CAX1800

User Manual

11-2019 / v1.0

Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd., Neihu Dist., Taipei City, Taiwan
Email: support@edimax.com.tw

Edimax Technology Europe B.V.
Fijenhof 2, 5652 AE Eindhoven, The Netherlands
Email: support@edimax.nl

Edimax Computer Company
3444 De La Cruz Blvd., Santa Clara, CA 95054, USA
Email: support@edimax.com

Contents

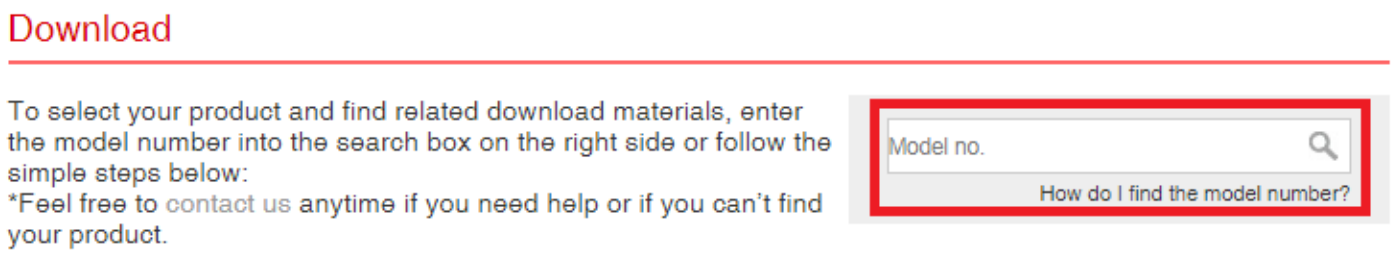
I. Product Information

The CAX1800 with the latest emerging IEEE 802.11ax Wi-Fi 6 technology effortlessly create a reliable internet connection. Place the CAX1800 between the router and the location where you need better wireless coverage and enjoy high-speed wireless connection throughout your home or office.

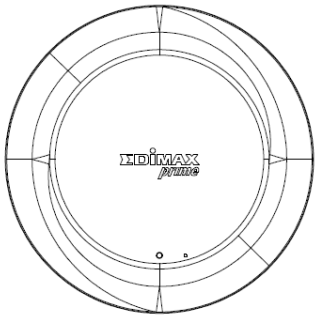
You can find all supporting documents from the link below or via QR Code:

https://www.edimax.com/download

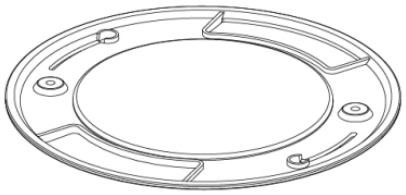
(Once you've visited the Edimax official website, please enter the model no. "CAX1800" into the search box to search for your product.)



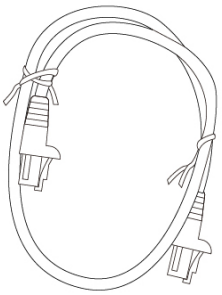
I-1. Package Contents



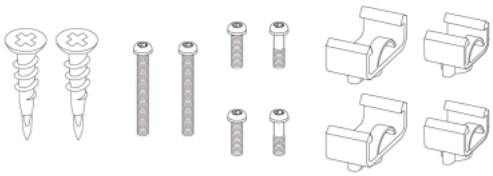
CAX1800



Ceiling Mount Bracket

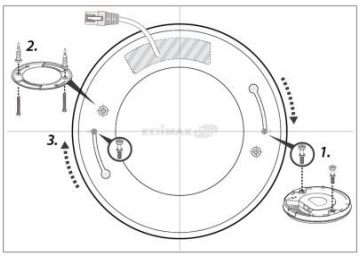


Ethernet Cable



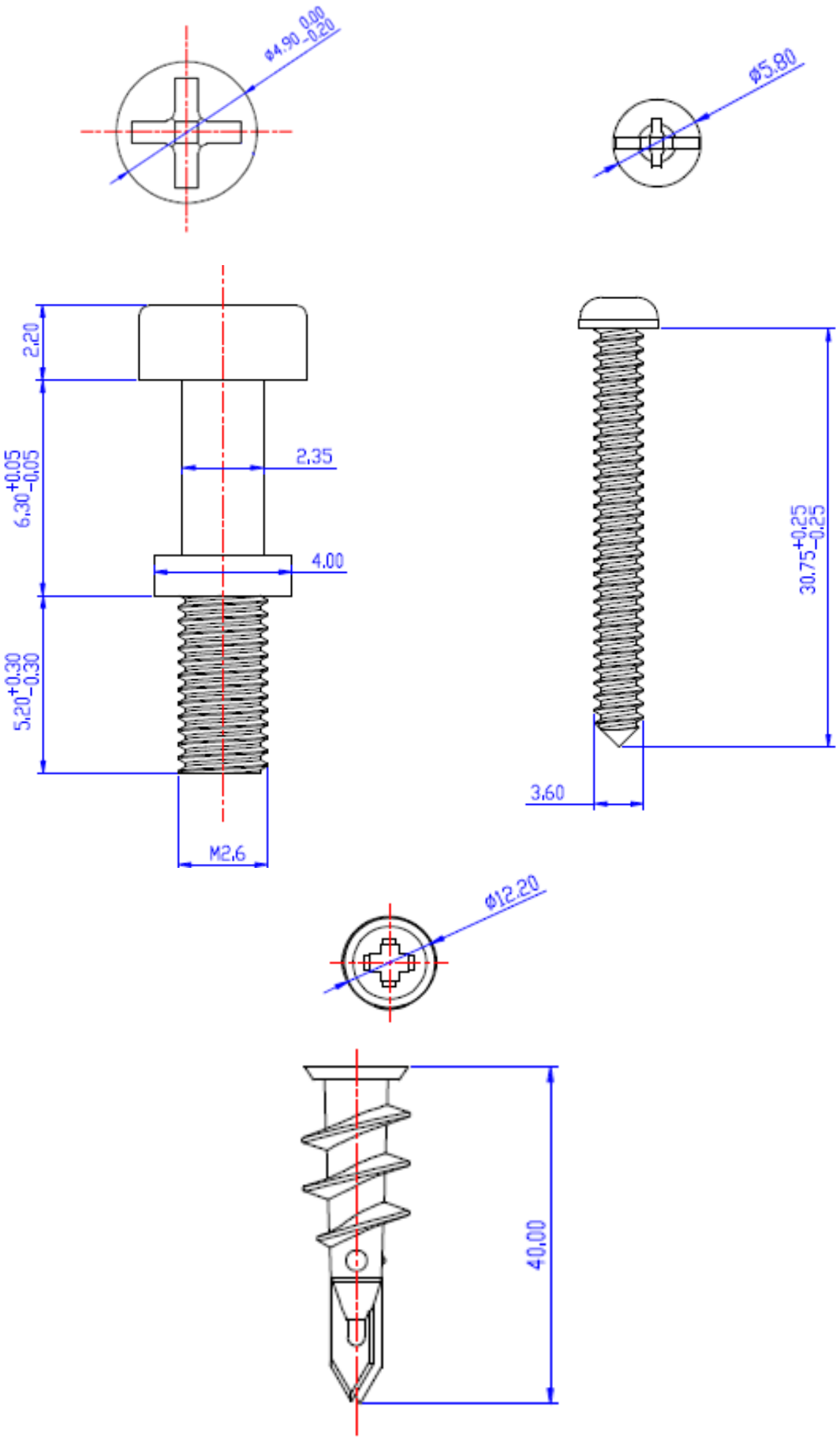
T-Rail Mounting Kit & Screws

Manual



Ceiling Mount Screw Template

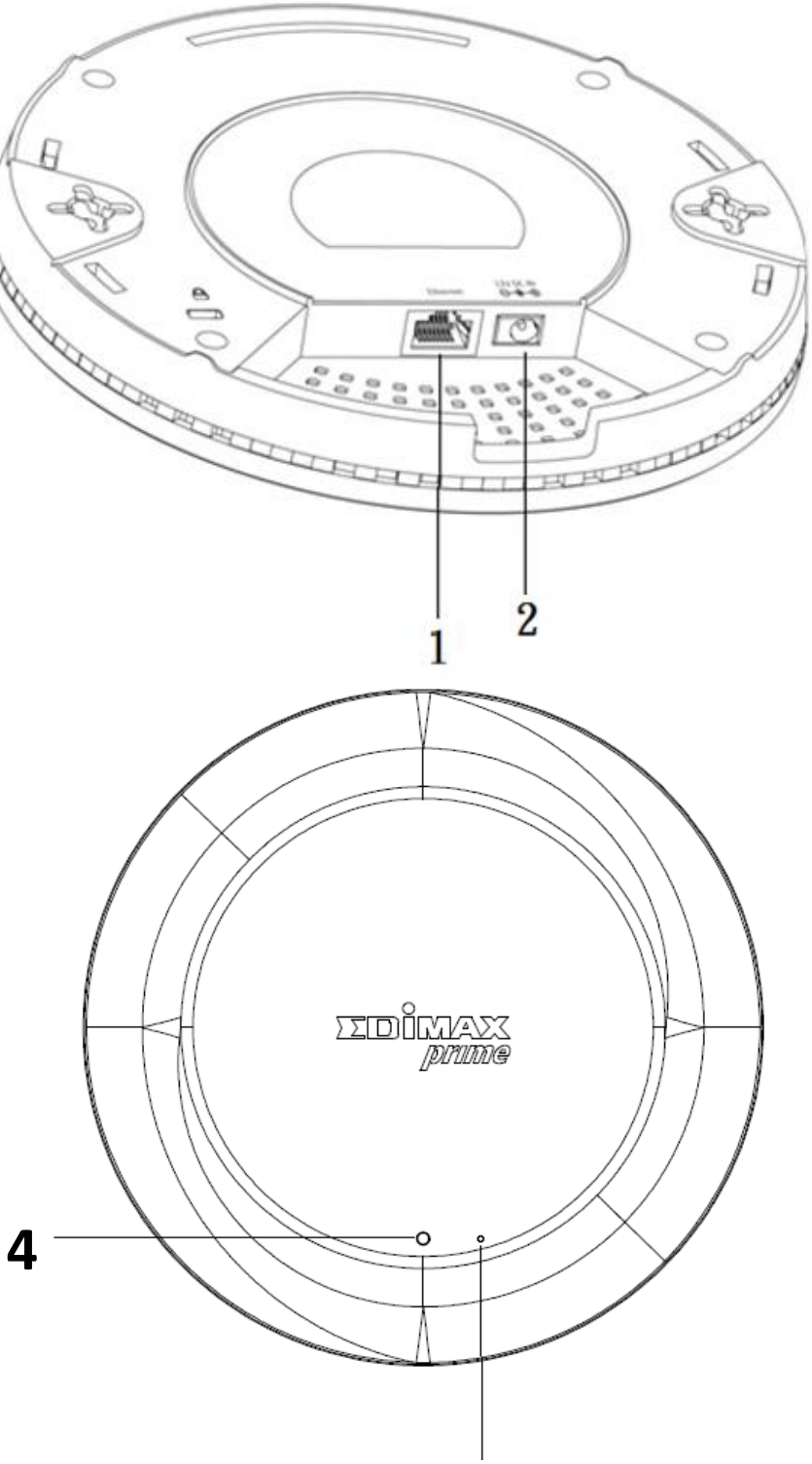
Screws Size:


Φ4.90 0.00 -0.20
Φ5.80
2.20
6.30 +0.05 -0.05
2.35
4.00
5.20 +0.30 -0.30
M2.6
30.75 +0.25 -0.25
3.60
Φ12.20
40.00

I-2. System Requirements

- Existing cable/DSL modem & router
- Computer with web browser for AP configuration

I-3. Hardware Overview



No.	Description
1	Ethernet Port (PoE)
2	Power Jack (12V/1.5A)
3	Reset Button
4	LED

I-4. LED Status

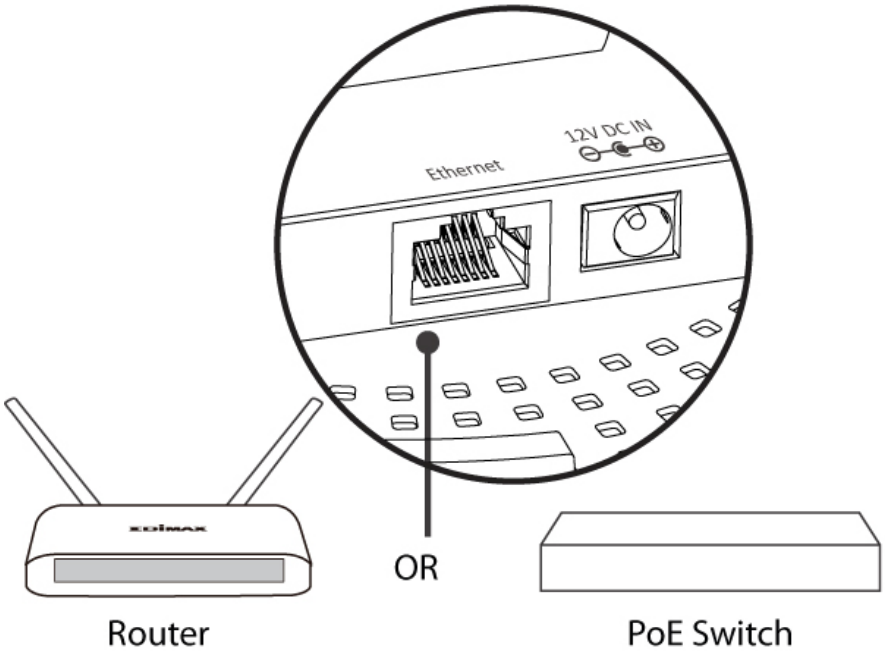
Color	Status	Description
Blue	On	Power is on.
	Flashing Slowly	Upgrading firmware.
	Flashing Quickly	Resetting to factory defaults.
Red	On	Starting up.
	Flashing	Error.
Off	Off	Power is off.

II. Hardware Installation

This section will guide you through the steps to set up your CAX1800.

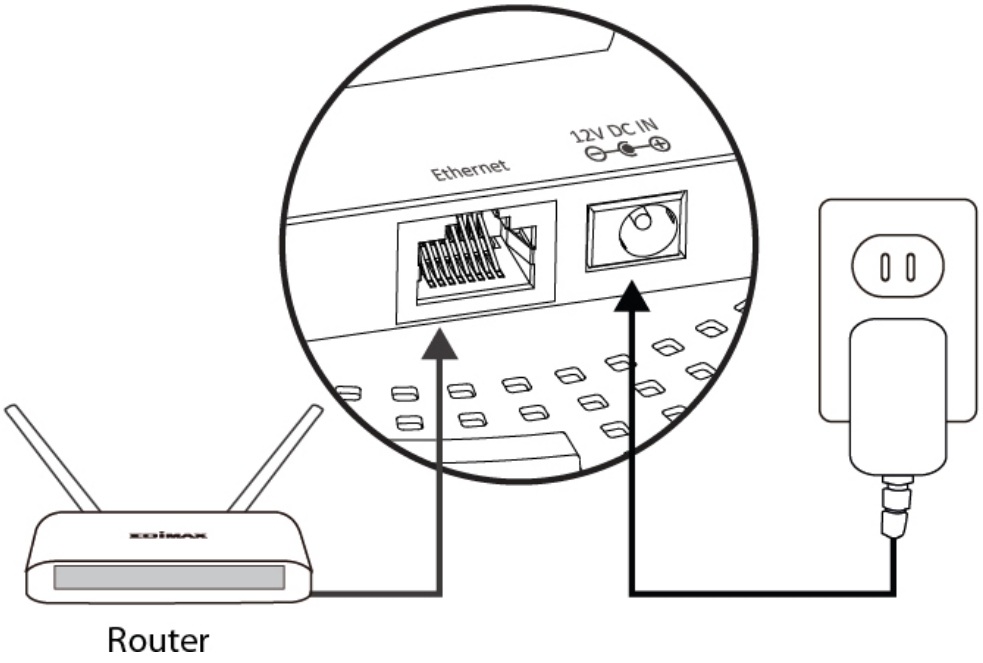
Router or Switch:

Connect the AP to a router or a PoE switch using an Ethernet cable.



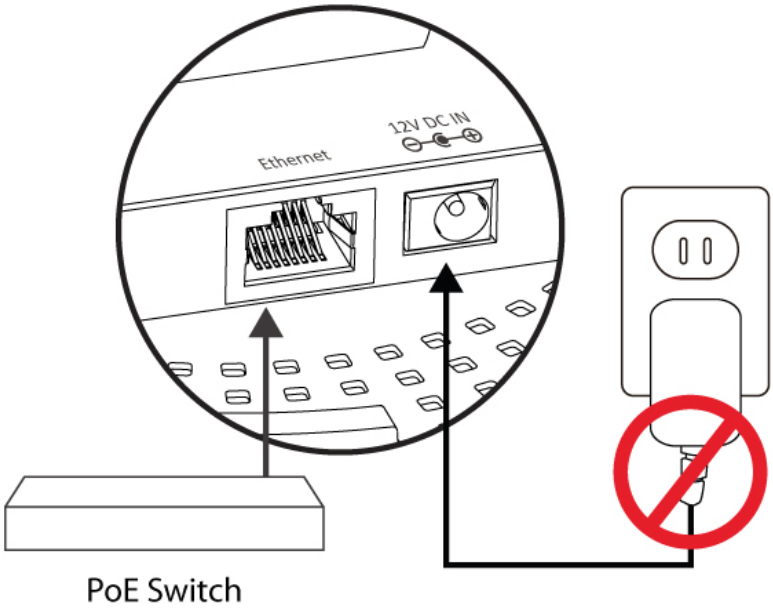
II-1. Connect AP to a router

If router is used, connect the power adapter to the AP and plug the power adapter into a power supply. Please wait a moment for the AP to start up. The AP is ready when the LED is **Blue**.



II-2. Connect AP to a switch

If PoE switch is used, make sure the Ethernet cable is connected to Ethernet port from the PoE switch. The AP will be powered by the switch.
Please wait a moment for the AP to start up. The AP is ready when the LED is **Blue**.



Do not use the power adapter if you are using a PoE switch.

II-3. Mounting

To mount the device to a ceiling, please follow the instructions below and refer to diagram **A** & **B**.

Wooden Ceiling:

Please refer to the figure below:

1. By using the holes **A** on the ceiling bracket, identify and mark correct screw positions of the desired mounting location.

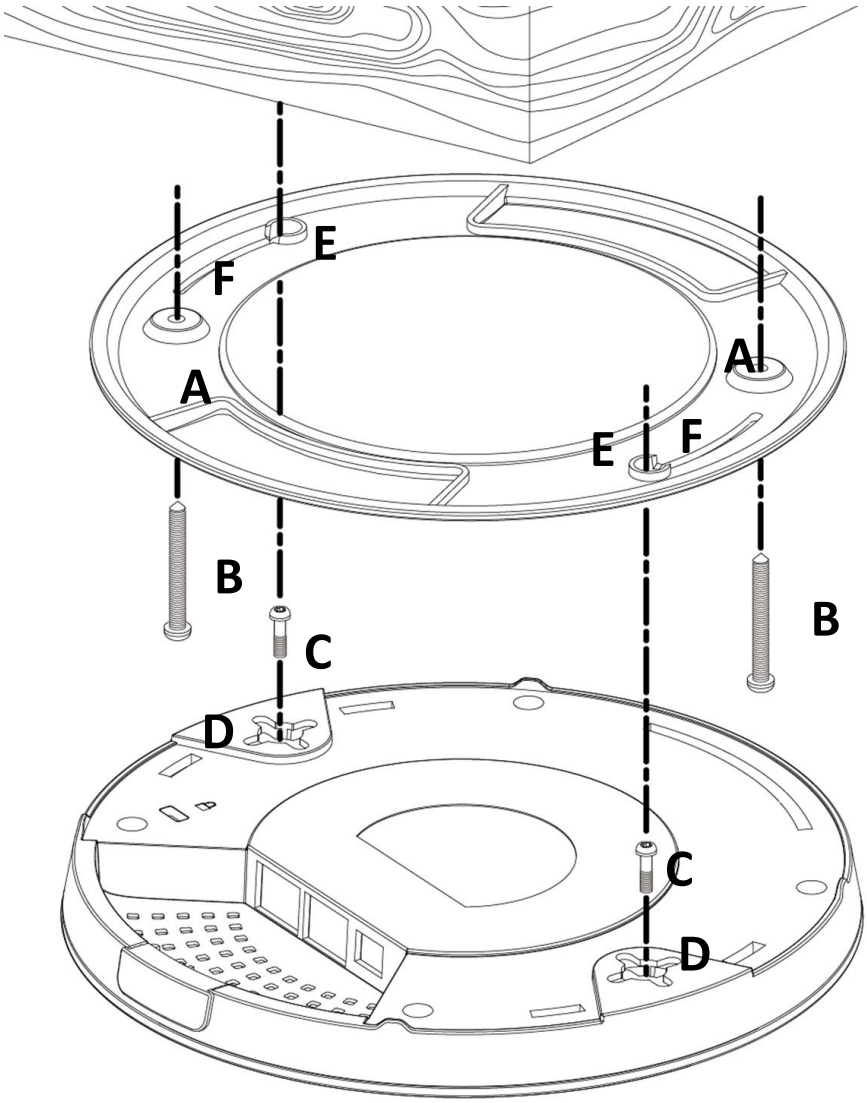
2. Where necessary, drill a hole (of radius smaller than the radius of the provided screws) on each of the marked screw positions.

3. Fix the ceiling mount bracket to the desired location by inserting the ceiling fixing screws **B** through the bracket ceiling holes **A**. Tighten the ceiling fixing screws **B** to the marked screw position using a screw driver to fix the bracket in place.

4. Fix the bracket rail screws **C** into the holes **D** on the device using a screw driver. The cap of the screws should be protruding outwardly from the holes **D**.

5. Insert the bracket rail screws **C** into the device fixing holes **E**.

6. Twist the device as the bracket rail screws **C** slide through the bracket rail **F**.
   Twist the device all the way until you feel that it is fixed in position.



Other Ceiling:

Please refer to the figure below:

1. By using the holes **A** on the ceiling bracket, identify and mark correct screw positions of the desired mounting location.

2. Where necessary, drill a hole on each of the marked screw positions.

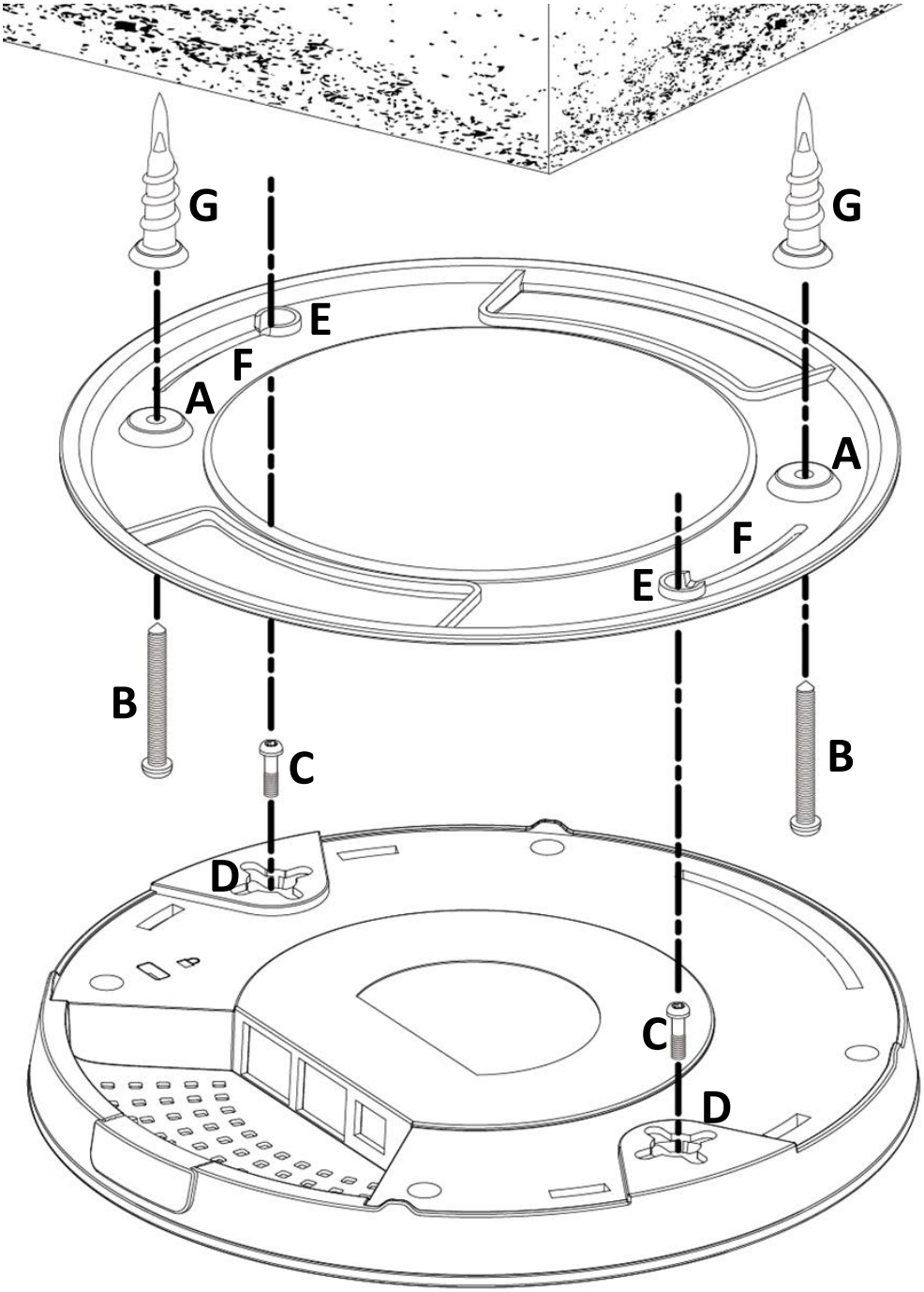
3. Insert the anchors **G** into the holes (use a screw driver where necessary) at the marked screw positions.

4. Fix the ceiling mount bracket to the desired location by inserting the ceiling fixing screws **B** through the bracket ceiling holes **A**. Tighten the ceiling fixing screws **B** onto the anchors **G** using a screw driver to fix the bracket to the ceiling.

5. Fix the bracket rail screws **C** into the holes **D** on the device using a screw driver. The cap of the screws should be protruding outwardly from the holes **D**.

6. Insert the bracket rail screws **C** into the device fixing holes **E**.

7. Twist the device as the bracket rail screws **C** slide through the bracket rail **F**.
   Twist the device all the way until you feel that it is fixed in position.


G
G
E
F
A
A
F
E
B
B
C
C
D
D

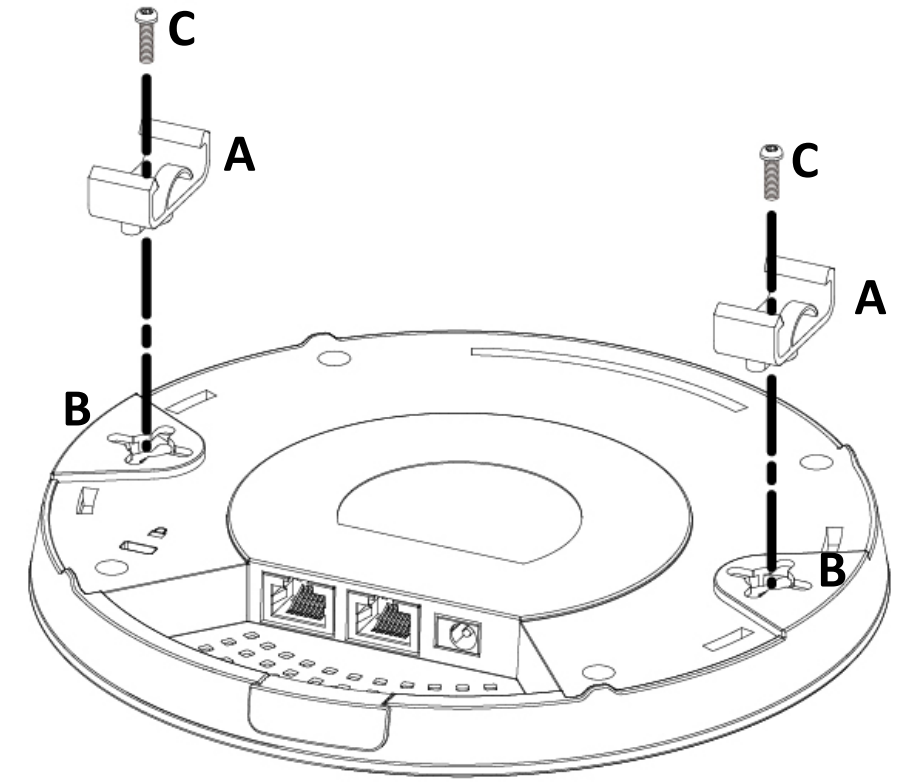
T-Rail Mount:

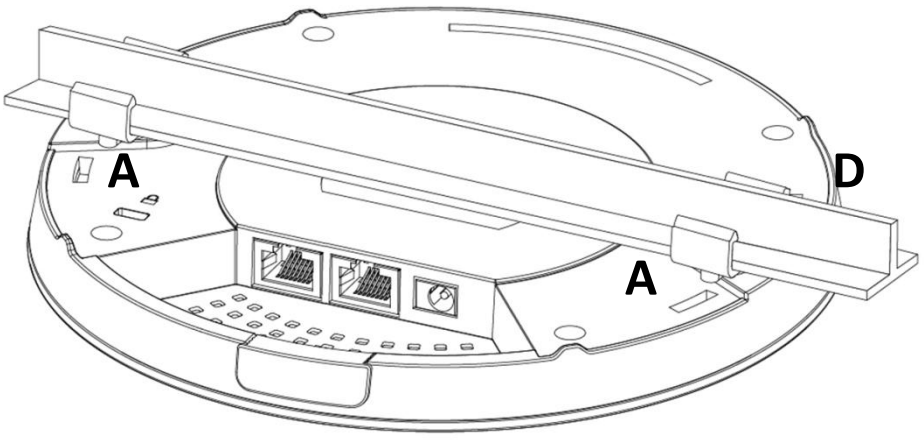
To mount the device to a T-Rail, please follow the instructions below and refer to the diagrams below.

1. Select the correct size T-Rail bracket included in the package contents.

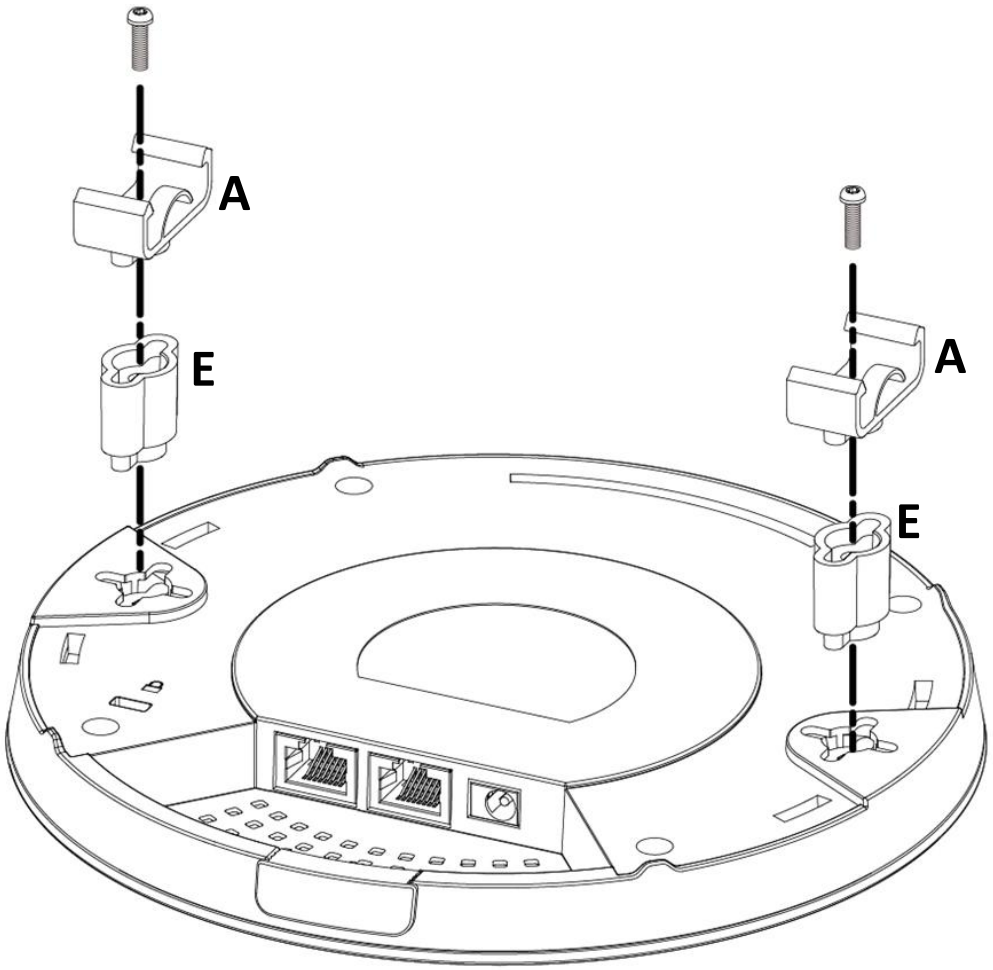
2. Attach the selected T-Rail brackets **A** to holes **B** using bracket fixing screws **C**.

