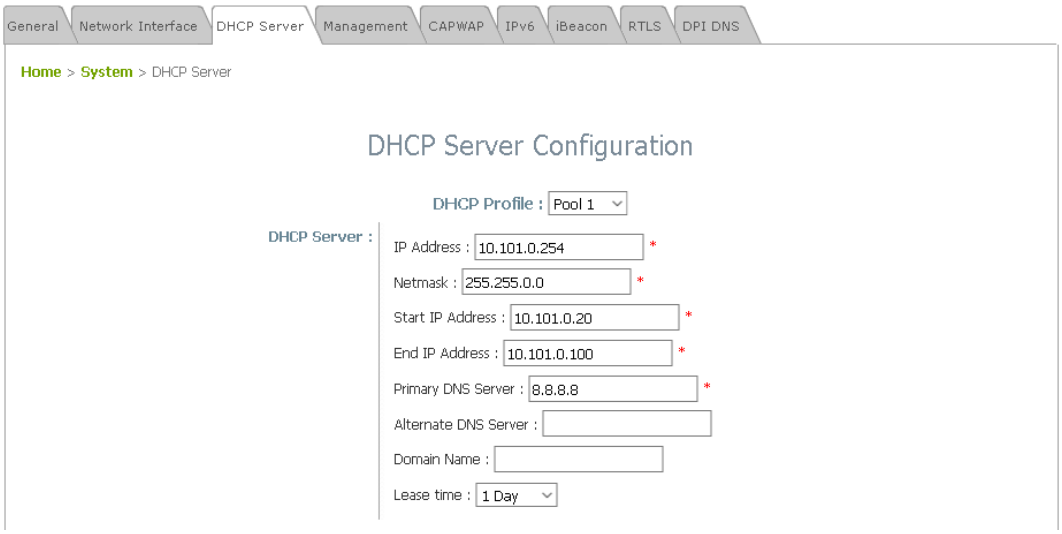
The 'TIP' in red at the bottom of the page explains that each service zone, from default to Service Zone 8, has its fixed, pre-determined VLAN ID number when utilizing CAPWAP. Admin needs to enter one of the numbers in order to direct traffic back to a certain Service Zone.

3.4 DHCP Server

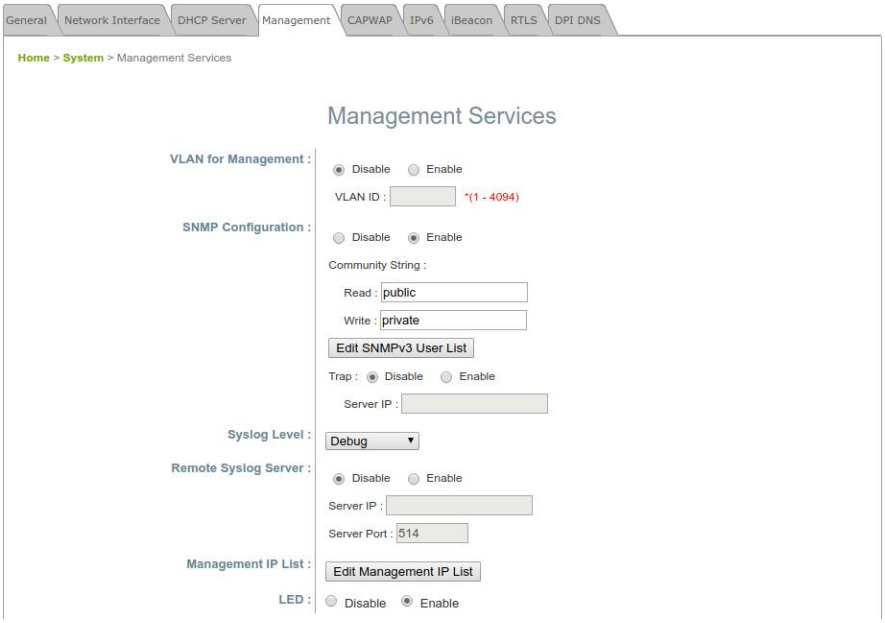
When one VAP is enabled to operate in NAT mode, associated client devices will be assigned a dynamic DHCP IP address from the configured DHCP pool on the SSID. The NAT and DHCP mode can be executed without tunnel or managed by Edgecore WLAN controller with split tunnel.



It is noted that Pool1 – Pool16 are all configured as A class DHCP IP addresses as default values, and only configurable at AP's Web Management Interface. It starts from 10.101.0.254/16 to 10.116.0.254/16 for 16 DHCP Profiles, and DHCP lease time is 1440 minutes in default.



3.5 Management



VLAN for Management: When this is enabled, management traffic from the system will be tagged with a VLAN ID. In other words, administrators who need to access the WMI must send management traffic with the same VLAN ID such as connecting to a specific VAP with the same VLAN ID. Enter a value between 1 and 4094 for the VLAN ID if the option is enabled.

SNMP Configuration: to obtain the system information remotely.

- **Enable/ Disable**: *Enable* or *Disable* this function.
- **Community String:** The community string is required when accessing the Management Information Base (MIB) of the system. **Read:** Enter the community string to access the MIB with Read privilege. **Write:** Enter the community string to access the MIB with Write privilege.
- **Edit SNMPv3 User List:** The system allows 5 SNMP Users with Read or Read & Write Access. Determine the Name and Authentication Password on the SNMP Account List.
- **Trap:** When enabled, events on Cold Start, Interface UP & Down, and Association & Disassociation can be reported to the assigned server.
- **Server IP Address:** Enter the IP address of the assigned server that will receive the trap report.

Syslog Level: Select the desired level of received events from the drop-down menu. “Debug” level is as default setting.

Remote Syslog Server: When this function is enabled, specify an external SYSLOG server to receive SYSLOG messages from the system remotely.

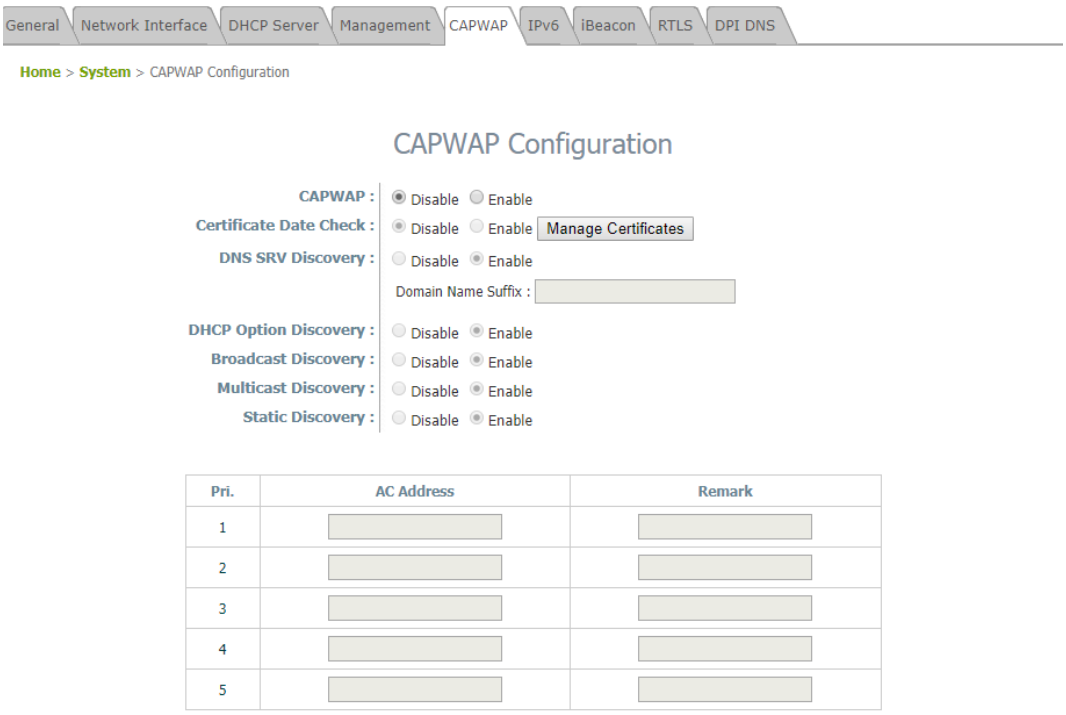
- **Enable/ Disable**: *Enable* or *Disable* this function.
- **SYSLOG Server IP:** The IP address of the Syslog server that will receive the reported events.
- **Server Port:** The port number of the Syslog server.

Management IP List: Enter source IP address/subnet of administrator PCs which are allowed to access the WMI of this AP. Anyone else that is not on this List will be denied for WMI access. The default entry 0.0.0.0/0.0.0.0 means that administrators are allowed to access the WMI from anywhere.

LED: To turn on or off the Status LED indicator on the AP.

3.6 CAPWAP

CAPWAP is a standard interoperable protocol that enables a controller to manage a collection of wireless access points. There are 5 methods of auto AP discovery, namely DNS SRV, DHCP option, Broadcast, Multicast, and Static.



CAPWAP: Enable or Disable the CAPWAP feature.

Certificate Date Check: To enable this item, select *Enable* and click *Manage Certificates* to enter the Upload Certificate page. Please refer to the section 4.4.5 Upload Certificate.
DNS SRV Discovery: Using DNS SRV to discover acess controller.

- **Domain Name Suffix:** Enter the suffix of the access controller, such as example.com.

DHCP Option Discovery: Using DHCP option to discover access controller.

Broadcast Discovery: Using Broadcast to discover access controller.

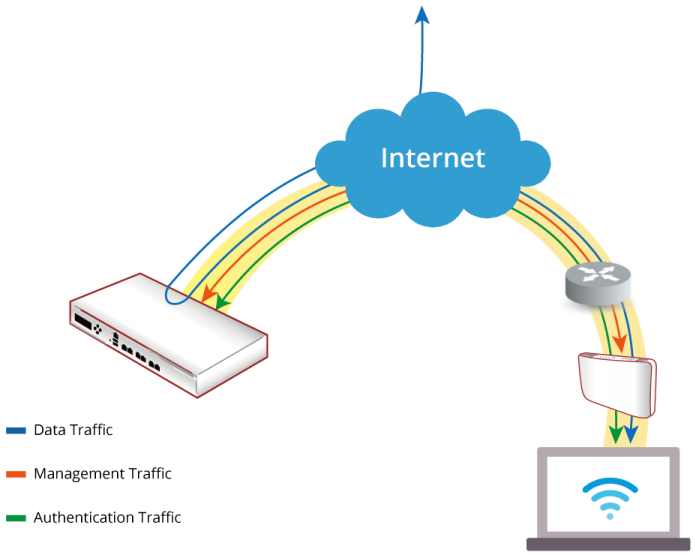
Multicast Discovery: Using muticast to discover access controller.

Static Discovery: Using Static approach to discover access controller.

- **AC Address:** The IP address of the access controller. If it can not discover the first AC, it will try to discover the second AC.

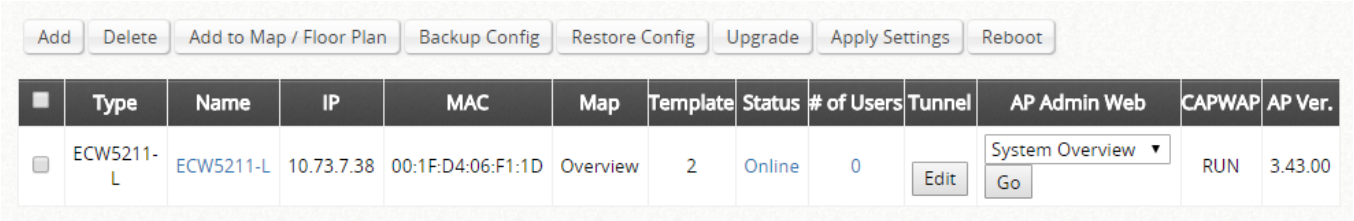
3.6.1 To Managed by WLAN Controller with Complete Tunnel

Complete Tunnel uses the CAPWAP protocol to communicate with an Access Point so that all management traffic, authentication traffic and data traffic from the service area AP provided are transmitted back to the Controller, before forwarding data traffic to the internet. The WLAN controller is able to implement role-based policies over Layer 3 networks, with user access control available in the remote sites. This feature allows the WLAN controller to fully support centralized AP management and user management.

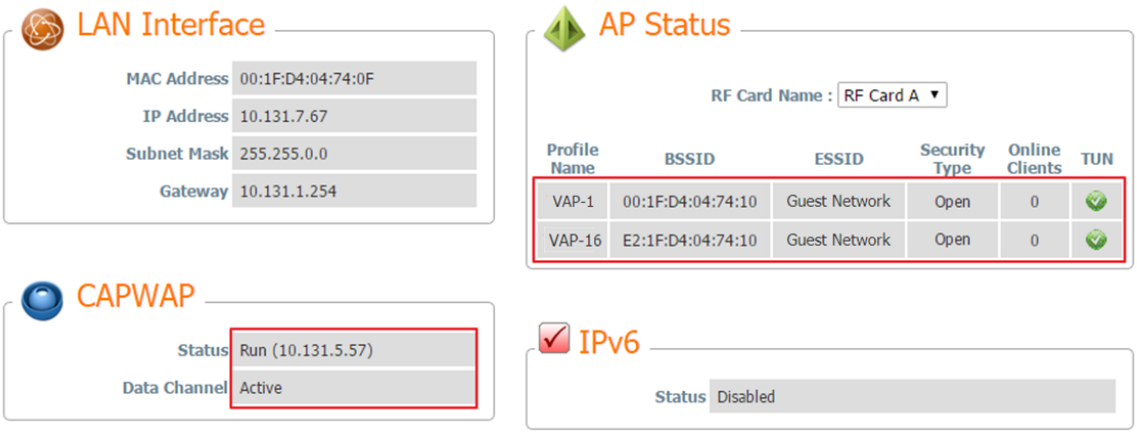


The following procedures may be helpful

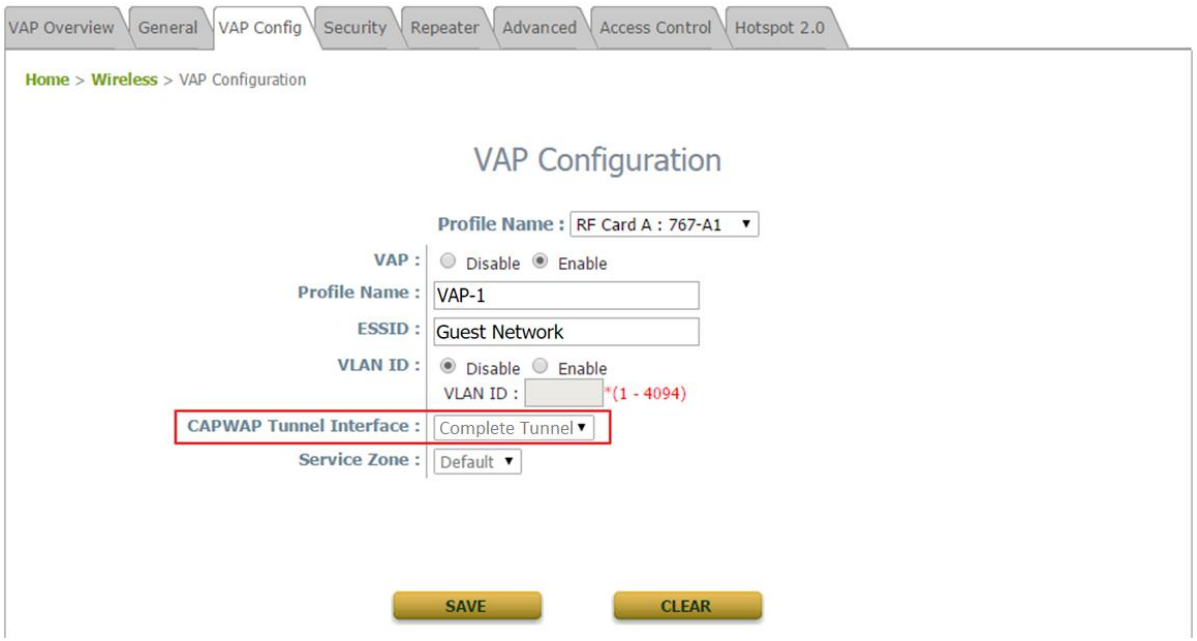
1. On AP: to type the IP address for **Static Discovery**, and wait until the CAPWAP column displays a "RUN" status.
2. On EWS: to prepare Template of the **VAP configuration** with **CAPWAP Tunnel Interface** – "**Complete Tunnel**"
3. On EWS: to apply the prepared Template to the CAPWAP-establish AP and the Tunnel status will show a clickable "Edit" button in black if a VAP is configured to be tunneled back to the controller.



4. On AP: to check the AP WMI showing Data Channel is “Active” with the VAP tunnel status in “Green” light on the System Overview page

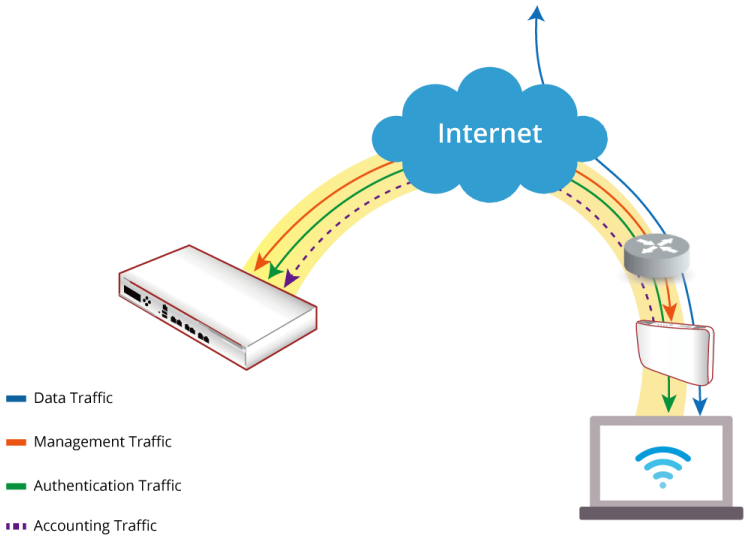


5. On AP: to reconfirm the specific VAP Configuration is under **Complete Tunnel**



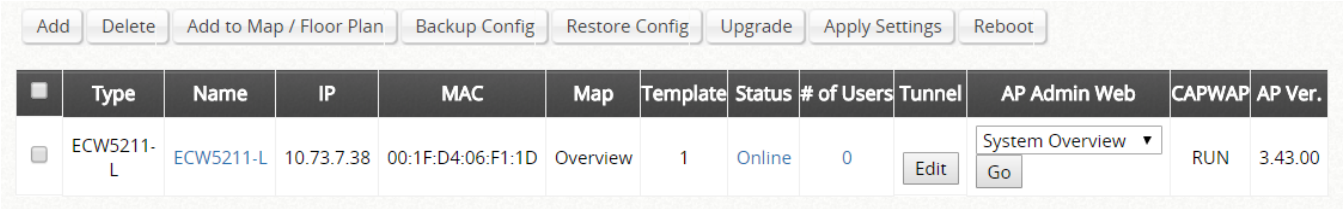
3.6.2 To Managed by WLAN Controller with Complete Tunnel

For **Split tunnel,** only user authentication related traffic will be directed back to the controller. For authenticated users, data traffic will go to the Internet through the local network directly. The user data can be transmitted with a shorter path and the network load of the controller can also be reduced.