3. Clip the device onto the T-Rail **D** using the now attached T-Rail brackets **A**.





If you need more space between the device and the T-Rail, additional cushion bracket E can be added between T-Rail brackets A and holes B (use the longer screws included).



III. *Quick Setup (AP Mode)*

This quick installation section will help you setup your AP in its default AP mode and configure its basic settings.

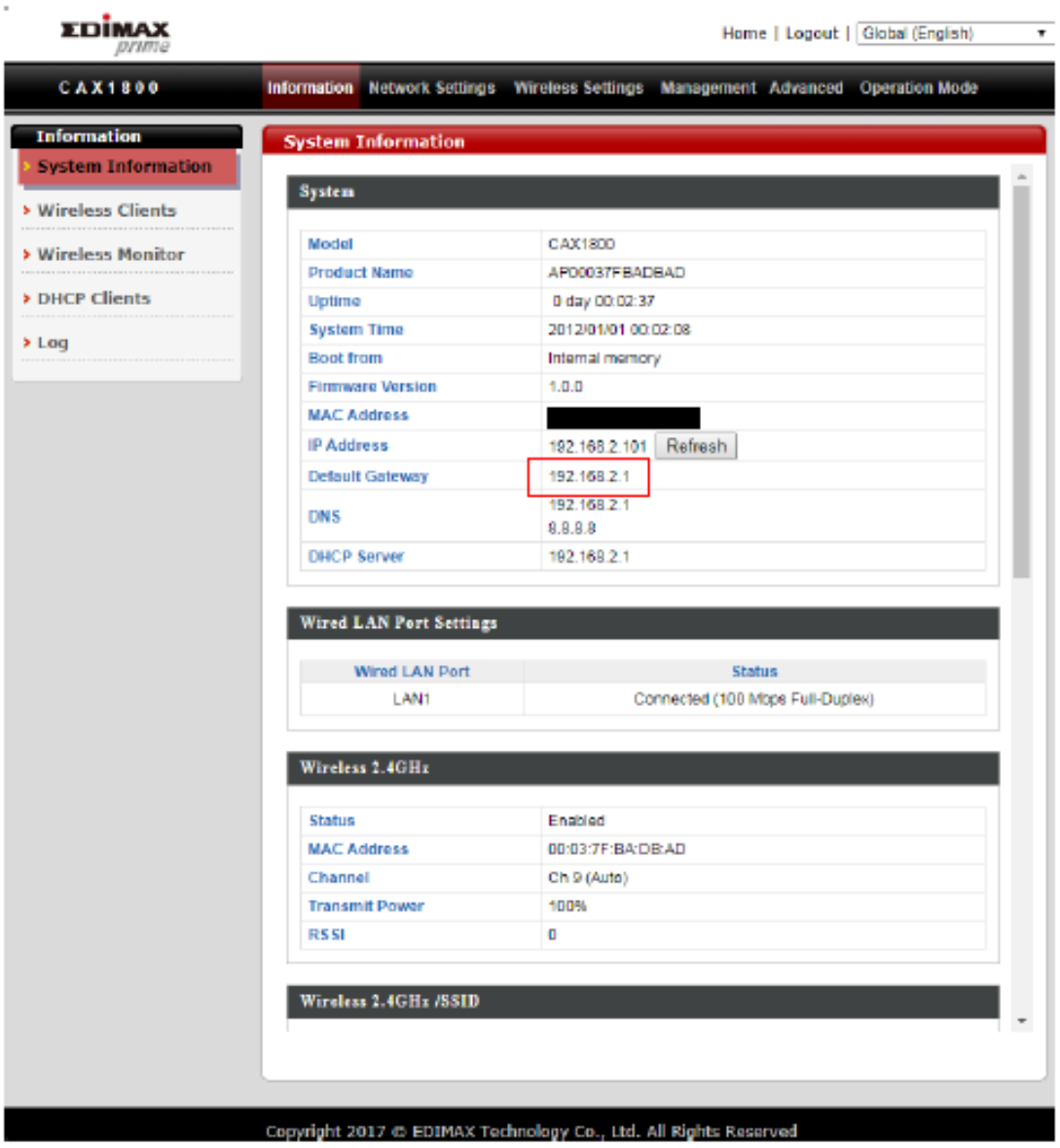
Please follow the steps below:

1. Enter the AP's default IP address "192.168.2.2" into the URL bar of a web browser.

Please ensure to set your computer's IP address to "192.168.2.X" where X is a number in the range 3 ~ 100.

2. You will be prompted for a username and password. Enter the default username "admin" and password "1234".

3. Home screen will be shown.

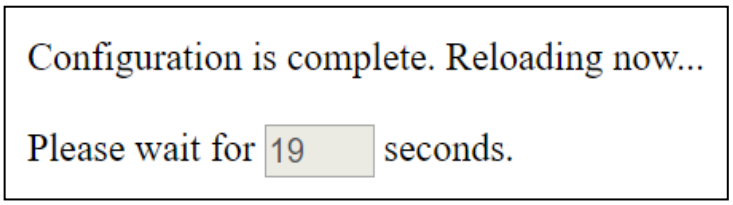


IV. Basic Settings

In our recommendation, please check each of the settings that listed below before using the AP.

- LAN IP Address
- 2.4GHz & 5GHz SSID & Security
- Administrator Name & Password
- Time & Date

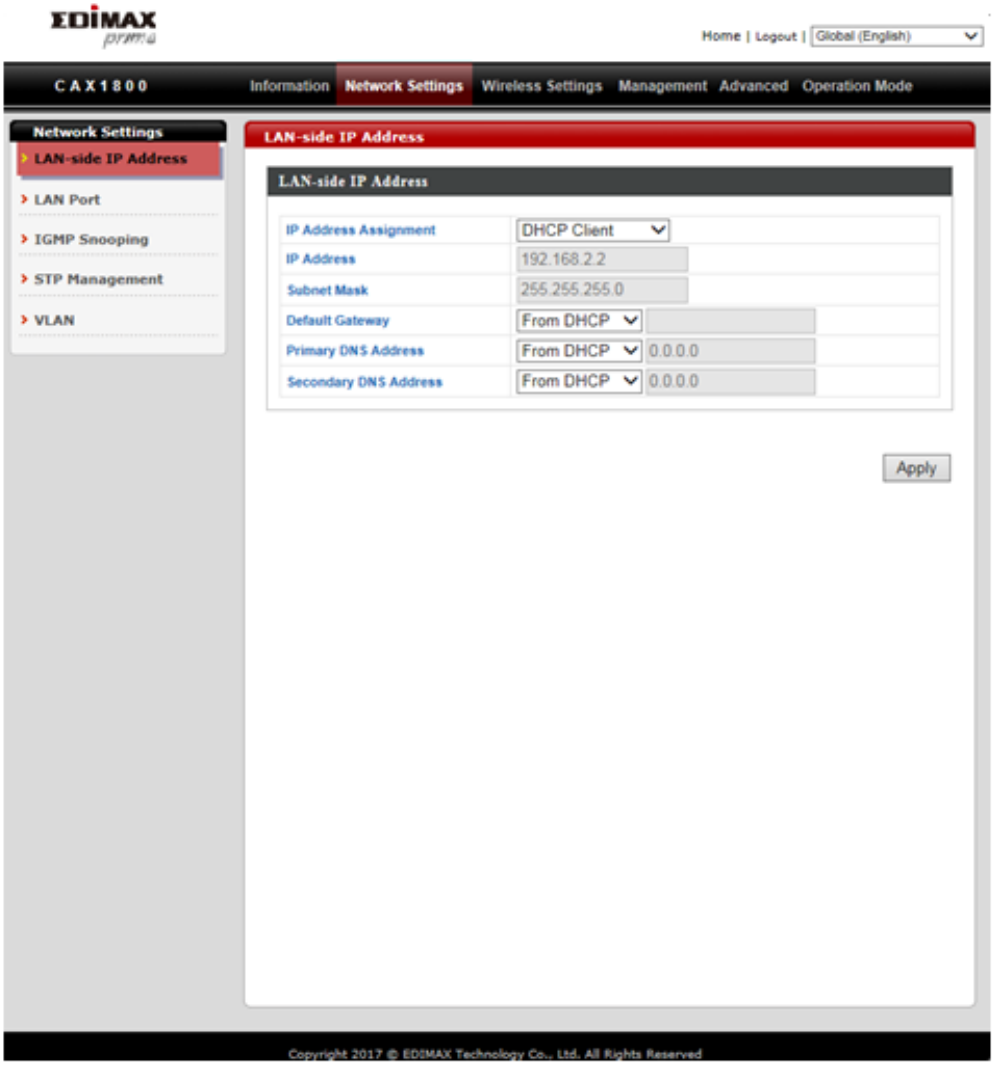
Please note that whenever a new setting is applied to the AP, the webpage will reload, as shown below:



Please follow the instructions below for the basic settings.

IV-1. Changing IP Address

1. Go to “Network Settings” and tap “LAN-side IP Address”.



2. Enter the IP address settings you wish to use for your AP. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click “Apply” to save the changes and wait a few moments for the AP to reload.

When you change your AP’s IP address, you need to use the new IP address to access the browser based configuration interface instead of the default IP 192.168.2.2.

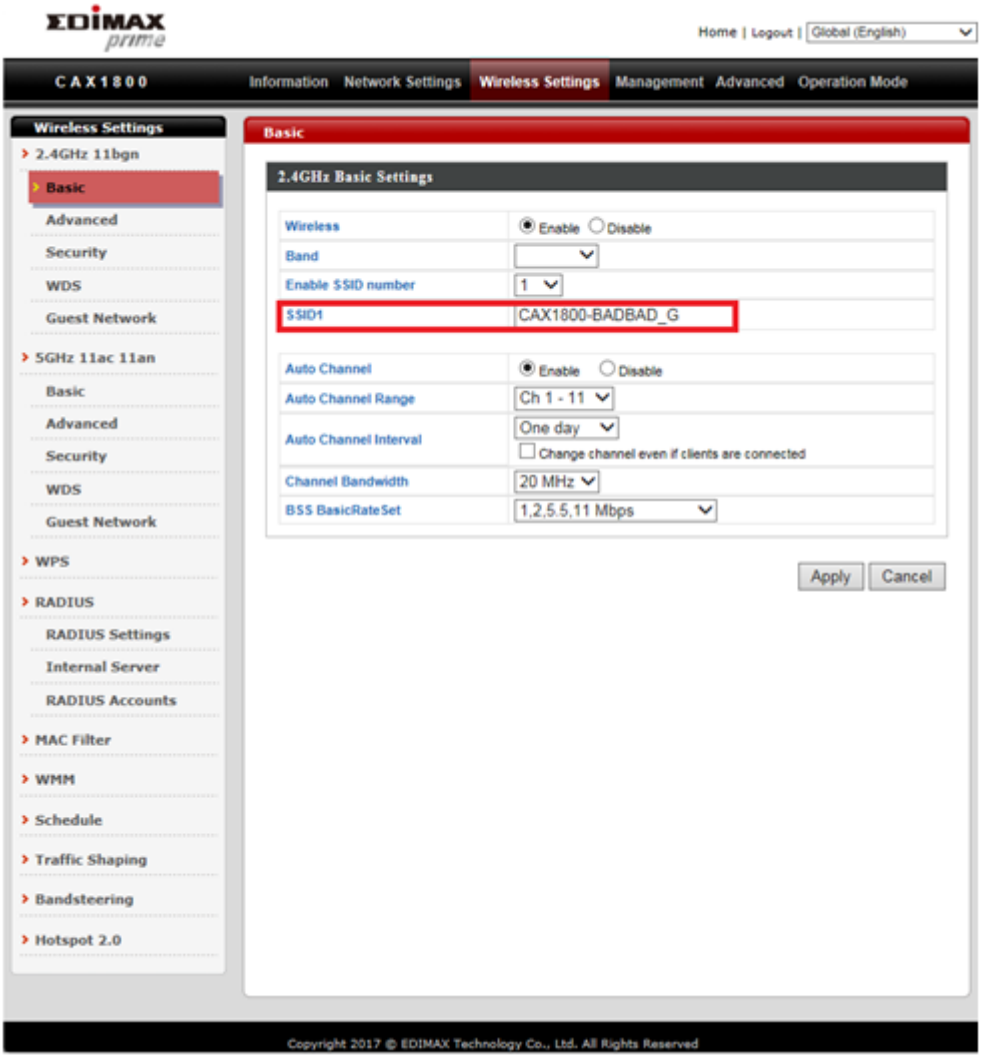
IV-2. Changing SSID For 2.4GHz Wireless Network

1. Go to “Wireless Settings”.

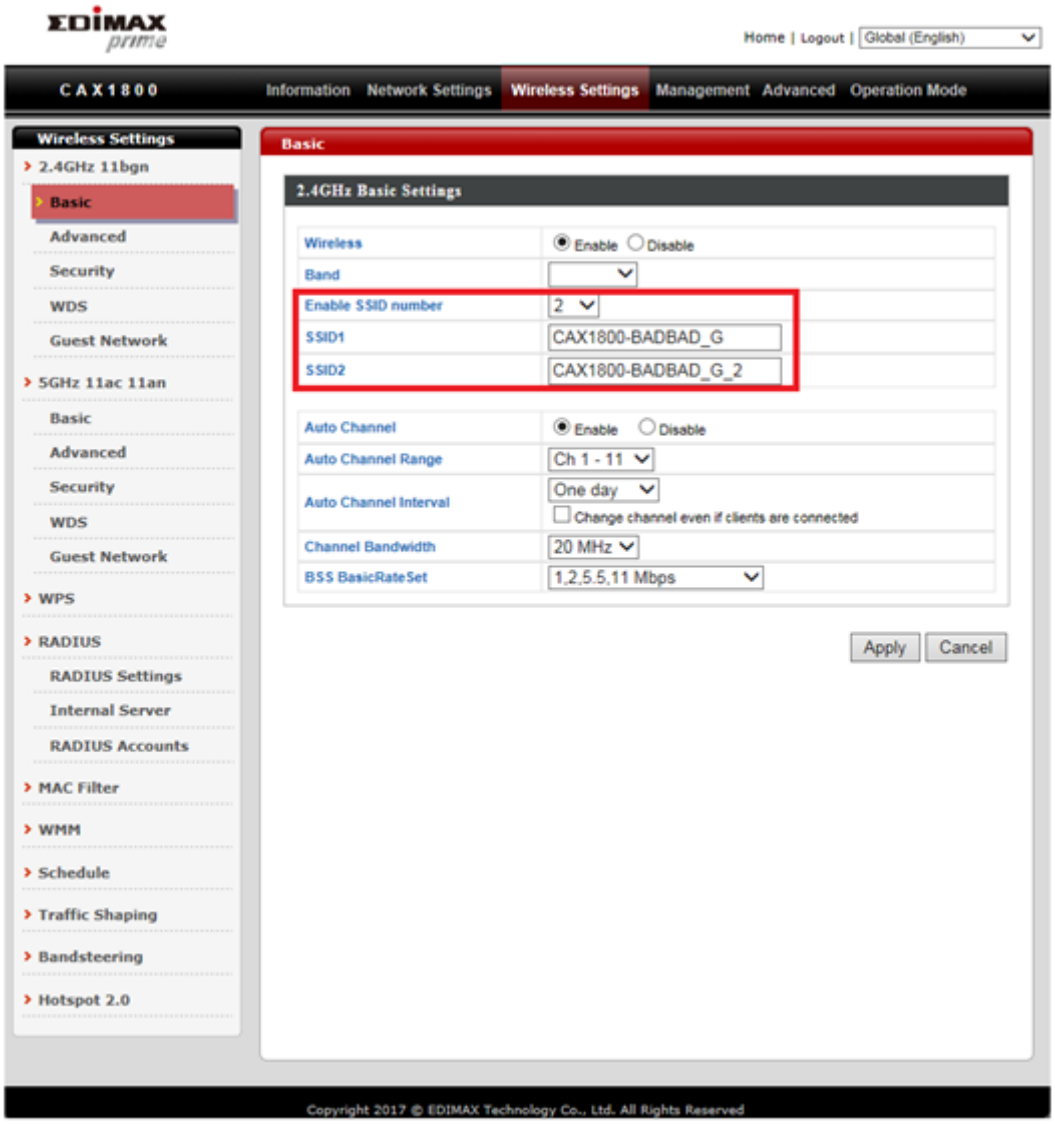
2. Tap “2.4GHz 11bgn”.

3. Tap “Basic”.

4. Enter the new SSID for your 2.4GHz wireless network in the “SSID1” field and click “Apply”.



To utilize multiple 2.4GHz SSIDs, open the drop down menu labelled “Enable SSID number” and select how many SSIDs you require. Then enter a new SSID in the corresponding numbered fields below, before clicking “Apply”.



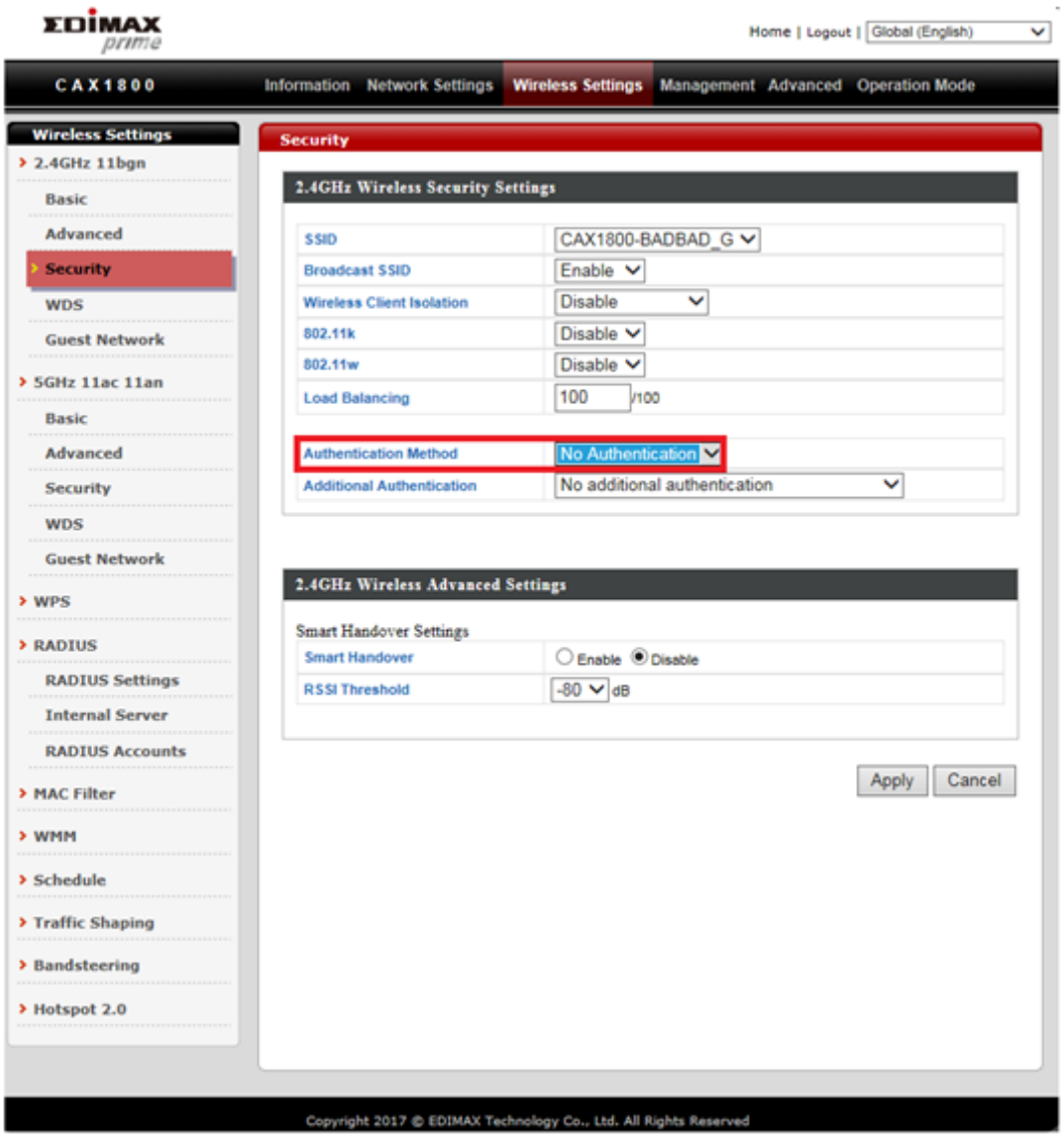
IV-3. Configuring Security Settings of 2.4GHz wireless network

1. Go to “Wireless Settings”.

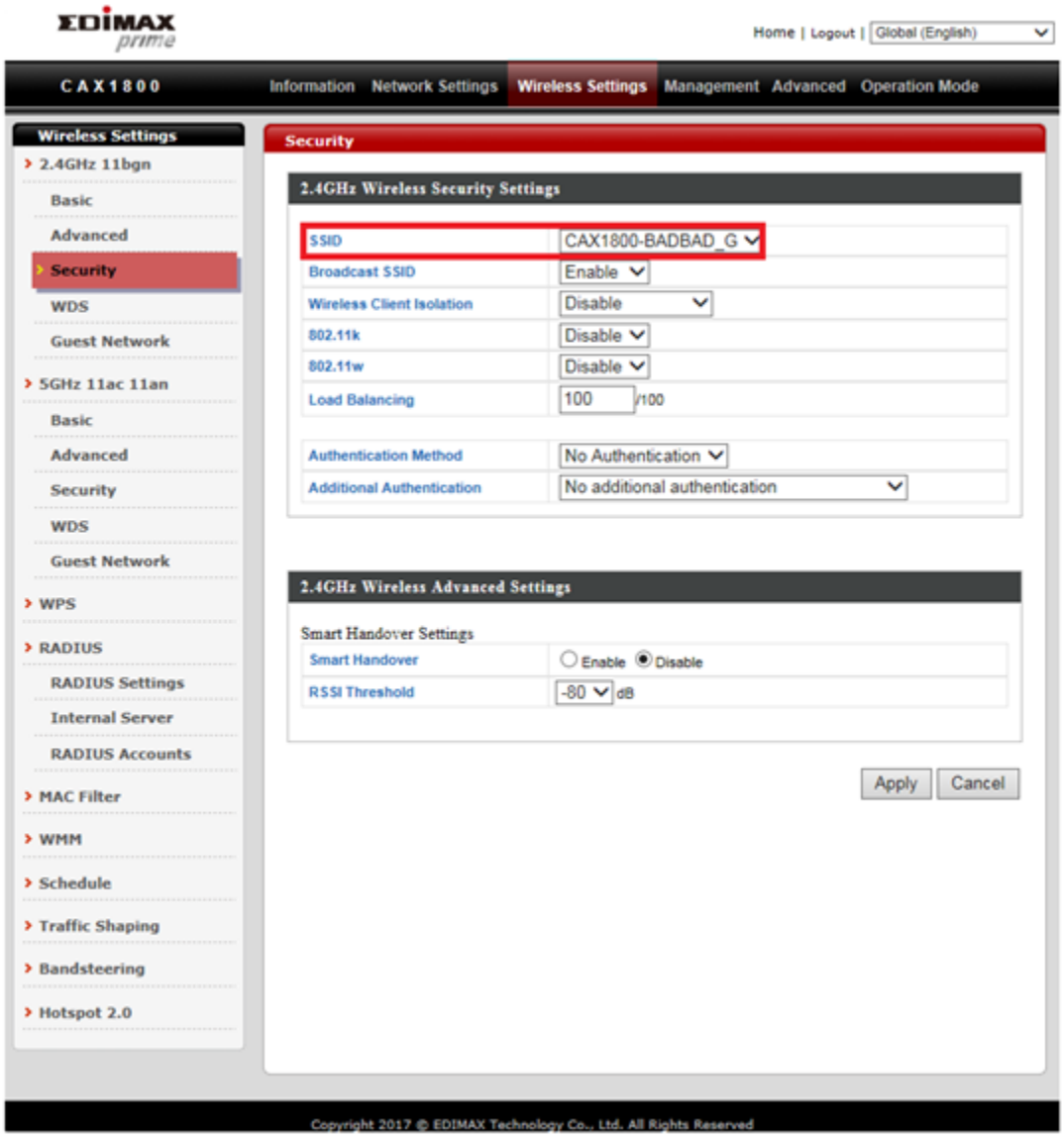
2. Tap “2.4GHz 11bgn”.

3. Tap “Security”.

4. Select an “Authentication Method”, enter or select fields where appropriate, and click “Apply”.



If multiple SSIDs are used, specify which SSID to configure using the "SSID" drop down menu.



IV-4. Changing Security Setting for 5GHz wireless network

Follow the steps outlined in “Changing SSID for 2.4GHz wireless network” and “Configuring Security Setting for 2.4GHz wireless network” but choose the 5GHz option instead.

IV-5. Changing Admin Name and Password

1. Go to “Management”.

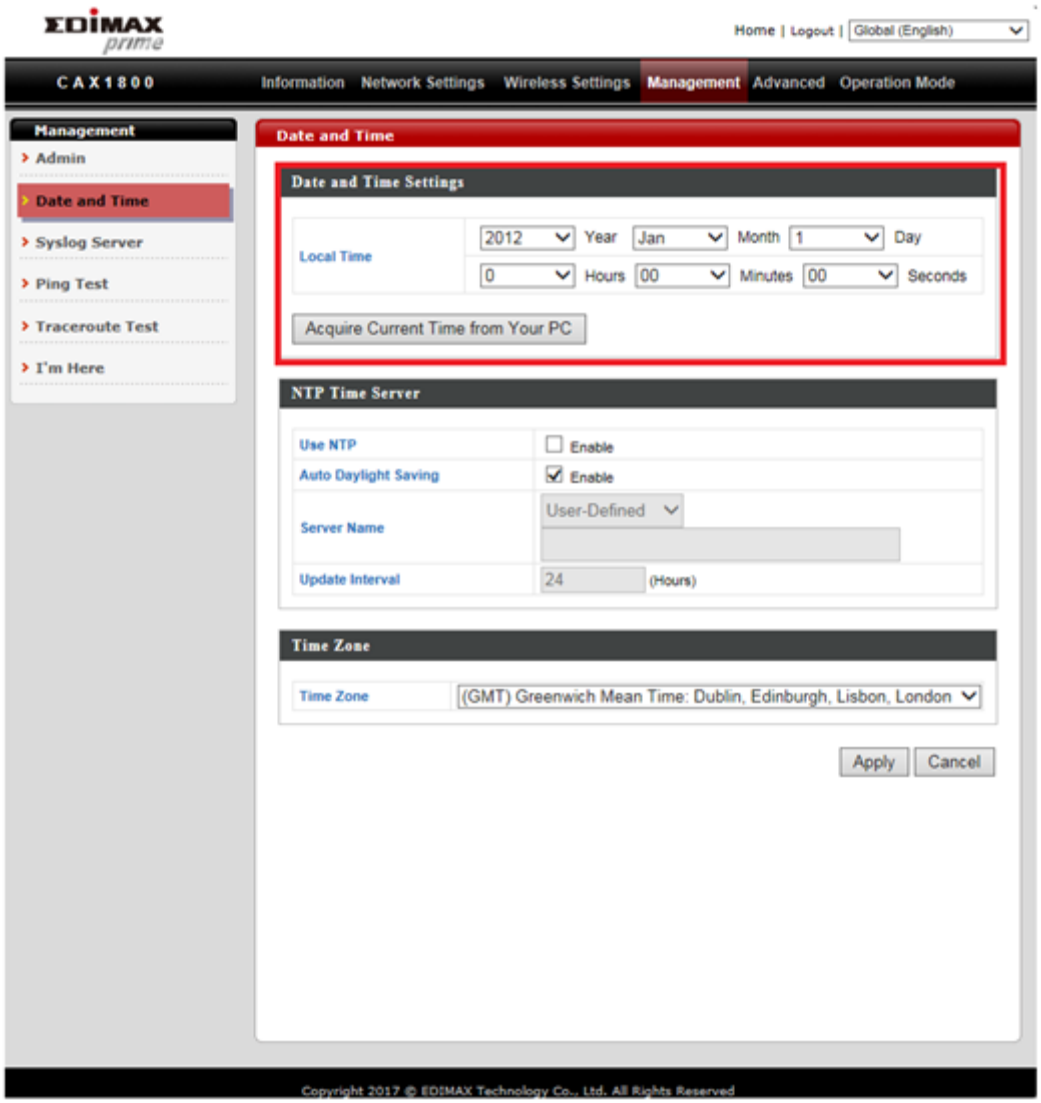
2. Tap “Admin”.

3. Complete the “Administrator Name” and “Administrator Password” fields and click “Apply”.

IV-6. Changing Date and Time

1. Go to “Management”.

2. Tap “Date and Time”.



3. Set the correct time and time zone for your AP using the drop down menus. The AP also supports NTP (Network Time Protocol). Alternatively, you can enter the host name or IP address of a time server. Click “Apply” when you are finished.

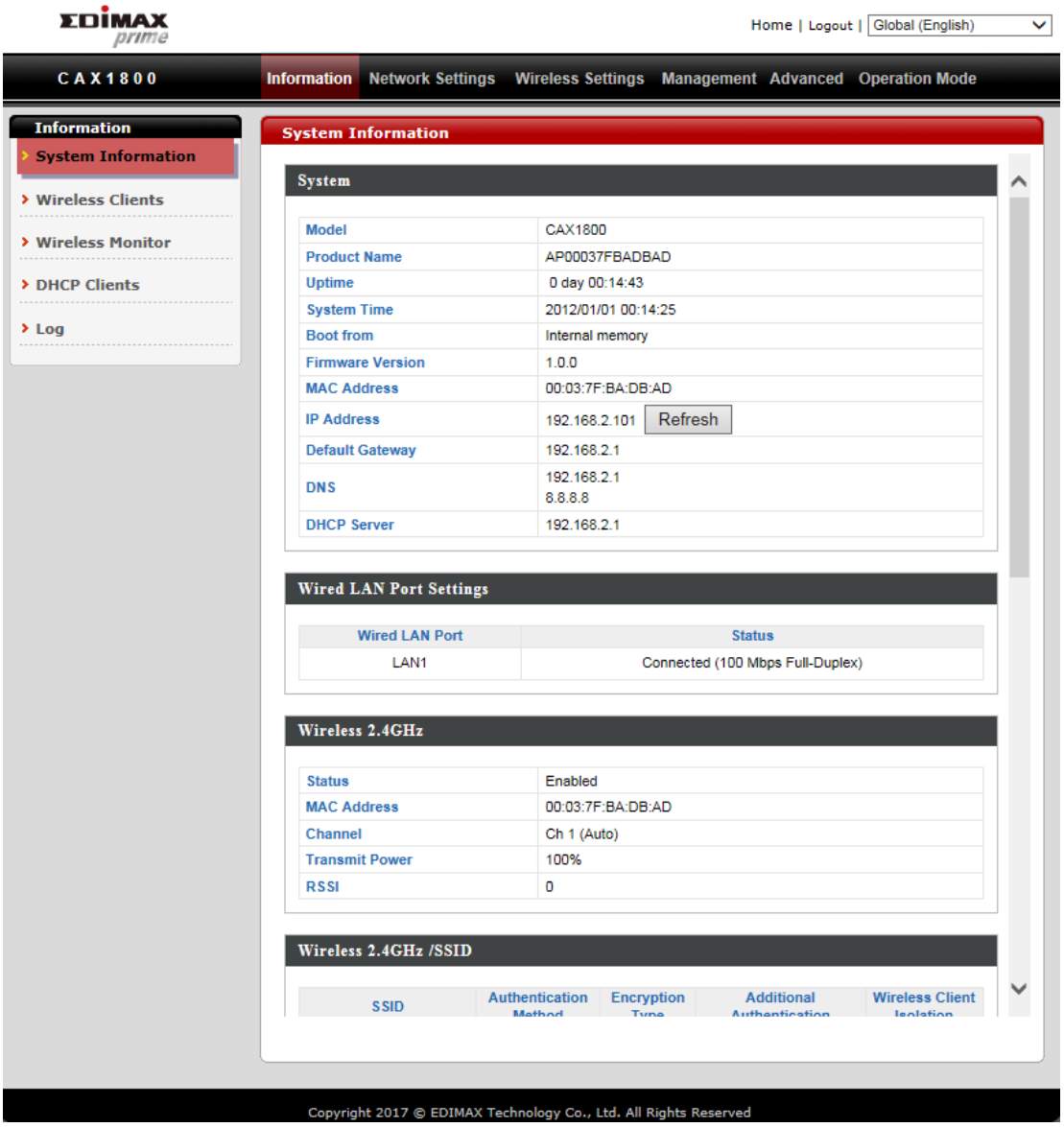
You can use the “Acquire Current Time from Your PC” button if you wish to set the AP to the same time as your PC.

Congrats! The basic settings of your AP are now configured and your AP is up and running!