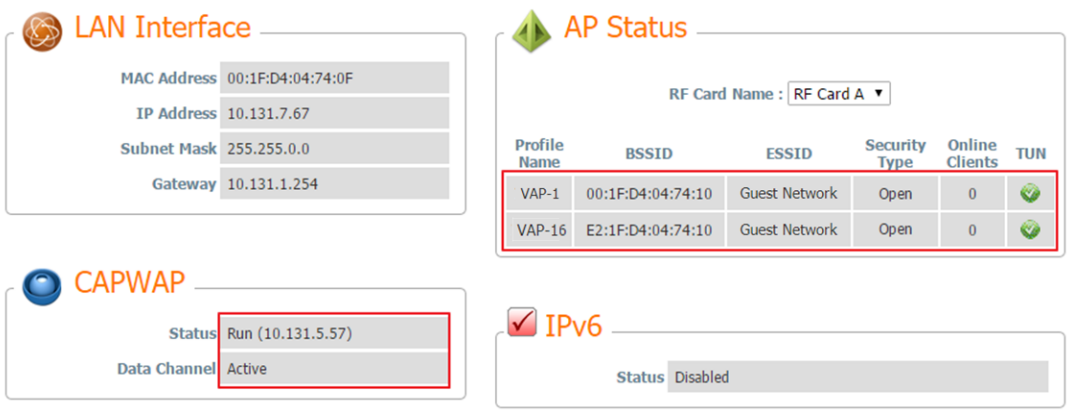


The following procedures may be helpful

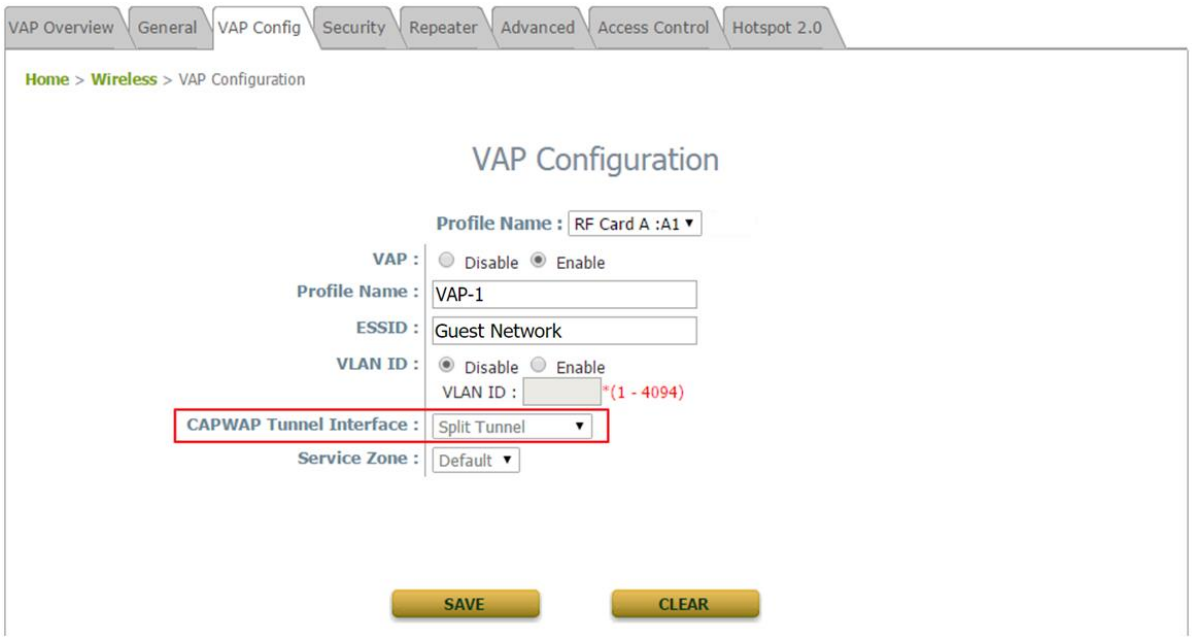
1. On AP: to type the IP address for **Static Discovery**, and wait until the CAPWAP column displays a "RUN" status.
2. On EWS: to prepare Template of the **VAP configuration** with **CAPWAP Tunnel Interface** – "**Split Tunnel**"
3. On EWS: to apply the prepared Template to the CAPWAP-establish AP and the Tunnel status will show a clickable "Edit" button in black if a VAP is configured to be tunneled back to the controller.



4. On AP: to check the AP WMI showing Data Channel is "Active" with the VAP tunnel status in "Green" light on the System Overview page

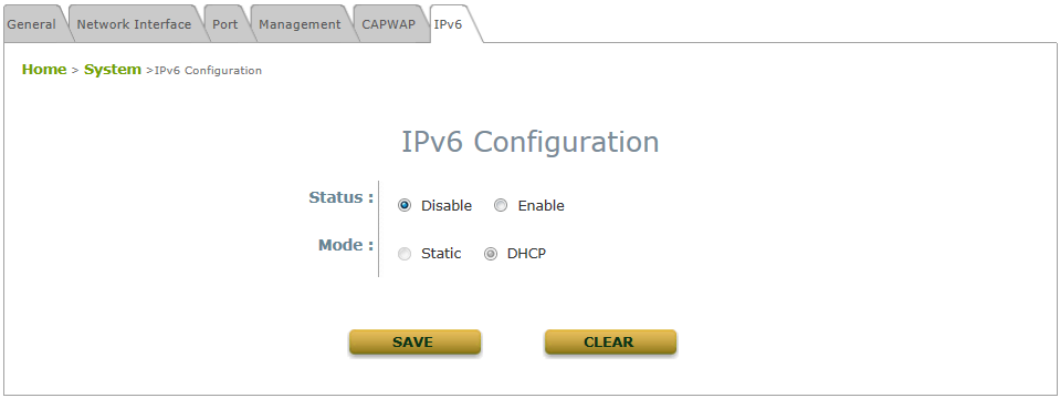


5. On AP: to reconfirm the specific VAP Configuration is under **Split Tunnel**



3.7 IPv6

IPv6 and IPv4 dual stack addressing capability is supported.



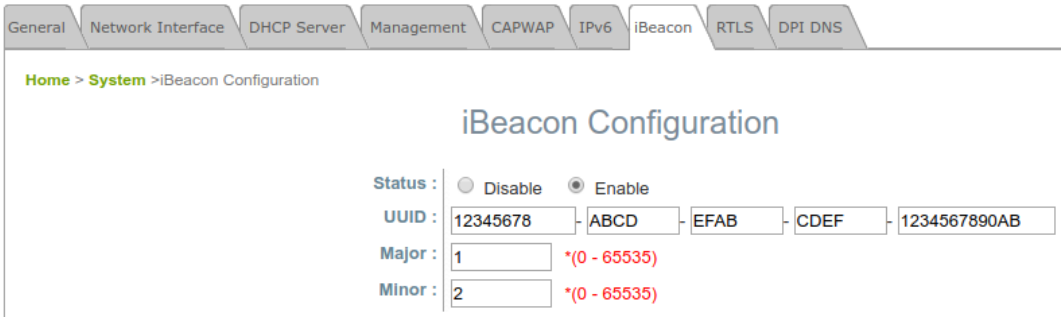
Status: IPv6 by default is disabled but it can be enabled on this tab page.

Mode: There are two options for acquiring an IPv6 address for this device.

- **Static:** Configuring IPv6 address manually via this option if you have already acquired a permanent IPv6 address for operation.
- **DHCP:** Acquire IPv6 address automatically from upstream server.

3.8 iBeacon

iBeacon is a technology, introduced by Apple in 2013, enabling new location awareness services. When properly configured, the AP becomes an iBeacon-compatible hardware transmitter which broadcasts information to nearby devices via Bluetooth Low Energy (BLE; a wireless connectivity technology).



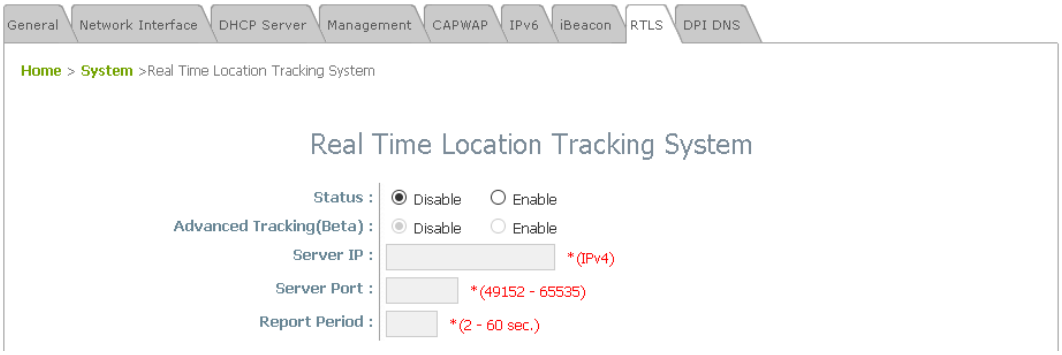
The UUID, Major and Minor are the identifying parameters used to make up the key component of the iBeacon "Advertising Packets" that are continually transmitted by the AP.

UUID: Universally Unique Identifier, a number to distinguish your own AP in the network, from all other iBeacon transmitters in networks outside your control. It contains 32 hexadecimal digits, split into 5 groups and should look something like this: 12345678-ABCD-EFAB-CDEF-1234567890AB

Major & Minor: These are numbers (integer values between 0 and 65535) assigned to your own AP in order to identify the AP with greater accuracy than using UUID alone. Normally, Major value is intended to identify and distinguish a group, while Minor value is intended to identify and distinguish an individual. For example, if there are many iBeacon transmitters deployed with the same UUID in a shopping center, and they are located at different floors/stores. Then these transmitters can be identified and distinguished by different Major (e.g. 1 for 1st floor) and Minor (e.g. 2 for 2nd store) values.

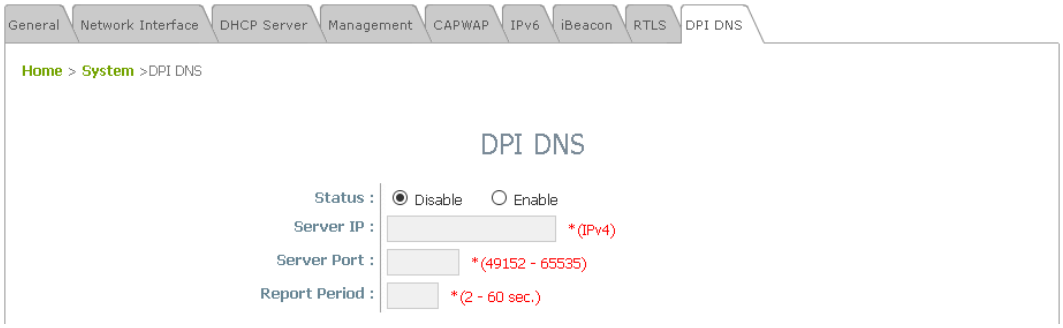
3.9 RTLS

To implement a Wi-Fi based location solution, customers can enable this feature to integrate the AP with the dedicated Linkyfi (Edgecore technology partner) server of Real Time Location System (RTLS), which is part of Linkyfi Location Engine - an advanced software solution for indoor location and real-time navigation in all types of venues.



3.10 DPI DNS

To perform WiFi marketing analytics, customers can enable this feature to integrate the AP with Linkyfi's DNS server, which is also part of Linkyfi Location Engine that analyzes DNS traffic via Deep Packet Inspection (DPI) technology.

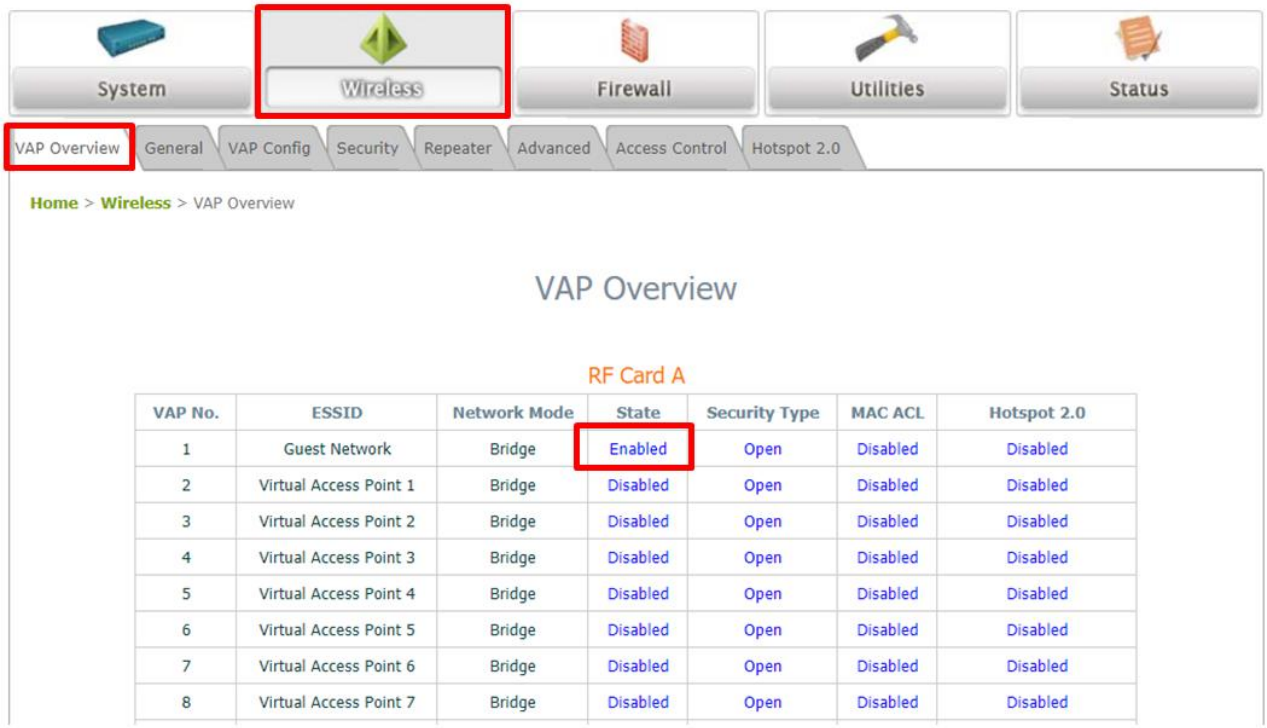


4. Wireless

This section includes the following functions: **VAP Overview**, **General**, **VAP Configuration**, **Security**, **Repeater**, **Advanced**, **Access Control** and **Hotspot 2.0**. The Edgecore Access Point supports up to sixteen Virtual Access Points (VAPs) per RF card. Each VAP can have its own settings (e.g. ESSID, VLAN ID, security settings, etc.). With such VAP capabilities, different levels of service can be configured to meet network requirements.

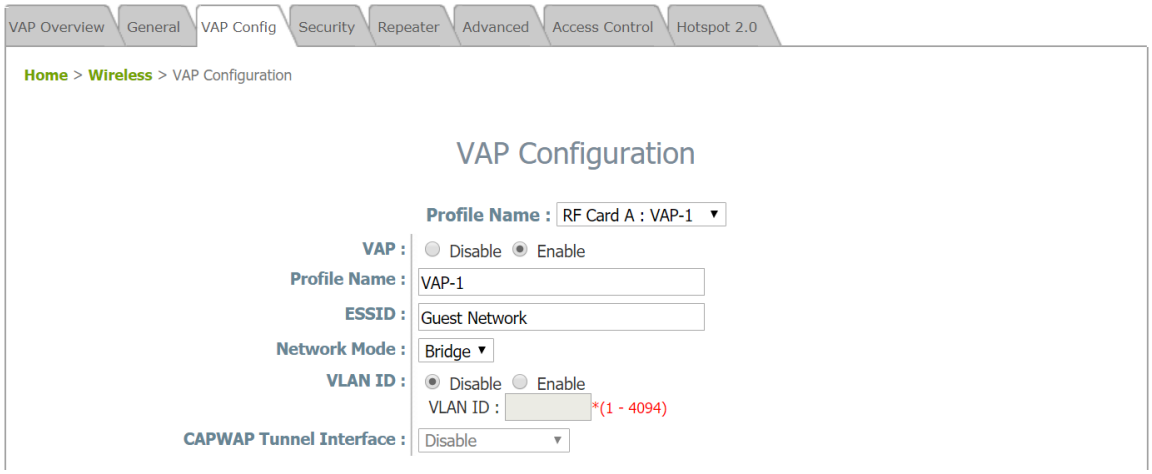
4.1 VAP Overview

An overall status is collected on this page, including **ESSID**, **Network Mode**, **State**, **Security Type**, **MAC ACL**, and **Hotspot 2.0,** where the AP features 16 VAPs per radio with respective settings. In this table, please click on the hyperlinks to further configure each individual VAP.



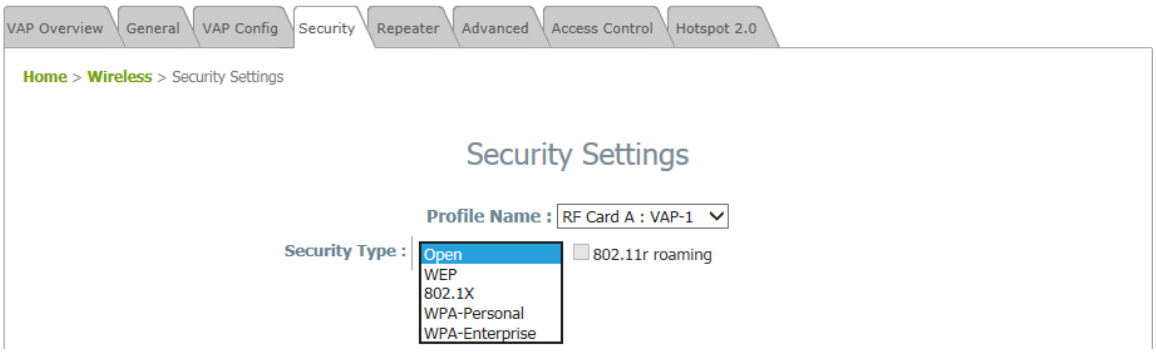
VAP No.	ESSID	Network Mode	State	Security Type	MAC ACL	Hotspot 2.0
1	Guest Network	Bridge	Enabled	Open	Disabled	Disabled
2	Virtual Access Point 1	Bridge	Disabled	Open	Disabled	Disabled
3	Virtual Access Point 2	Bridge	Disabled	Open	Disabled	Disabled
4	Virtual Access Point 3	Bridge	Disabled	Open	Disabled	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: The hyperlink showing ***Enable*** or ***Disable*** links to the **VAP Configuration** page.



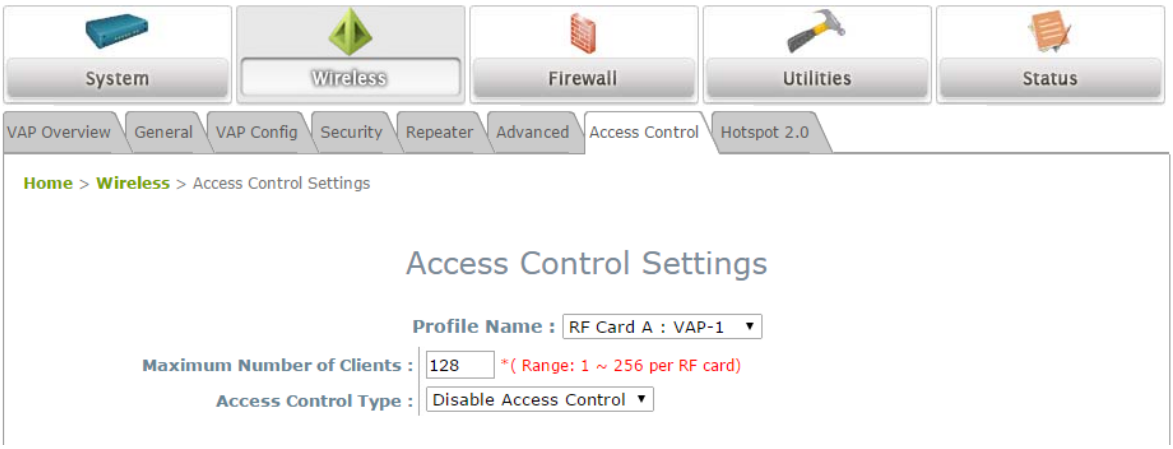
VAP – State Page

Security Type: The hyperlink showing the security type links to the **Security Settings** Page.