V. CAX1800 Settings

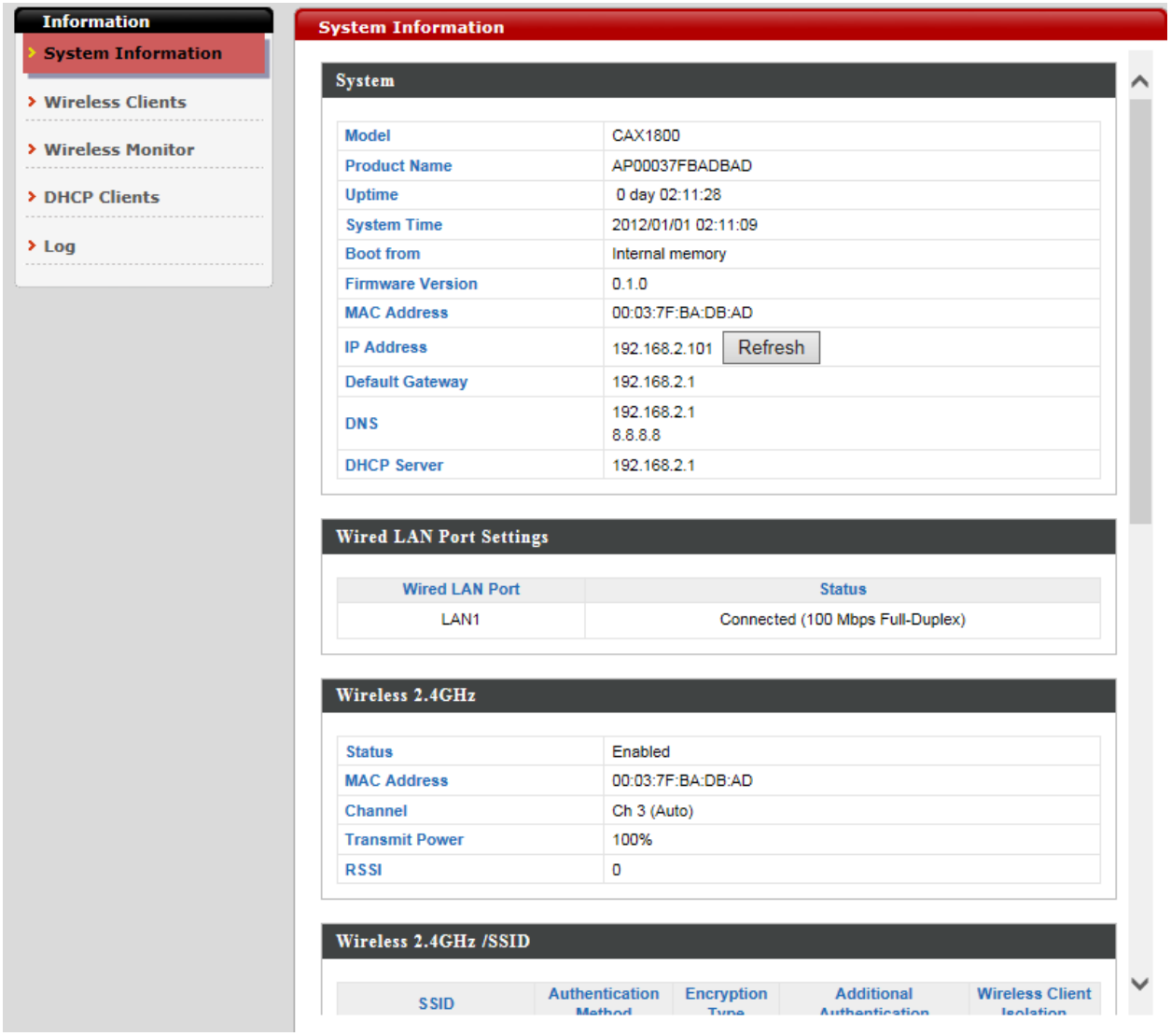
The CAX1800 features a range of advanced functions. Please open a browser and enter the CAX1800 default IP address “192.168.2.2” to access the AP configuration webpage.

V-1. Information



i. System Information

"System Information" page displays basic system information.



System	
Model	Displays the model number of the AP.
Product Name	Displays the product name for reference, which consists of "AP" plus the MAC address.
Uptime	Displays the total time since the device was turned on.
System Time	Displays the system time.
Boot From	Displays information for the booted hardware, booted from internal memory.
Firmware Version	Displays the firmware version.
MAC Address	Displays the AP's MAC address.
Management VLAN ID	Displays the management VLAN ID.
IP Address	Displays the IP address of this device. (Click "Refresh" to update this value)
Default Gateway	Displays the IP address of the default gateway.
DNS	IP address of DNS (Domain Name Server)
DHCP Server	IP address of DHCP Server.

Wired LAN Port Settings	
Wired LAN Port	Specifies which LAN port.
Status	Displays the status of the specified LAN port. (Connected or disconnected)
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port.

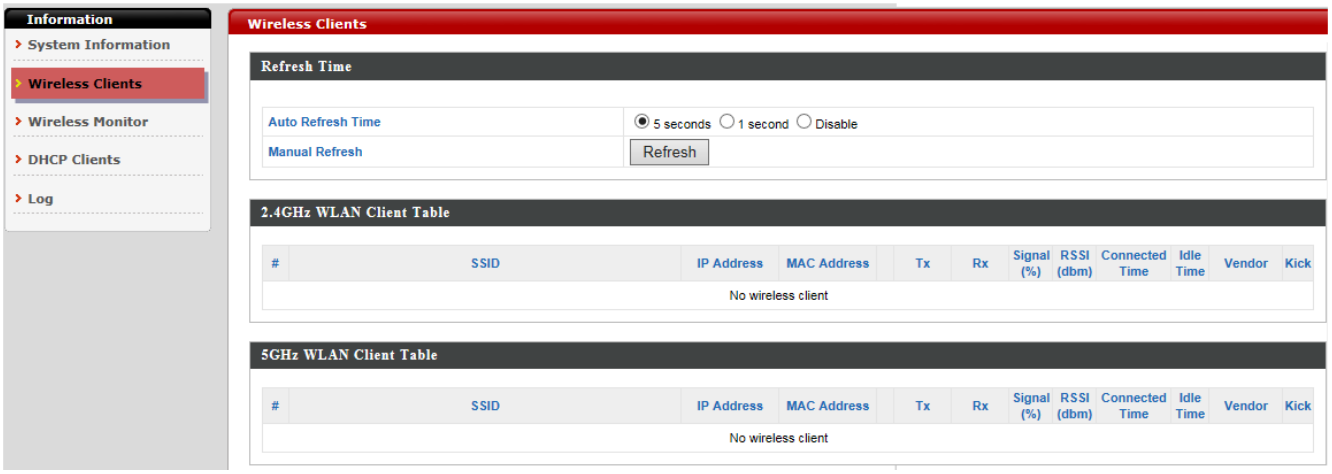
Wireless 2.4GHz (5GHz)	
Status	Displays the status of the 2.4GHz or 5GHz wireless. (Enabled or disabled)
MAC Address	Displays the AP MAC address.
Channel	Displays the channel number the specified wireless frequency is using for broadcast.
Transmit Power	Displays the wireless radio transmit power level as a percentage.
RSSI	Received Signal Strength Indicator (RSSI) is a measurement of the power present in a received radio signal.

Wireless 2.4GHZ (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID.
Encryption Type	Displays the encryption type for the specified SSID.
VLAN ID	Displays the VLAN ID for the specified SSID.
Additional Authentication	Displays the additional authentication type for the specified SSID.
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID.

Wireless 2.4GHZ (5GHz) / WDS Status	
MAC Address	Displays the peer AP MAC address.
Encryption Type	Displays the encryption type for the specified WDS.
VLAN Mode/ID	Displays the VLAN ID for the specified WDS.

ii. Wireless Clients

"Wireless Clients" page displays information about all wireless clients connected to the device on the 2.4GHz or 5GHz frequency.

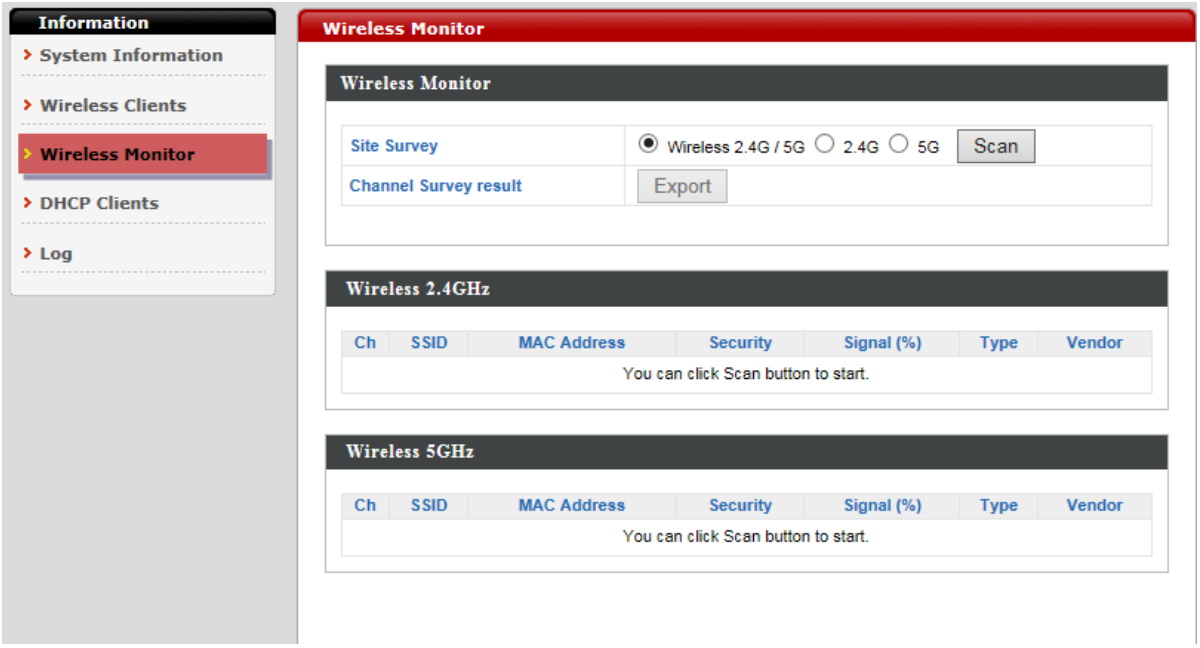


Refresh time	
Auto Refresh Time	Select a time interval for the client table list to automatically refresh.
Manual Refresh	Click refresh to manually refresh the client table.

2.4GHz (5GHz) WLAN Client Table	
SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.
Signal (%)	Displays the wireless signal strength for the specified client.
Connected Time	Displays the total time the wireless client has been connected to the AP.
Idle Time	Client idle time is the time for which the client has not transmitted any data packets.
Vendor	The vendor of the client's wireless adapter is displayed here.

iii. Wireless Monitor

"Wireless Monitor" is a tool built into the device to scan and monitor the surrounding wireless environment. Select a frequency and click "Scan" to display a list of all SSIDs within range along with relevant details for each SSID.



Wireless Monitor	
Site Survey	Select which frequency (or both) to scan, and click "Scan" to begin.
Channel Survey Result	After a scan is complete, click "Export" to save the results to local storage.

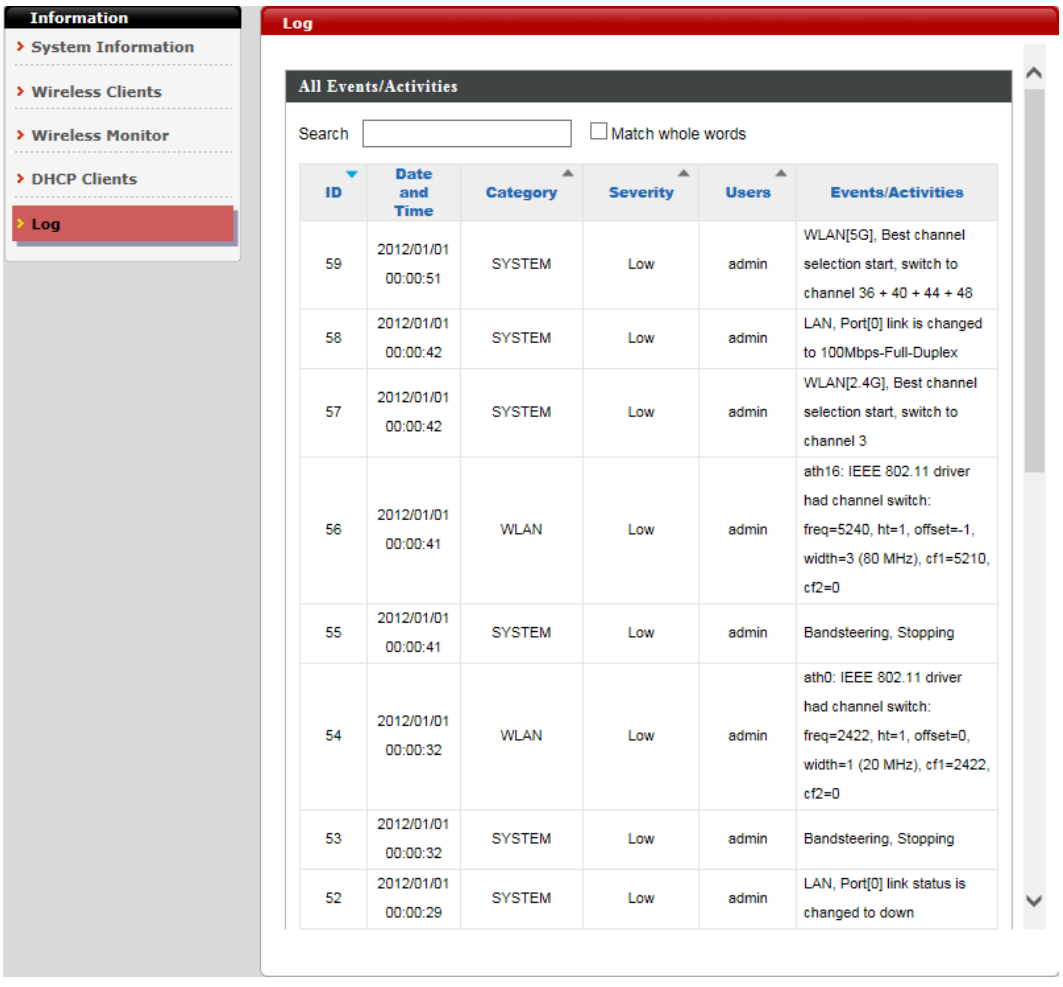
Site Survey Results	
Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/AP for the specified SSID.
Security	Displays the authentication/encryption type of the specified SSID.
Signal (%)	Displays the current signal strength of the SSID.
Type	Displays the 802.11 wireless networking standard(s) of the specified SSID.
Vendor	Displays the vendor of the wireless router/AP for the specified SSID.

iv. DHCP Clients

"DHCP Clients" shows information of DHCP leased clients.

v. Log

"System log" displays system operation information such as up time and connection processes. This information is useful for administrators.



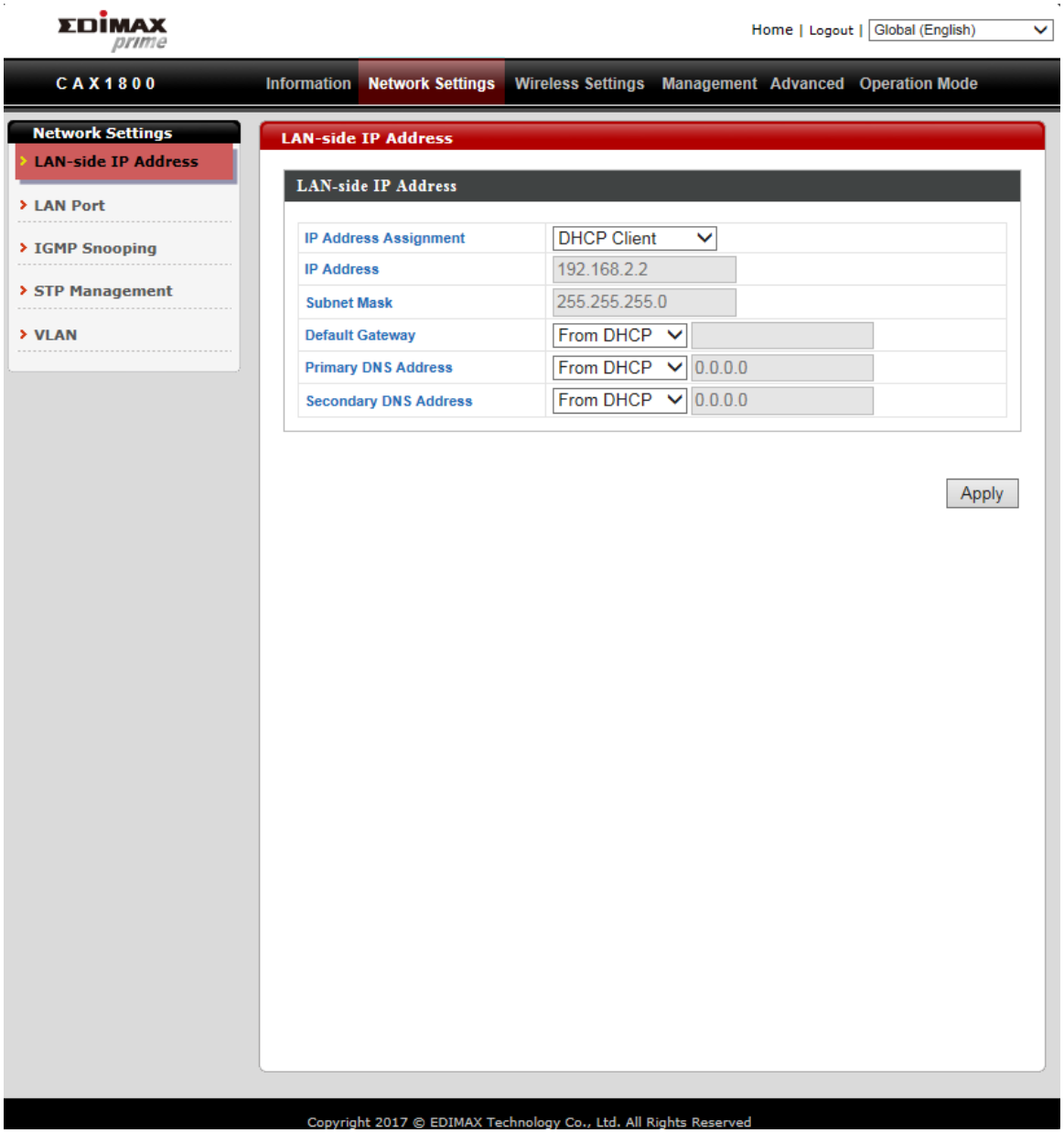
ID	Date and Time	Category	Severity	Users	Events/Activities
59	2012/01/01 00:00:51	SYSTEM	Low	admin	WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
58	2012/01/01 00:00:42	SYSTEM	Low	admin	LAN, Port[0] link is changed to 100Mbps-Full-Duplex
57	2012/01/01 00:00:42	SYSTEM	Low	admin	WLAN[2.4G], Best channel selection start, switch to channel 3
56	2012/01/01 00:00:41	WLAN	Low	admin	ath16: IEEE 802.11 driver had channel switch: freq=5240, ht=1, offset=-1, width=3 (80 MHz), cf1=5210, cf2=0
55	2012/01/01 00:00:41	SYSTEM	Low	admin	Bandsteering, Stopping
54	2012/01/01 00:00:32	WLAN	Low	admin	ath0: IEEE 802.11 driver had channel switch: freq=2422, ht=1, offset=0, width=1 (20 MHz), cf1=2422, cf2=0
53	2012/01/01 00:00:32	SYSTEM	Low	admin	Bandsteering, Stopping
52	2012/01/01 00:00:29	SYSTEM	Low	admin	LAN, Port[0] link status is changed to down

Older entries will be overwritten when the log is full.

The following information/events are recorded by the log:

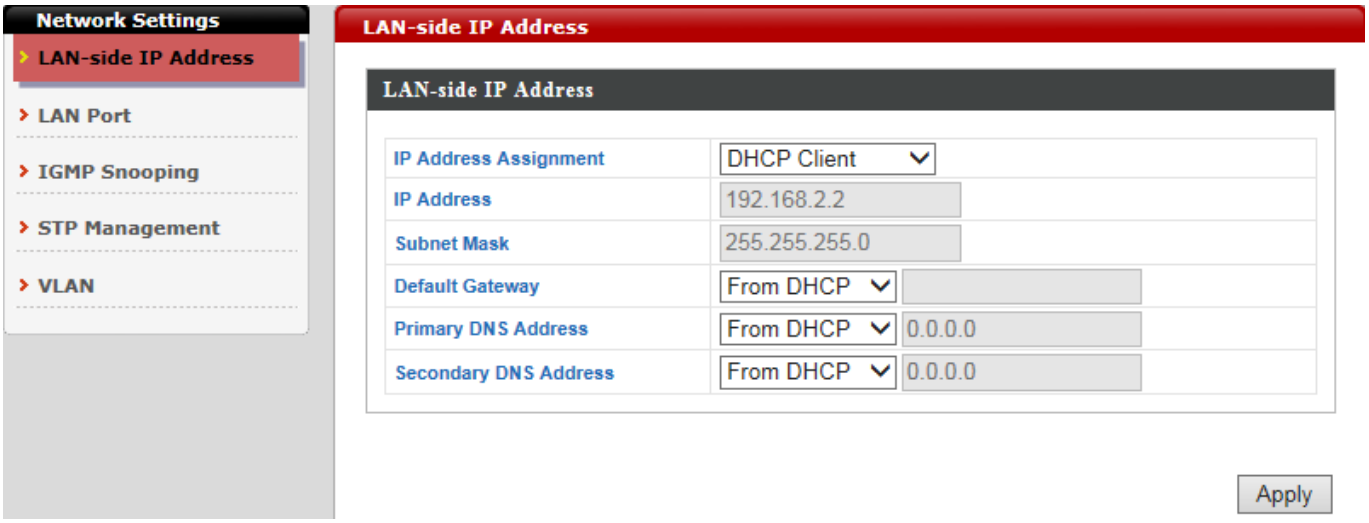
Log (Category)	
USB	Mount & un-mount
Wireless Client	Connected & disconnected Key exchange success & fail
Authentication	Authentication fail or successful
Association	Success or fail
WPS	M1 - M8 messages WPS success
Change Settings	Displays the total time the wireless client has been connected to the AP
System Boot	Displays current model name
Vendor	The vendor of the client's wireless adapter is displayed here
NTP Client	Syncing time with NTP server
Wired Link	LAN Port link status and speed status
Proxy ARP	Proxy ARP module start & stop
Bridge	Bridge start & stop
SNMP	SNMP server start & stop
HTTP	HTTP start & stop
HTTPS	HTTPS start & stop
SSH	SSH-client server start & stop
Telnet	Telnet-client server start or stop
WLAN (2.4G) and (5G)	WLAN (2.4G) and (5G) channel status and country/region status

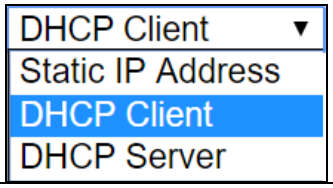
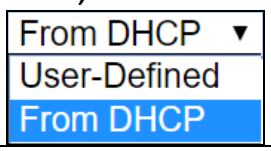
V-2. Network Settings

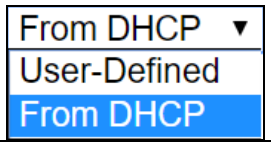
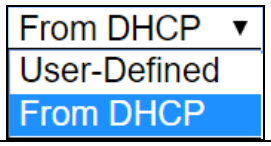


i. LAN-side IP Address

"LAN-side IP address" allows users to configure your AP on your LAN. You can enable the AP to dynamically receive an IP address from your router's DHCP server or you can specify a static IP address for your AP, as well as configure DNS servers.



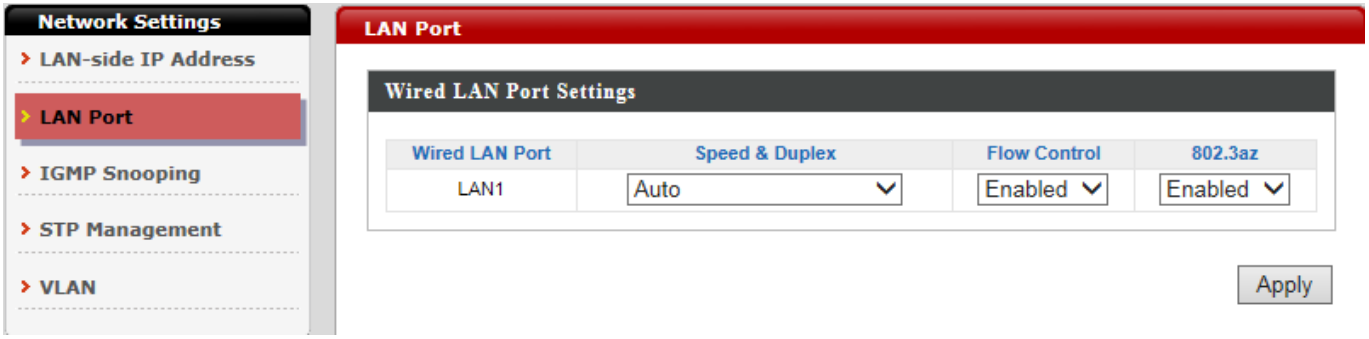
LAN-side IP Address	
IP Address Assignment	Select “DHCP Client” for your AP to be assigned a dynamic IP address from your router’s DHCP server. Select “Static IP” to manually specify a static/fixed IP address for your AP. Select “DHCP Server” for your AP to assign a dynamic IP address to your PC. You will have to set a Primary DNS address and a Secondary DNS address. For example, Google’s Primary DNS address is 8.8.4.4 and Secondary DNS address is 8.8.8.8. 
IP Address	Specify the IP address here. This IP address will be assigned to your AP and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank. 

Primary DNS Address	DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank. 
Secondary DNS Address	Users can manually enter a value when DNS server’s primary address is set to “User-Defined”. 

NOTE: DHCP users can select to get DNS servers’ IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

ii. LAN Port

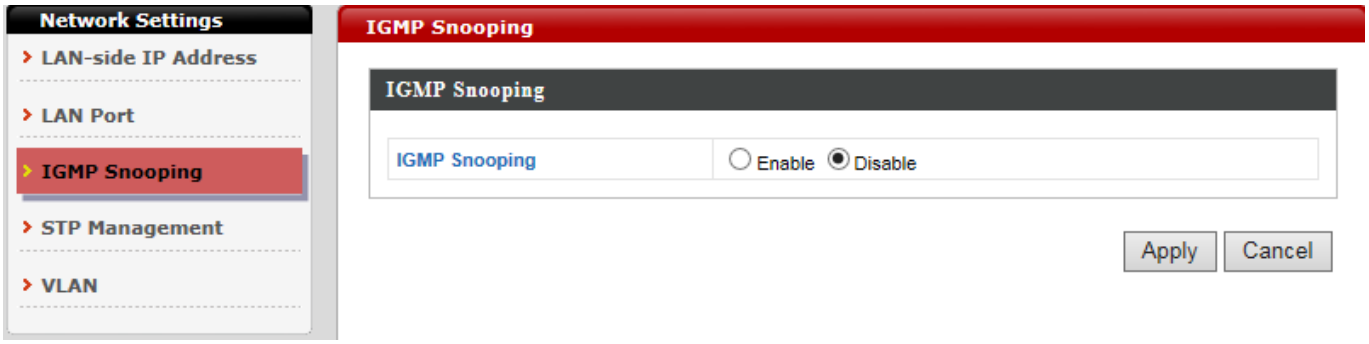
"LAN Port" allows users to configure the settings for LAN port.



Wired LAN Port	Identifies LAN port 1.
Enable	Enable/disable specified LAN port.
Speed & Duplex	Select a speed & duplex type for specified LAN port, or use the "Auto" value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packets transfer/receive. Auto Auto 10 Mbps Half-Duplex 10 Mbps Full-Duplex 100 Mbps Half-Duplex 100 Mbps Full-Duplex 1000 Mbps Full-Duplex
Flow Control	Enable/disable flow control. Flow control can pause new session request until current data processing is complete, in order to avoid device overloads under heavy traffic.
802.3az	Enable/disable 802.3az. 802.3az. 802.3az is an energy efficient Ethernet feature which disables unused interfaces to reduce power usage.

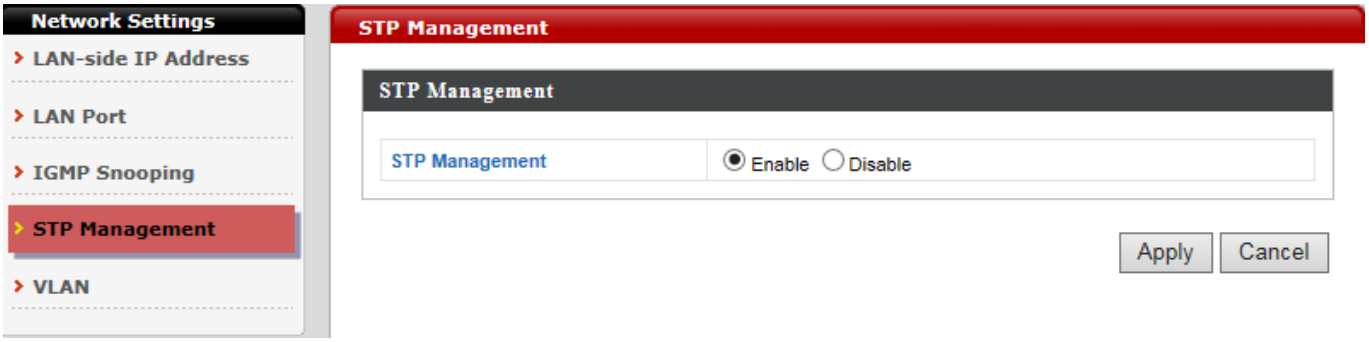
iii. IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams.



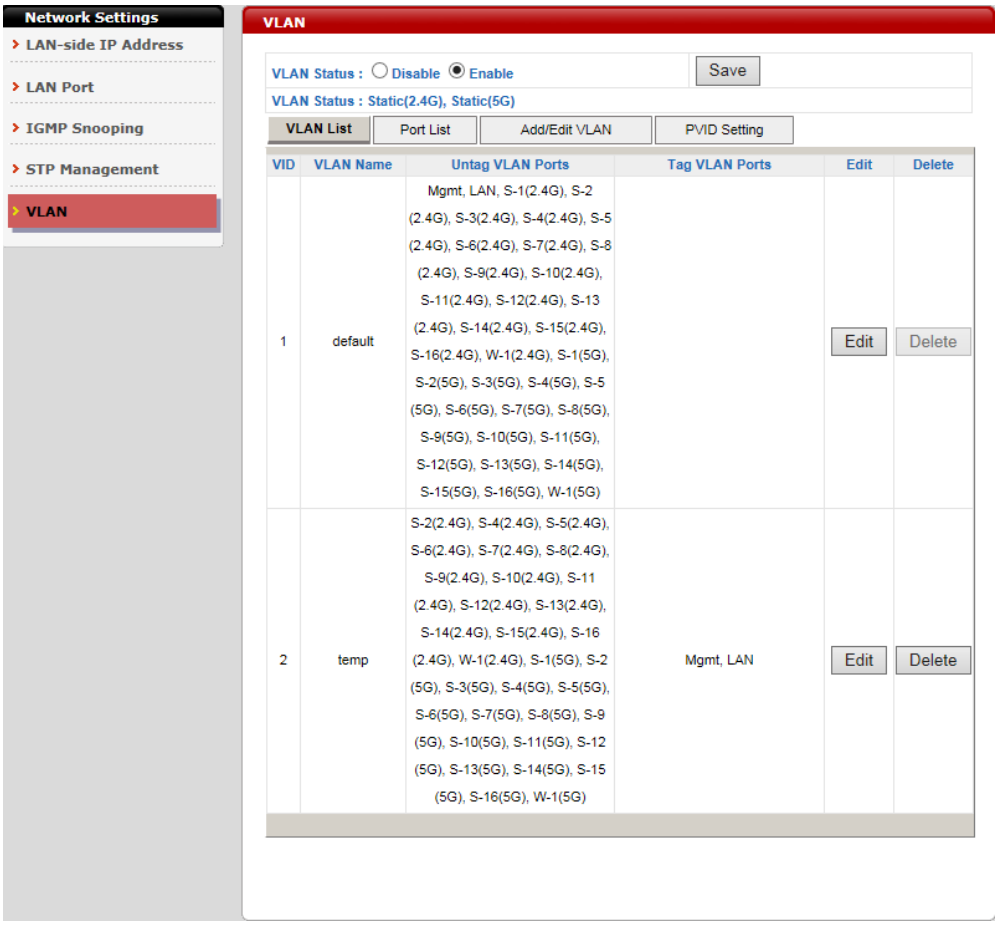
iv. STP Management

When enabled, STP ensures that you do not create loops when you have redundant paths in your network.



v. VLAN

VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other.