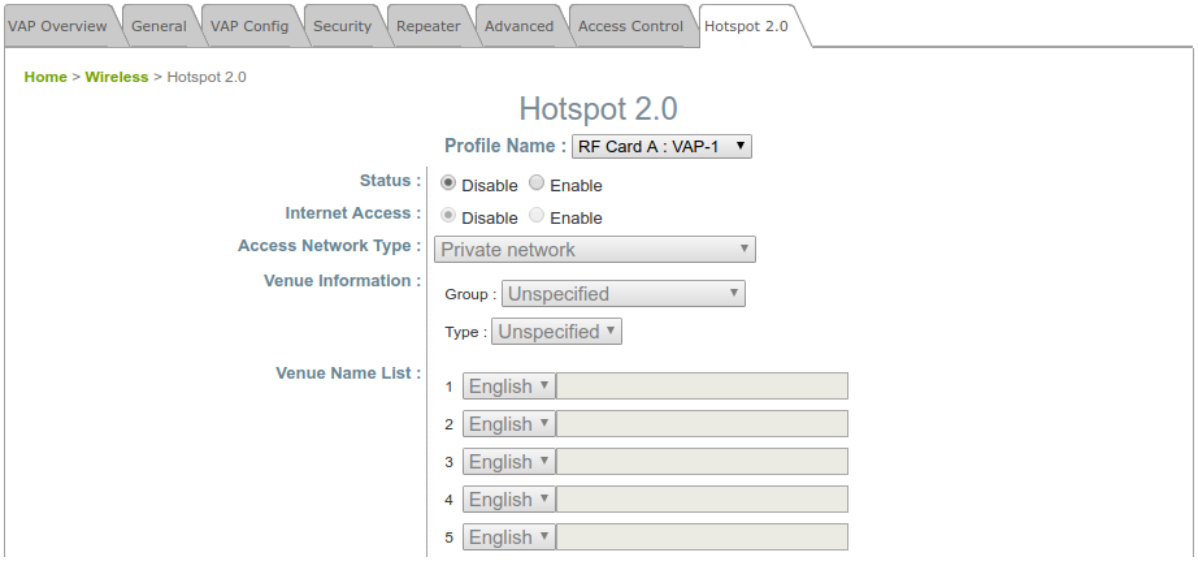
VAP – Security Type Page

MAC ACL: The hyperlink showing **Allow** or **Disable** links to the **Access Control Settings** Page.



VAP – MAC ACL Page

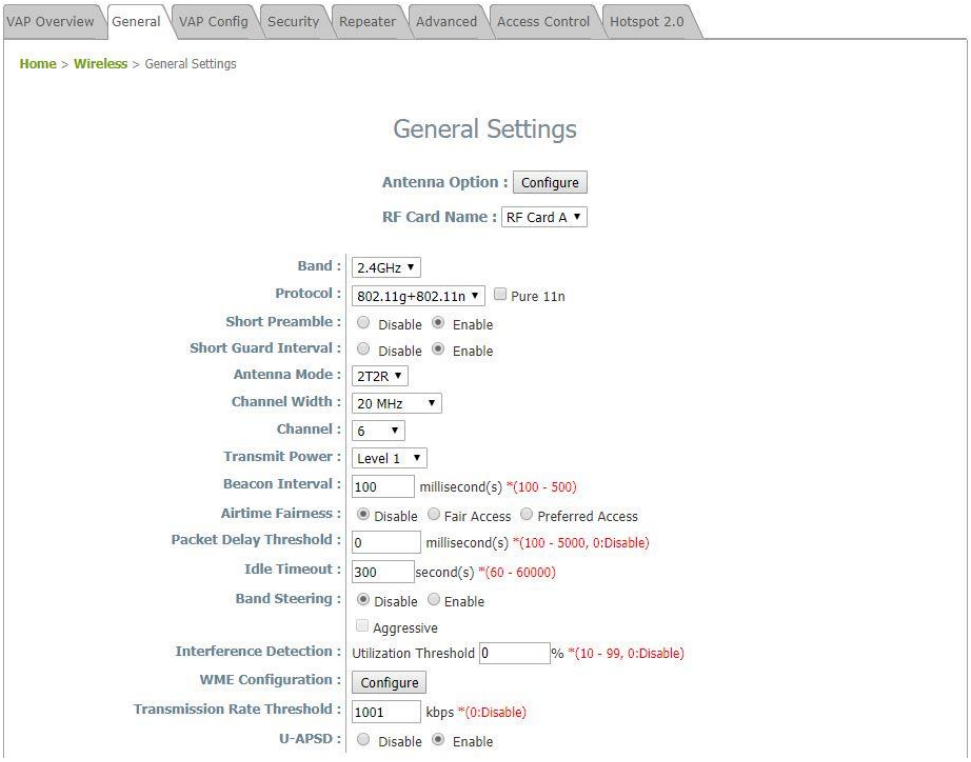
Hotspot 2.0: The advanced settings hyperlink links to the **Hotspot 2.0** Page.



VAP – Hotspot 2.0 Page

4.2 General

AP's system general wireless settings can be configured



Antenna Option (OAP100 Only): The device comprises four antennas, two for 2.4GHz and two for 5GHz. There are two options for different services.

- **Hotspot:** Use for hotspot purposes. Two 2.4GHz adopt omni antennas, used to providing services for clients; two 5GHz adopt directional antennas with 30 degrees of azimuth and elevation, used for point to point connections.
- **Point to Point:** Use for point-to-point purposes. Two 2.4GHz and two 5GHz both adopt directional antennas with 90 degrees of azimuth and 30 degrees of elevation.

RF Card Name: Select one RF card for further configuration.

Band: Select ***Disable*** if the wireless function is not required.

Protocol: Select an appropriate wireless protocol: ***802.11a***, ***802.11a+802.11n***, ***802.11ac*** or ***802.11b***, ***802.11g***, ***802.11b+802.11g***, ***802.11g+802.11n***. The protocol is dependent or the **Band** of the **RF Card**.

- **Pure 11n:** Enable 802.11nnetwork only.

Short Preamble: The short preamble with a 56-bit synchronization field can improve WLAN transmission efficiency. Select ***Enable*** to use Short Preamble or ***Disable*** to use Long Preamble with a 128-bit synchronization field.

Short Guard Interval (available when Band is 802.11g+802.11n or 802.11a+802.11n or 802.11ac): The guard interval is the space between symbols (characters) being transmitted to eliminate inter-symbol interference. In order to further boost throughput with **802.11n**, short guard interval is half of what it used to be; please select ***Enable*** to use Short Guard Interval or ***Disable*** to use normal Guard Interval.

Antenna Mode: Select the number of spatial streams for the RF card – select 1T1R for one spatial
Select 1T1R for one spatial stream or 2T2R for two spatial streams.

Channel Width (available when Band is 802.11g+802.11n or 802.11a+802.11n or 802.11ac): Double channel bandwidth to 40 MHz or 80 MHz to enhance throughput.

Channel: Select the appropriate channel from the drop-down menu to meet the regularity.

- When configured as "Auto" in Radio Card B, there is channel selector table for channel switching when the chosen channel is interfered or DFS channel signal is detected
- For outdoor AP models, the "Outdoor mode" will affect the channel selection

Channel Selector: This option is displayed for RF card B when Band is set to 5GHz and Channel is set to Auto or DFS channels. Select the desired channels for operation so that

- When the system boots up and Channel is set to Auto, the system would choose a channel from the selected channels based on which channel is clearer.
- When the system decides that it will switch to another channel due to reasons such as when radar signal is detected on a DFS channel, or when interference threshold (if set) is reached, it will only switch to one of the selected channels based on which channel is clearer.

Transmit Power: The signal strength transmitted from the system can be selected by Levels.

- Each Level signifies a decrement of 1dBm from the highest power.
- Level 1 is the actual highest power, while Level 2 is the highest power minus 1dBm, so on and so forth.

Distance: It refers to the distance from the system to the client or to another access point when connected via WDS. After entering a value for distance, the value of ACK Timeout below will be auto-adjusted.

ACK Timeout: It indicates a period of time when the system waits for an Acknowledgement frame sent back from a station without retransmission. In other words, upon timeout, if the Acknowledgement frame is still not received, the frames will be retransmitted. This option can be used to tune network performance for extended coverage. For regular indoor deployments, please keep the default setting.

Beacon Interval (ms): The entered amount of time indicates how often the beacon signal will be sent from the access point.

- The Beacon Interval must be greater than 500ms when more than 7 VAPs are enabled.
- The Beacon Interval must be greater than 250ms when more than 3 VAPs are enabled

Airtime Fairness: when 802.11a/b/g/n legacy devices occupy airtime, throughput for 802.11ac devices is affected.

- **Enable:** to ensure all devices with different band compatibilities have the same air time. This feature is ideal for networks with devices supporting different bands.
- **Preferred Access:** N band clients are prioritized. This feature is ideal for networks with devices supporting different bands.

Packet Delay Threshold (ms): An Access Point may be occupied trying to transmit a packet to a busy client or a client out of range, hence delaying transmission to other connected clients. When Enabled, this Tx queue flushing mechanism drops packets and immediately begins to process others if the queue has been processed for more than x milliseconds, where Default = 0 (disabled). This feature improves the performance of complex wireless networks but may require some packets to be resent.

Idle Timeout (s): Client disconnects when inactivity reaches the configured amount of time in seconds, where default = 300s.

Band Steering: When enabled, clients with 5GHz connectivity will be steered towards the 5GHz band to reduce congestion in the 2.4GHz band. This is applicable only when the AP is set to 2.4GHz and 5GHz on the 2 RF Cards.

- **Aggressive:** clients with 5GHz connectivity are forced to connect to the 5GHz band.
- Note that this is a general setting for the Access Point, and is not set per RF Card.

Interference Detection: When Utilization, Latency (and Invalid Packet Rate) of the current channel or adjacent channel reaches the configured threshold (in %), the AP switches to a different Channel.

WME Configuration: Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. Access priority can be configured using with different parameters. CW Min: Contention Window Minimum, CW Max: Contention Window Maximum, AIFS: Arbitration Inter Frame Spacing, TXOP Limit: Transmission Opportunity Limit.

Transmission Rate Threshold: The client will be kicked when transmission rate is lower than the configured threshold. This ensures high connection speed for all associated clients.

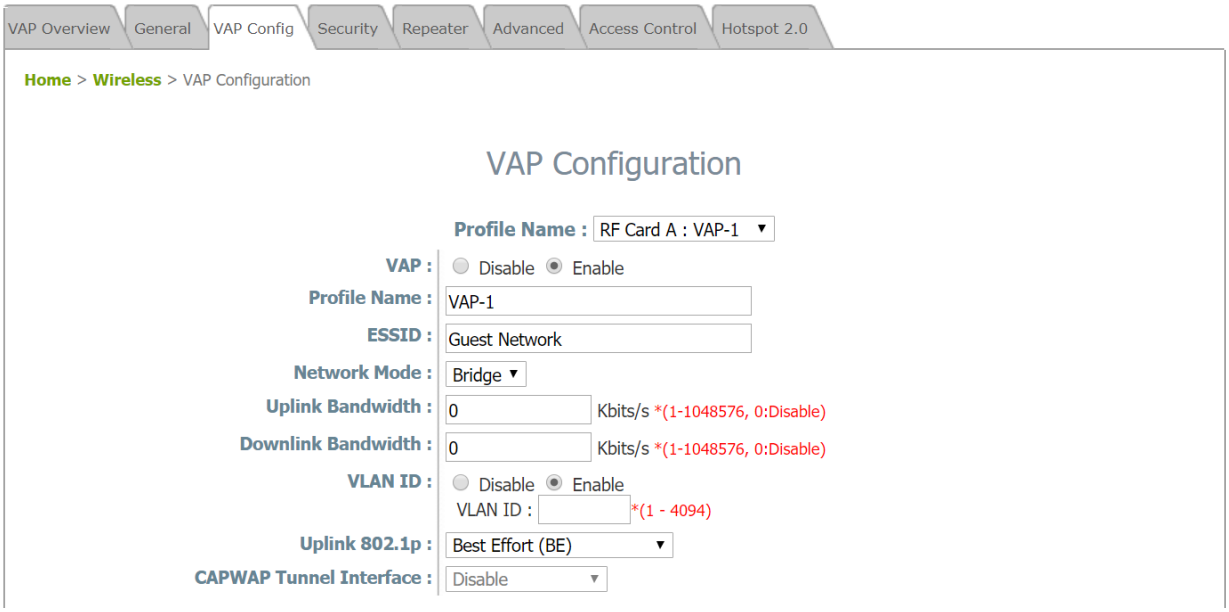
CCA Minimum Power: Clear Channel Assessment (CCA) is a method to determine if a radio frequency is occupied. CCA Minimum Power is the minimum signal strength the system considers resolvable, that is, the received signal is treated as noise if the power level is lower than CCA Minimum Power.

U-APSD: U-APSD stands for **U**nscheduled **A**utomatic **P**ower **S**ave **D**elivery, an 802.11 power save mechanism that works with WMM. When a client device is in Power Save mode (i.e. its receiver is turned off and thus cannot receive any data frames), the AP will temporarily buffer all frames destined to the client.

Note: Features such as Short Preamble, ACK Timeout, and may be limited on RF Card B.

4.3 VAP Config

This section provides configuration of each Virtual Access Point with settings such as **Profile Name**, **ESSID**, and **VLAN ID**. To enable specific VAP, select the VAP from the drop-down list of Profile Name.

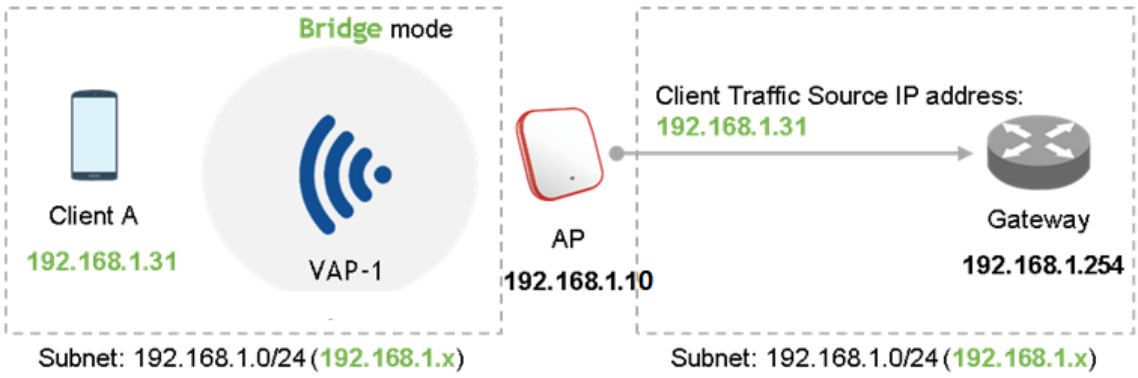


VAP: Disable or Enable this VAP.

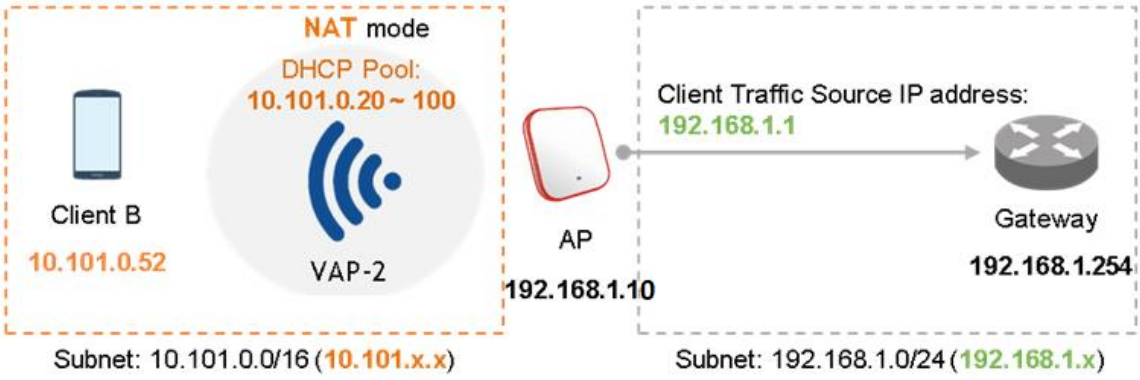
Profile Name: Name of the VAP profile for identity / management purposes.

ESSID: Extended Service Set Identifier (ESSID) serves as an identifier for clients to associate with the specific VAP.

Network Mode – Bridge mode: the VAP operates transparently (i.e. no NAT, no DHCP) such that client devices will be assigned a dynamic IP address from a DHCP server on the LAN side. The source IP address of client traffic seen by the uplink gateway/switch will remain the original IP address of the client (in this case, 192.168.1.31, as shown in the diagram below).



Network Mode – NAT mode: the VAP operates like a Network Address Translation (NAT) device with a built-in DHCP server on this SSID such that client devices will be assigned a dynamic IP address from the configured DHCP pool on this SSID. After NAT conversion, the source IP address of client traffic seen by the uplink gateway/switch will be the IP address of the AP (in this case, 192.168.1.10, as shown in the diagram below).



Uplink/Downlink Bandwidth: Bandwidth control is configurable on the VAP in Kbits per second. Set 0 for unlimited bandwidth control.

VLAN ID: Per-SSID VLAN tagging function – when enabled, clients' traffic which enters the AP through this SSID will be tagged with the configured VLAN ID.

Uplink 802.1P per VAP: Priority levels for uplink traffic can be selected here. The options available are Background, Best Effort, Excellent Effort, Critical Applications, Video, Voice, Internetwork Control, Network Control. For more information, please refer to IEEE Standards 802.1P.

DHCP Profile (for NAT mode): Built-in DHCP Server profile; IP settings of DHCP Server are under Home > System > DHCP Server.

CAPWAP Tunnel Interface: Three states indicating the connectivity between AP and Controller, when AP is managed by Controller

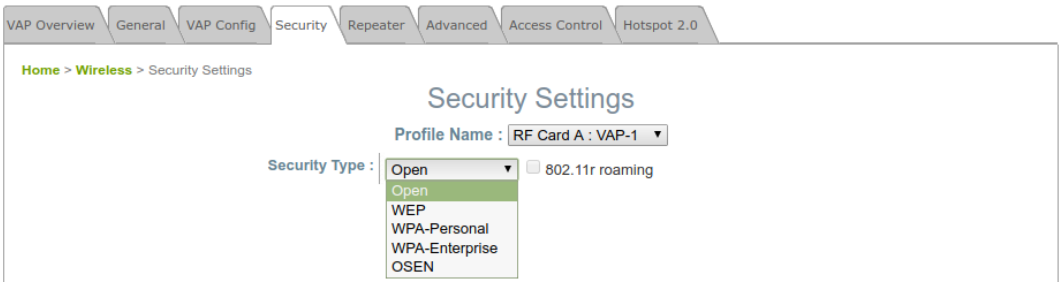
- **Disable** (No Tunnel)**:** the AP is operating with no CAPWAP Tunnel connection to the Controller
- **Split Tunnel:** the AP passes only "control" traffic to the Controller via the CAPWAP Tunnel; i.e. "data" traffic will go out locally without passing through the Tunnel
- **Complete Tunnel:** the AP passes both "control" and "data" traffic to the Controller via the CAPWAP Tunnel

Note:

- VLAN ID is supported only when the VAP is in Bridge mode.
- DHCP Profile and DHCP Server are activated only when the VAP is set to NAT mode.
- If the VAP is in NAT mode, the CAPWAP Tunnel Interface will only work in two states:Disable (No Tunnel) or Split Tunnel.

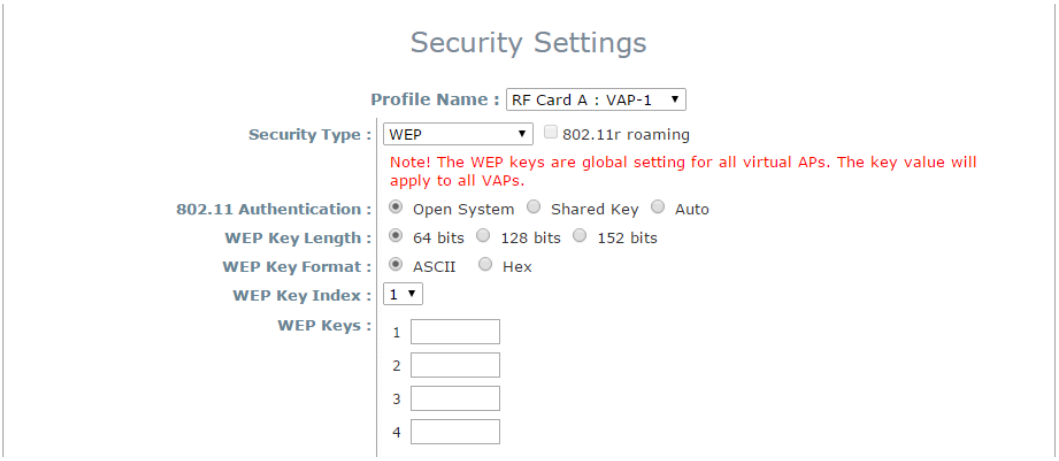
4.4 Security

The AP supports various wireless authentication and data encryption methods in each VAP profile. With this, the administrator can provide different service levels to clients. The security type includes **Open**, **WEP**, **WPA-Personal**, **WPA-Enterprise**, and **OSEN**.