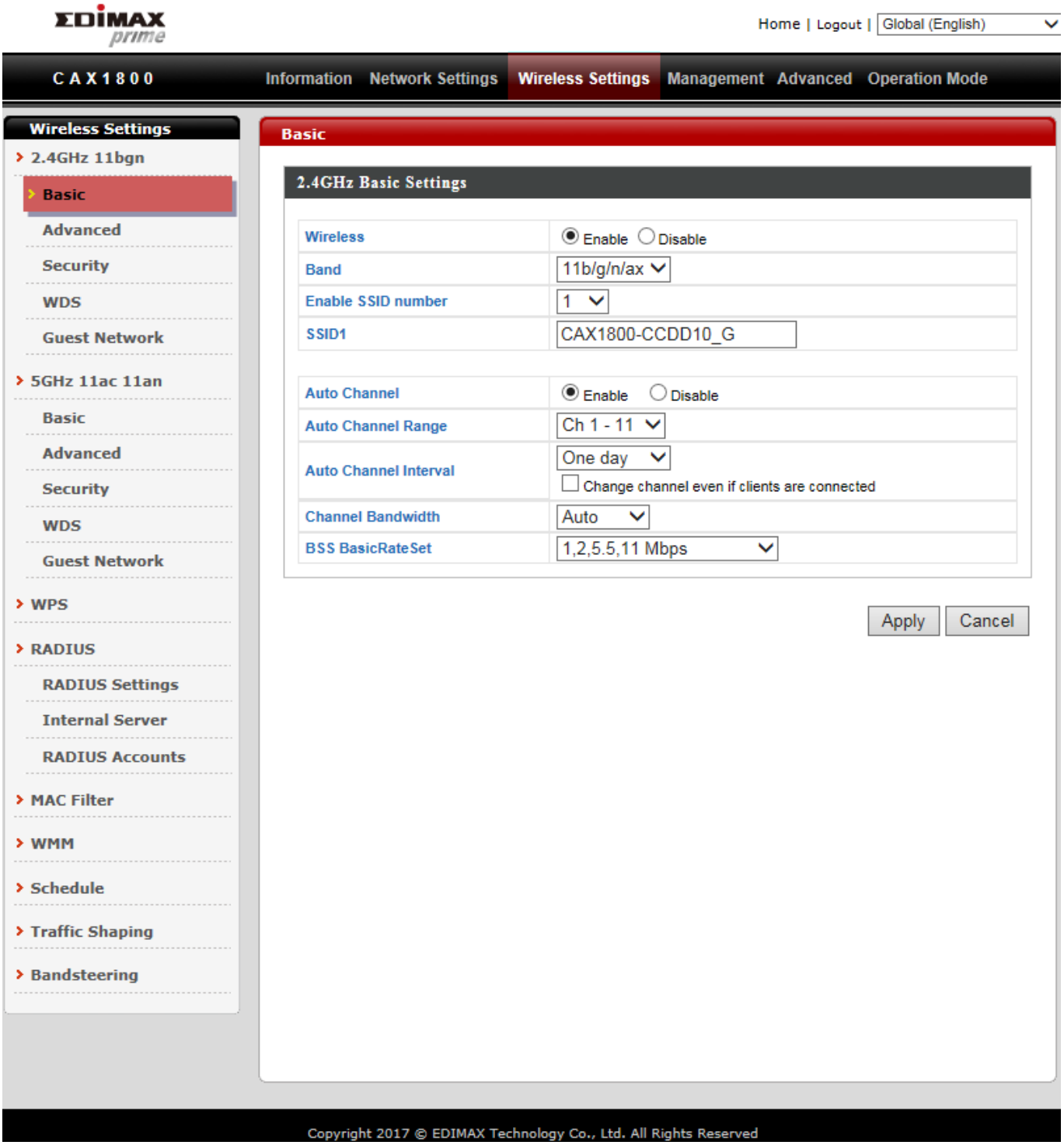


VLAN Interface	
Wired LAN Port/Wireless	Identifies LAN port 1 and wireless SSIDs.
VLAN Mode	Select “Tagged Port” or “Untagged Port” for specified LAN interface.
VLAN ID	Set a VLAN ID for specified interface, if “Untagged Port” is selected.

Management VLAN	
VLAN ID	Specify the VLAN ID of the management VLAN. Only the hosts belonging to the same VLAN can manage the device.

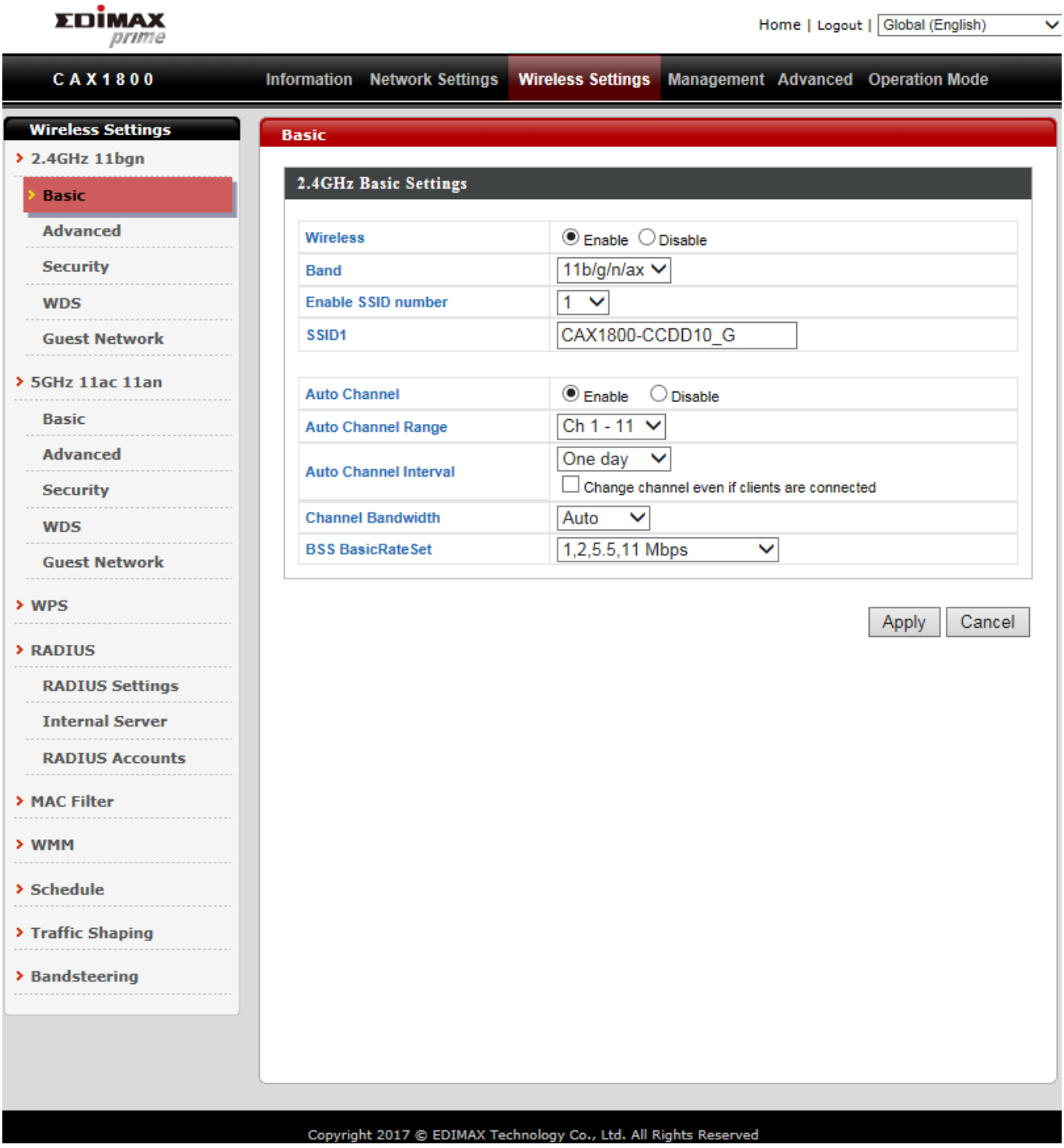
NOTE: VLAN IDs in the range 1 – 4095 are supported.

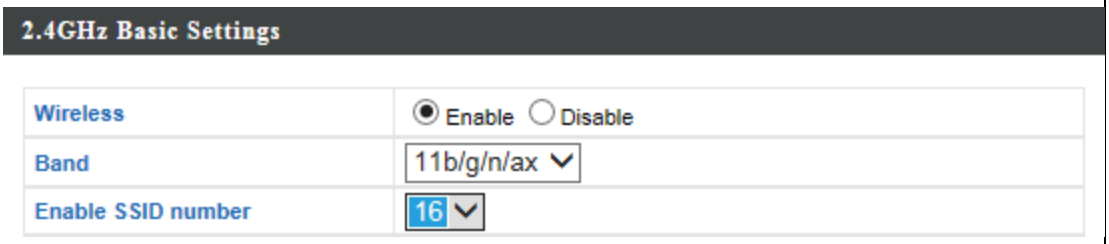
V-3. Wireless Settings



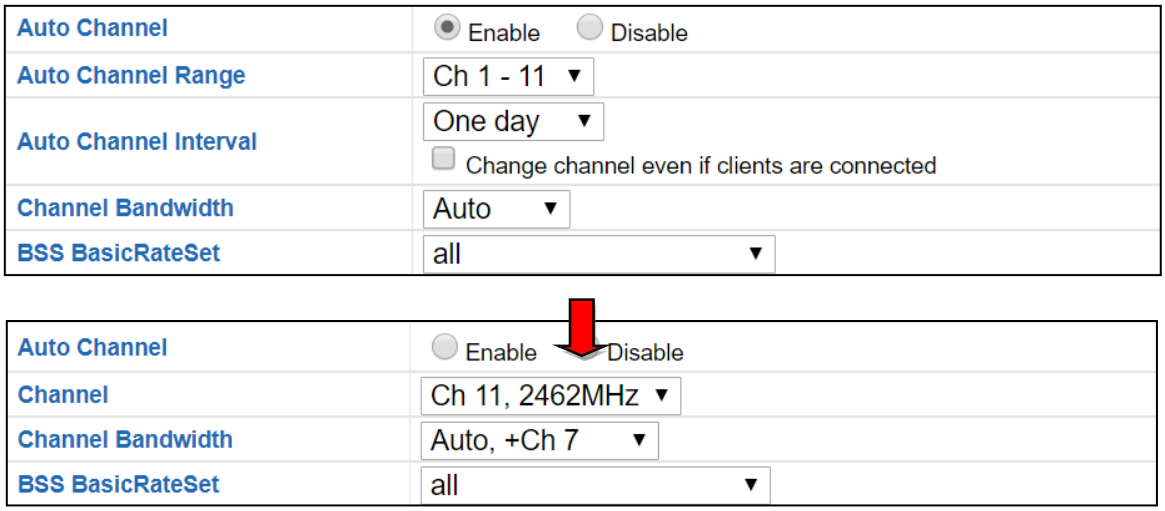
i. Basic (2.4GHz 11bgn)

You can set up basic settings for AP 2.4GHz Wi-Fi network.



Wireless	Enable or disable the AP 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active.
Band	Wireless standard used for the AP. Combinations of 802.11b, 802.11g & 802.11n can be selected.
Enable SSID Number	 Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. (A maximum of 16 can be enabled)
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Enable: Auto channel selection will automatically set the wireless channel for the AP2.4GHz frequency based on availability and potential interference. Disable: Select a channel manually as shown in the next table.
Auto Channel Range	Select a range to which auto channel selection can choose from.
Auto Channel Interval	Select a time interval for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the “Change channel even if clients are connected” box according to your preference.
Channel Bandwidth	Select the channel bandwidth: - 20MHz (lower performance but less interference). - 40MHz (higher performance but potentially higher interference). - Auto (automatically select based on interference level).
BSS BasicRateSet	This is a series of rates to control communication frames for wireless clients.

When auto channel is disabled, configurable fields will change. Select a wireless channel manually:

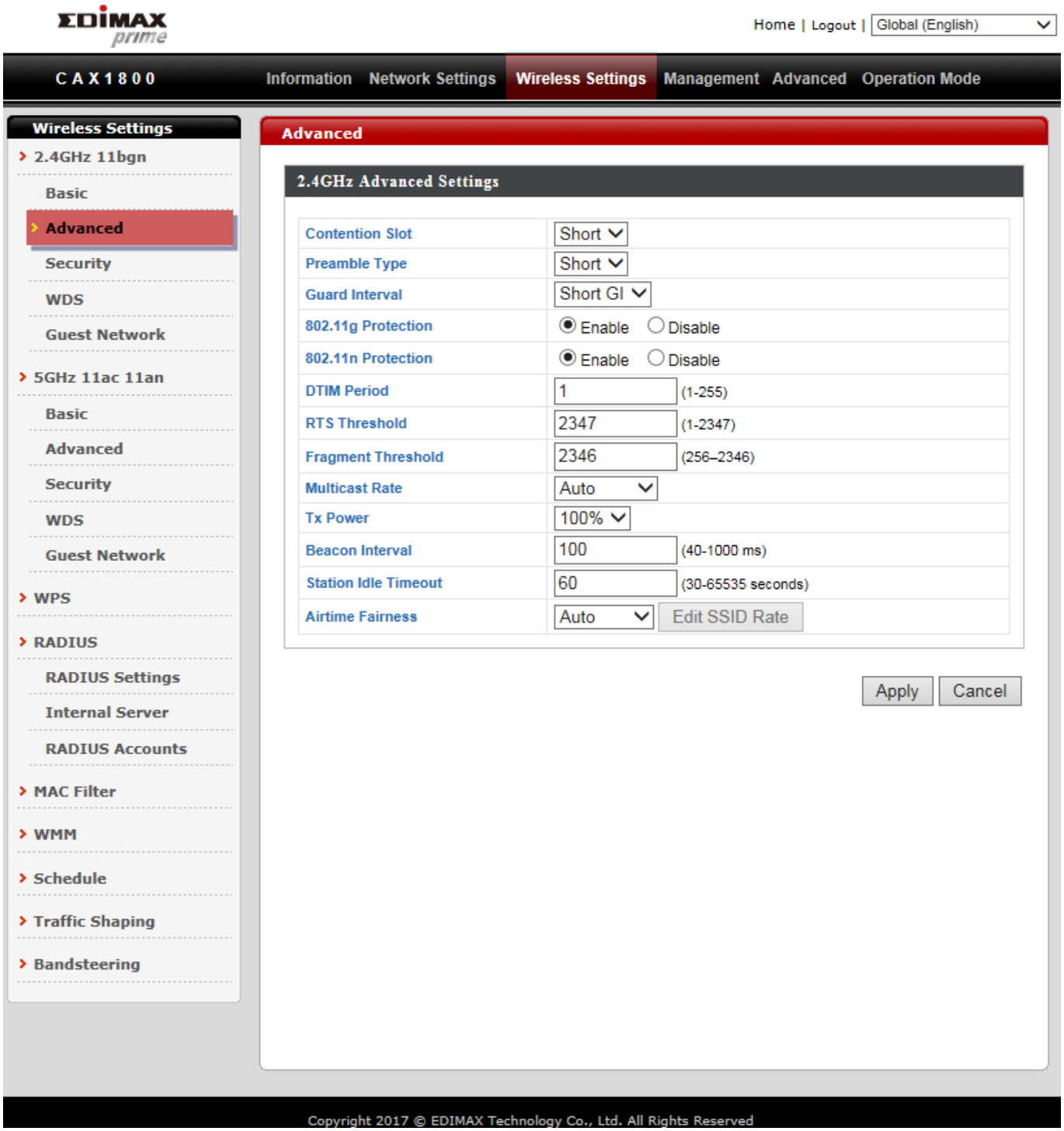


Channel	Select a wireless channel from 1 – 11.
Channel Bandwidth	Set the channel bandwidth: - 20MHz (lower performance but less interference). - 40MHz (higher performance but potentially higher interference) - Auto (automatically select based on interference level).
BSS BasicRateSet	This is a series of rates to control communication frames for wireless clients.

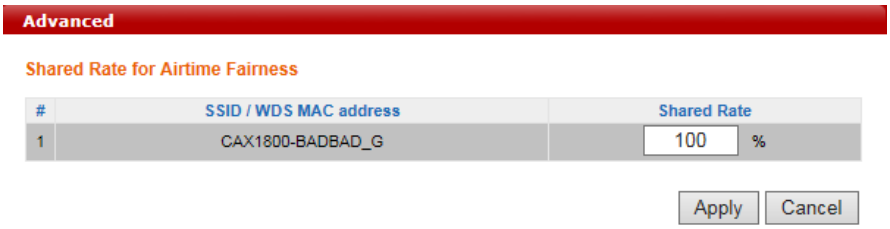
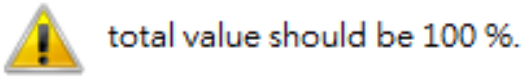
ii. Advanced (2.4GHz 11bgn)

In our recomandations, these settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

Changing these settings can adversely affect the performance of your AP.



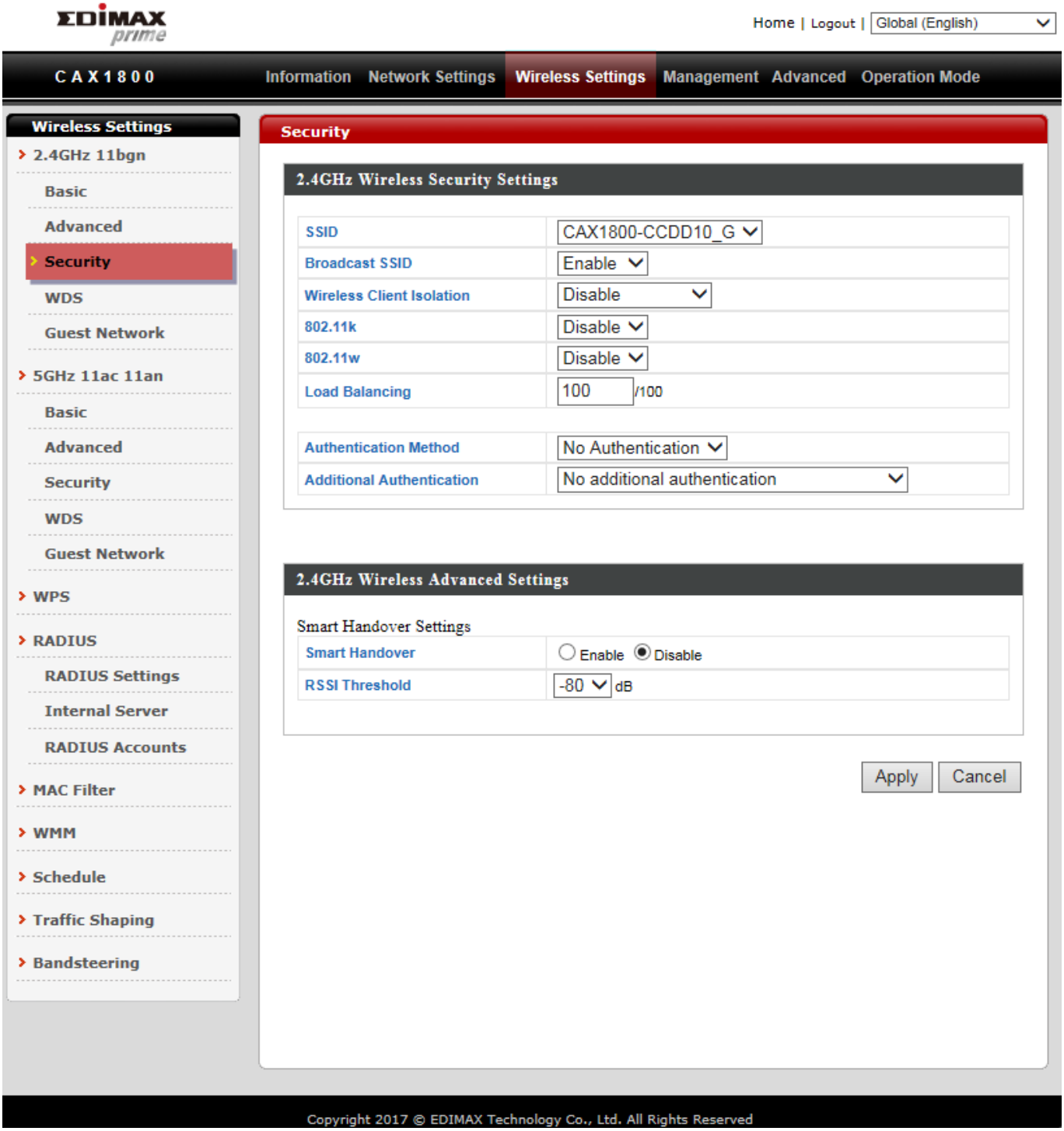
Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM.
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communications defines the length of the CRC (Cyclic Redundancy Check) block for communication between the AP and roaming wireless adapters. (The default value is “Short Preamble”)
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11g Protection	Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to AP, and AP will broadcast Clear to Send (CTS), before a packet is sent from client).
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to AP, and AP will broadcast Clear to Send (CTS), before a packet is sent from client).
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. (The default value is 1)
RTS Threshold	Set the RTS threshold of the wireless radio. (The default value is 2347)
Fragment Threshold	Set the fragment threshold of the wireless radio. (The default value is 2346)
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting. The range of the transfer rate is between 1Mbps to 54Mbps
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output may enhance security since access to your signal can be potentially prevented from malicious/unknown users in distant areas.
Beacon Interval	Set the beacon interval of the wireless radio. (The default value is 100)
Station idle timeout	Set the interval for the AP to send keepalive messages to a wireless client to check if the station is still alive/active.

Airtime Fairness	Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate. Set airtime fairness to “Auto”, “Static” or “Disable”. When “Auto” is selected, the share rate is automatically managed. When “Static” is selected, press “Edit SSID Rate” to enter a % for each SSID’s share rate as shown below:  The % field has to add up to 100% or the system will display a message:  Airtime fairness is disabled if “Disable” is selected.

iii. Security (2.4GHz 11bgn)

The AP provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It is essential to configure wireless security in order to prevent unauthorised access to your network.

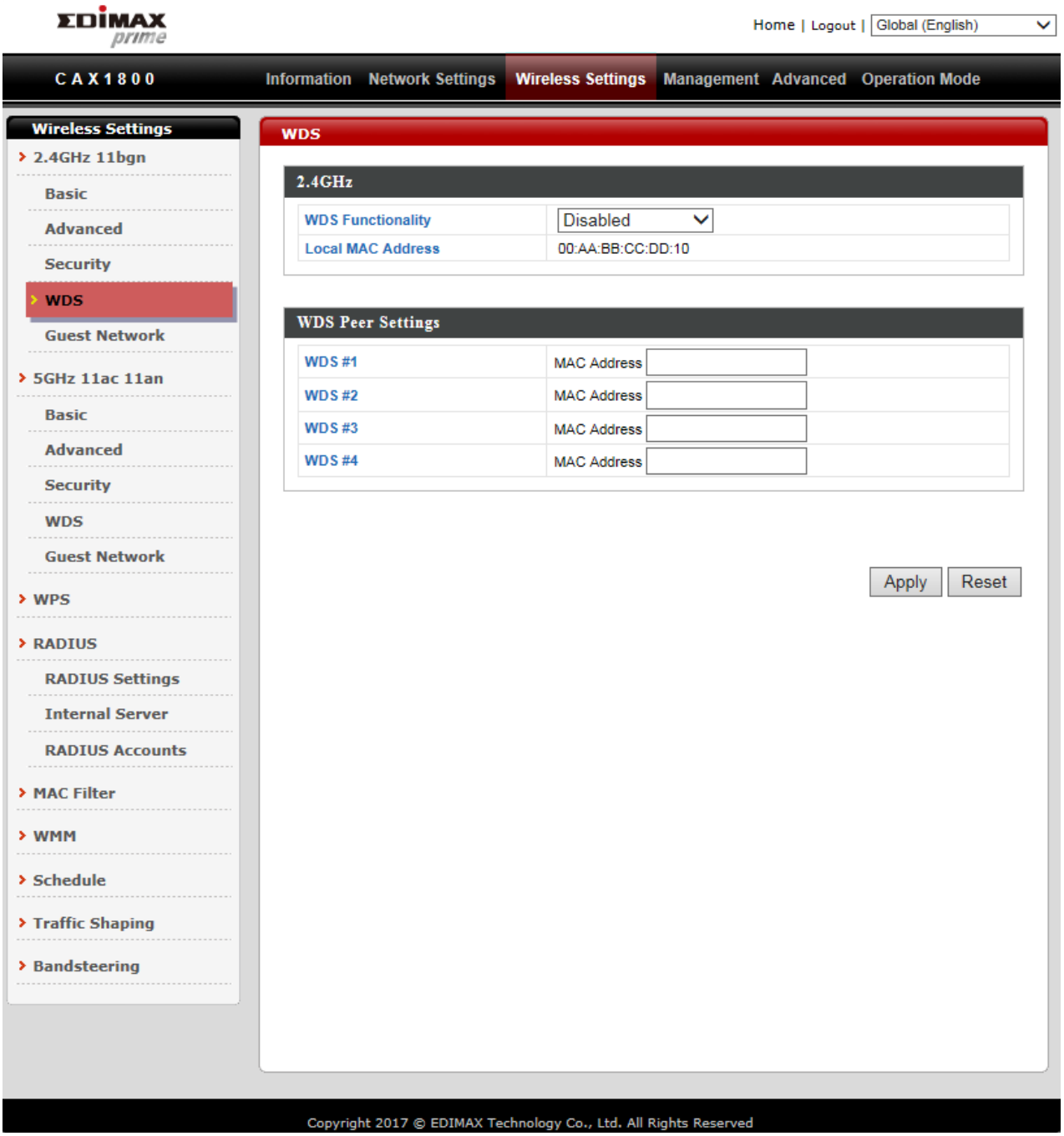


SSID Selection	Select a SSID to configure its security settings.
Broadcast SSID	Enable or disable SSID broadcast. Enable: the SSID will be visible to clients as an available Wi-Fi network. Disable: the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the APt from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu and refer to the appropriate information below for your method.

iv. WDS (2.4GHz 11bgn)

WDS can bridge/repeat AP together in an extended network and must be configured on each AP, using correct MAC addresses. All APs should use the same wireless channel and encryption method.

When using WDS, configure the IP address of each AP to be in the same subnet and ensure there is only one active DHCP server among connected APs, preferably on the WAN side.



WDS settings can be configured as shown below:

2.4GHz	
WDS Functionality	Select “WDS with AP” to use WDS with AP or “WDS Dedicated Mode” to use WDS and also block communication with regular wireless clients. When WDS is used, each AP should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your AP.

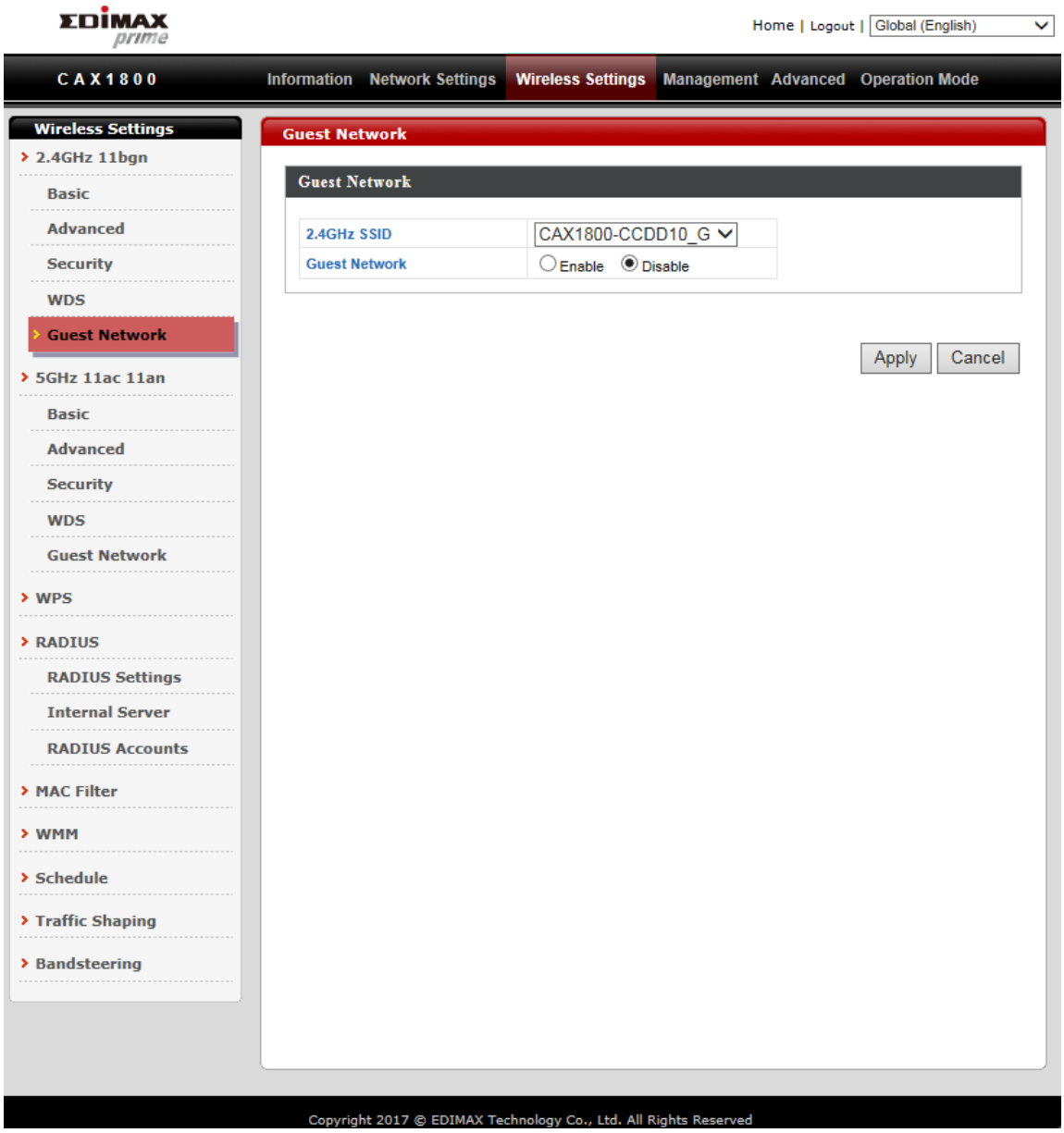
WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDS devices you wish to connect.

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

WDS Encryption method	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES consisting of 8-63 alphanumeric characters.

v. Guest Network (2.4GHz 11bgn)

Enable or disable guest network to allow clients to connect as guests.



vi. 5GHz 11ac 11an

The “5GHz 11ac 11an” menu allows you to configure your AP 5GHz wireless network across five categories: Basic, Advanced, Security, WDS & Guest Network. Please refer to 2.4GHz 11bgn section for how to set up.

vii. WPS

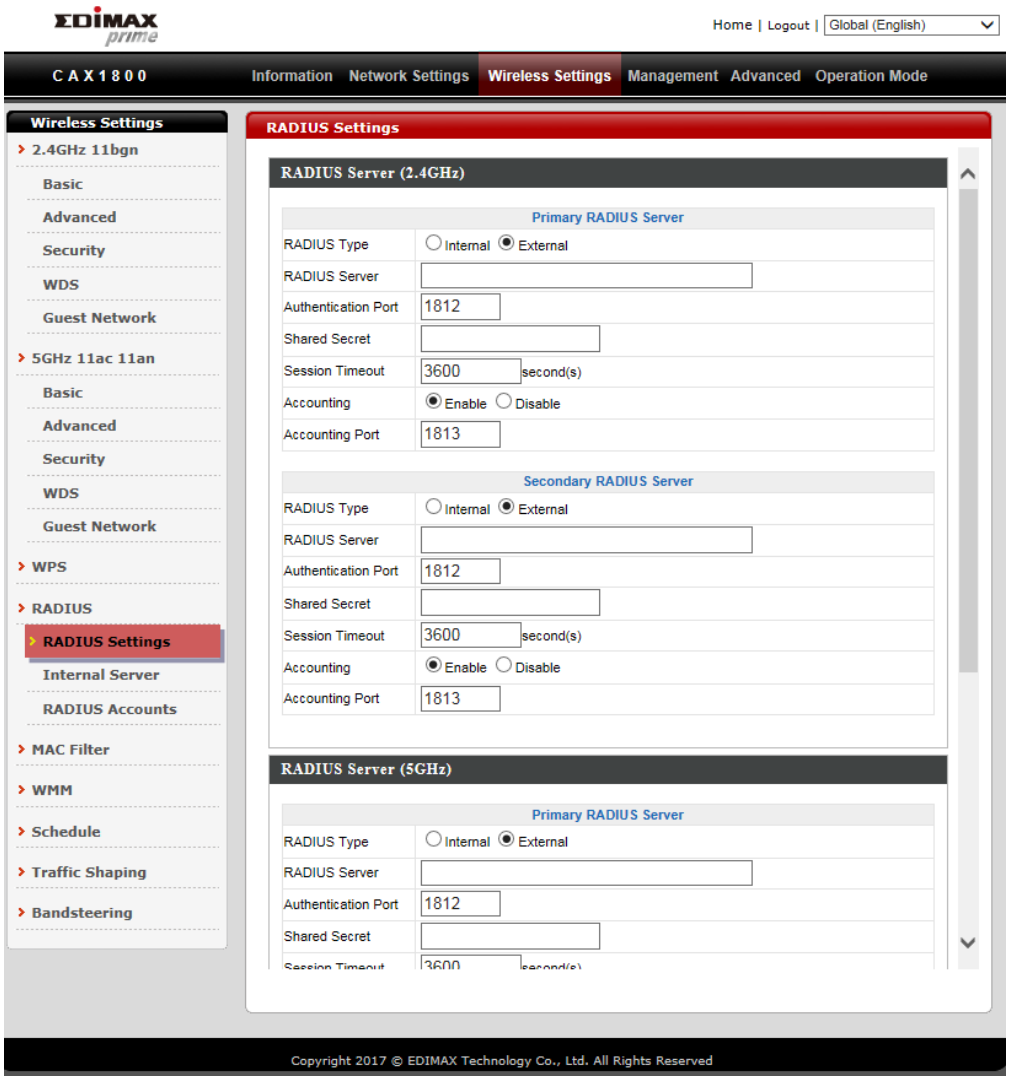
Please refer to PG.246 for more details.