Open: Authentication is not required and data is not encrypted during transmission.

WEP: Wired Equivalent Privacy is a data encryption mechanism based on a 64-bit, 128-bit, or 152-bit shared key algorithm.

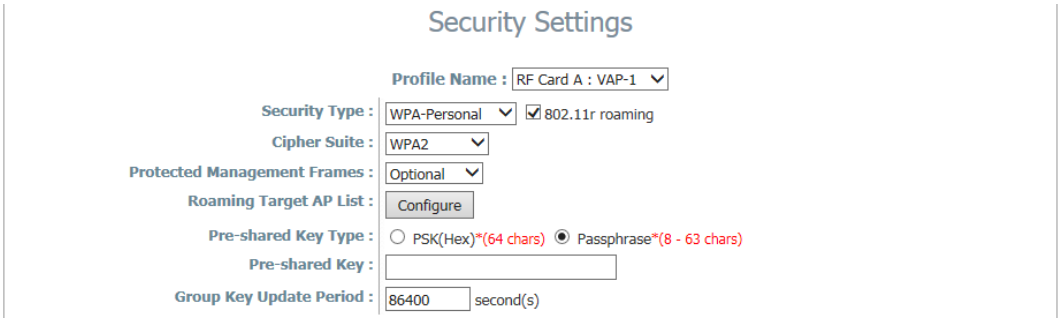


- **802.11 Authentication**: Select from *Open System*, *Shared Key*, or *Auto*.
- **WEP Key Length**: Select a key length from *64-bit*, *128-bit*, or *152-bit*.
- **WEP Key Format:** Select a WEP key format from ***ASCII*** or ***Hex***.
- **WEP Key Index:** Select a key index from ***1~4***. The WEP key index is a number that specifies which WEP key will be used for the encryption of wireless frames during data transmission.
- **WEP Keys:** Provide the pre-defined WEP key value; the system supports up to 4 sets of WEP keys.

Note: Its WEP key length may be limited on selected AP models.

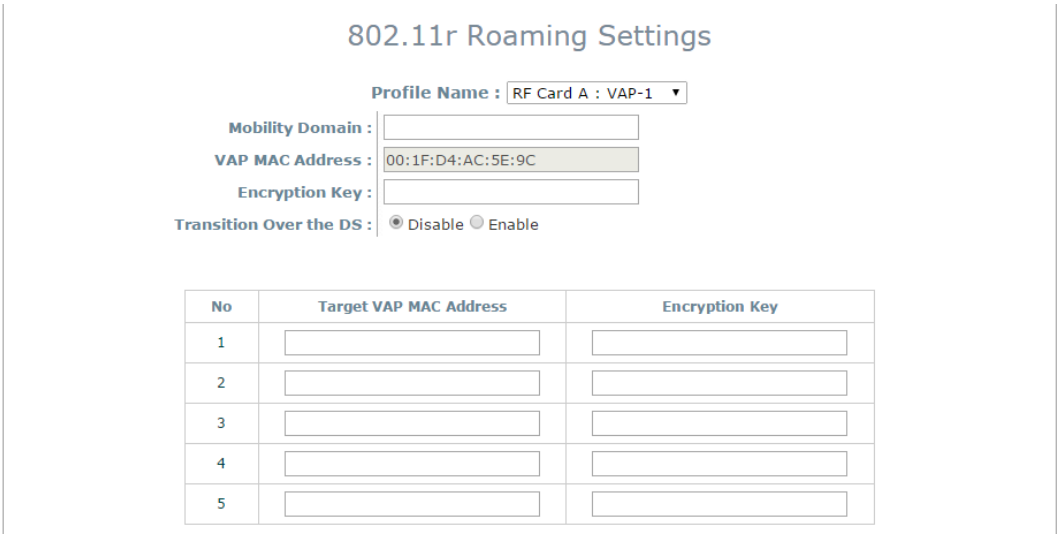
WPA-Personal: WPA-Personal is a Pre-Shared Key (PSK) authentication method.

- **802.11r Roaming:** Roaming is possible for clients within the same Mobility Domain on different APs with the same Encryption Key.



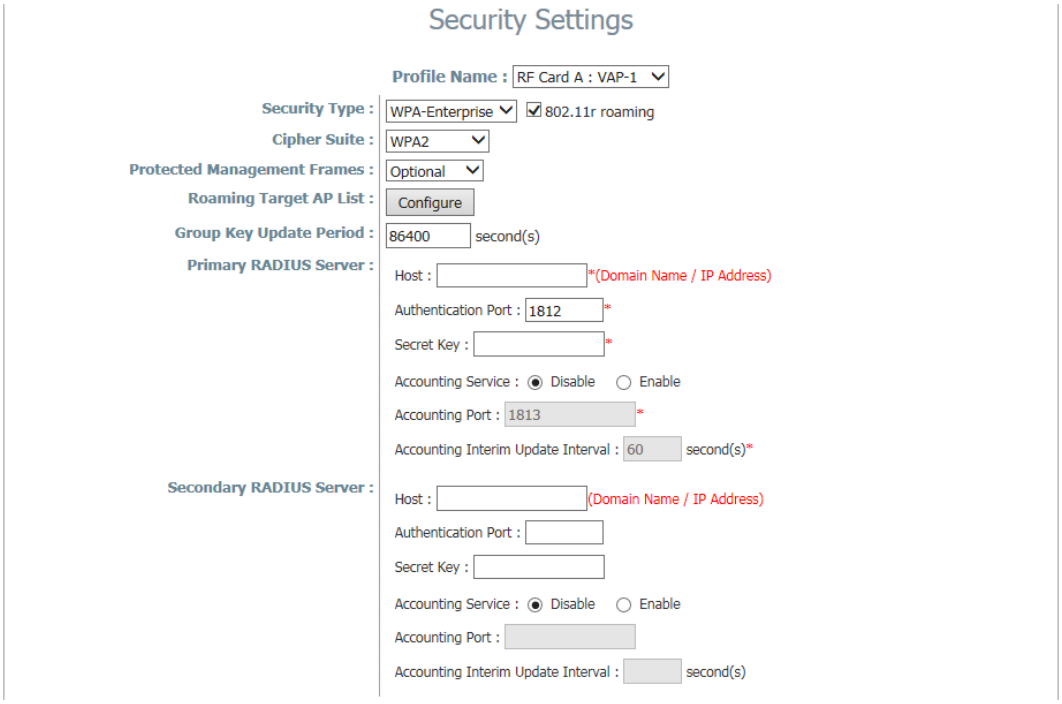
Security Settings: WPA-Personal

- **Cipher Suite:** Select an encryption method from ***WPA2*** or ***WPA2/WPA***.
- **Protected Management Frames**: Select Disable, Optional or Mandatory.
- **Roaming Target AP List** (when 802.11r is enabled)



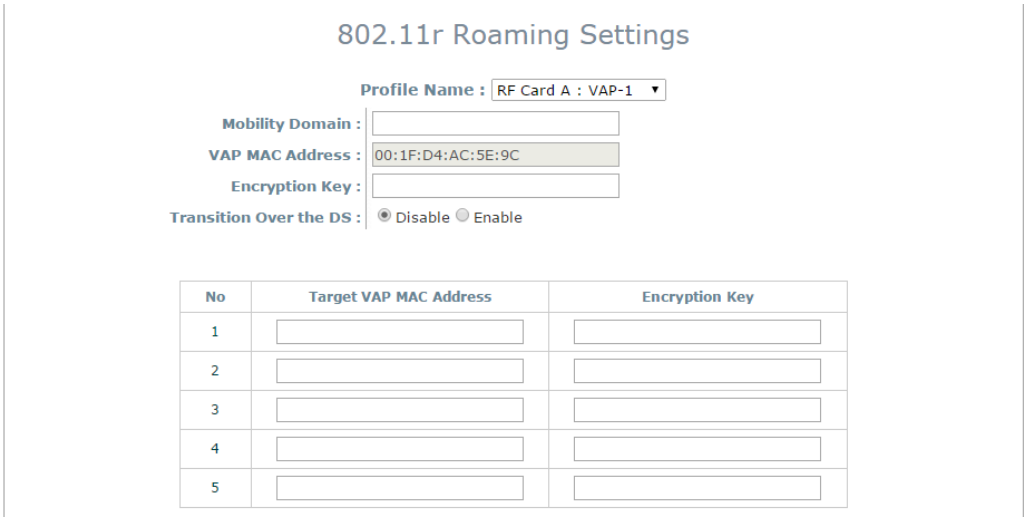
- **Pre-shared Key Type:** Select a pre-shared key type: PSK (Hex) or Passphrase.
- **Pre-shared Key:** Enter the key value for the pre-shared key; the format of the key value depends on the key type selected.
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.

WPA-Enterprise: When selected, the RADIUS authentication and data encryption will both be enabled.



Security Settings: WPA-Enterprise

- **Cipher Suite:** Select an encryption method from ***WPA2*** or **WPA2/WPA**.
- **Protected Management Frames**: Select Disable, Optional or Mandatory.
- **Roaming Target AP List** (when 802.11r is enabled)



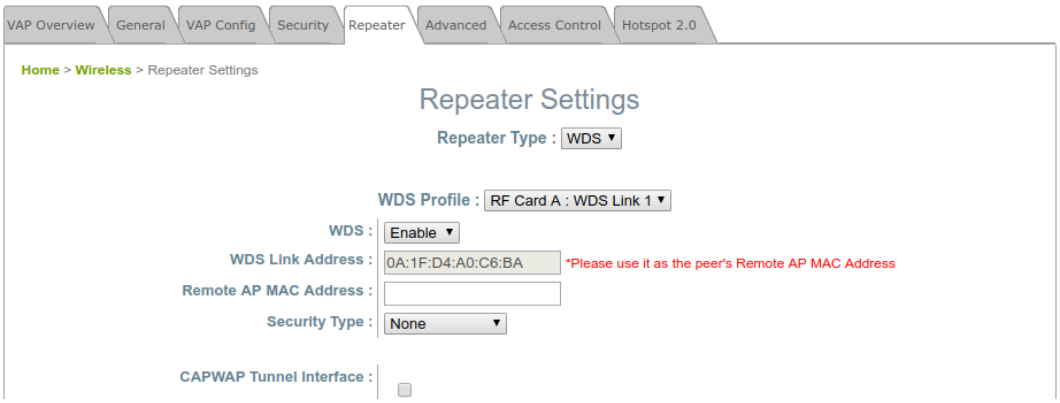
- **Group Key Update Period:** The time interval for the Group Key to be renewed; the time unit is in seconds.
- **RADIUS Server Settings (Primary/Secondary)**:
  - **Host:** Enter the IP address or domain name of the RADIUS server.
  - **Authentication Port:** The port number used by the RADIUS server. Specify a port number or use the default, 1812.
  - **Secret Key:** The secret key for the system to communicate with the RADIUS server.
  - **Accounting Service:** *Enabling* this option allows accounting of login and logouts through the RADIUS server.

- **Accounting Port:** The port number used by the RADIUS server for accounting purposes. Specify a port number or use the default, 1813.
- **Accounting Interim Update Interval:** The system will update accounting information to the RADIUS server every interval period.

OSEN: OSEN stands for "The Online Signup (**O**SU) **S**erver-only authenticated layer 2 **E**ncryption **N**etwork, which is "Hotspot 2.0 Release2" (HS2.0 R2) authentication method. Before setting HS2.0 R2, we should check the security of each VAP, HS2.0 VAP (VAP1: WPA-Enterprise) or OSEN VAP (VAP2: OSEN). Further configuration detail; please check *"session 4.8 Hotspot 2.0."*

4.5 Repeater

The AP is capable of utilizing WDS to extend wireless network coverage. It supports up to 8 WDS links to its peer APs per radio. Fill in remote peer's MAC address and click ***SAVE*** to proceed.



WDS: *Enable* or *Disable* the selected WDS Link profile.

WDS Link Address: The MAC address of the AP interface for the selected WDS Link.

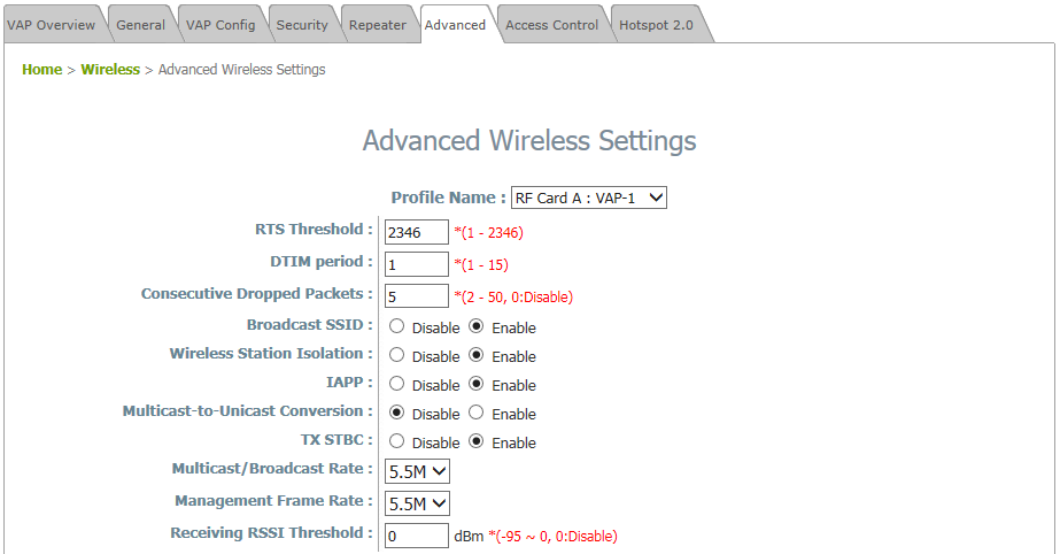
Remote AP MAC Address: The MAC address of remote peer.

Security Type: None, WEP, or WPA-Personal.

CAPWAP Tunnel Interface: Check this option to designate WDS traffic to pass through CAPWAP Tunnel established between the AP and the controller.

4.6 Advanced

The administrator can adjust the following parameters to improve network communication performance if a poor connection occurs.



RTS Threshold: Enter a value between 1 and 2346. RTS (Request to Send) Threshold determines the packet size at which the system issues a request to send (RTS) before sending the fragment to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value provided. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the AP or in areas where the clients are far apart and can detect only the AP but not each other.

Fragmentation Threshold (802.11a, 802.11b and 802.11g Modes): Enter a value between 256 and 2346. A packet size larger than this threshold will be fragmented (sent with several pieces instead of one chunk) before transmission. A smaller value results in smaller frames but allows a larger number of frames in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

DTIM Period: Input the DTIM Interval that is generated within the periodic beacon at a specified frequency. Higher DTIM will allow the wireless client to save more energy, but the throughput will be lowered.

Consecutive Dropped Packets: This is the maximum number of transmission retries the AP will attempt when packet transmission is dropped before deciding the client is out of transmission reach. When transmission retries fails for the set number of times, the Access Point kicks the client to optimize performance for other connected clients.

Broadcast SSID: Disabling this function will stop the system from broadcasting its SSID. If broadcast of the SSID is disabled, only devices that have the correct SSID can connect to the system.

Wireless Station Isolation: By enabling this function, all stations associated with the system are isolated and can only communicate with the system.

IAPP: IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations connected to them. When this function is enabled, the system will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.

Multicast-to-Unicast Conversion: When Multicast-to-Unicast Conversion is enabled, the Access Point intelligently forwards traffic only to those ports that request multicast traffic. Adversely, when disabled, multicast traffic is treated like broadcast traffic, with packets forwarded to all ports causing network inefficiencies.

TX STBC: STBC is a pre-transmission encoding done by MIMO transmitter that allows it to improve the signal-to-noise ratio even at a single RF receiver (non-MIMO).

Multicast/Broadcast Rate: Bandwidth configuration for multicast/broadcast packets. If your wireless clients require a larger or smaller bandwidth for sending multicast/ broadcast packets, the administrator can customize the Access Point's multicast/ broadcast bandwidth here.

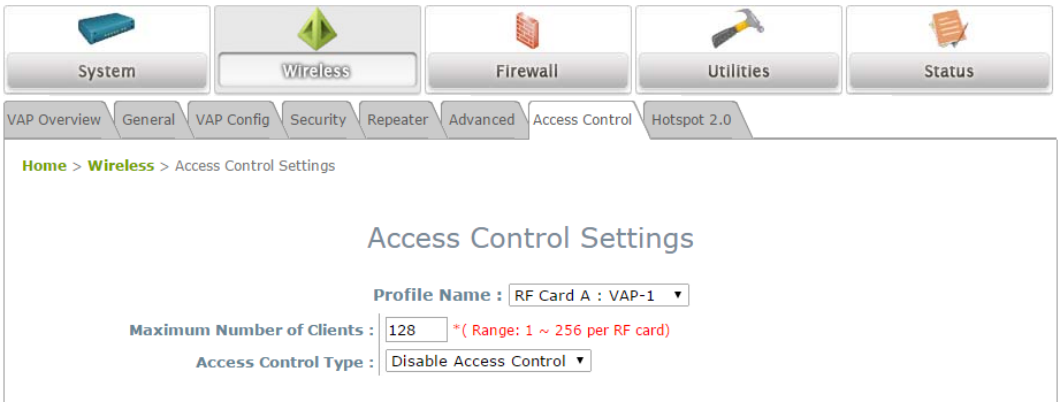
Management Frame Rate: This feature controls the bandwidth for Management Frames.

Receiving RSSI Threshold: To ensure connected stations have quality connection speeds, a station will not be able to associate to the network unless its receiving sensitivity meets the configured threshold.

Note: TX STBC may be limited on selected AP models.

4.7 Access Control

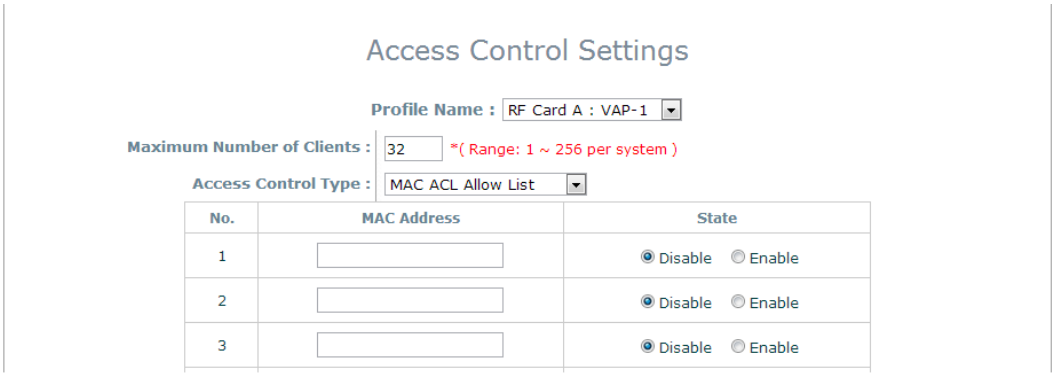
On this page, the network administrator can restrict the total number of clients connected to the Access Point, as well as specify particular MAC addresses that can or cannot access the device.



Maximum Number of Clients: The default policy is unlimited access without any authentication requirement. To restrict the station number of wireless connections, simply change the value to a desired number. For example, when the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

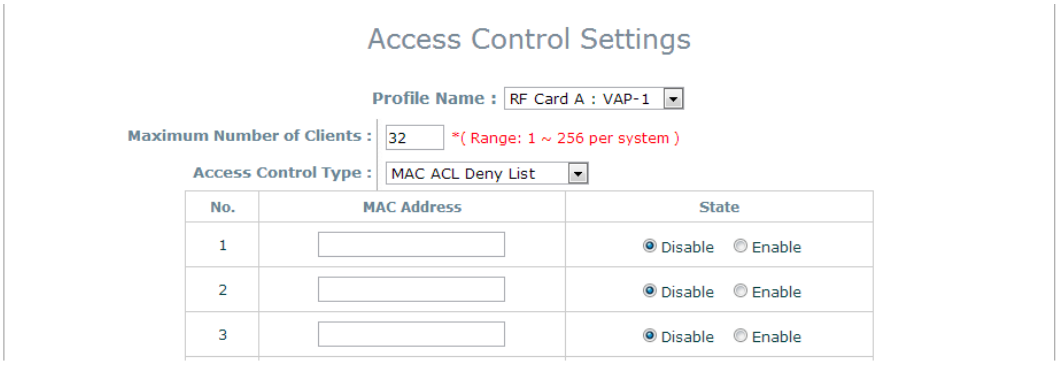
Access Control Type – Disable Access Control: When Disable is selected, there is no restriction for client devices to access the system.

Access Control Type – MAC ACL Allow List: When selecting ***MAC ACL Allow List***, only the client devices (identified by their MAC addresses) listed in the Allow List ("allowed MAC addresses")are granted access to the system. The administrator can temporarily block any allowed MAC address by checking ***Disable***, until the administrator re-Enables the listed MAC.

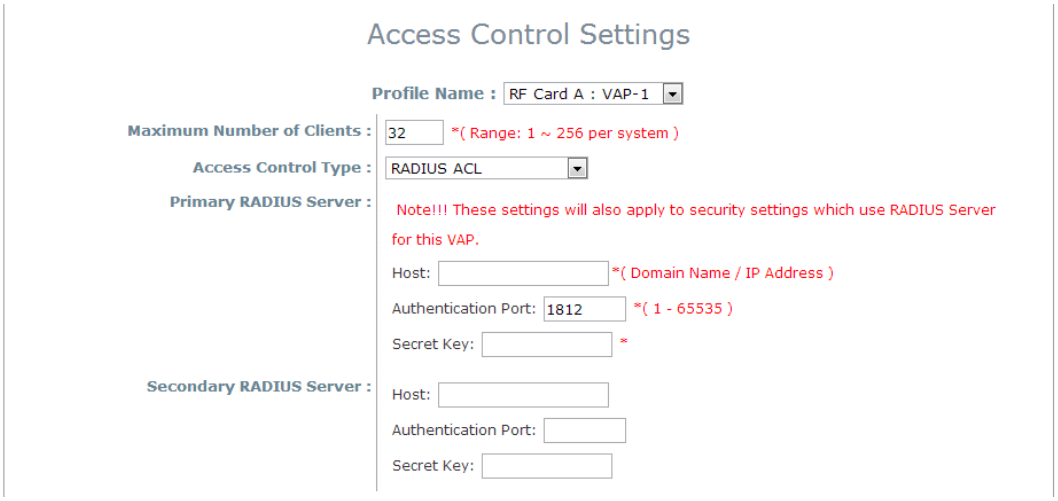


Note: An empty Allow List means that there is no allowed MAC address. Make sure at least the MAC of the management system is included (e.g. network administrator's computer)

Access Control Type – MAC ACL Deny List: When selecting ***MAC ACL Deny List***, all client devices are granted access to the system except those listed in the Deny List ("denied MAC addresses"). The administrator can allow any denied MAC address to connect to the system temporarily by checking ***Disable***.

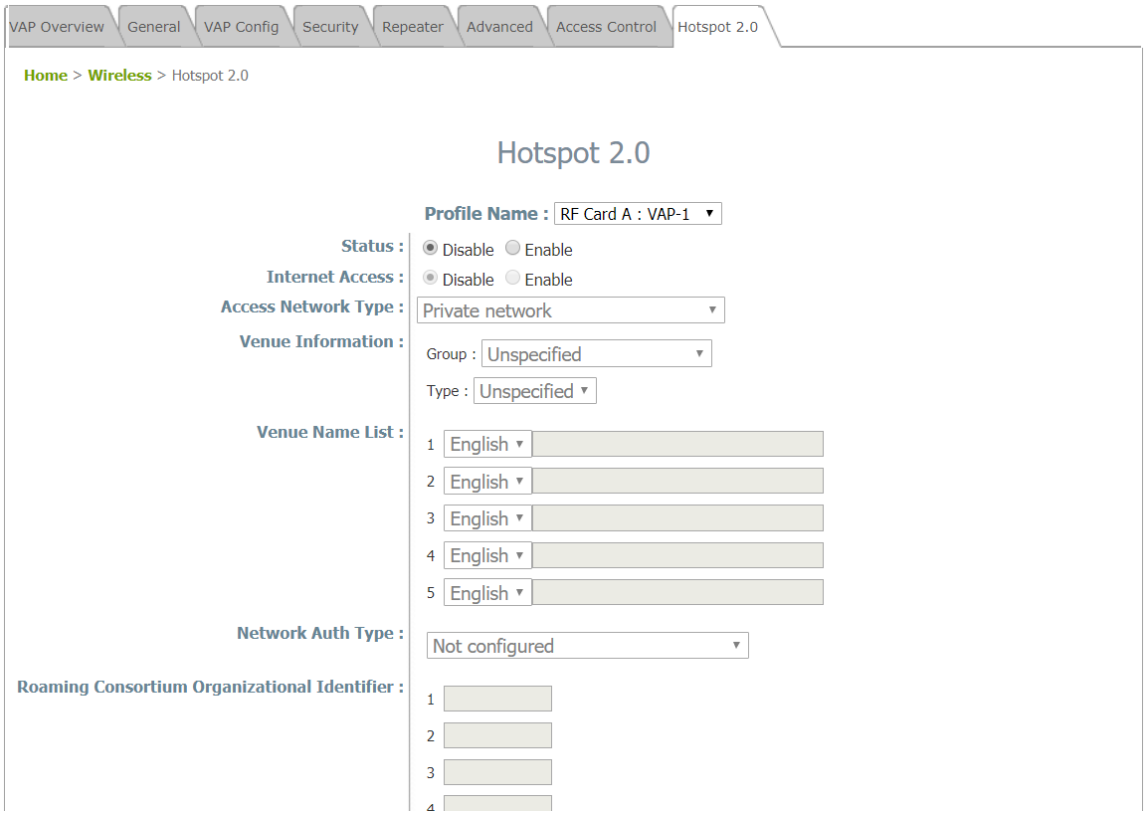


Access Control Type – RADIUS ACL: Authenticate incoming MAC addresses by an external RADIUS. When ***RADIUS ACL*** is selected, all incoming MAC addresses will be authenticated by an external RADIUS. Please note that each VAP's MAC ACL and its security type (shown on the **Security Settings** page) share the same RADIUS configuration.



4.8 Hotspot 2.0

Hotspot 2.0 is also known as WiFi Certified Passpoint initiated by the WiFi Alliance to provide better bandwidth and services for public WiFi subscribers.



Status: Enable or Disable Hotspot 2.0

Internet Access: Enable if this network provides access to the internet

Access Network Type

- **Private:** Home and Enterprise Networks
- **Private and Guest Access:** Enterprises offering guest connectivity
- **Chargeable Public Network:** Available to all but requires a fee
- **Free Public Network:** Available to all without fees
- **Personal Device Network:** For peripherals in an ad-hoc mode
- **Emergency Services**
- **Test/Experimental/Wild Card**

Venue Information: The Group/Type of the venue is selected here. This identifies the general class of the venue and the specific type of venue within each Group.

Venue Name List: The Name of the Network Venue, which is useful to end users for network selection.

Network Authentication Type: The additional steps to acquire access for an unsecure network

- **Acceptance of terms and conditions**
- **Online enrollment supported:** may require user accounting
- **HTTP/HTTPS redirection:** the URL to which the browser is redirected is indicated
- **DNS redirection:** Note that the Hotspot 2.0 specification forbids network operators from supporting protocols that are not interoperable with DNSSEC. DNS redirection for captive portals violates this requirement.
-

Roaming Consortium Organizational Identifier: A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Roaming consortiums are identified by an organization identifier (OI) that is assigned by the IEEE—similar to the first half of a MAC address. An OI is often 24 bits in length, but can also be 36 bits (i.e. OUI-36).

IP Address Type: IPv4 or IPv6

NAI Realm List: An NAI Realm identifies the proper authentication server or domain for the user's authentication exchange. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred networks.

- **EAP Type:** The NAI Realm list can also optionally indicate the Extensible Authentication Protocol (EAP) types supported by each realm as well as the authentication parameters for that EAP type.

Domain Name List: Lists one or more domain names for the entity operating the AP. This is a critical for Hotspot 2.0 network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home or visited Hotspot.

Cellular Network Information List (PLMN): Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator.

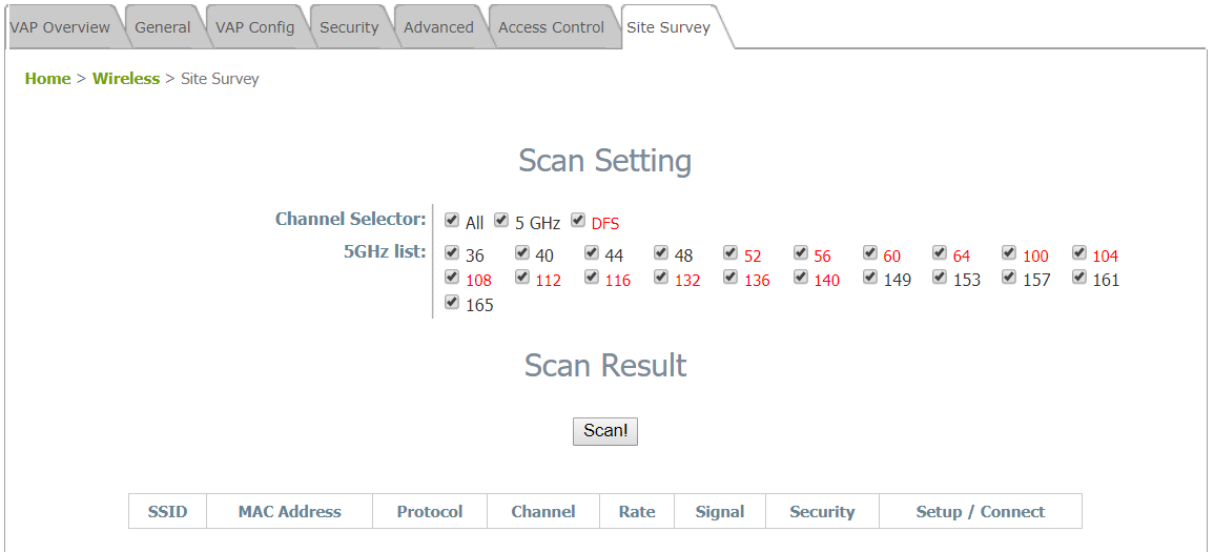
Hotspot 2.0 R2 (Hotspot 2.0 Release 2)**:** It includes improvements over Hotspot 2.0 Release 1.

- **OSU SSID:** the SSID name of the OSEN VAP
- **OSU Server URI:** the URI of the OSU server
- **OSU Friendly Name:** Name of the OSU provider in human language, which matches the name drawn from the OSU server certificate exactly. Now only support English
- **OSU NAI:** to authenticate to the OSU (if configured for OSEN)
- **OSU Service Description:** the description for the OSU. Now only support English

4.9 Site Survey (CPE mode only)

The system is able to scan and display surrounding available access points (APs). The administrator can select an AP to be associated with the system on this page.

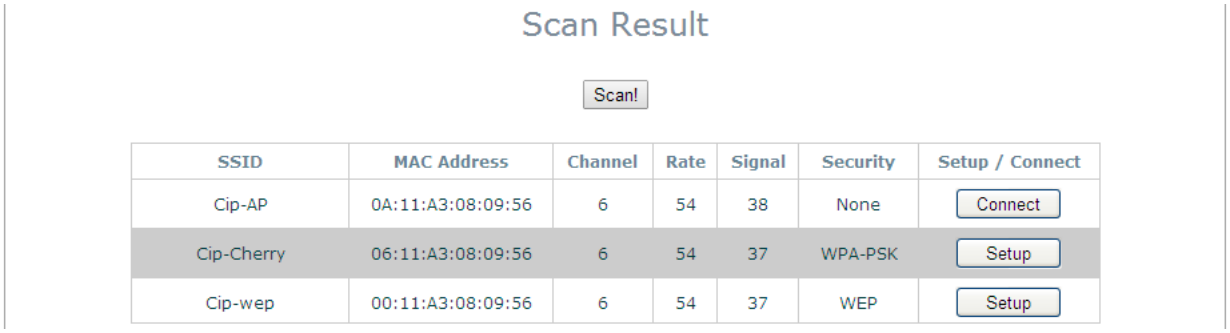
Site Survey is a useful tool to provide information on the surrounding wireless environment; available APs are shown with their respective SSID, MAC Address, Channel, Rate setting, Signal reading and Security type. The administrator can click Setup or Connect to configure the wireless connection according to the mentioned readings.



Channel Selector: Select the channel types to be scanned.

5GHz list: Select the specific channels to be scanned.

Scan Result: After Selecting Channel Selector and 5GHz list and clicking the “Scan!” button, the scan result will be shown below.



Setup / Connect:

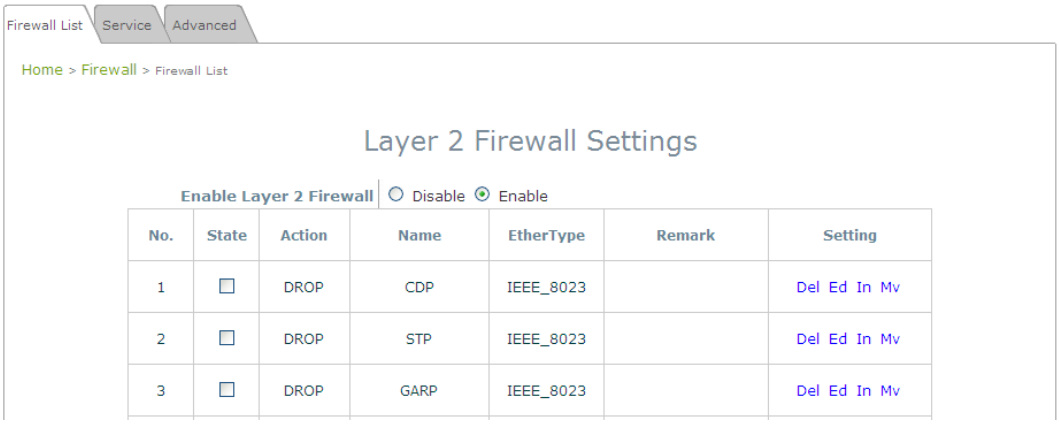
- **Connect:** Click “Connect” button to associate with the respective AP directly; no further configuration is required.
- **Setup:** Click “Setup” button to configure security settings for associating with the respective AP.

5. Firewall

The system provides an added security feature, Layer2 Firewall, in addition to the typical AP security. Layer2 Firewall offers a firewall function that is tailored specifically for Layer2 traffic, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured on gateways, this extra security feature will assist to mitigate possible security breach. This section provides information in the following functions: **Firewall Lists**, **Service** and **Advanced Firewall Settings**.

5.1 Firewall List

It provides an overview of firewall rules in the system; 6 default rules with up to a total of 20 firewall rules are available for configuration.



From the overview table, each rule is designated with the following field;
No.: The numbering will decide the priority for the system to carry out the available firewall rules in the tables.

State: The check marks will enable the respective rules.

Action: ***DROP*** denotes a block rule; ***ACCEPT*** denotes a pass rule.

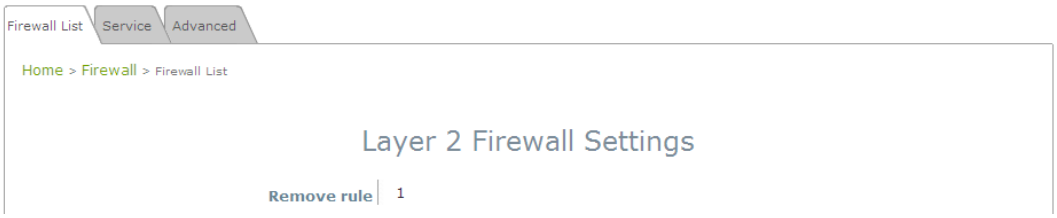
Name: Shows the name of the rule.

EtherType: Denotes the type of traffic subjected to this rule.

Remark: Shows the note of this rule.

Setting: 4 actions are available; ***Del*** denotes to delete the rule, ***Ed*** denotes to edit the rule, ***In*** denotes to insert a rule, and ***Mv*** denotes to move the rule.

To delete a specific rule,
Del in the Setting column of firewall list will lead to the following page for removal confirmation. After the ***SAVE*** button is clicked and system is rebooted, the rule will be removed.



To edit a specific rule,
Ed in the Setting column of the firewall list will lead to the following page for detail configuration. From this page, the rule can be edited from scratch or from an existing rule for revision. The following fields will be displayed:

Rule ID: The numbering of this specific rule will decide its priority among available firewall rules in the table.

Rule name: The rule name can be specified here.

EtherType: The drop-down list will provide the available types of traffic subjected to this rule.

Interface: It indicates inbound/outbound direction with desired interfaces.

Service (when EtherType is **IPv4**)**:** Select the available upper layer protocols/services from the drop-down list.

DSAP/SSAP (when EtherType is **IEEE 802.3**)**:** The value can be further specified for the fields in 802.2 LLC frame header.

Type (when EtherType is **IEEE802.3**)**:** The field can be used to indicate the type of encapsulated traffic.

VLAN ID (when EtherType is **802.1 Q**)**:** The VLAN ID is provided to associate with certain VLAN-tagging traffic.

Priority (when EtherType is **802.1 Q**)**:** It denotes the priority level with associated VLAN traffic.

Encapsulated Type (when EtherType is **802.1 Q**)**:** It can be used to indicate the type of encapsulated traffic.

Opcode (when EtherType is **ARP/RARP**)**:** This list can be used to specify the ARP Opcode in ARP header.

Source: MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.

Destination: MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is **IPv4**); ARP IP/MAC & MASK indicate the ARP payload fields.

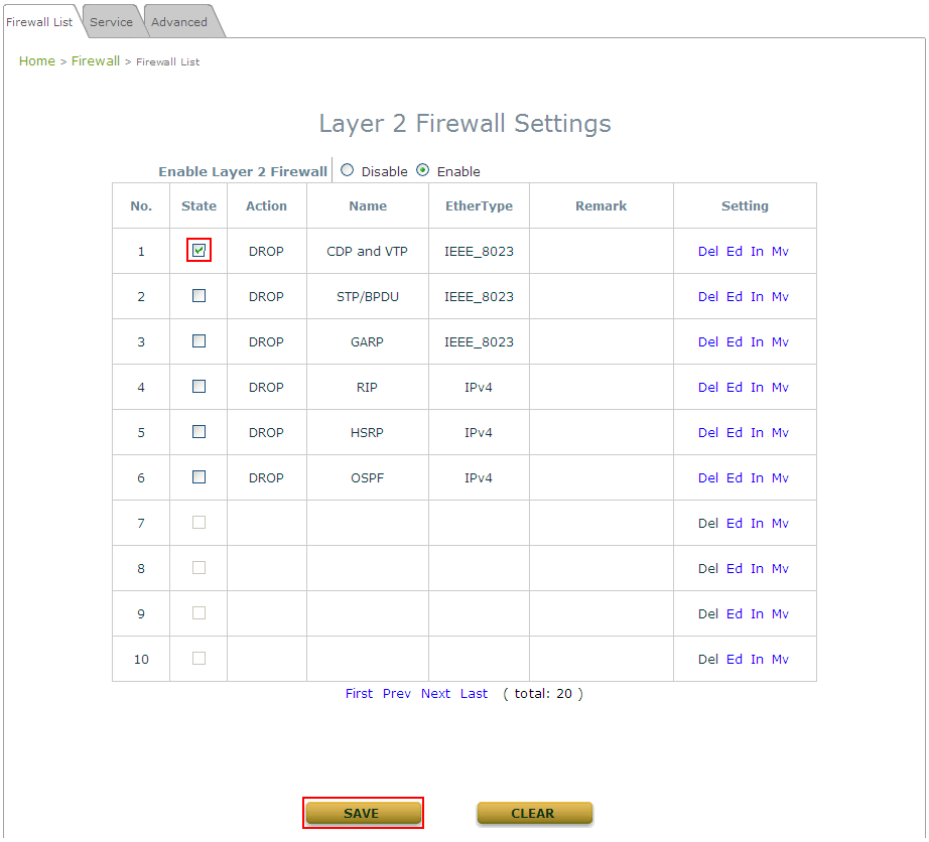
Action: The rule can be chosen to be **Block** or **Pass**.