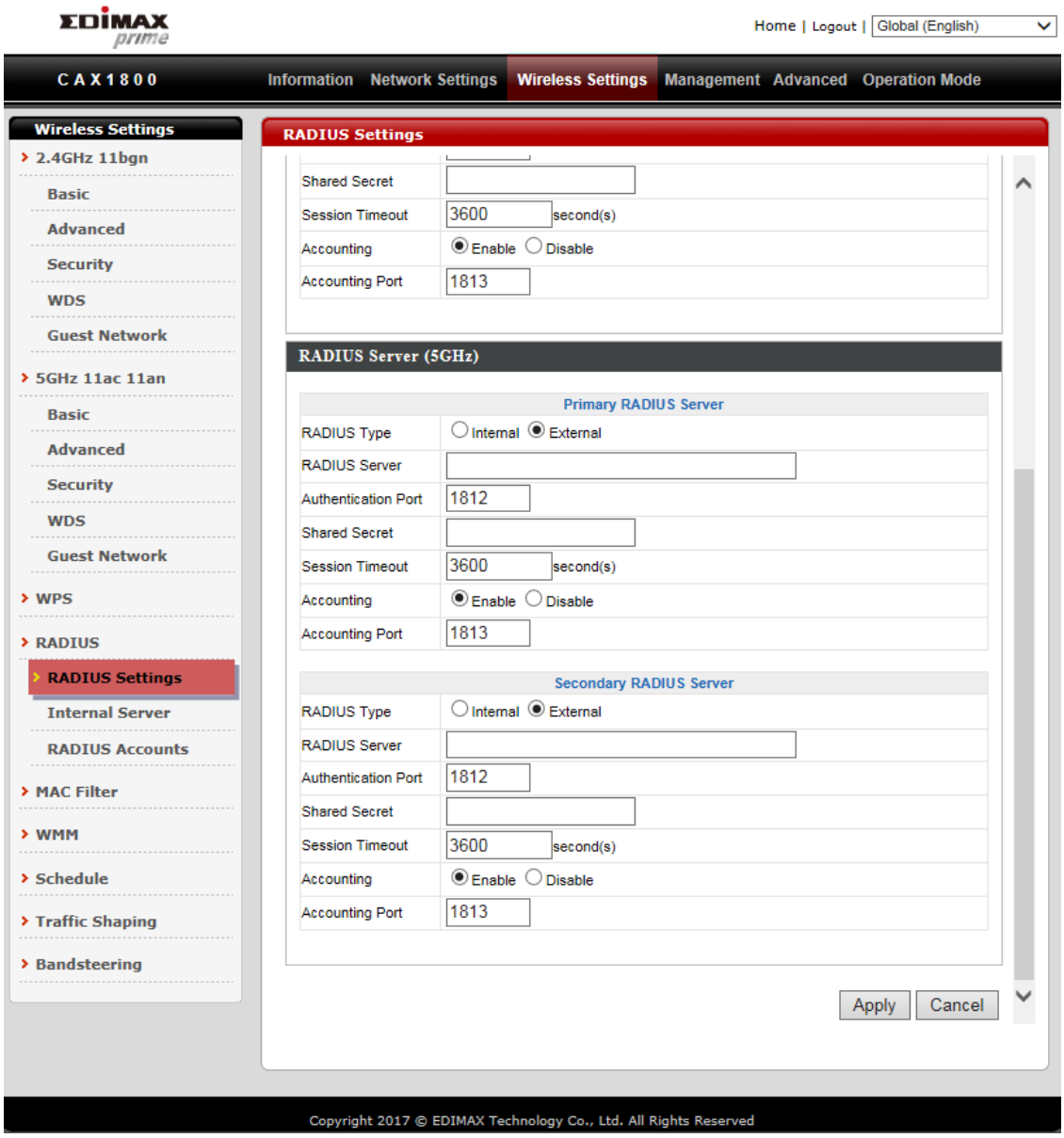
viii. RADIUS (RADIUS Settings)

The RADIUS allows users to configure the device's external RADIUS server settings.

A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The device can utilize a primary and a secondary (backup) external RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz).

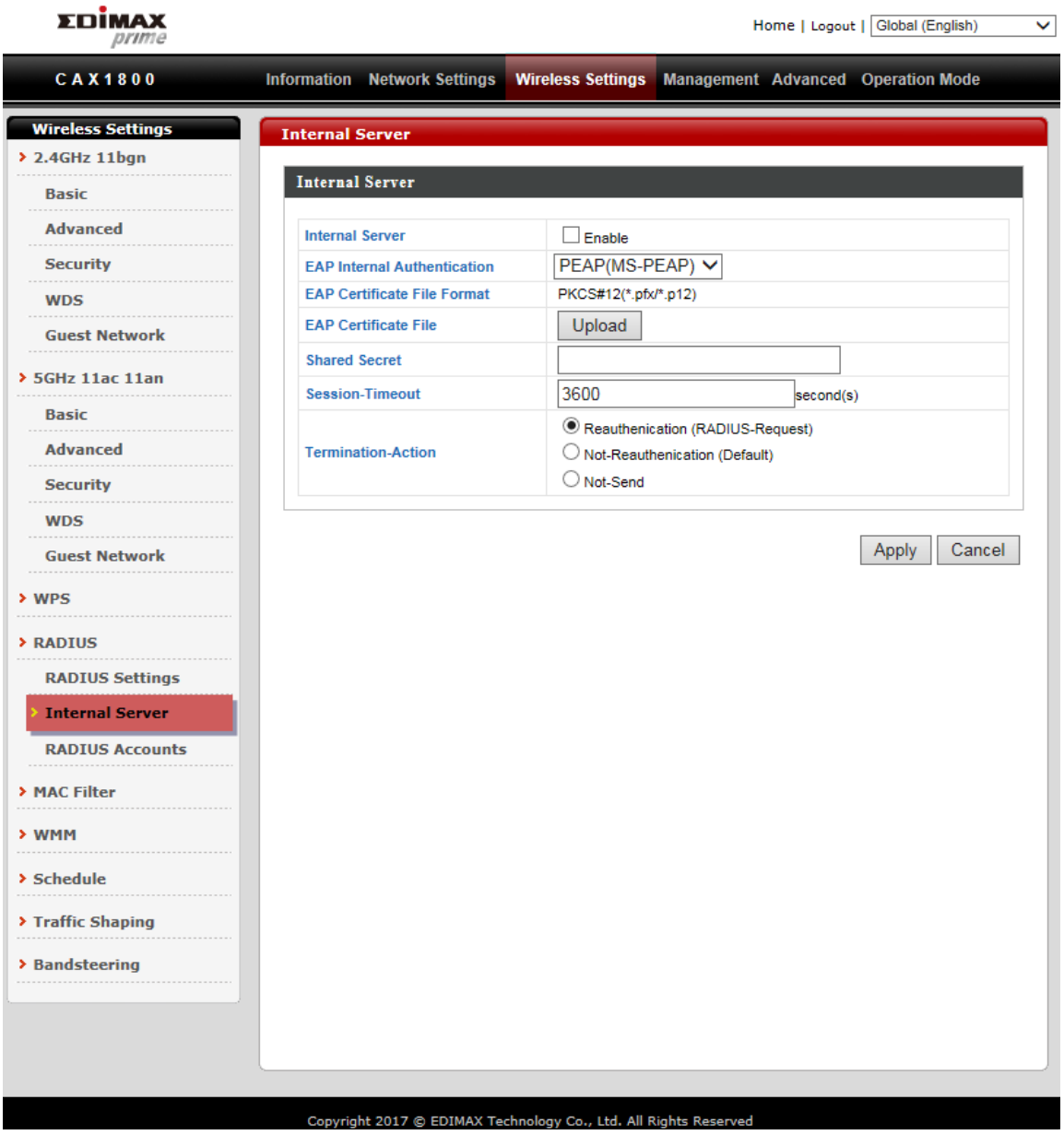




RADIUS Type	Select “Internal” to use the AP built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. (Value must be between 1 – 65535)
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Accounting	Enable or disable RADIUS accounting.
Accounting Port	When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. (Value must be between 1 – 65535)

ix. Internal Server

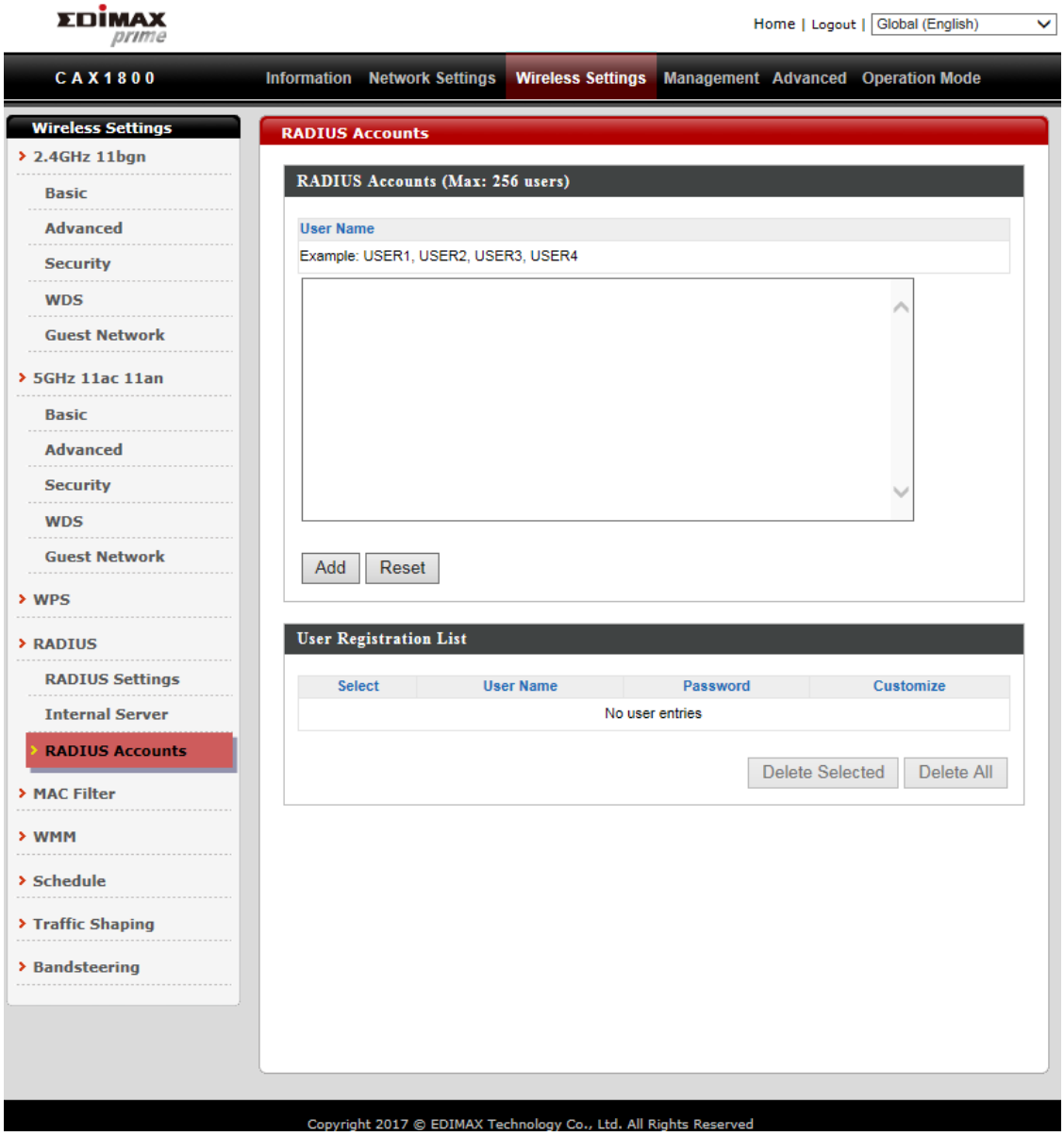
The AP features a built-in RADIUS server which can be configured as shown below used when “Internal” is selected for “RADIUS Type”.



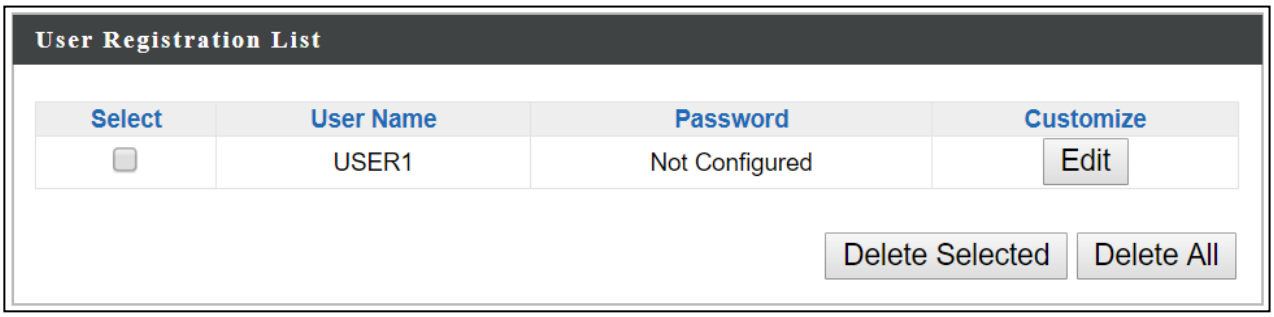
Internal Server	Check/uncheck to enable/disable the AP's internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click "Upload" to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.
Shared Secret	Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Termination Action	Select a termination-action attribute: Reauthentication: sends a RADIUS request to the AP; or, Not-Reauthentication: sends a default termination-action attribute to the AP; or Not-Send: no termination-action attribute is sent to the AP.

x. RADIUS Accounts

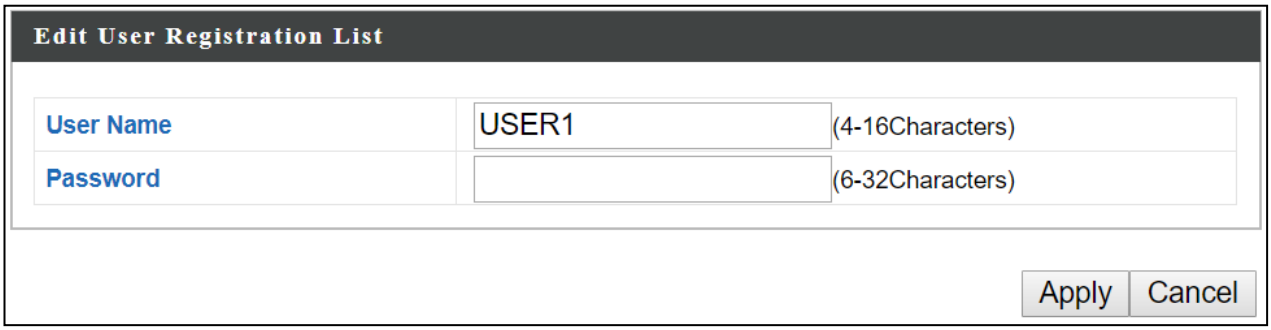
The internal RADIUS server allows you to configure and manage users and can authenticate up to 256 user accounts.



Enter a username in the box below and click “Add” to add the username.



Select “Edit” to edit the username and password of the RADIUS account:



User Name	Enter the user names here, separated by commas.
Add	Click “Add” to add the user to the user registration list.
Reset	Clear text from the user name box.

Select	Check the box to select a user.
User Name	Displays the user name.
Password	Displays if specified user name has a password (configured) or not (not configured).
Customize	Click “Edit” to open a new field to set/edit a password for the specified user name.

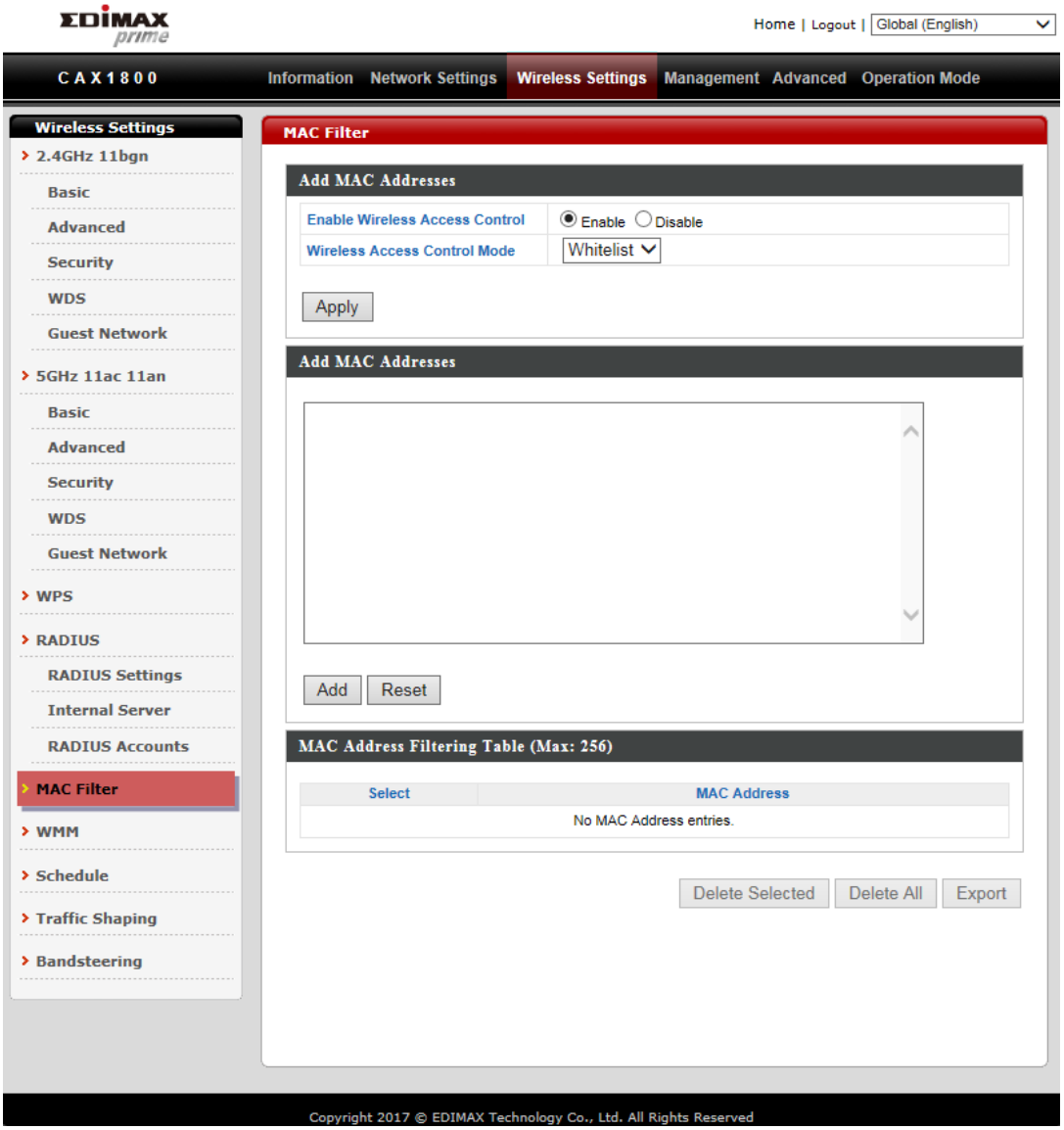
Delete Selected	Delete selected user from the user registration list.
Delete All	Delete all users from the user registration list.

xi. MAC Filter

MAC filtering is a security feature that can help to prevent unauthorized users from connecting to your AP.

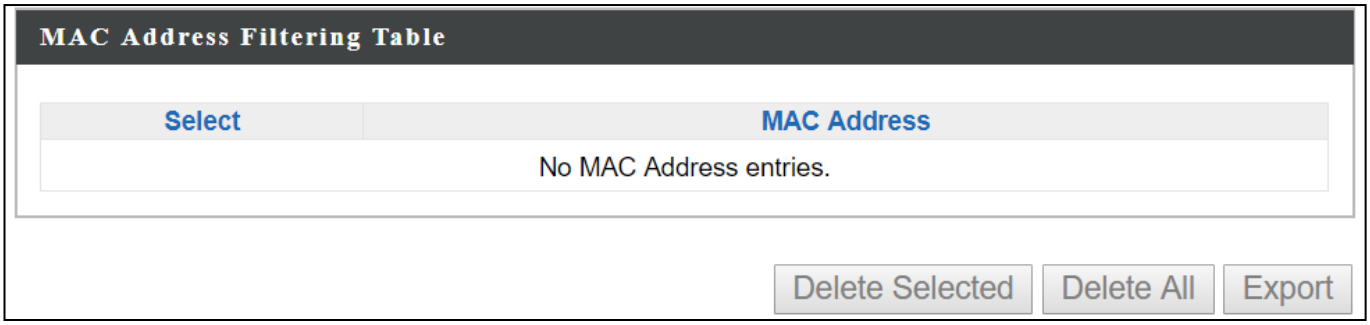
This function allows users to define a list of network devices permitted to connect to the AP. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the AP, it will be denied.

The MAC address filtering table is displayed below:



Add MAC Address	Enter a MAC address of computer or network device manually e.g. ‘aa-bb-cc-dd-ee-ff’. Or enter multiple MAC addresses separated with commas, e.g. ‘aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg’.
Add	Click “Add” to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

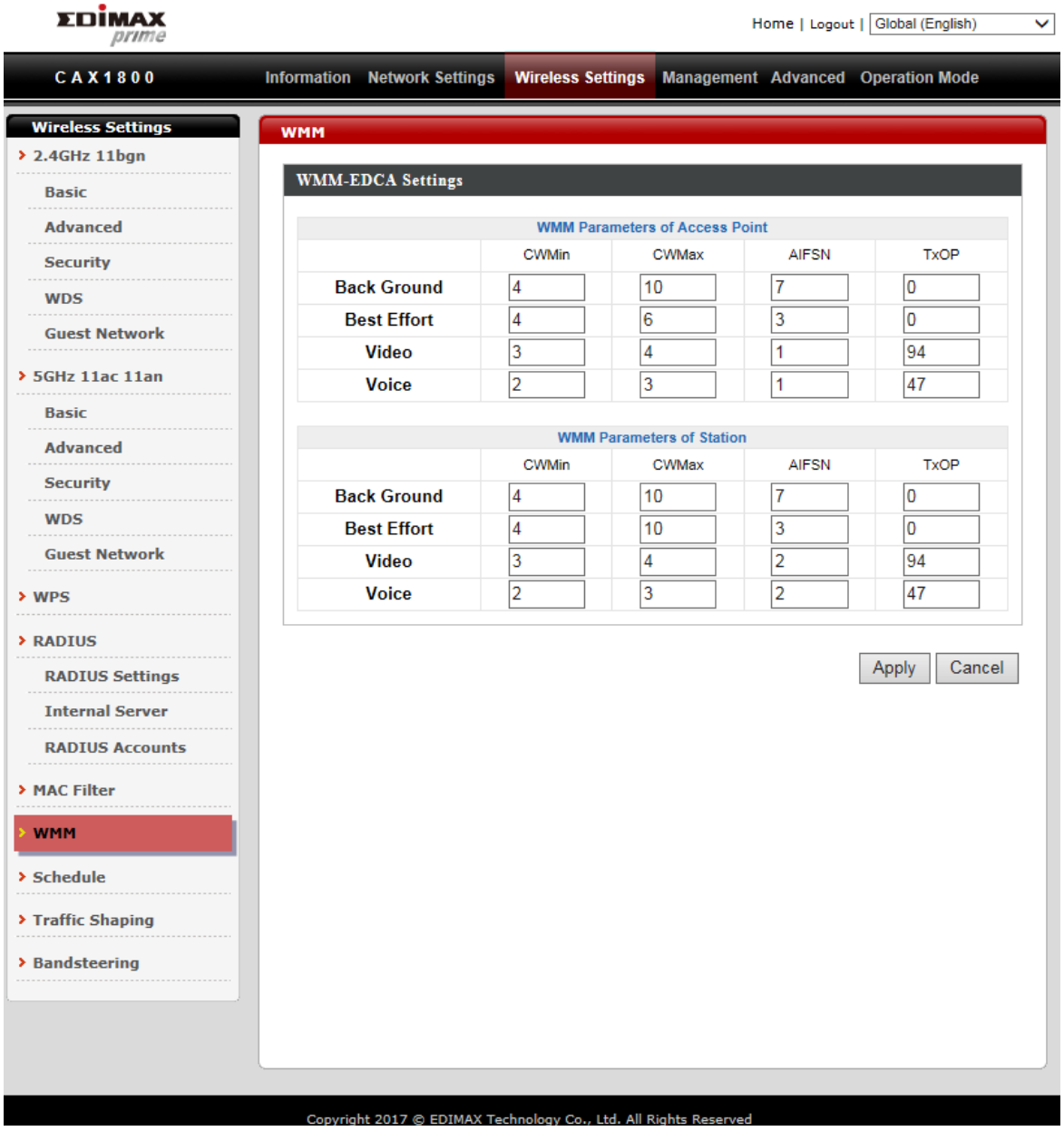
MAC address entries will be listed in the “MAC Address Filtering Table”. Select an entry using the “Select” checkbox.



Select	Delete selected or all entries from the table.
MAC Address	The MAC address is listed here.
Delete Selected	Delete the selected MAC address from the list.
Delete All	Delete all entries from the MAC address filtering table.
Export	Click “Export” to save a copy of the MAC filtering table. A new window will pop up for you to select a location to save the file.

xii. WMM

WMM is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.



Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

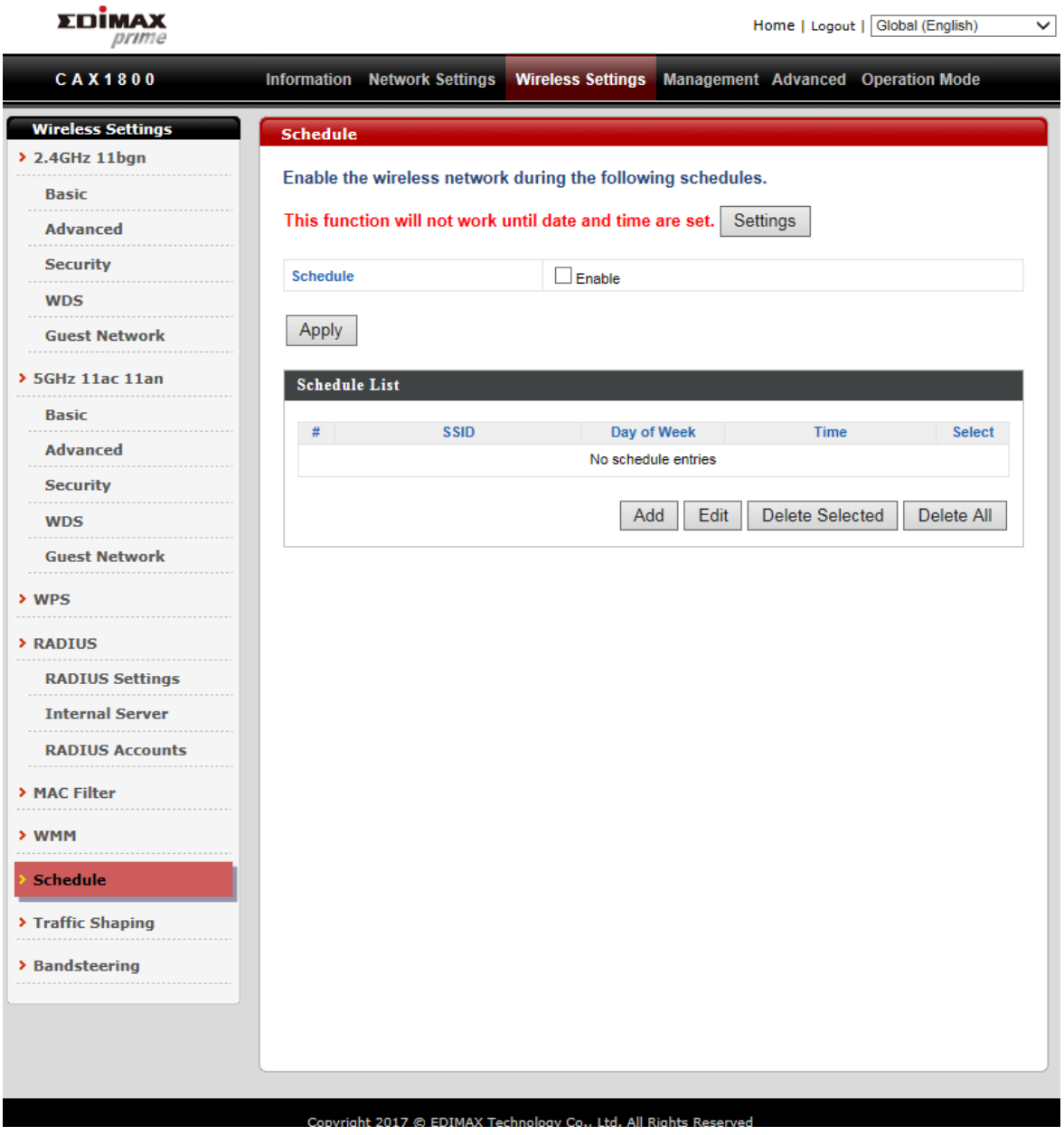
Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
Best Effort	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP and streaming media with minimum time delay.

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can be adjusted further manually:

CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value reaches the number defined by CWMax (below). The CWMin value must be lower than the CWMax value.
CWMax	Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above).
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. (Traffic with a lower AIFSN value has a higher priority)
TxOP	Transmission Opportunity (milliseconds): The maximum interval of time an AP can transmit. This makes channel access more efficiently prioritized. (A greater value means higher priority)

xiii. Schedule

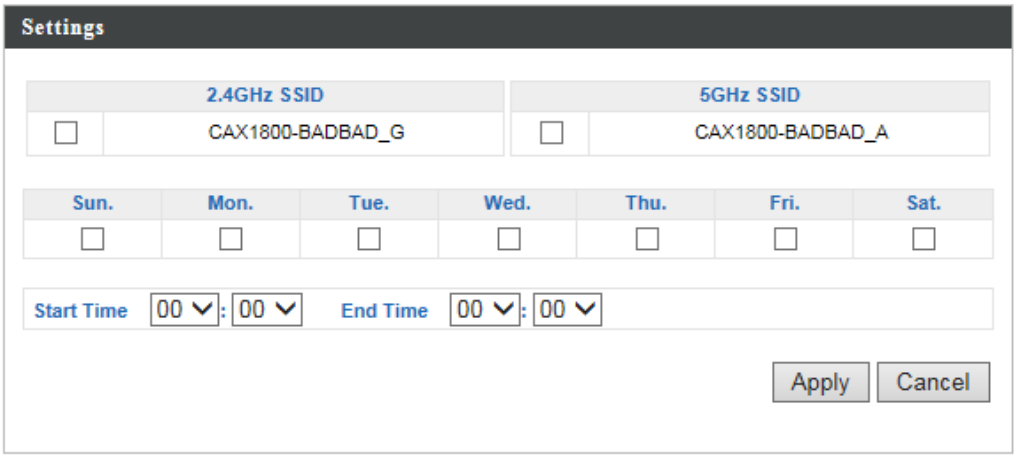
The schedule feature allows users to automate the wireless network for the specified time ranges. Wireless scheduling can save energy and increase the security of your network.