Remark: Any note of this rule can be specified here.
When the configuration for firewall rule is completed; please click ***SAVE*** and ***Reboot*** system to let the firewall rule take effect.

To insert a specific rule,
In in the Setting column of the firewall list will lead to the following page for detail configuration with rule ID for the current inserted rule.

To move a specific rule,
Mv in the Setting column of the firewall list will lead to the following page for reordering confirmation. After the ***SAVE*** button is clicked and system is rebooted, the order of rules will be updated.

Please make sure all desired rules (state of rule) are checked and saved in the overview page; the rules will be enforced upon system reboot.



5.2 Service

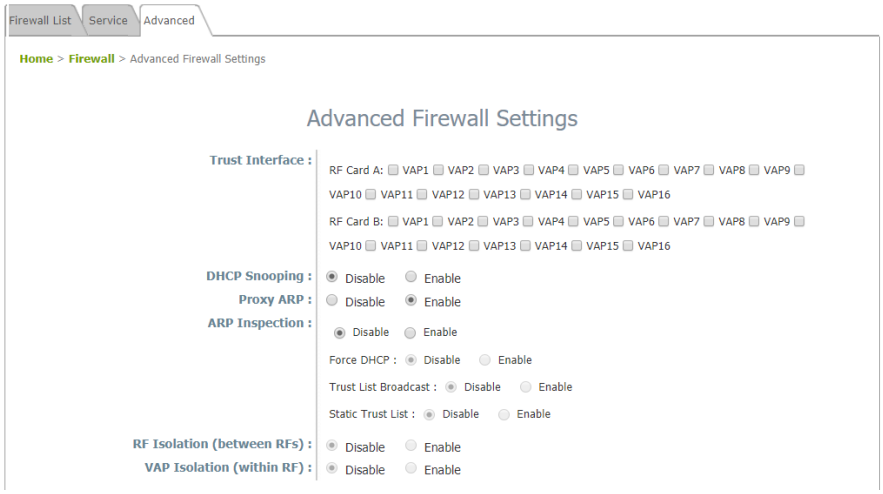
The administrator can add or delete firewall services here; the services in this list will become options to choose in firewall rule (when EtherType is IPv4).

The Access Point provides a list of rules to block or pass traffic of layer-3 or above protocols. These services are available to choose from a drop-down list of layer2 firewall rule edit page with Ether Type IPv4. The first 28 entries are default services and the administrator can add/delete any extra desired services.

There are 28 firewall services available in default settings; these default services cannot be deleted but can be disabled. If changes are made, please click ***SAVE*** to save the settings before leaving this page.

5.3 Advanced

At **Firewall > Advanced,** more advanced settings on firewall rules can be configured, providing extra security enhancement against DHCP and ARP traffic traversing the available interfaces of the system.



Trust Interface: Each VAP interface can be checked individually to mark as trusted interfaces; security enforcements on DHCP/ARP like DHCP snooping and ARP inspection will be carried out on non-trusted interfaces.

DHCP Snooping: When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the trusted DHCP server (IP/MAC) can be specified to prevent rouge DHCP server.

ARP Inspection: When enabled, ARP packets will be validated against ARP spoofing.

- **Proxy ARP** option when enabled, AP will reply ARP requests on behalf of downlink stations. The ARP table maintained by the AP will be used as a look up table upon receipt of ARP request from AP uplink. Adversely, without Proxy ARP, ARP request is broadcasted down into the AP's wireless network causing network inefficiencies.
- **Force DHCP** option when enabled, the AP only learns MAC/IP pair information through DHCP packets. Since devices configured with static IP address does not send DHCP traffic, any clients with static IP address will be blocked from internet access unless its MAC/IP pair is listed and enabled on the **Static Trust List.**
- **Trust List Broadcast** can be enabled to let other APs (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** can be used to add MAC or MAC/IP pairs of devices that are trusted to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears on the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

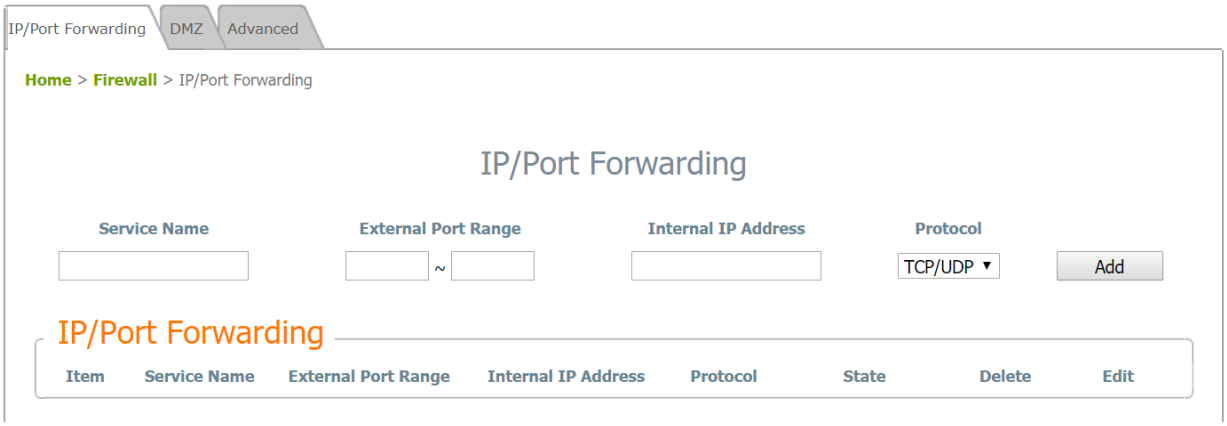
RF Isolation (between RFs): Clients are isolated between RF Card A and RF Card B.
VAP Isolation (within RF): Clients on different VAPs on the same RF Card are isolated.

If any settings are changed, please click ***SAVE*** to save the configuration before leaving this page.

Note:	- RF Isolation (between RFs) may be limited on selected AP models. - VAP Isolation (within RF) may be limited on selected AP model.

5.4 IP/Port Forwarding (CPE mode only)

A certain part of the network can be exposed to the Internet in a limited and controlled way for special-purpose Internet services such as on-line game or video conferencing on this page. Please ensure that the internal port to be used is not occupied by other applications.



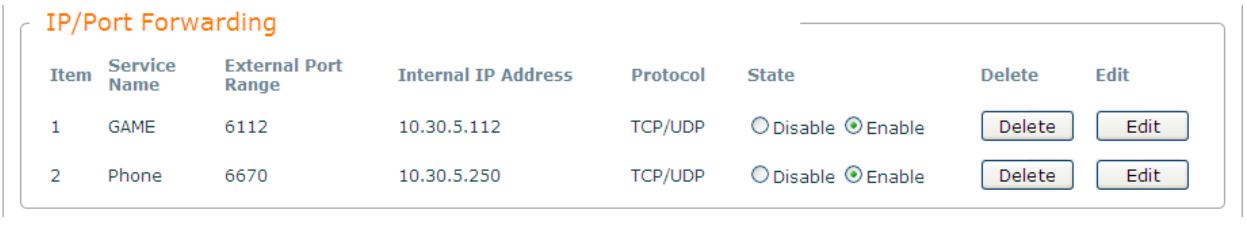
Service Name: The administrator can provide an easy remembered alias for the specific forwarding.

External Port Range: The range of external port for forwarding traffic can be defined manually by the administrator.

Internal IP Address: Enter the LAN IP address to receive the forwarding traffic.

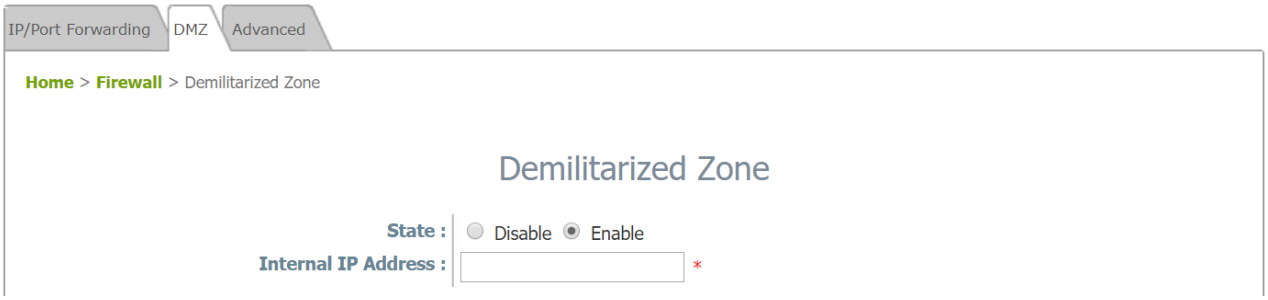
Protocol: Forwarding traffic protocol can be selected from drop-down list to be TCP/ UCP, TCP or UDP.
Add: Click Add to activate the new service.

IP/ Port Forwarding: Details of current services available. Click Delete to remove the specified service. Click Edit to configure the current setting.



5.5 DMZ (CPE mode only)

The DMZ (Demilitarized Zone) allows one local computer or server (used as a DMZ host) to be exposed to the Internet for special-purpose Internet services such as functioning as a web server. External users can access the DMZ host without authentication.



Enable: Select “Enable” to activate this function or “Disable” to deactivate it.

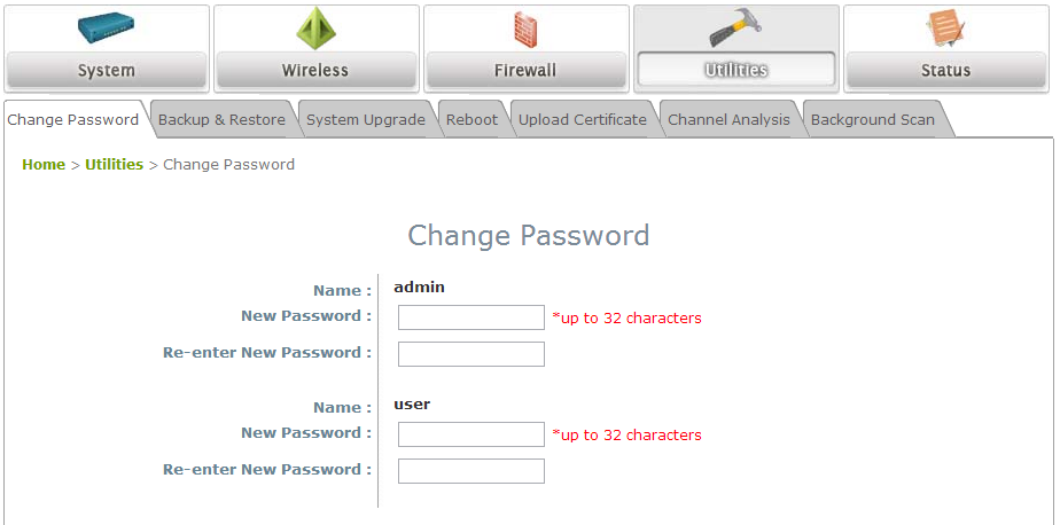
Internal IP Address: Fill in the internal IP address to allow system forwarding traffic other than those specifically listed in IP/Port Forwarding.

6. Utilities

The following utility features on this page allow the administrator to maintain the system: Change Password, Backup & Restore, System Upgrade, Reboot, Upload Certificate, Channel Analysis, Background Scan.

6.1 Change Password

To protect the Web Management Interface from unauthorized access, it is highly recommended to change the administrator's password to a secure password. Only alpha-numeric characters are allowed, and it is also recommended to make use of a combination of both numeric and alphabetic characters.

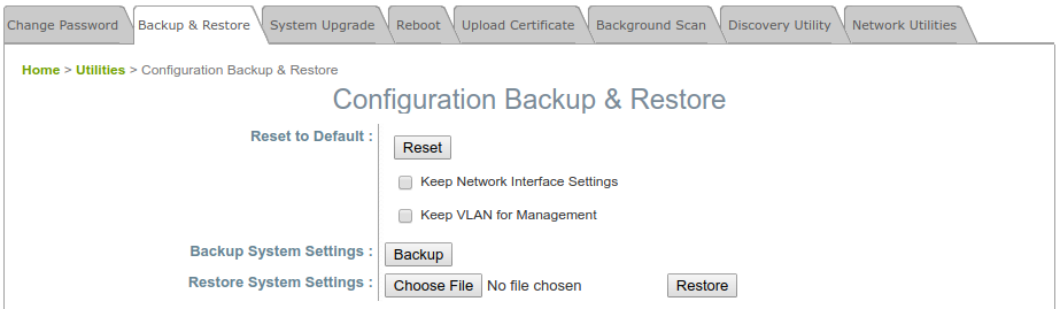


The administrator can change password on this page. Enter the original password (**"admin"**) and new password, and then re-enter the new password in the ***Re-enter New Password*** field. Click ***SAVE*** to save the new password.

In addition to the admin account, there is a "**user**" account capable of accessing the web management interface with configuration limitations. The "user" account will not be able to reboot AP, change wireless settings or enable the Channel Analysis function. This account is typically issued by IT staff for employees to monitor AP statuses.

6.2 Backup & Restore

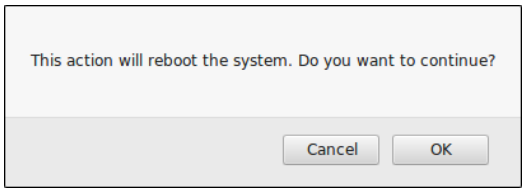
This function is used to backup and restore the Access Point's settings. The AP can also be restored to factory default using this function. It can be used to duplicate settings to other access points (backup settings of this system and then restore on another AP).



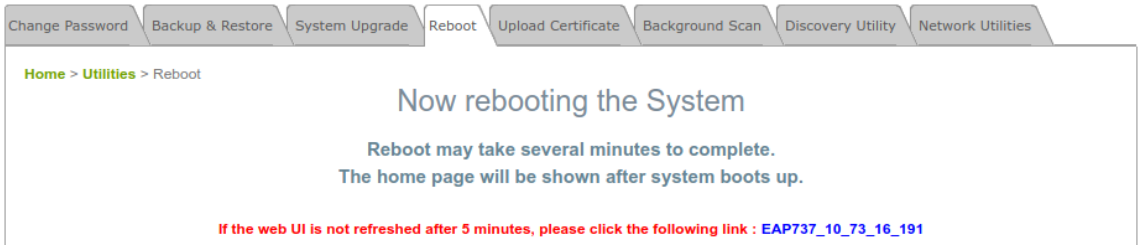
Reset to Default

Typically, administrators can reset the system to factory default from the Web Management Interface as below description. Additionally, there is another way to from the Console Interface and just refer to "*session 8.2 Remote Connection by SSH Interface*"

- **Keep Network Interface Settings:** in some cases, it is helpful to check this option to ensure the original Network Interface settings remain even after a system reset-to-default.
- **Keep VLAN for Management:** in some cases, it is helpful to check this option to ensure the original VLAN for Management settings remain even after a system reset-to-default.
- Click ***Reset*** to load the factory default settings. A pop-up message will appear to re-confirm the request to reboot the system. Click ***OK*** to proceed, or click ***Cancel*** to cancel the action.



- A message as displayed below will appear during the reboot period. The system power must be kept on before the completion of the reboot process. The **System Overview** page will appear upon reboot completion.

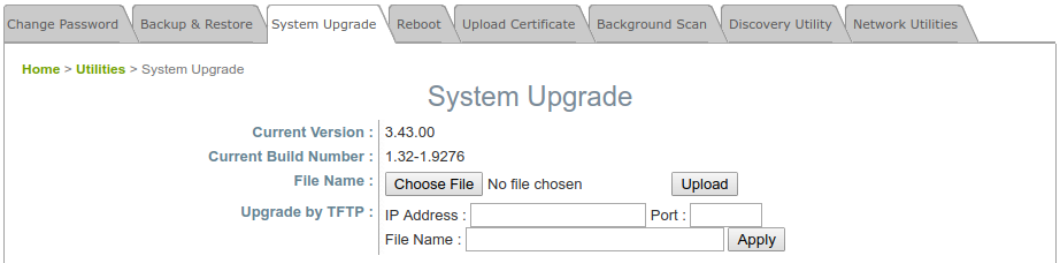


Backup System Settings: to save the current system configurations to a backup file on a local disk of the management console. A backup file can be restored to the system by clicking ***Choose File*** button to select the backup file and then clicking ***Restore*** button to execute the process.

Restore System Settings: to click ***Choose File*** to search for a .db database backup file created by the controller and click ***Restore*** to restore to the same settings at the time when the backup file was saved.

6.3 System Upgrade

There are two methods of firmware upgrade: via the WMI or via a TFTP server. The administrator can obtain the latest firmware from the Edgecore Support Team. To upgrade the firmware, click “Choose File” to select the new firmware file you downloaded onto your PC and then click “Upload” to execute the process. To upgrade by TFTP, enter the designated IP address, Port, and File Name, then click “Apply”. Please restart the system after upgrading the firmware.

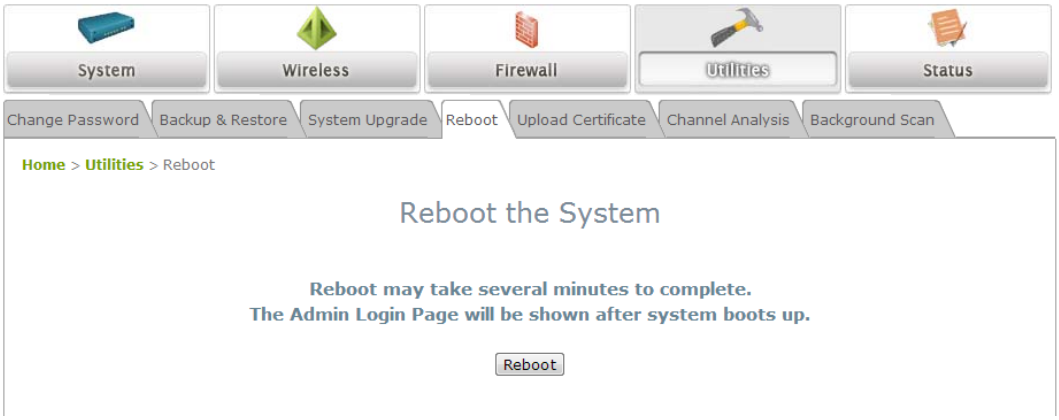


Note:

- It is recommended to check the firmware version number before proceeding further. Please make sure you have the correct firmware file.
- Firmware upgrade may sometimes result in the loss of data. Please ensure that all necessary settings are written down before upgrading the firmware.
- During firmware upgrade, please do not turn off the power. This may permanently damage the system.
- Upgrade by TFTP may be limited on selected AP models.

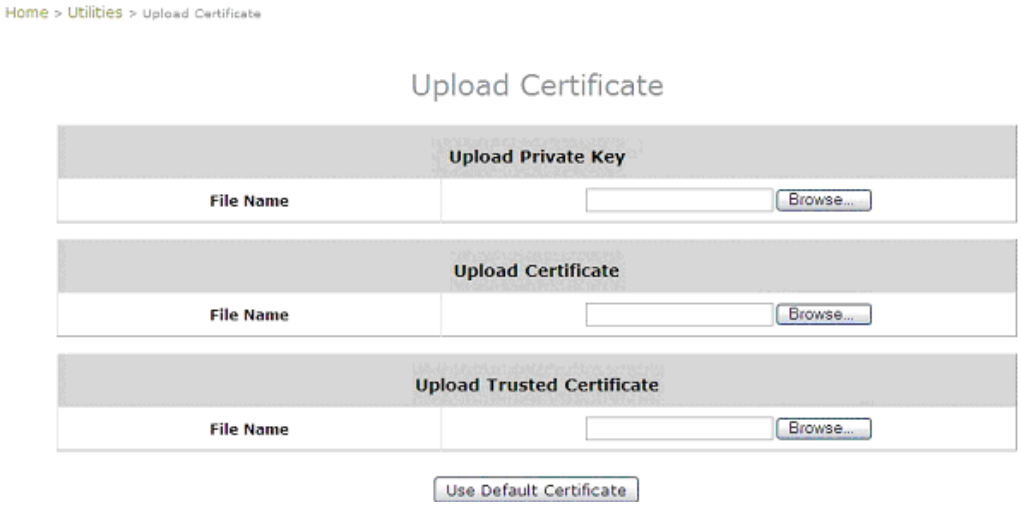
6.4 Reboot

Click ***Reboot*** to restart the AP safely. The process takes approximately three minutes. The System Overview page will appear after a successful reboot. Note: in some cases, it is necessary to reboot the AP to ensure that parameter changes are submitted.