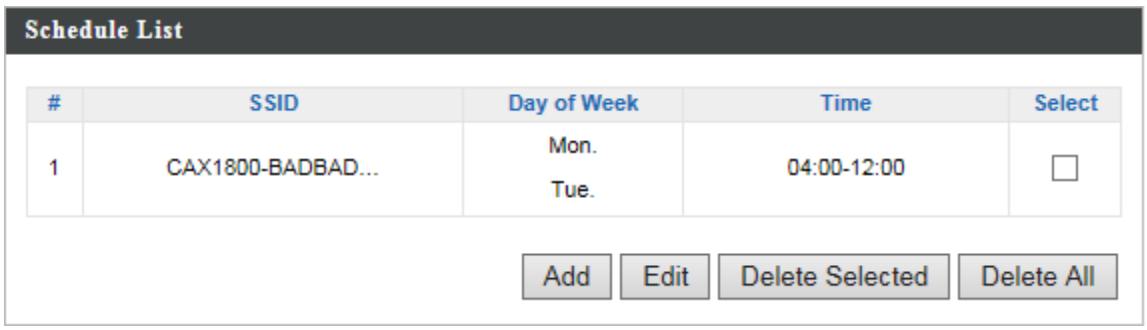


Please follow the steps below for how to set up schedule,

1. Select “Add” to add a schedule.

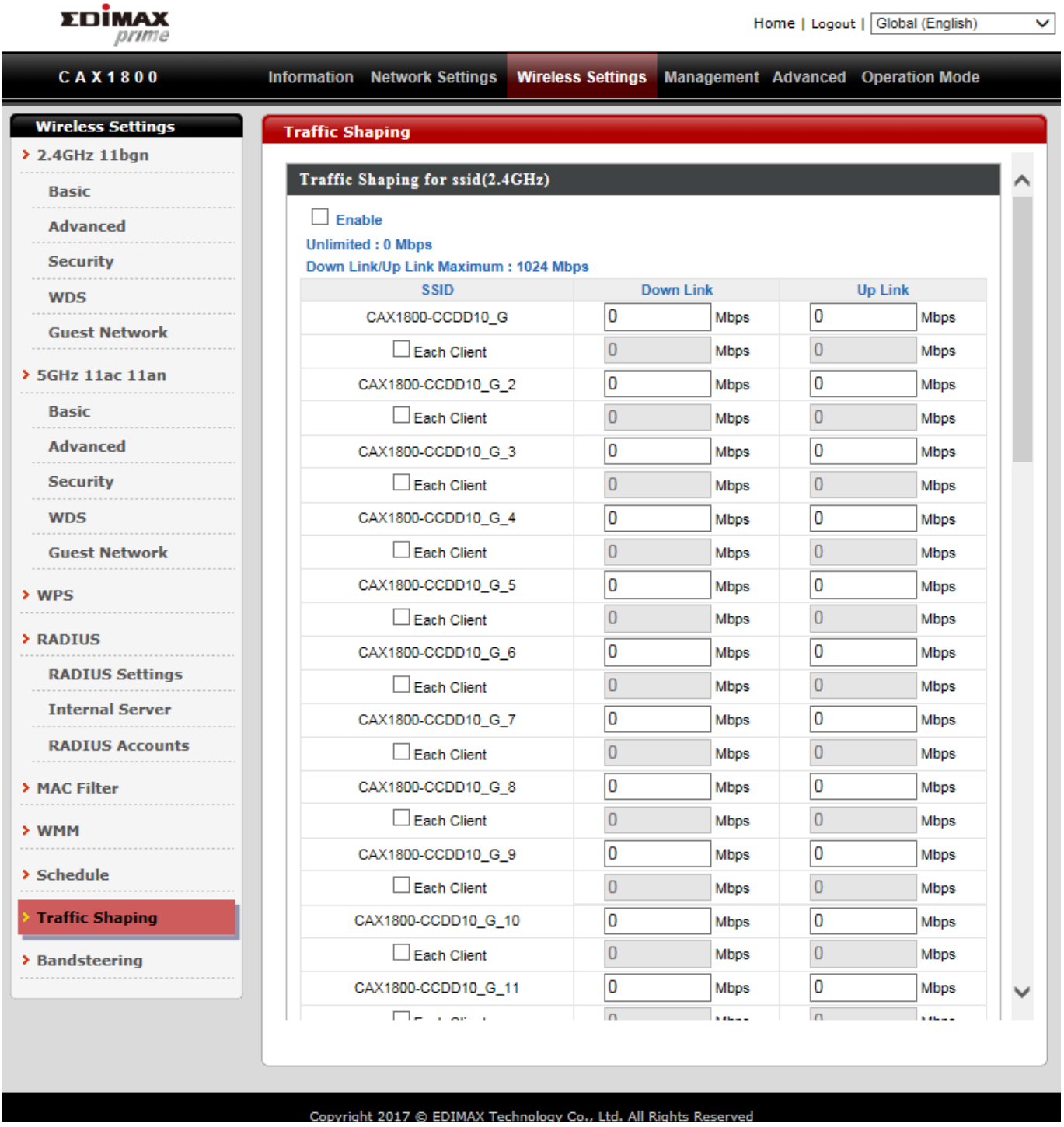
2. Settings page will be shown if “Continue” is selected. Check the box of the desired SSID network, day of schedule and select the Start Time and End Time.





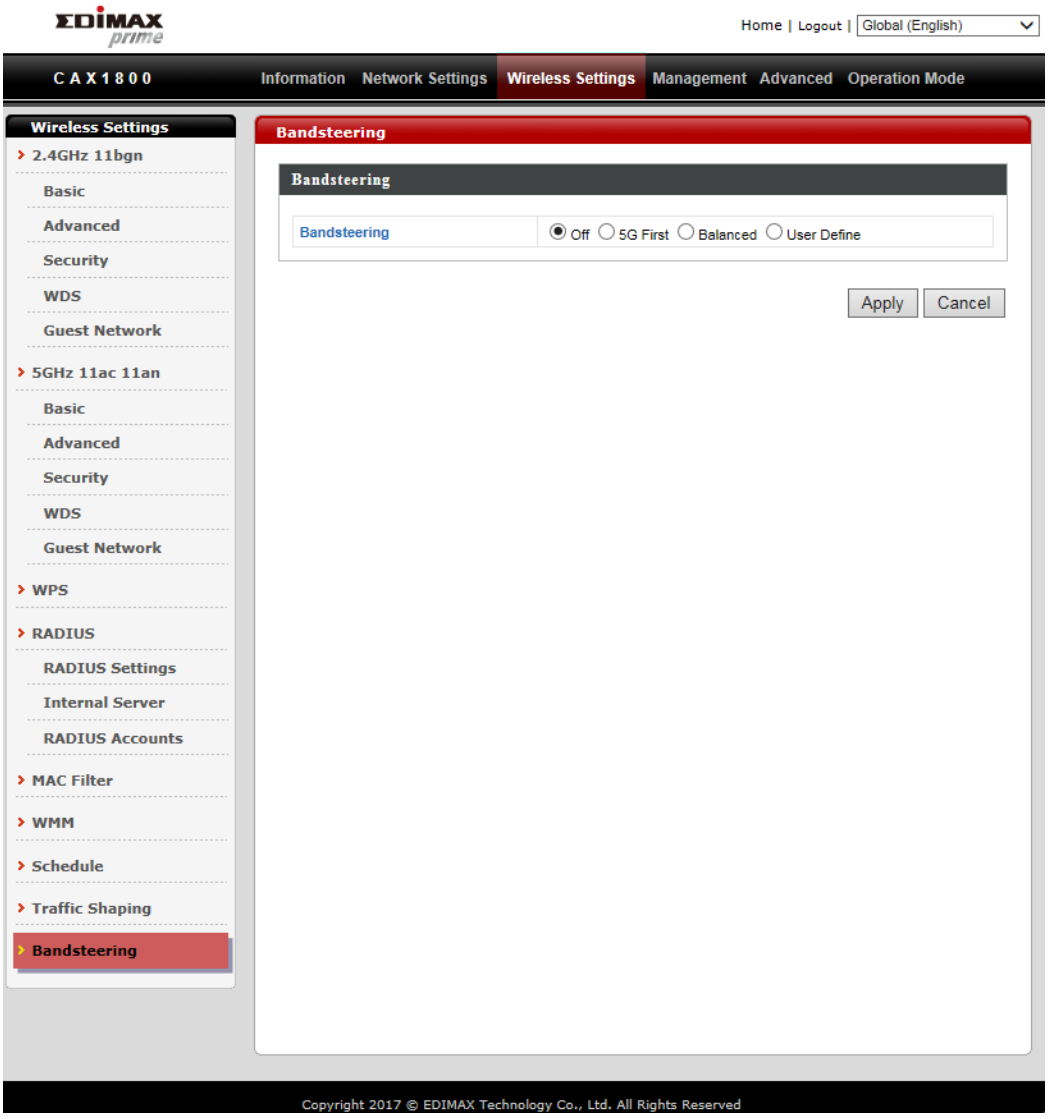
xiv. Traffic Shaping

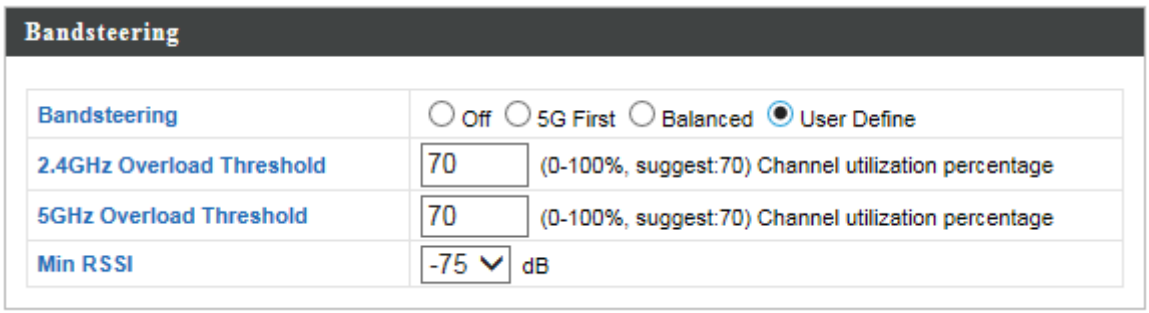
Traffic shaping is used to optimize or guarantee performance, improve latency, or increase usable bandwidth for some kinds of packets by delaying other kinds.



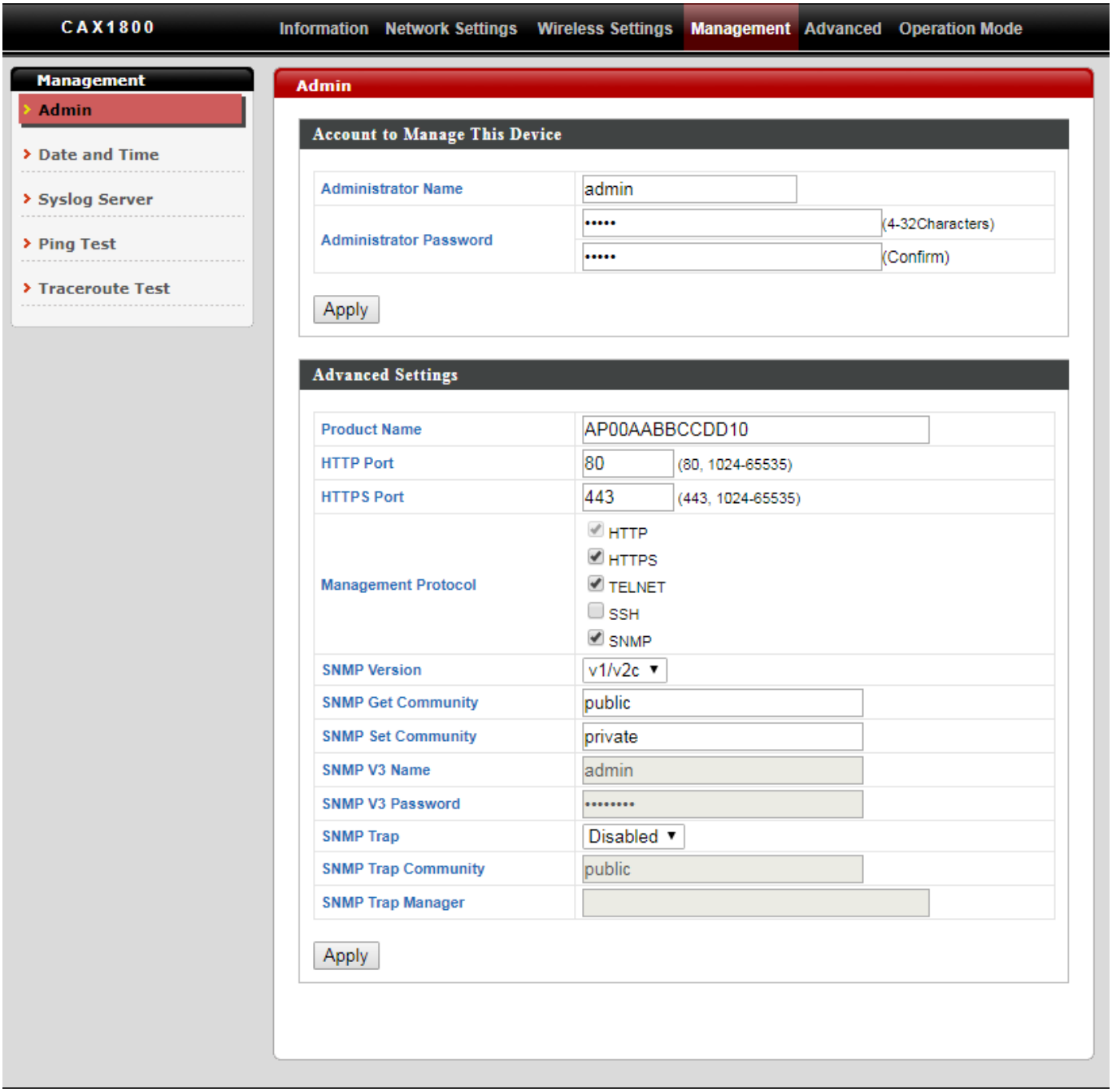
xv. Bandsteering

Bandsteering detects clients capable of 5GHz operation and steers them there to make the more crowded 2.4 GHz band available for clients only capable of connecting to 2.4GHz band. This helps improve end user experience by reducing channel utilization, especially in high density environments.



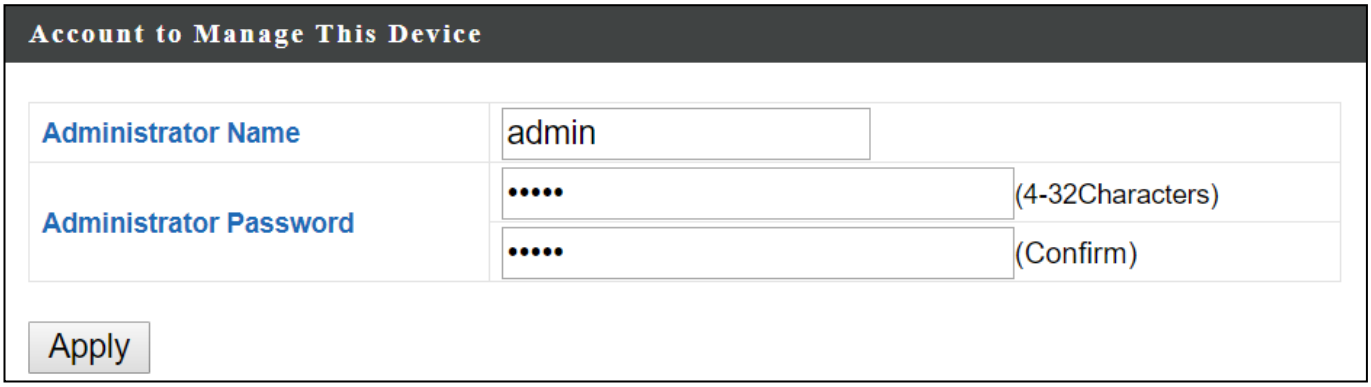


V-4. Management

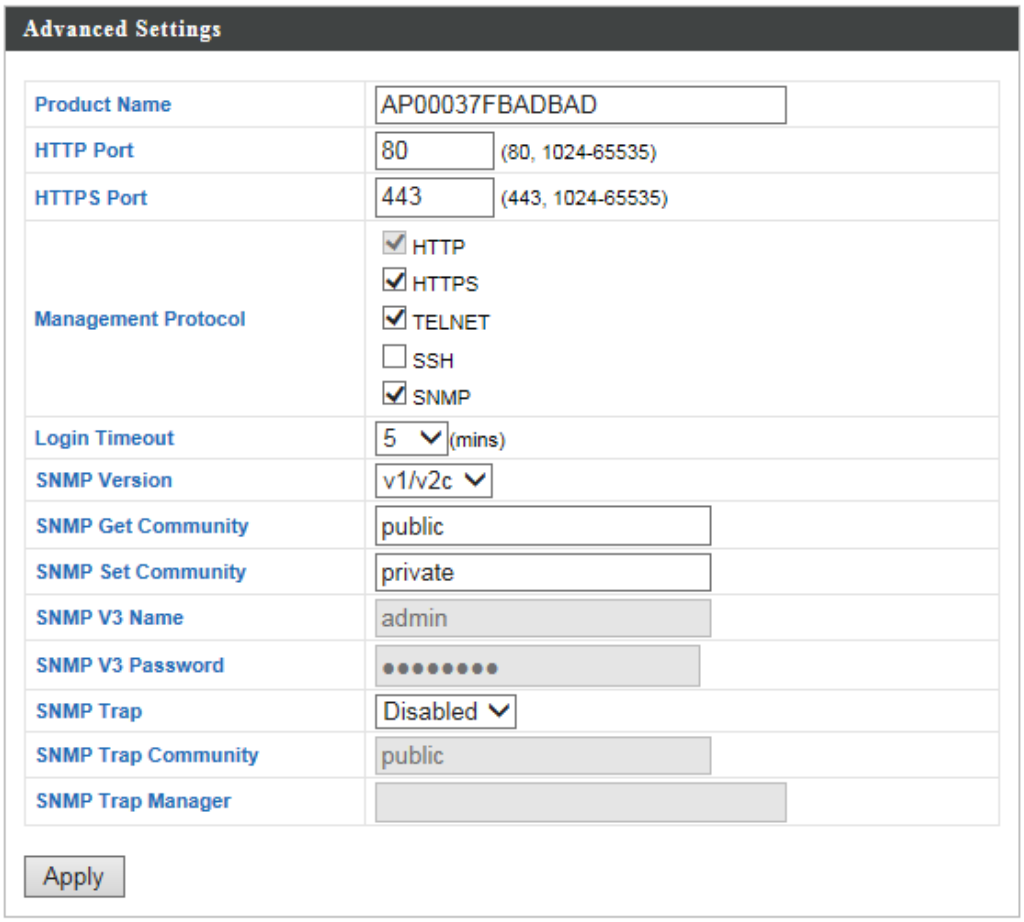


i. Admin

You can change the admin name/password and configure the “Advanced Settings” in here. It is advised to do so for security purposes.



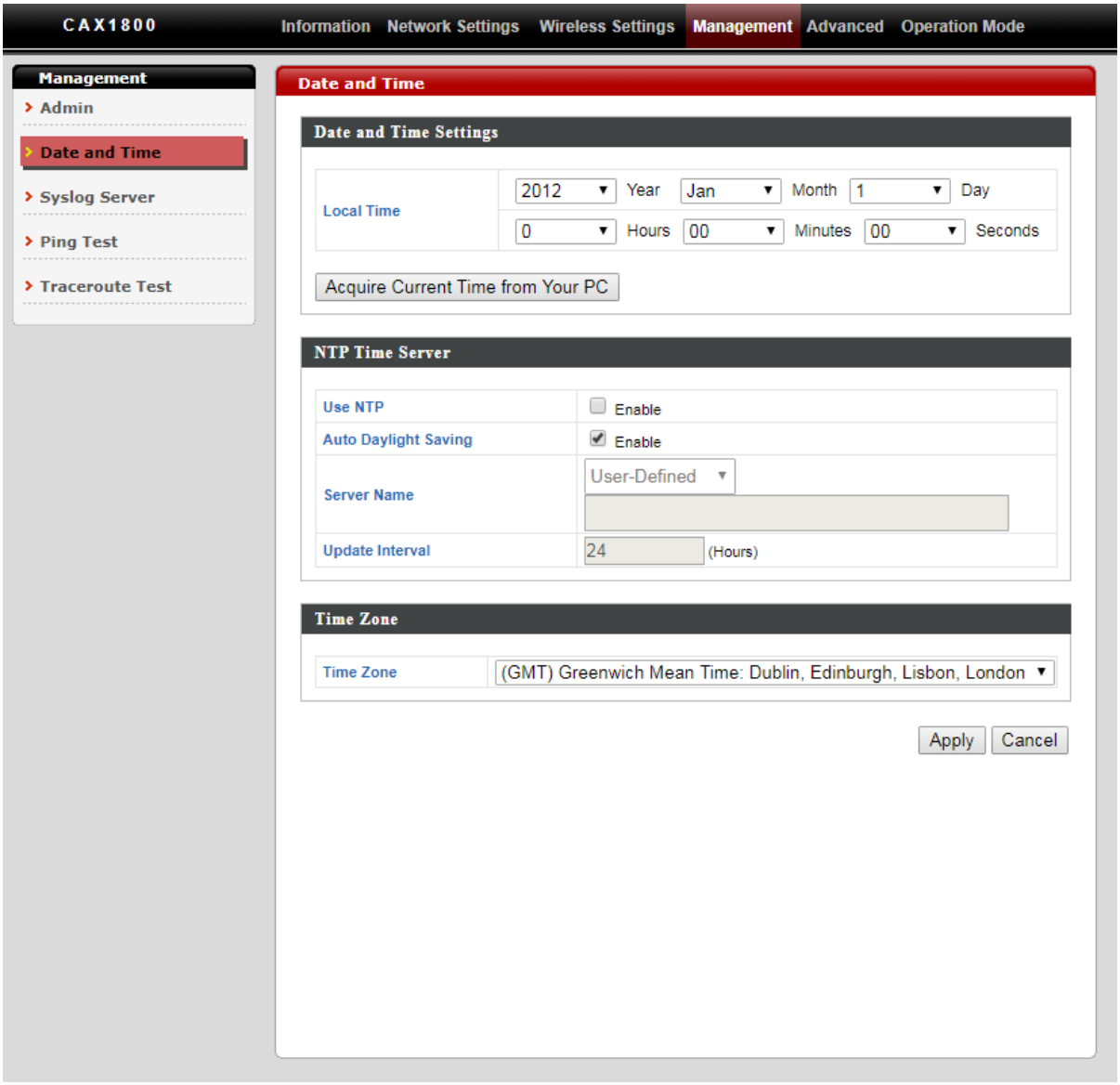
Account to Manage This Device	
Administrator Name	Set the AP administrator name. (Must be between 4-16 alphanumeric characters)
Administrator Password	Set the AP administrator password. (Must be between 4-32 alphanumeric characters)



Advanced Settings	
Product Name	Edit the product name according to your preference consisting of 1-32 alphanumeric characters. This name is used for reference purposes.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces.
SNMP Version	Select SNMP version appropriate for your SNMP manager.
SNMP Get Community	Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests.
SNMP Set Community	Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests.
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of network errors.
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (2-128 alphanumeric characters) of the SNMP manager.

ii. Date and Time

Users can configure the date and time settings of the AP here. The date and time of the device can be configured manually or can be synchronized with a time server.



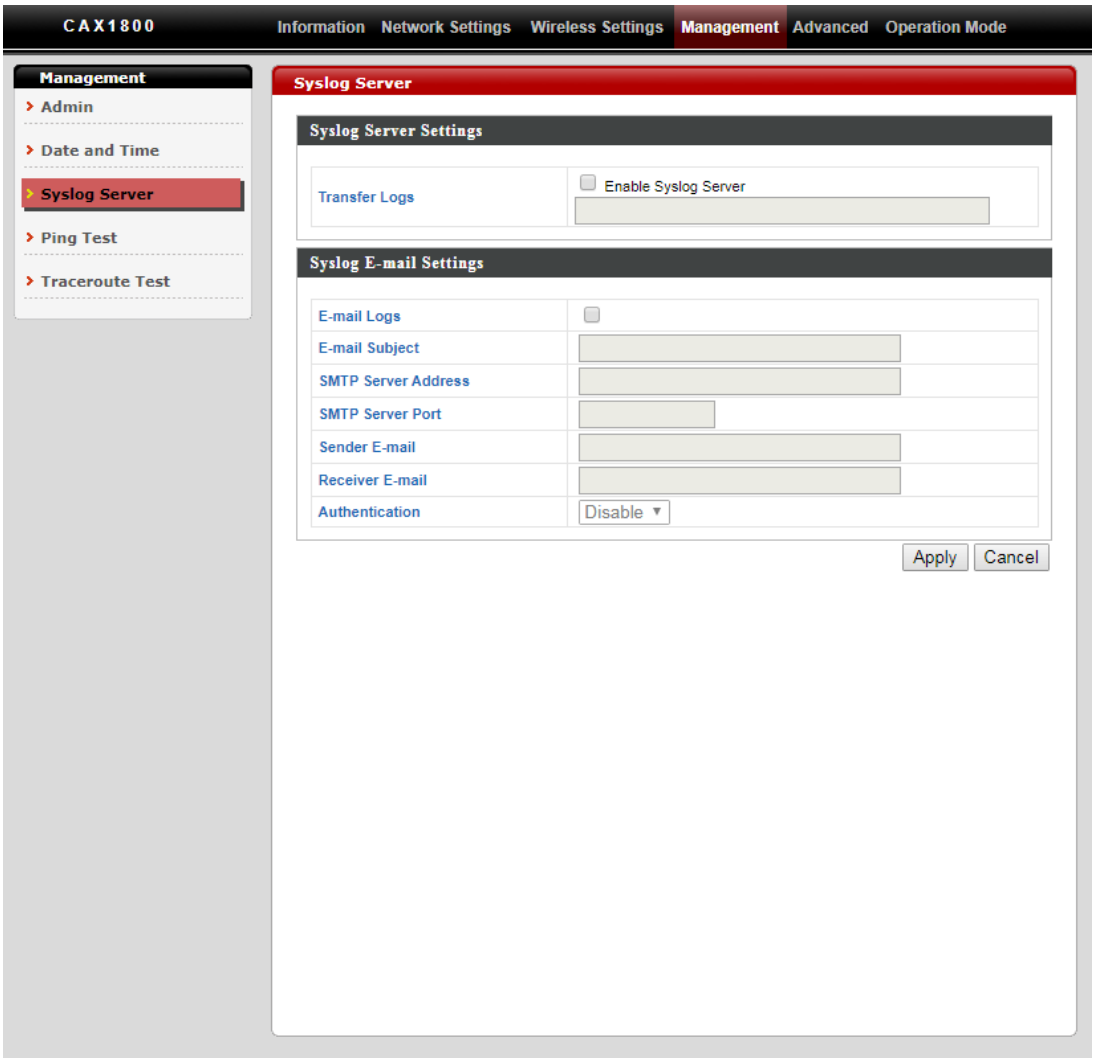
Date and Time Settings	
Local Time	Set the AP date and time manually using the drop down menus.
Acquire Current Time from your PC	Click “Acquire Current Time from Your PC” to enter the required values automatically according to your computer’s current time and date.

NTP Time Server	
Use NTP	The AP also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the AP to update/synchronize with the NTP server.

Time Zone	
Time Zone	Select the time zone of your country/region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.

iii. Syslog Server

You can send the system log to a server.

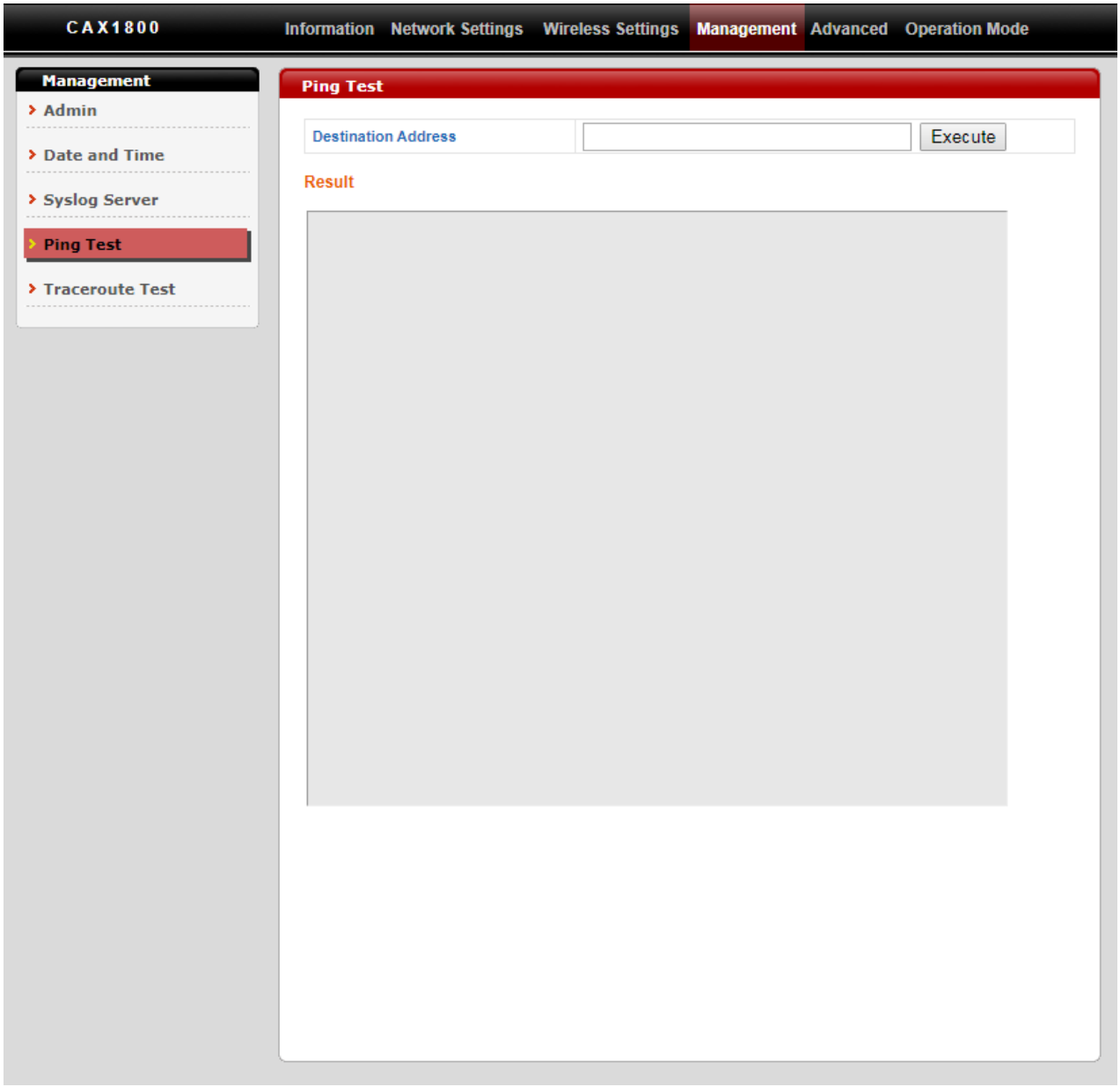


Syslog Server Settings	
Transfer Logs	Check the box to enable the use of a syslog server. Enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.

Syslog E-mail Settings	
E-mail Logs	Check the box to enable/disable e-mail logs.
E-mail Subject	Specify the subject line of log emails.
SMTP Server Address	Specify the SMTP server address used to send log emails.
SMTP Server Port	Specify the SMTP server port used to send log emails.
Sender E-mail	Specify the sender email address.
Receiver E-mail	Specify the email to receive log emails.
Authentication	Disable or select authentication type: SSL or TLS. When using SSL or TLS, enter the username and password.

iv. Ping Test

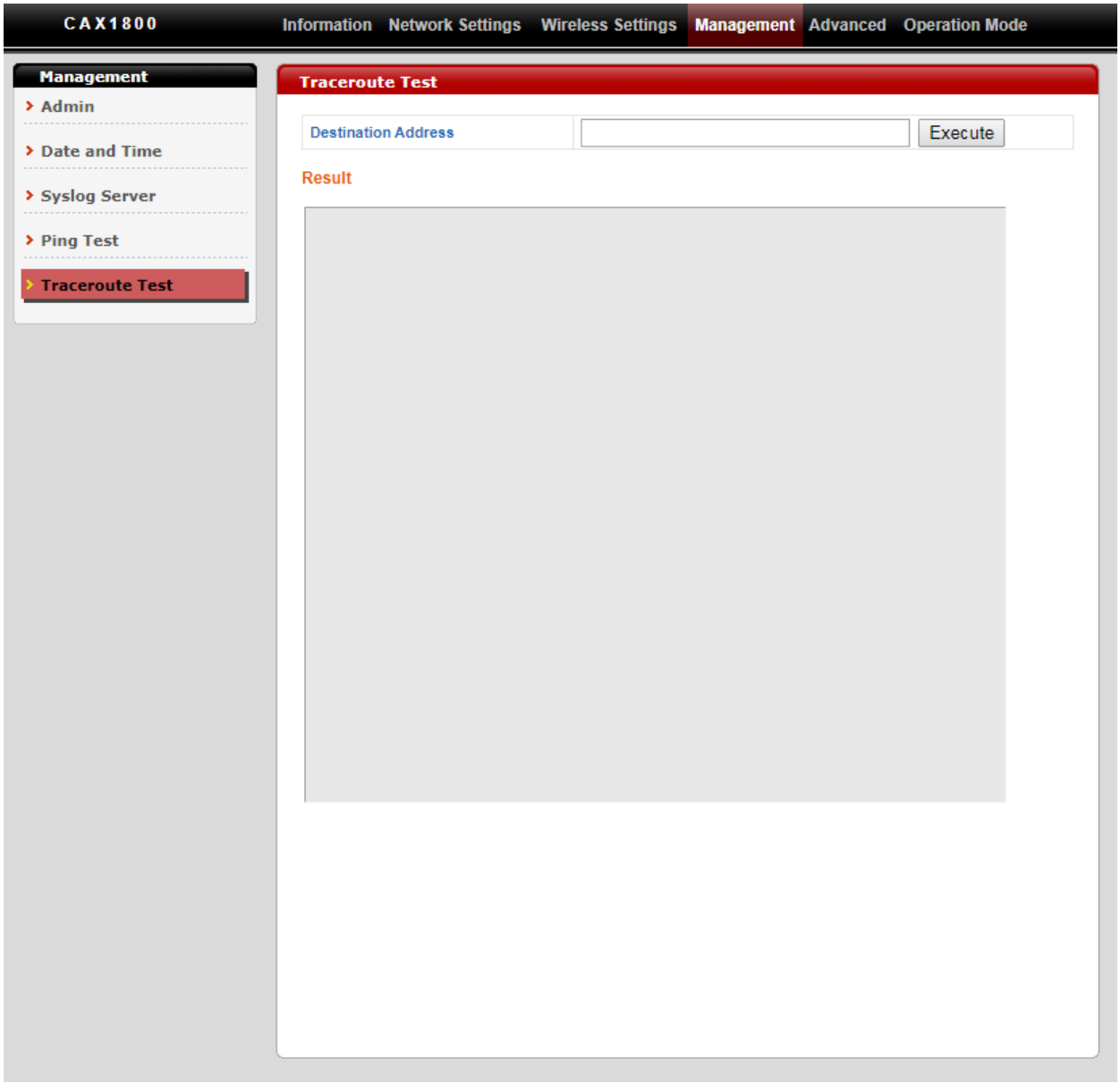
The AP includes a built-in ping test function.