6.5 Upload Certificate

This function is used to configure a valid certificate for security validation required in CAPWAP.

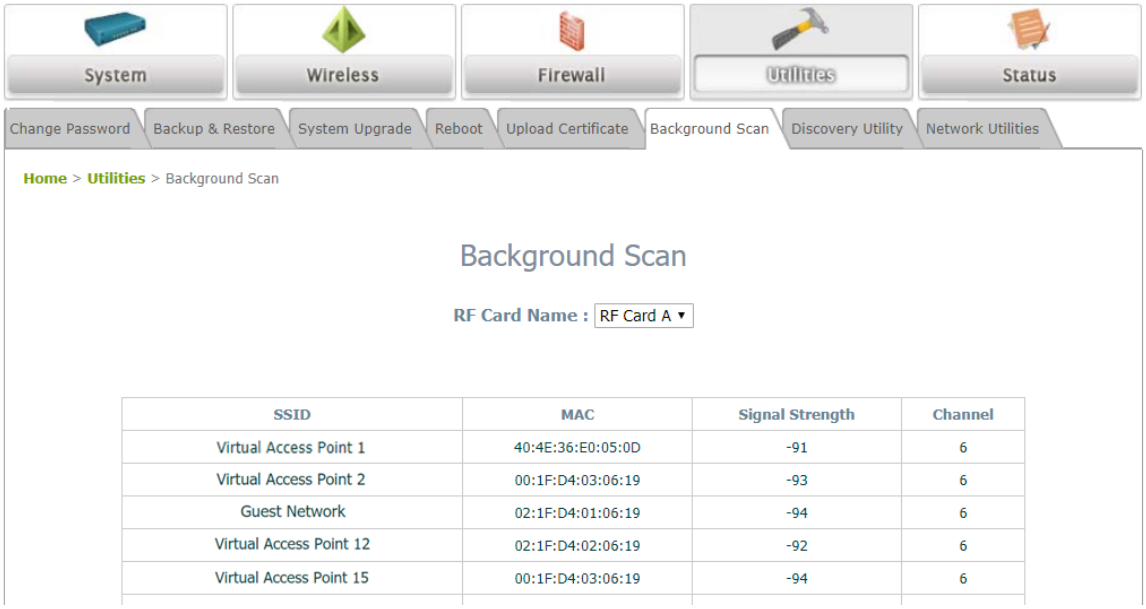


Upload Certificate: It provides flexibility to support customer's own Certificate, Private Key, or Trusted Certificate for a means of security verification for CAPWAP or other security needs to ensure the authenticity of this AP to other network entities.

Use Default Certificate: Click ***Use Default Certificate*** to use the default certificate and key.

6.6 Background Scan

The Access Point is capable of doing background scanning without affecting service. This works in complement with Channel Analysis so administrators have a complete overview of the wireless environment.

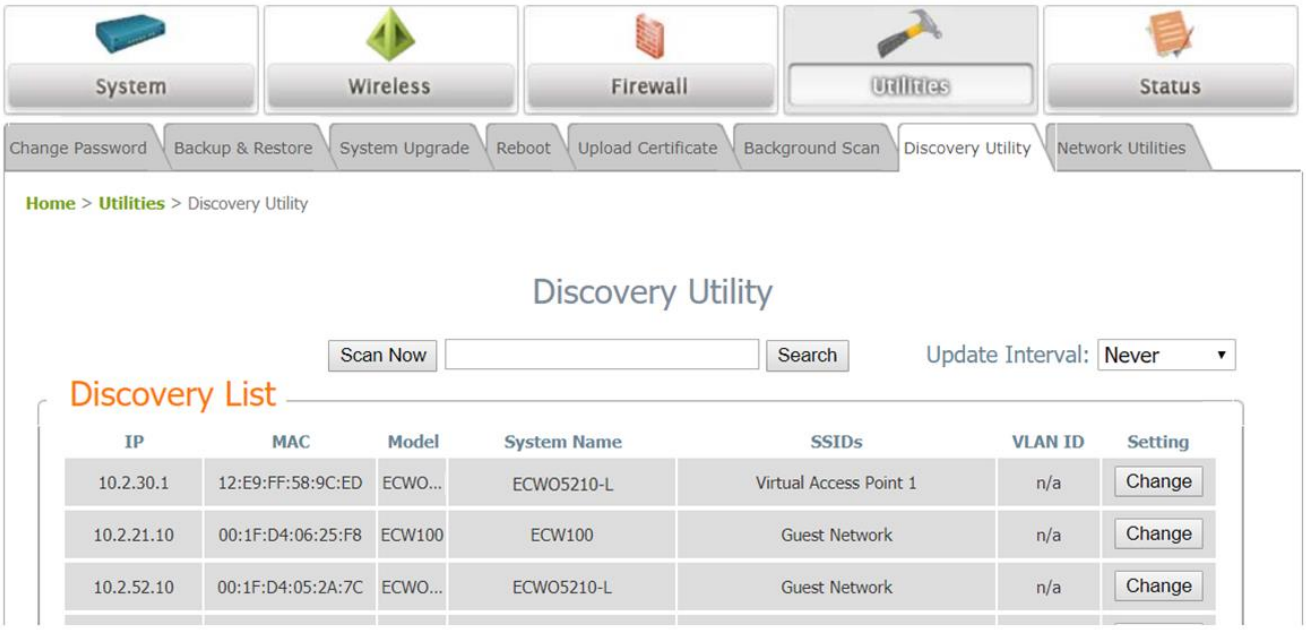


The Scan Whole Channel button triggers the AP to scan all channels in the configured band. Note that the Radio is only capable of scanning in its configured band.

6.7 Discovery Utility

The network administrators need to access or change some information without entering AP interface, such as forget the IP address of the AP, forget the admin's password, or configure the IP address of the AP.

All they need to do is connect Edgecore AP within the same Layer 2 from the ports of the current system, and press the "Search" button to execute the IP Discovery Utilities. The scanning results would be devices' corresponding IP address, MAC address, Model, System Name, SSID (each VAP), VLAN ID. The LAN ports of devices could connect through switch to other devices (APs).

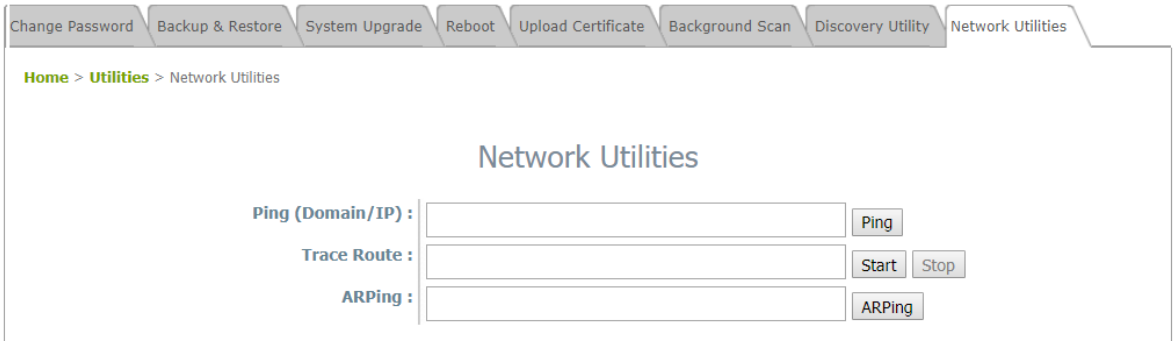


Scan Now: Click this button to start the discovery process, and the results will be displayed in the Discovery List table.

Search: Enter a keyword to search for the particular AP(s).

Change: This allows administrators to change the particular AP's settings, including IP address, Netmask, Gateway, Primary DNS Server, Username, and Password.

6.8 Network Utilities

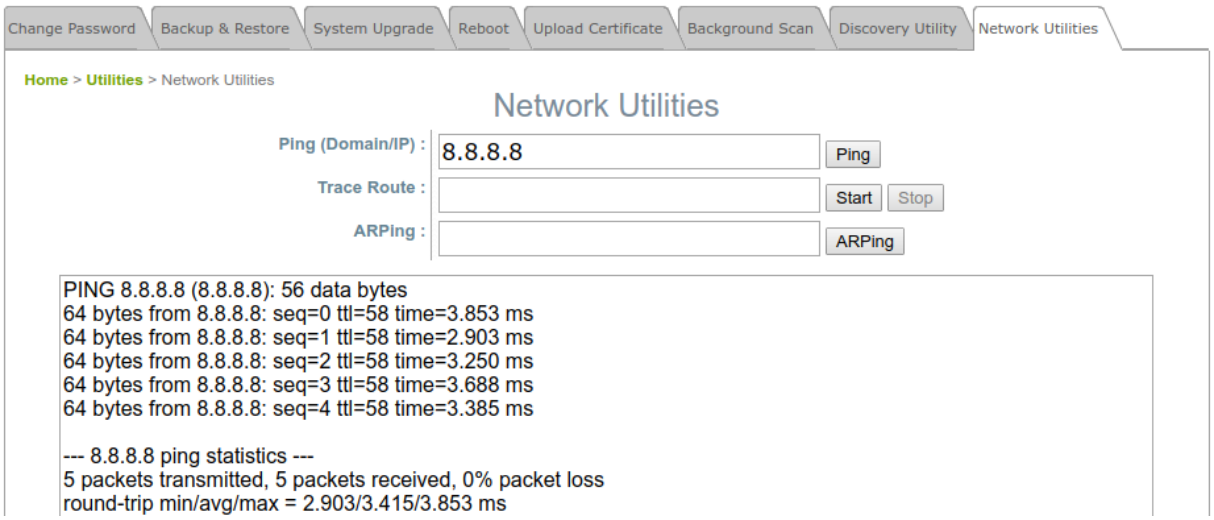


Ping: It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.

Trace Route: It allows administrator to recover the real path of packets from the gateway to a destination using IP address or Host domain name.

ARPing: Allows the administrator to send ARP request for a specific IP address or domain name.

Result: The operation result is displayed here.

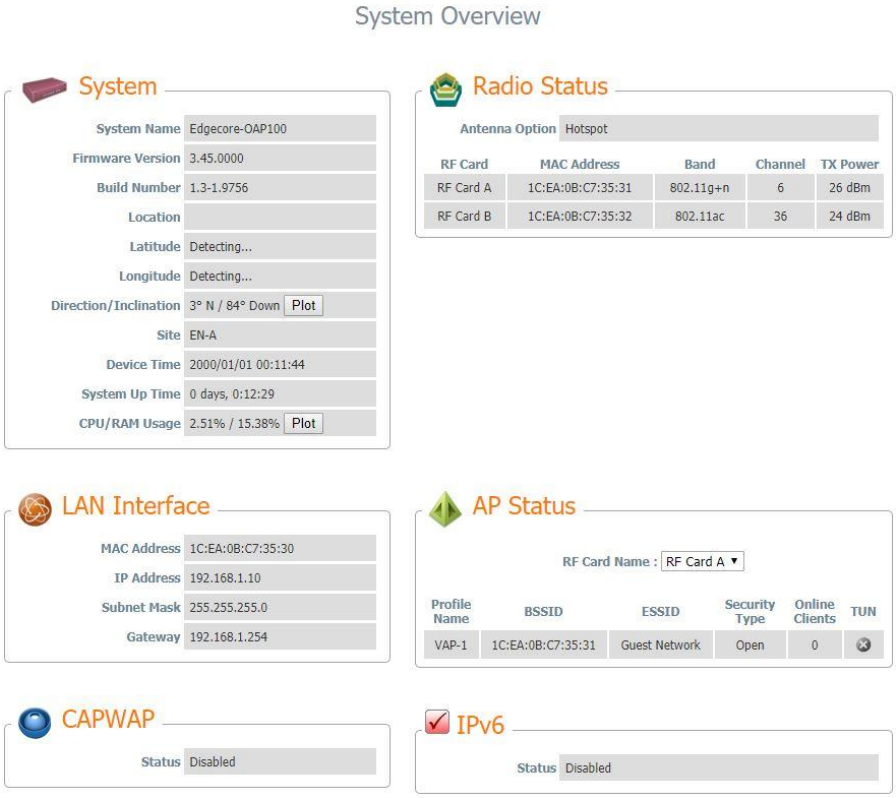


7. Status

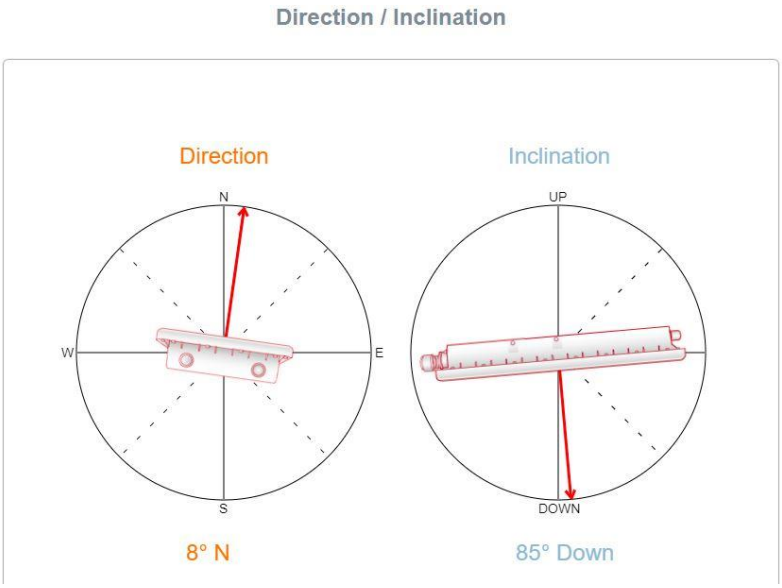
The following function tabs present the current condition and state of the system: Overview, Interfaces, Associated Clients, DHCP Lease, Link Status, Event Log, Wireless Log, and Monitor.

7.1 Overview

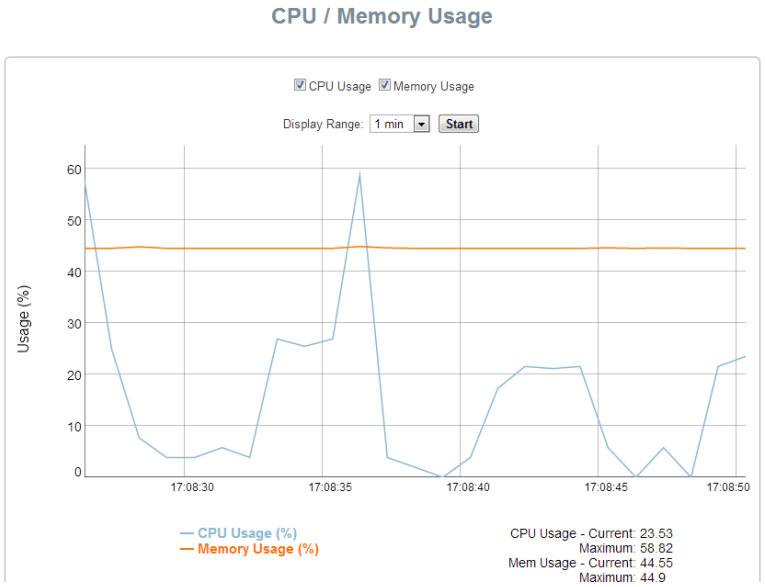
The **System Overview** page provides an overview of the system status for the administrator.



Clicking ***Plot*** button (OAP100 only) shows the plot of Direction/Inclination. The left side shows the horizontal angle of the device. The right side shows the vertical inclined angle of the device.:

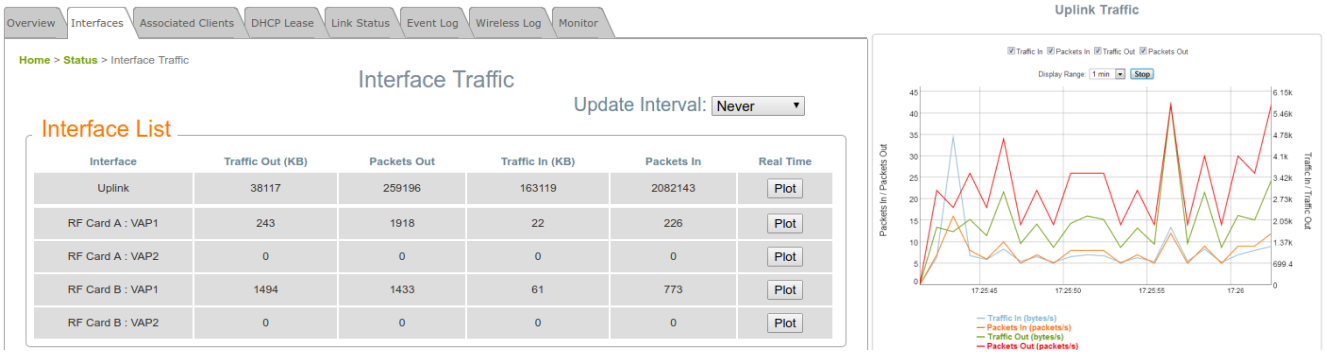


Clicking ***Plot*** button shows the real time plot of CPU/RAM usage. Left click and drag the mouse to zoom in the desired regions. Double click on the graph to return the plot to its original scale.:



7.2 Interfaces

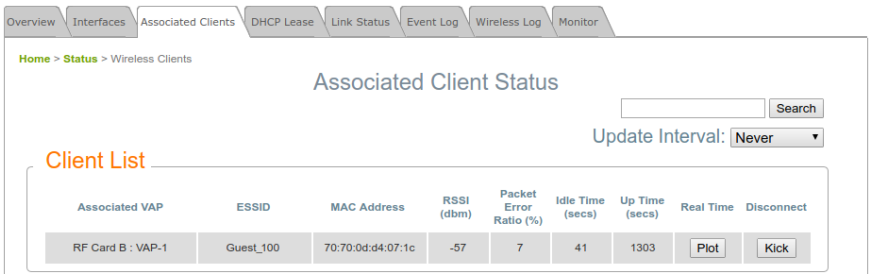
Traffic information is available per interface. Recorded data includes **Packets In**, **Packets Out**, **Traffic In (kb)**, and **Traffic Out (kb)**.

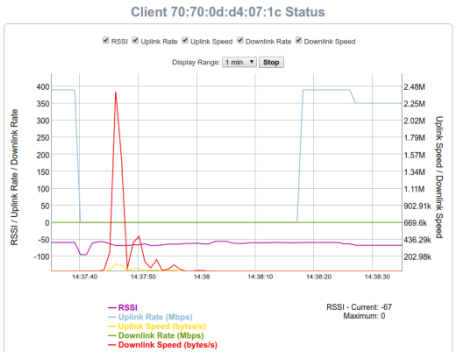


A real time plot is also available for each interface, whose time axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

7.3 Associated Clients

The administrator can remotely oversee the status of all associated clients on this page. When a low SNR is found here, the administrator can tune the corresponding parameters or investigate the settings of associated clients to improve network communication performance.





A real time plot is also available for each interface, whose time axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.

Associated VAP: The name of the VAP that the client is associated with.

ESSID: The Extended Service Set ID which the client is associated with.

MAC Address: The MAC address of associated clients.

RSSI: The Received Signal Sensitivity Index of respective client's association.

Packet Error Ratio: Indication of the associated client's service quality to see if packets are not received.

Idle Time: Time period that the associated client is inactive for; the time unit is in seconds.