Destination Address	Enter the address of the host.
Execute	Click the “Execute” button to ping the host.

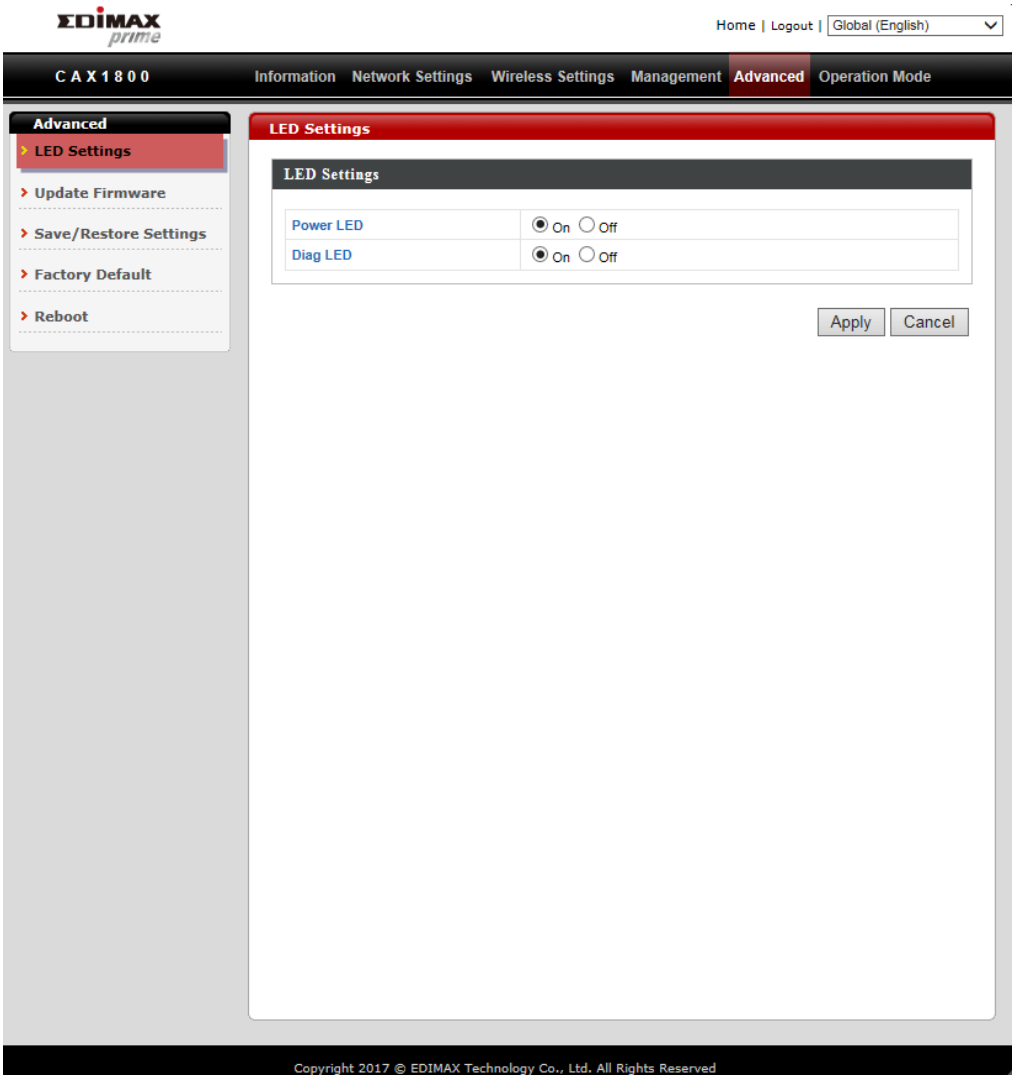
v. Traceroute Test

Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IP network.



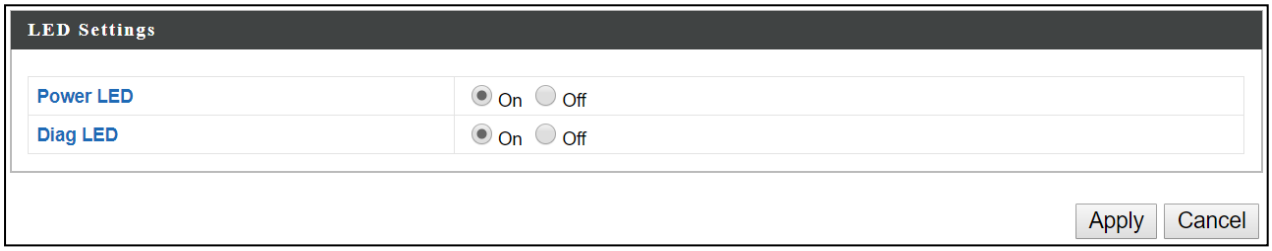
Destination Address	Enter the address of the host.
Execute	Click the “Execute” button to execute the traceroute command.

V-5. Advanced



i. LED Settings

The AP LEDs can be manually enabled or disabled according to your preference.

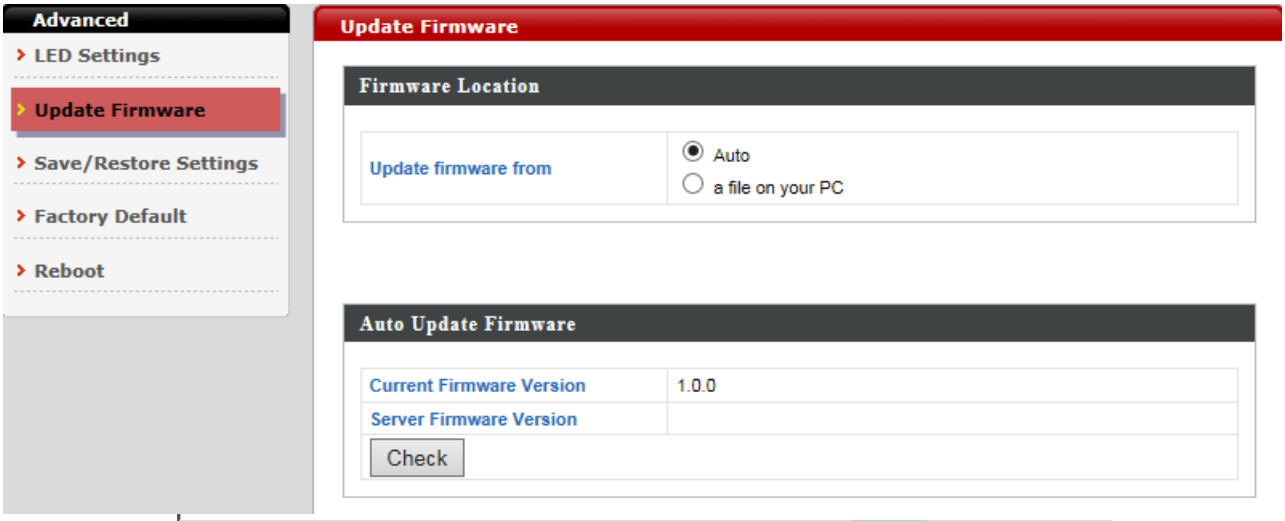


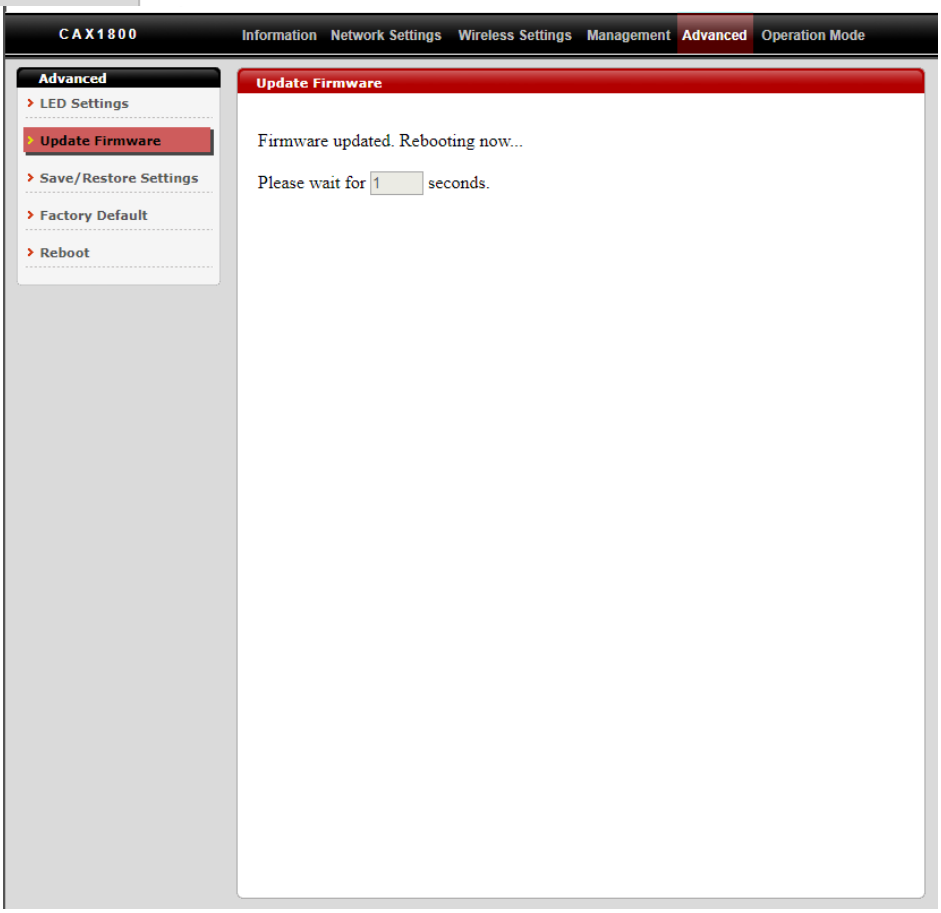
Power LED	Select on or off.
Diag LED	Select on or off.

ii. Update Firmware

The “Firmware” page allows users to update the firmware of the system.

Do not switch off or disconnect the AP during a firmware upgrade, as this could damage the device.

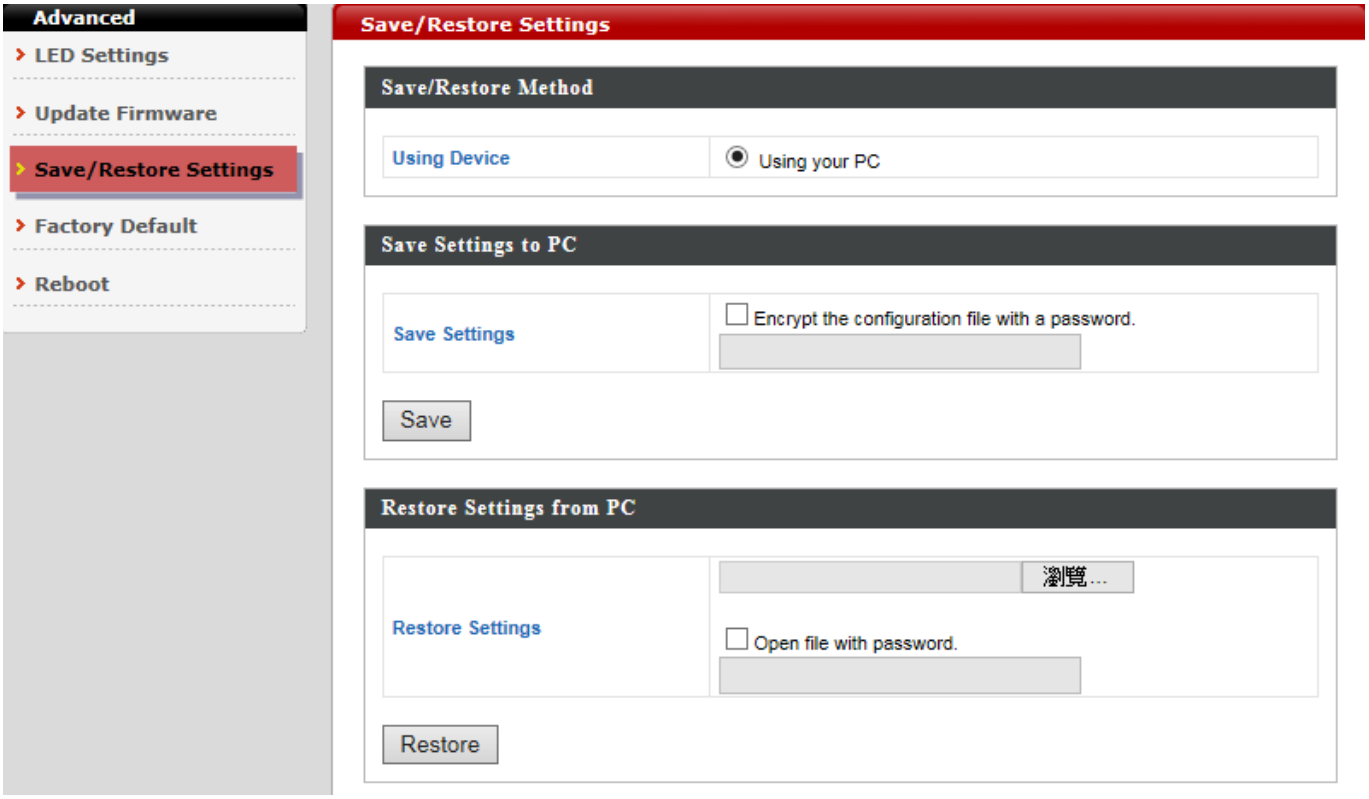




Firmware Location	Click “Choose File” to upload firmware from your local computer.

iii. Save / Restore Settings

Users can save / backup the device's current settings as a file to your local computer, and restore the device to previously saved settings.

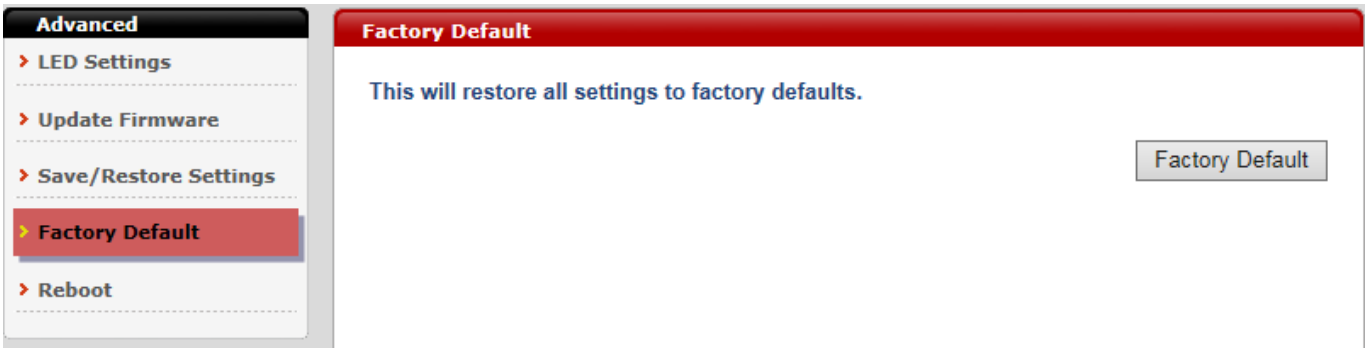


Save Settings to PC	
Save Settings	Encryption: If you wish to encrypt the configuration file with a password, check the "Encrypt the configuration file with a password" box and enter a password. Click "Save" to save current settings. A new window will open to allow you to specify a location to save to.

Restore Settings from PC	
Restore Settings	Click the "Choose File" button to find a previously saved settings file on your computer. If your settings file is encrypted with a password, check the "Open file with password" box and enter the password in the following field. Click "Restore" to replace your current settings.

iv. Factory Default

If the AP malfunction or is not responding, rebooting the device maybe an option to consider. If rebooting does not work, try resetting the device back to its factory default settings.

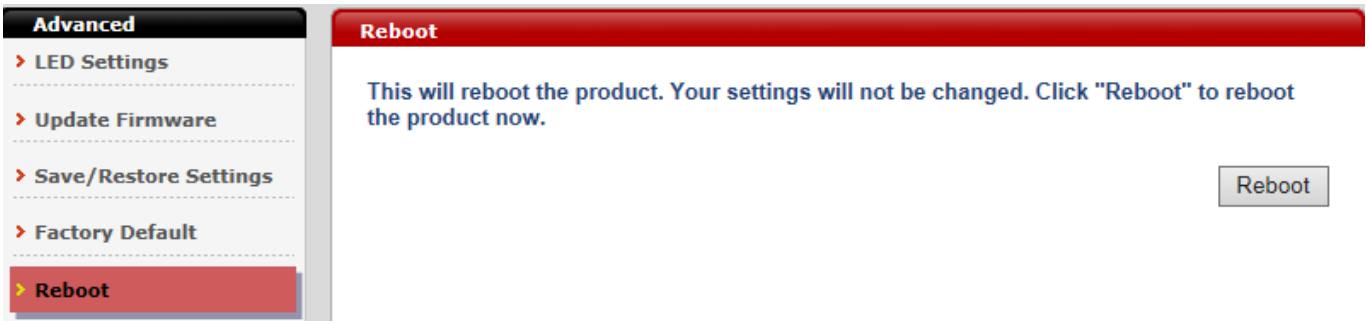


Factory Default	Click “Factory Default” to restore settings to the factory default. A pop-up window will appear and ask you to confirm.

After resetting to factory defaults, please wait for the AP to reset and restart.

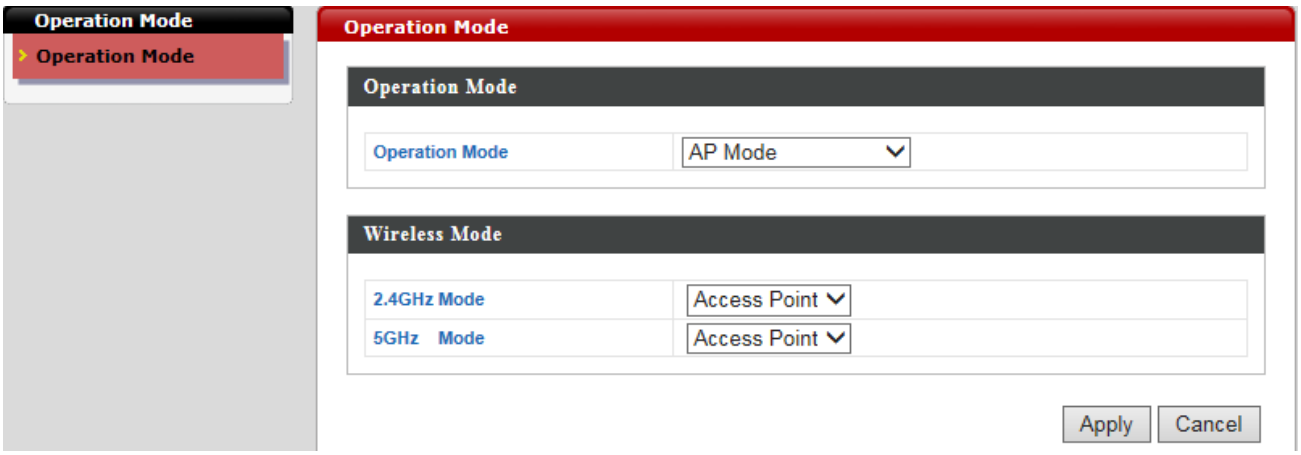
v. Reboot

If the AP malfunctions or is not responding, rebooting the device may be an option to consider.



Reboot	Click “Reboot” to reboot the device. A countdown will indicate the progress of the reboot.

V-6. Operation Mode

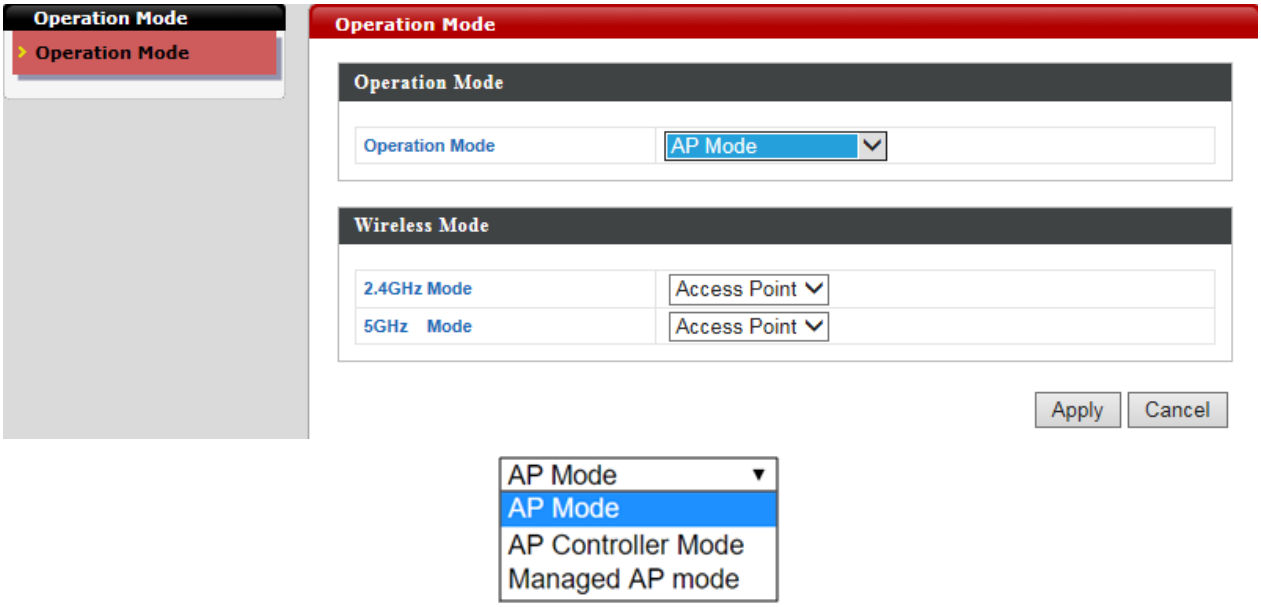


The AP can function in three different modes. Set the operation mode of the AP here.

1. AP Mode: The device acts as a standalone AP
2. AP controller Mode: The device acts as the designated master of the AP array
3. Managed AP Mode: The device acts as a slave AP within the AP array.

In Managed AP mode some functions of the AP will be disabled in this user interface and must be set using Edimax Pro NMS on the AP Controller.

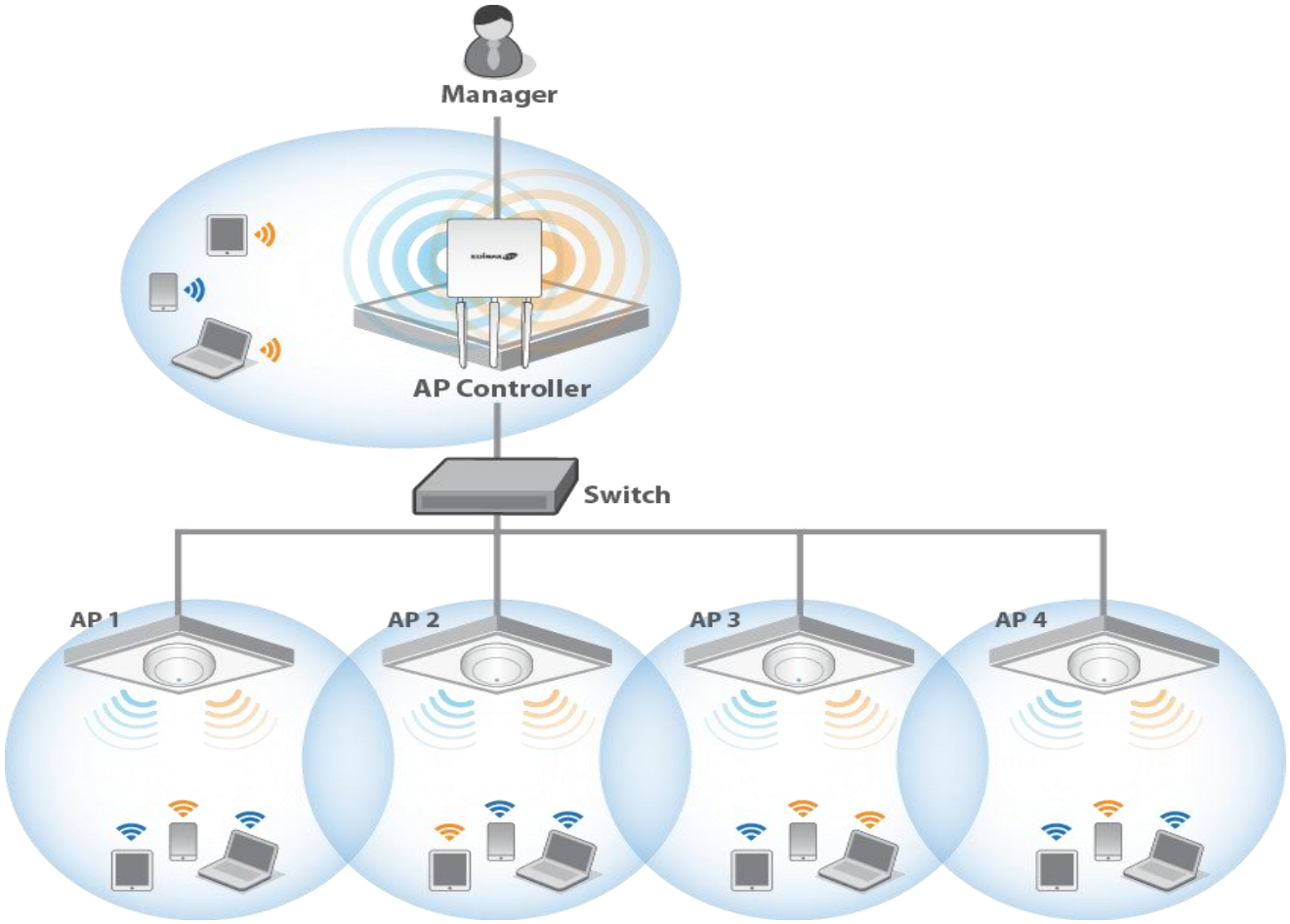
In AP Controller Mode the AP will switch to the Edimax Pro NMS user interface.



VI. Edimax Pro NMS

Edimax Pro Network Management Suite (NMS) supports the central management of a group of APs, otherwise known as an AP Array. NMS can be installed on one AP and support up to 16 Edimax Pro APs with no additional wireless controller required, reducing costs and facilitating efficient remote AP management.

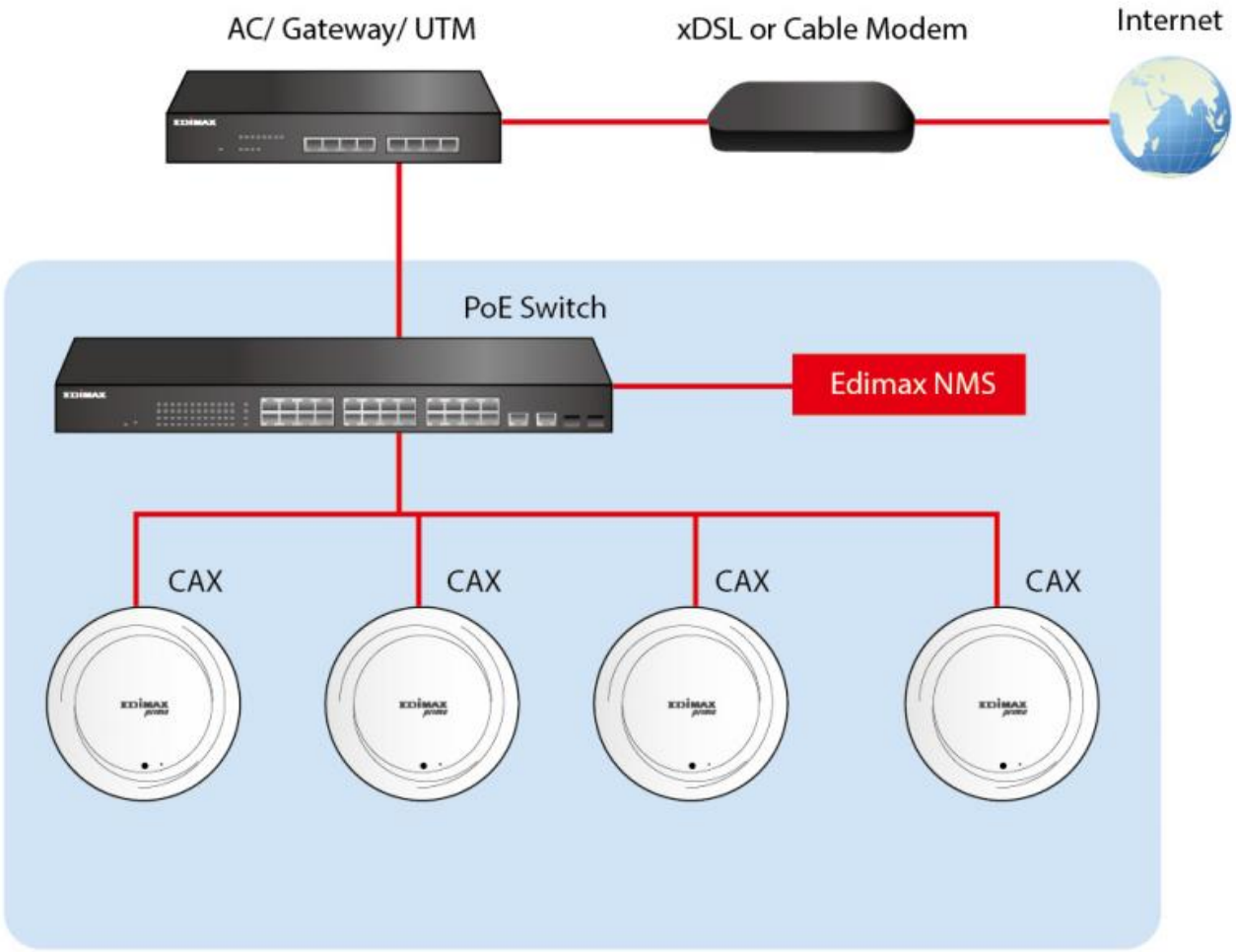
APs can be deployed and configured according to requirements, creating a powerful network architecture which can be easily managed and expanded in the future, with an easy to use interface and a full range of functionality – ideal for small and mid-sized office environments. A secure WLAN can be deployed and administered from a single point, minimizing cost and complexity.



VI-1. *Quick Setup – NMS*

Edimax Network Management System (NMS) supports the central management of a group of APs, otherwise known as an AP Array. NMS can be installed on one AP and support up to 16 Edimax APs with no additional wireless controller required, reducing costs and facilitating efficient remote AP management.

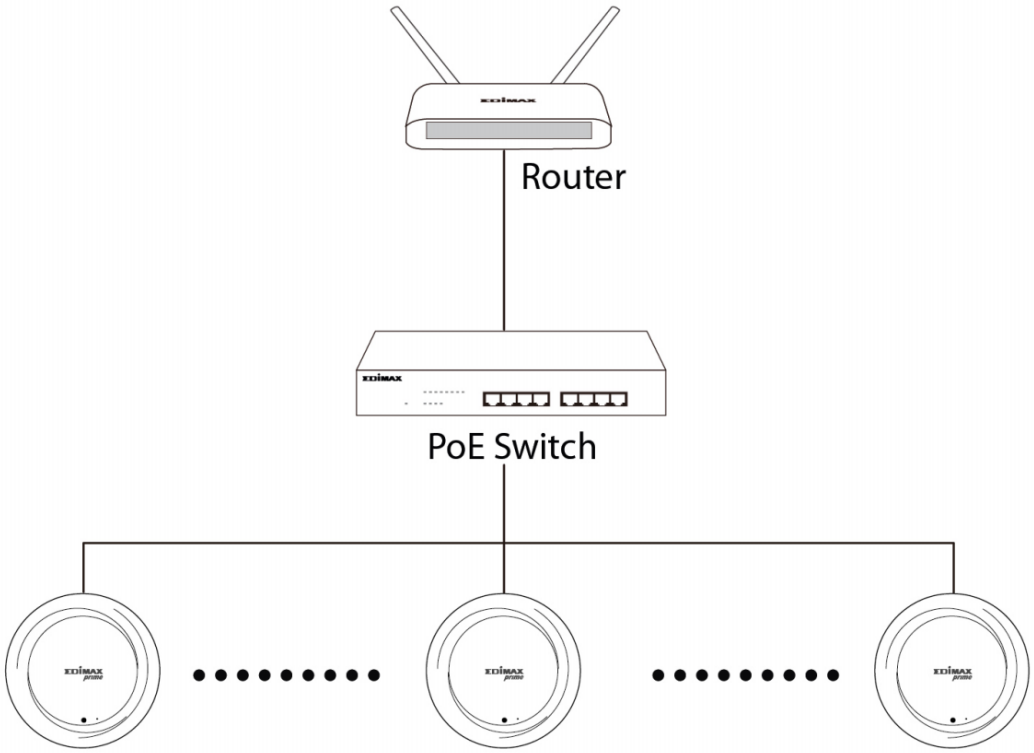
NMS is simple to setup. An overview of the system is shown below:



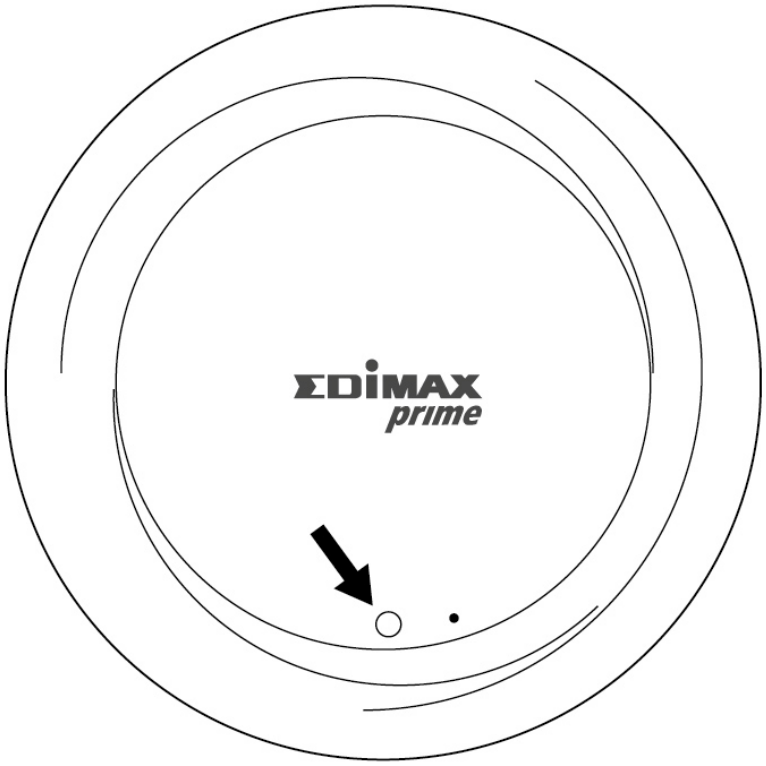
One AP is designated as the AP Controller (master) and other connected Edimax APs are automatically designated as Managed APs (slaves). Using Edimax NMS you can monitor, configure and manage all Managed APs (up to 16) from the single AP Controller.