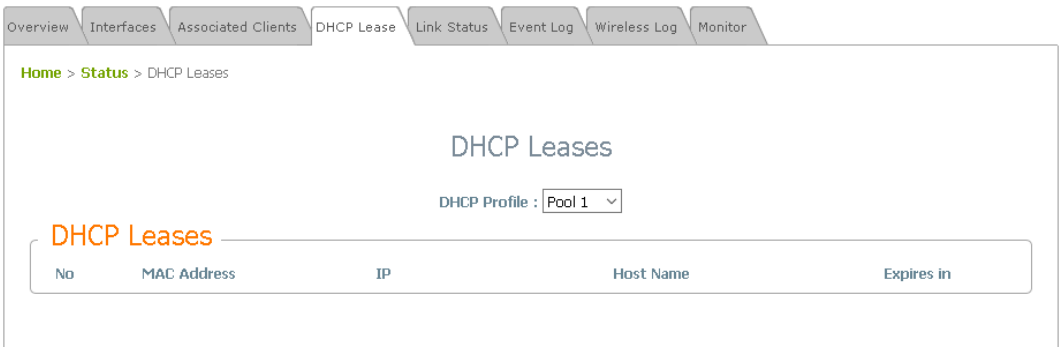
Up time: Time period that the client is associated for; the time unit is in seconds.

Real Time (Plot): A real time plot of each associated client's traffic information including Packets In/Out, Traffic In/Out in Kb, RSSI, Uplink/Downlink Rates, and etc.

Disconnect: Upon clicking ***Kick***, the client will be disconnected from the system.

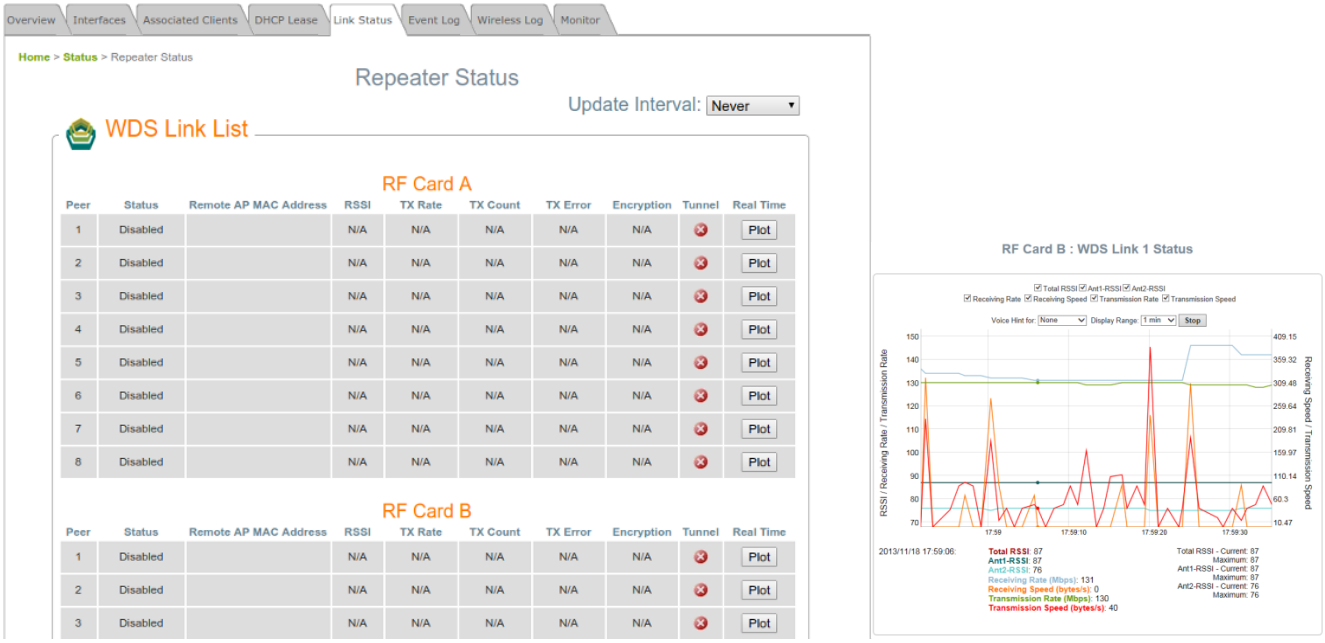
7.4 DHCP Lease

When any VAP operates in NAT mode, DHCP Lease information will be displayed in this table.



7.5 Link Status

The administrator can review detailed information of the repeater function at **Status > Link Status**. Information of WDS status, traffic statistics, encryption and other details are provided.

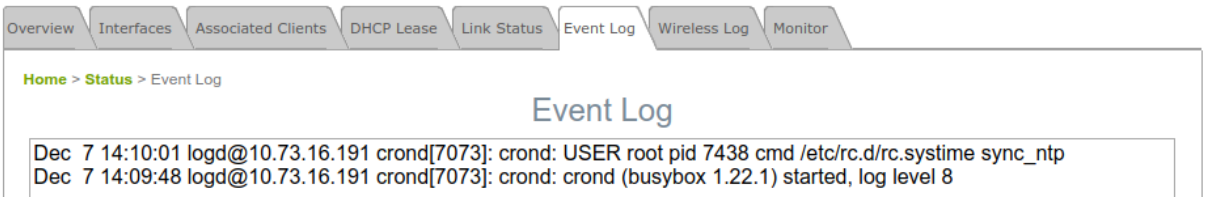


By clicking plot, a dynamic graph for WDS link status is displayed. Information on the plot includes Total RSSI, Ant1 RSSI, Ant2 RSSI, Transmission Rate, Receiving Rate, Transmission Speed, and Receiving Speed.

A real time plot is also available for each interface, whose time axis is configurable with the following options: 1 minute, 2 minutes, 5 minutes, or 10 minutes. Double click to return the plot to its original scale.
Voice hint may also be enabled for convenience during antenna adjustment.

7.6 Event Log

The Event Log provides a record of system event. Administrators can monitor the system status by checking this log. Internal storage is limited so it is recommended to back up all logs via an external Syslog Server.



Each entry in the Event Log represents an event record; in each line, there are 4 fields:

Date and Time: The time and date when the event happened.

IP Address: to indicate which LAN IP address of the system recorded this event. Note that all events on this page are local events, so the IP address in this field is always the same. In remote SYSLOG service however, this field will help the administrator identify which event is from this Access Point.

Process name: to indicate the event generated by the running instance

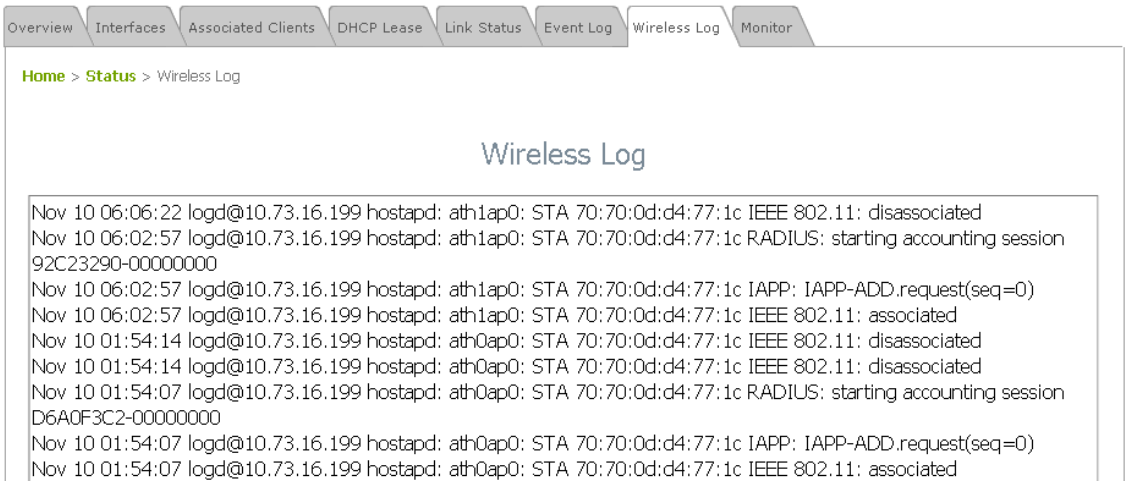
Description: to display the message of each event

SAVE LOG: to save the file to local disk as a .txt file

CLEAR: to clear all of the records

7.7 Wireless Log

This Wireless Log keeps track of client association and WDS connection related activities. Administrators can monitor the system status by checking this log. Internal storage is limited so it is recommended to back up all logs via an external Syslog Server.



Each entry in the Wireless Log represents an event record; in each line, there are 4 fields:

Date and Time: The time and date when the event happened.

IP Address: to indicate which LAN IP address of the system recorded this event. Note that all events on this page are local events, so the IP address in this field is always the same. In remote SYSLOG service however, this field will help the administrator identify which event is from this Access Point.

Process name: to indicate the event generated by the running instance

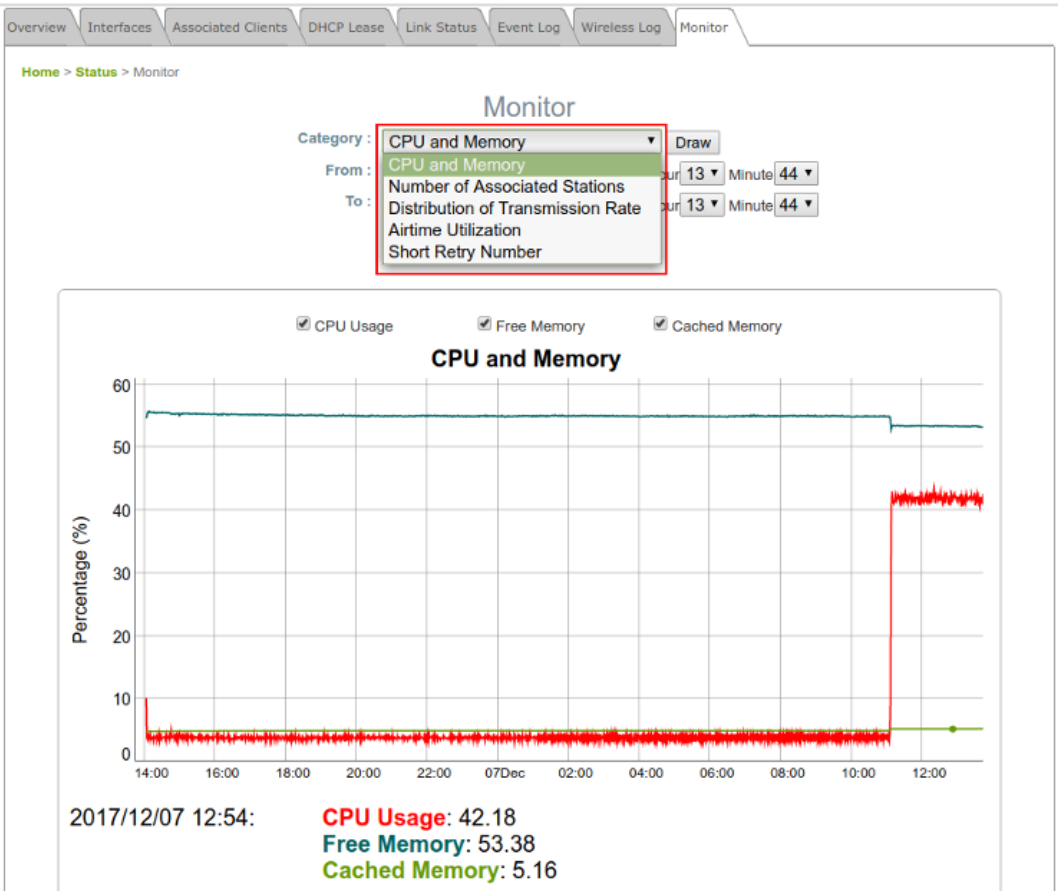
Description: to display the message of each event

SAVE LOG: to save the file to local disk as a .txt file

CLEAR: to clear all of the records

7.8 Monitor

Multiple monitor charts provide a quick overview on the AP's performance in time dimension. Begin and End time for each chart can be selected for filtering data. Left click on the mouse to zoom in on desired regions. Double click to return the plot to its original scale.



CPU and Memory: to view the usage of the devices. CPU < 90% and RAM < 90% is acceptable

Number of Associated Station: to view the number of devices connected to the selected radio (RF Card A or RF Card B).

Distribution of Transmission Rate: to view the number of packets transmitted categorized by Transmission Rates.

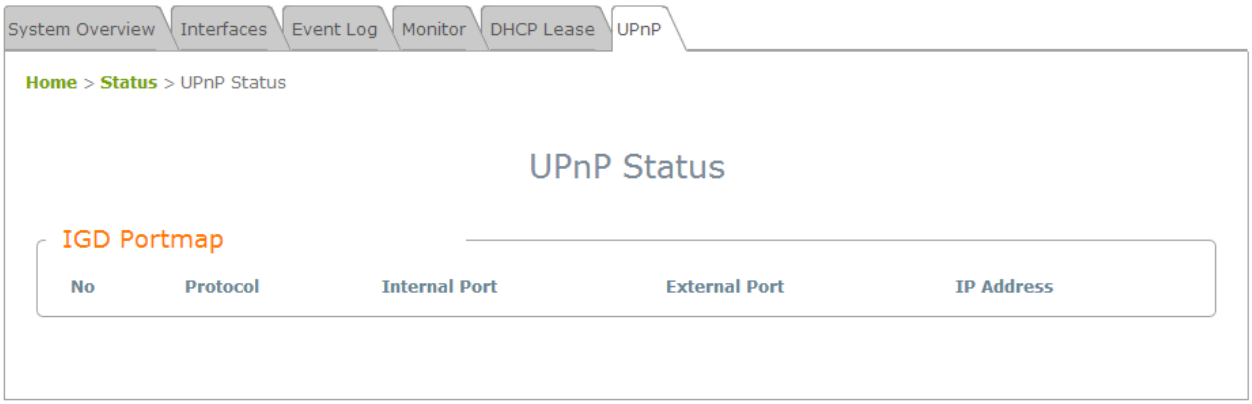
Airtime Utilization: to view the Signal-to-Noise of the Wireless Environment. Airtime Utilization < 70% is optimal

- **RX Clear Rate**: The percentage of the airtime the current channel utilizes.
- **RX Frame Rate**: The percentage of airtime that the AP receives and decrypts.
- **TX Frame Rate**: The percentage of airtime from the AP transmitting data.

Short Retries Number: to view the number of packets re-transmitted. Short Retry < 200 is optimal

7.9 UPnP (CPE mode only)

The table provides information about the UPnP overview such as Protocol, Internal Port, External Port, and IP Address.



IGD Portmap:

- **No:** The item number of an UPnP device.
- **Protocol:** The Protocol used by the UPnP device.
- **Internal Port:** The internal port number of the UPnP device.
- **External Port:** The mapped external port number of the system.
- **IP Address:** The IP address of the UPnP device.

8. Console Interface

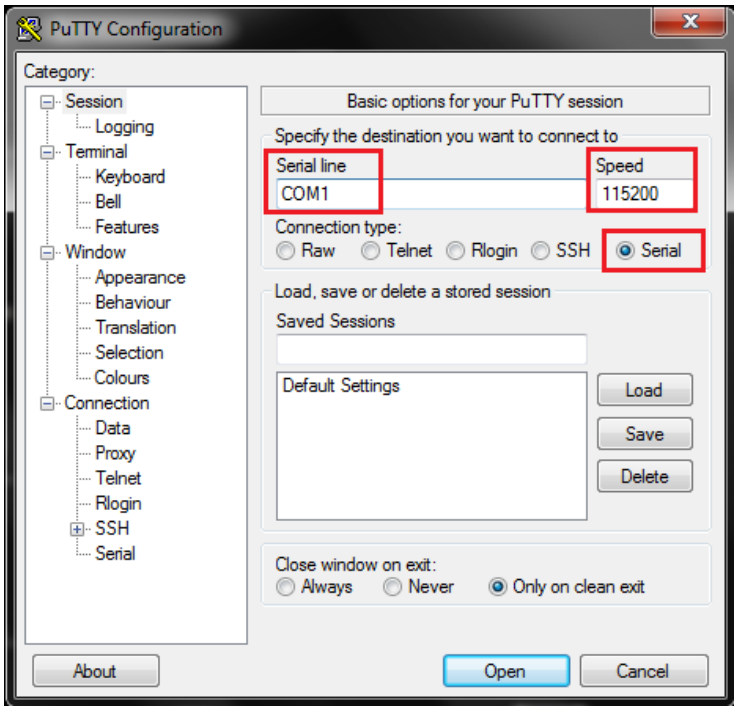
Via the console port, administrators are able to enter the console interface to reset the AP to its factory default settings. In order to connect to the console port of a The AP, a console cable, and a terminal simulation program (e.g. PuTTy) are needed. There are 2 ways to access the console interface

8.1 Direct Connection by Console Cables

PC > USB to RS-232 DB9 Serial Converter Cable > Console Cable (DB9-to-RJ45) > Console Port
The USB-to-RS232 cable is not supplied with standard packaging. It is recommended to use only the console cable provided with the packaging.

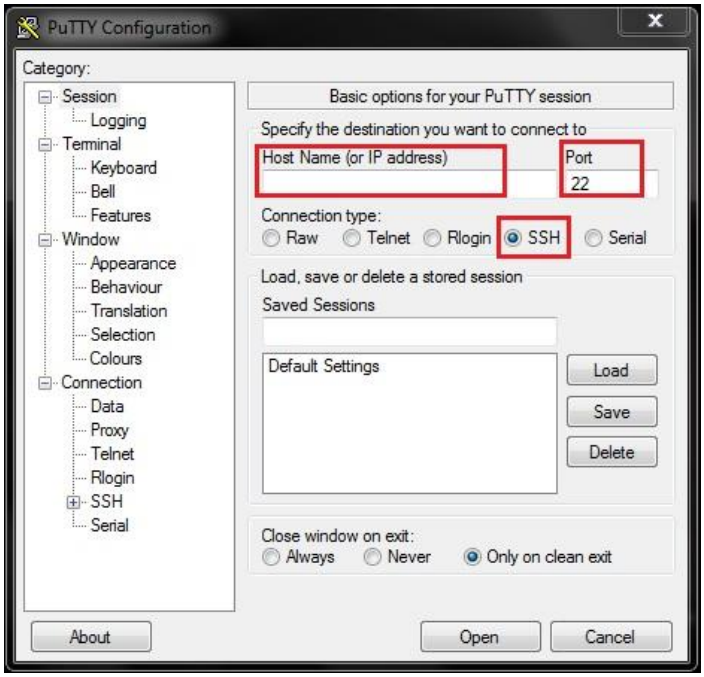
Cable	Description
	USB to RS-232 Serial Converter Cable (USB to DB9 Male)
	Console Cable (DB9 Female to RJ45 Male)

The speed (baud rate) is 115200.

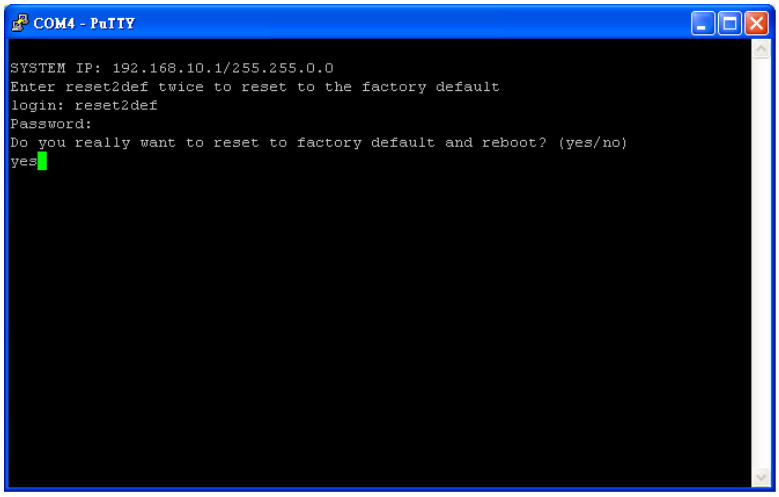


8.2 Remote Connection by SSH Interface

The system supports access to the console interface via SSH. Typically SSH utilizes Port 22 and would require the WAN IP address for access.



To reset the system to factory default through the console interface, Login as “reset2def” and enter “reset2def” as your password.



If the console connection is not readily available, the IP address of the AP can be retrieved with the Discovery Utility of another AP (Home > Utilities > Discovery Utility). Simply connect via an Ethernet cable and run the Discovery Utility.