Please follow the steps below for how to setup:

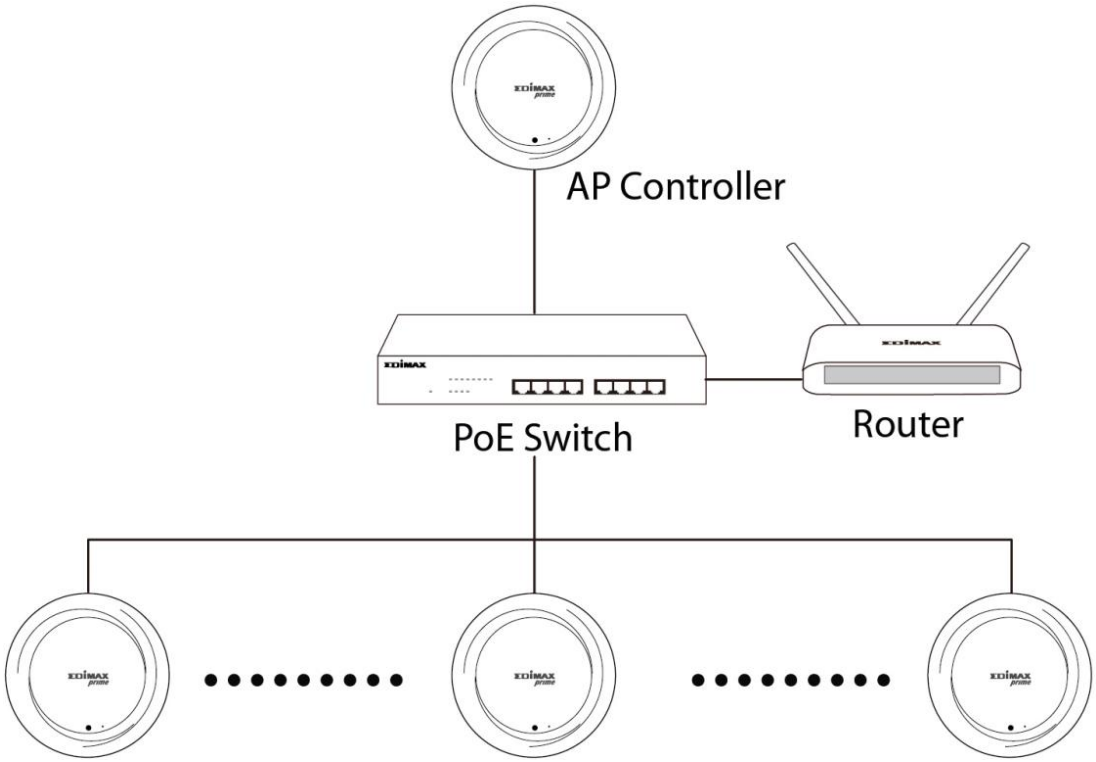
1. Connect all APs to a switch which is connected to a router.



2. Ensure all APs are powered on and check their LEDs.



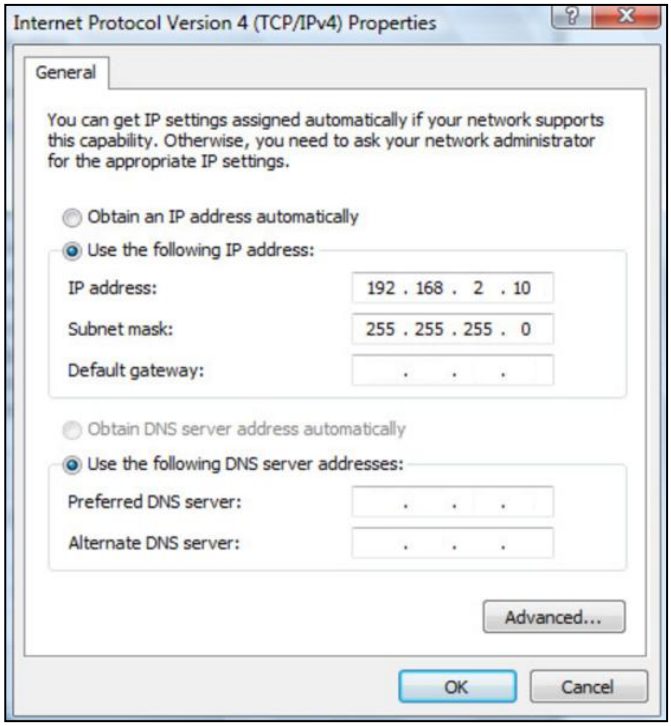
3. Designate one AP as the AP Controller which will manage all other connected APs (up to 16).



4. Connect a computer to the designated AP Controller using an Ethernet cable.

Ensure you have the latest firmware from the Edimax website for your Edimax Pro products.

5. Open a web browser and enter the AP Controller's IP address in the address field. (The default IP address is 192.168.2.2)



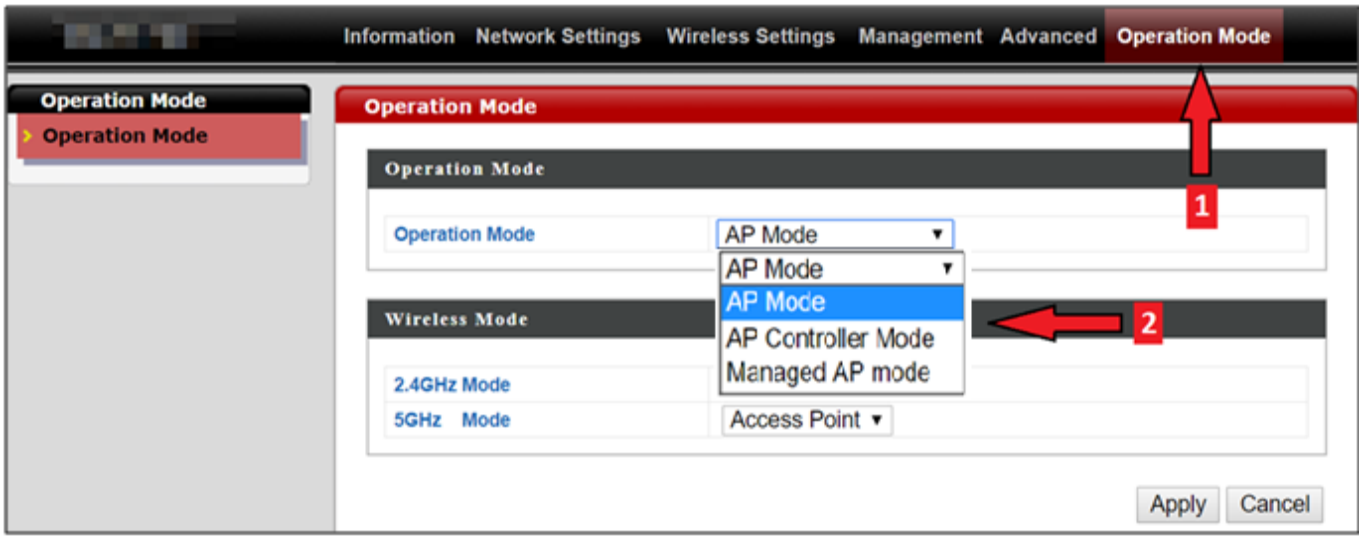
Your computer's IP address must be in the same subnet as the AP Controller. Refer to the user manual for help.

If you changed the AP Controller's IP address, or if your router uses a DHCP server, ensure you enter the correct IP address. Refer to your router's settings.

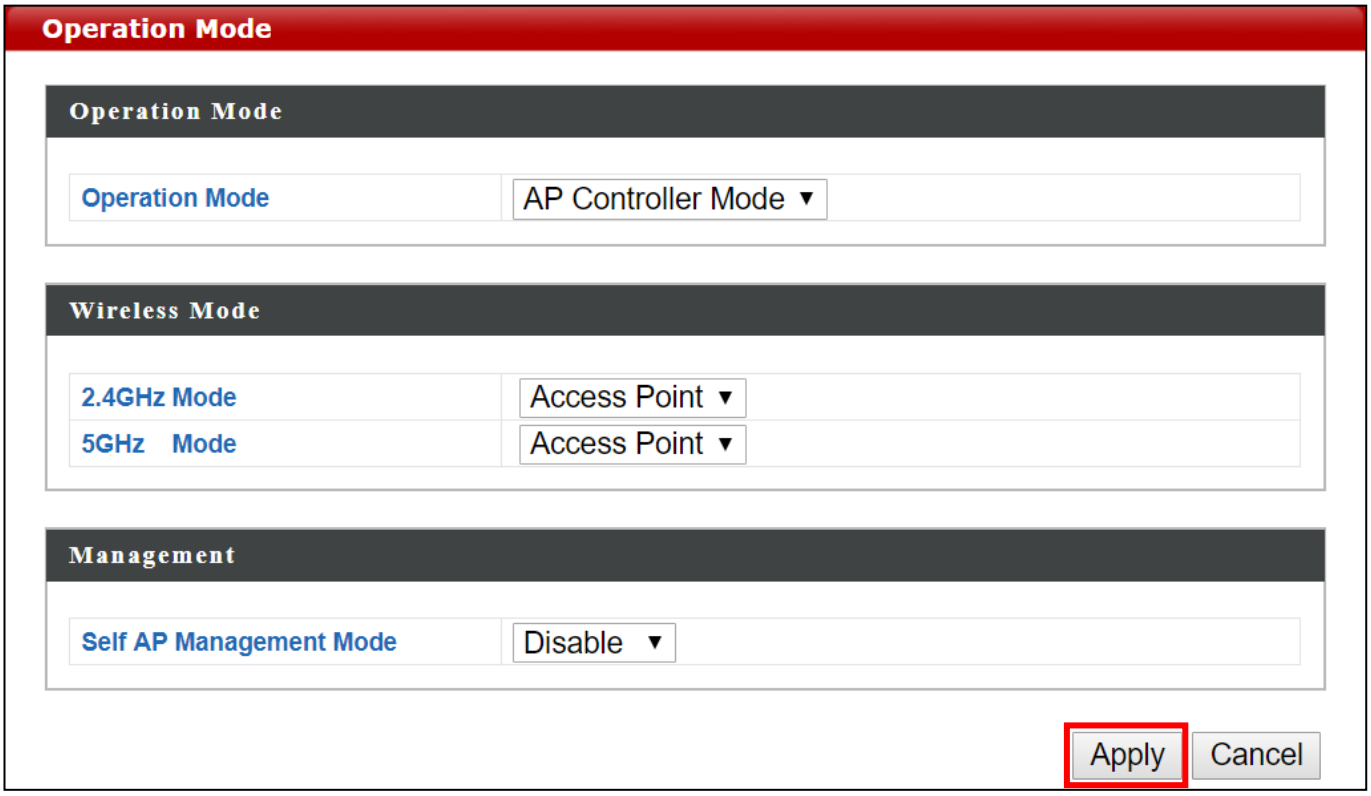
6. Enter the default Username / Password to login. (admin / 1234)
You will arrive at the Edimax Pro NMS Dashboard.

7. Follow the steps below to change the operation Mode,

i. Go to “Management”.
ii. Tap “Operation Mode”.
iii. Select “AP Controller Mode” from the drop down menu.

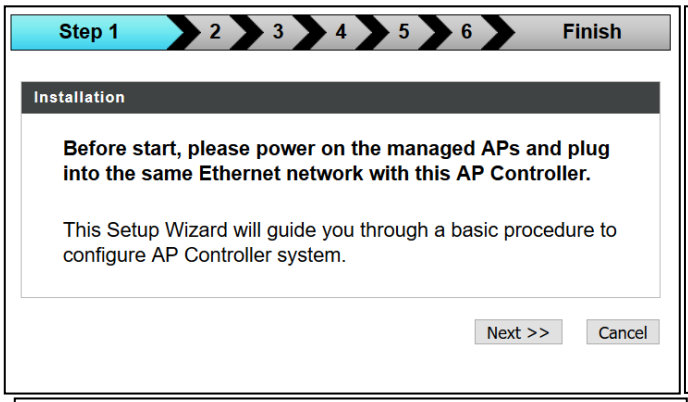


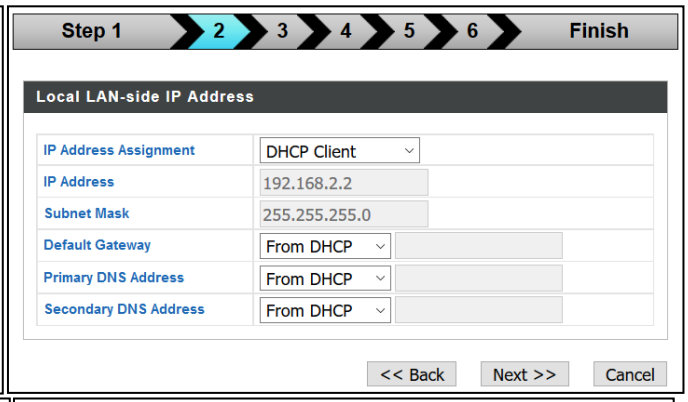
7. Click “Apply” to save the settings.

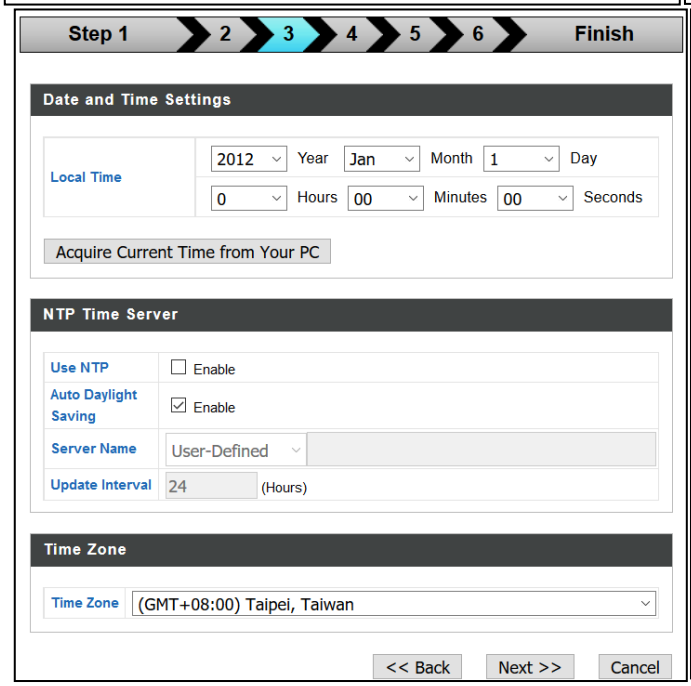


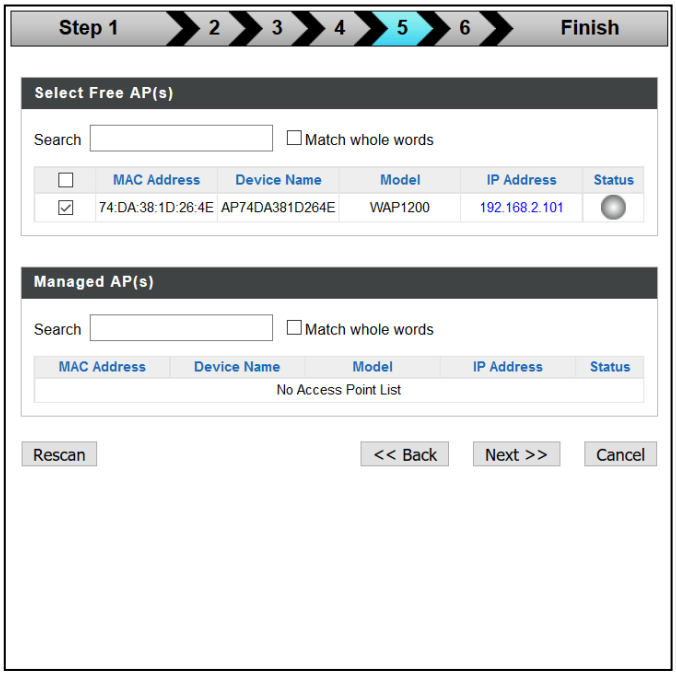
8. Edimax Pro NMS includes a wizard to quickly setup the SSID & security for Managed APs. Click “Wizard” in the top right corner to begin.

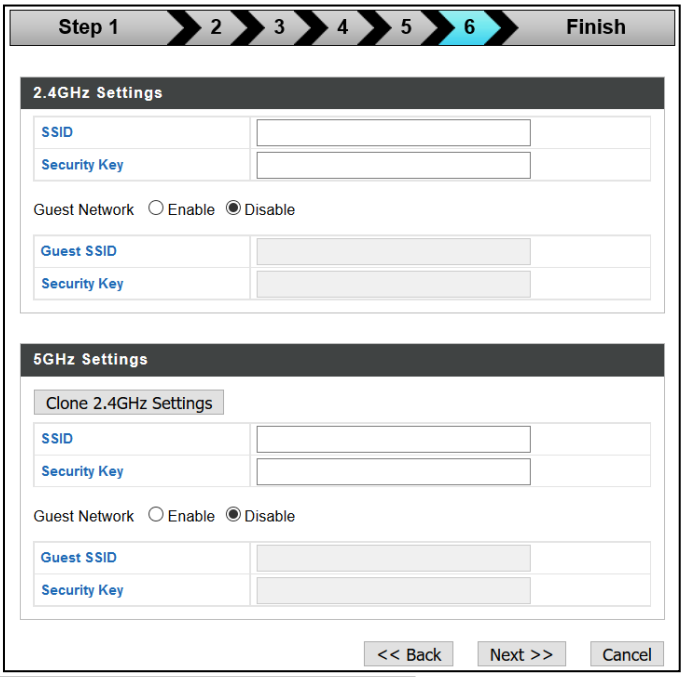
9. Follow the instructions on-screen to complete Steps 1-6 and click “Finish” to save the settings.

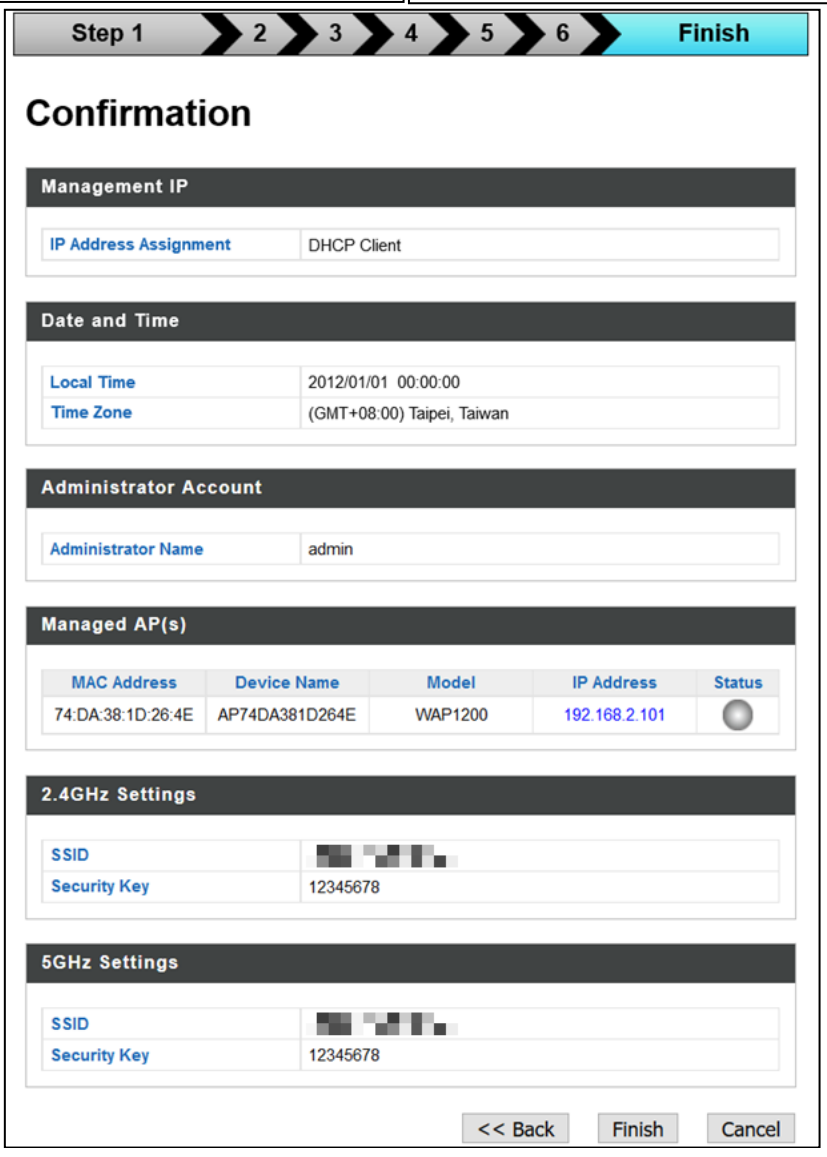






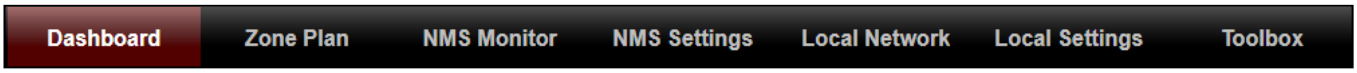






If any of your Managed APs cannot be found, reset it to its factory default settings.

10. Your AP Controller & Managed APs should be fully functional. Use the top menu to navigate around Edimax Pro NMS.



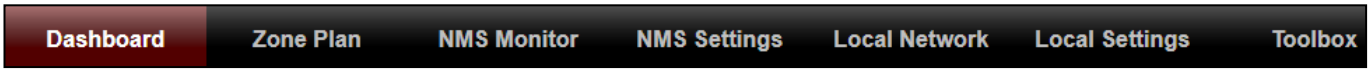
Use Dashboard, Zone Plan, NMS Monitor & NMS Settings to configure Managed APs.

Use Local Network & Local Settings to configure your AP Controller.

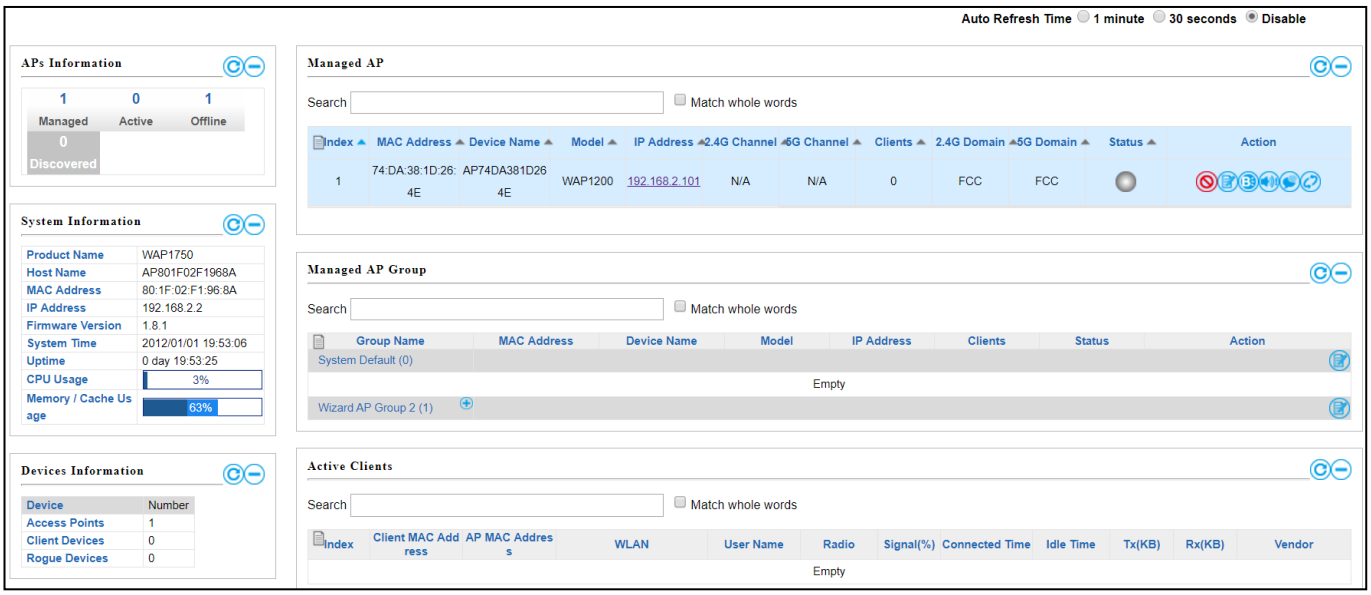
VI-2. Webpage Layout - NMS

The top menu features 7 panels: Dashboard, Zone Plan, NMS Monitor, NMS Settings, Local Network, Local Settings & Toolbox.

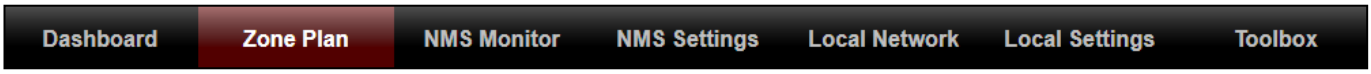
Dashboard:



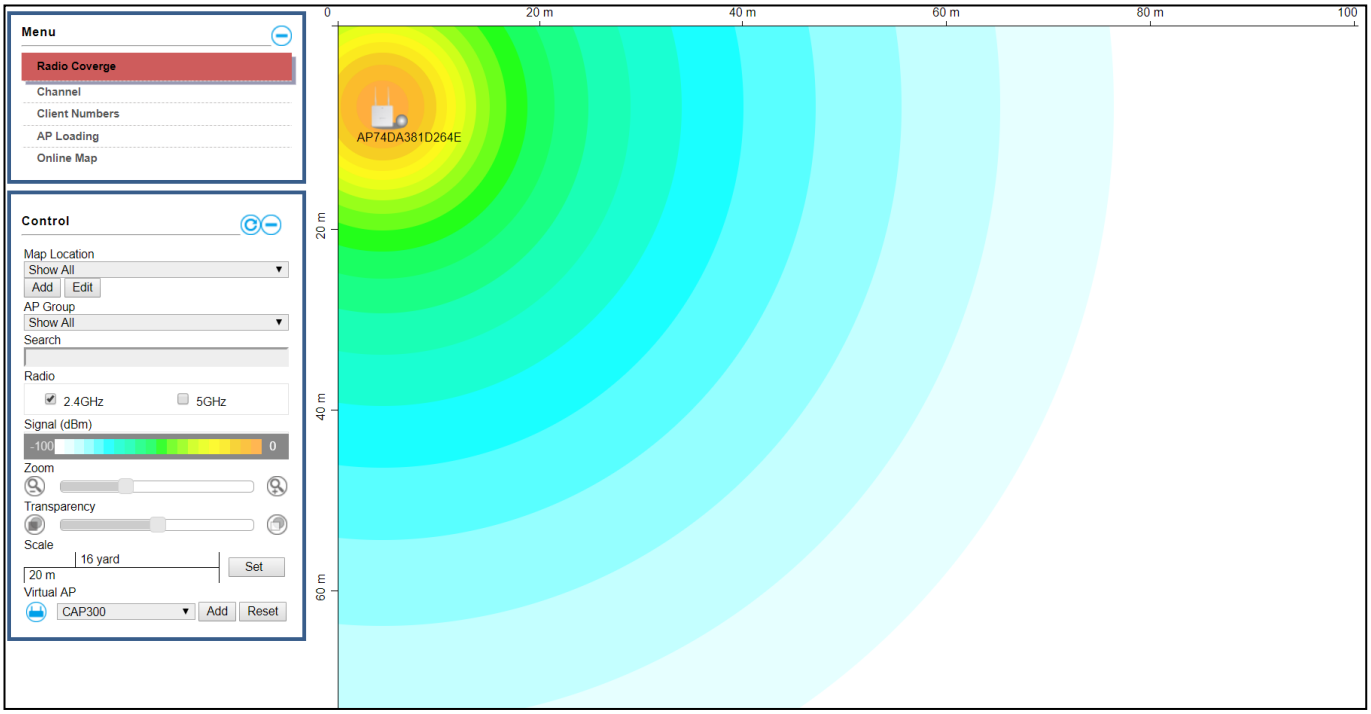
The Dashboard panel displays an overview of your network and key system information, with quick links to access configuration options for Managed APs and Managed AP groups. Each panel can be refreshed, collapsed or moved according to your preference.



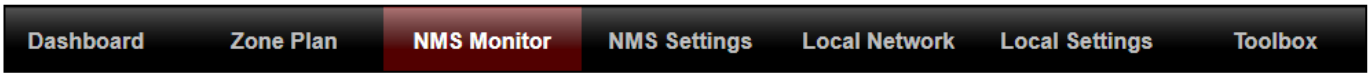
Zone Plan:



Zone Plan displays a customizable live map of Managed APs for a visual representation of your network coverage. Each AP icon can be moved around the map, and a background image can be uploaded for user-defined location profiles using NMS Settings → Zone Edit. Options can be configured using the menu on the right side and signal strength is displayed for each AP.



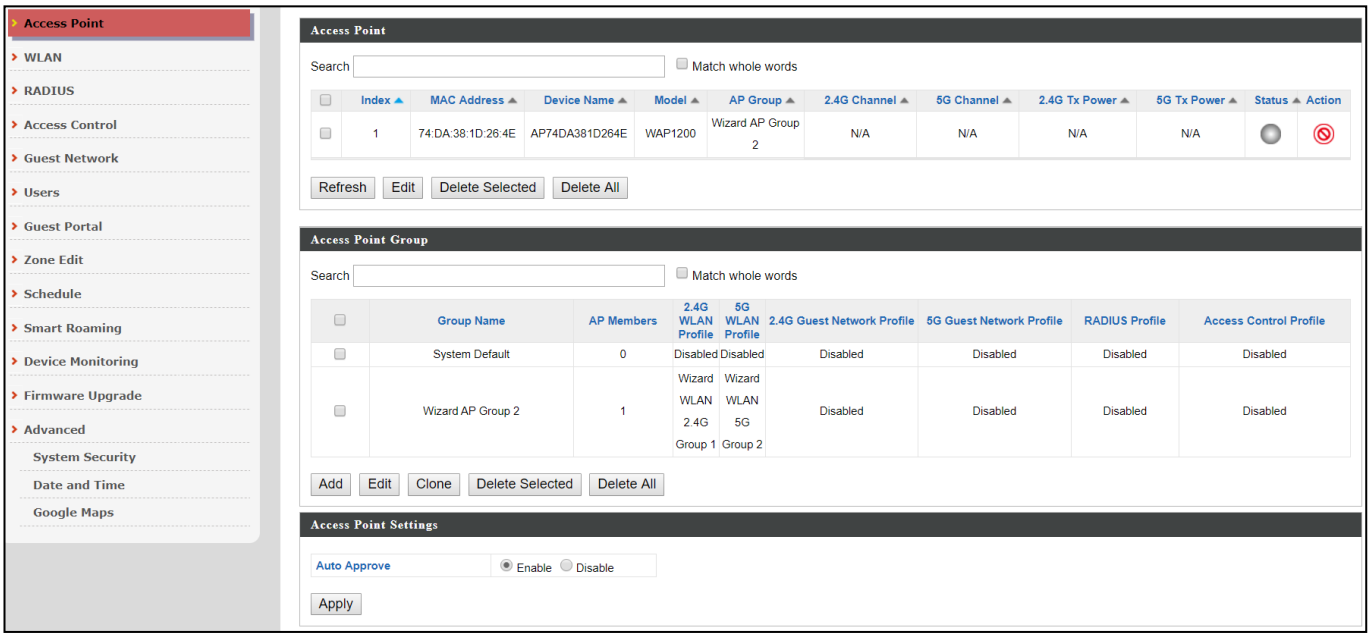
NMS Monitor:



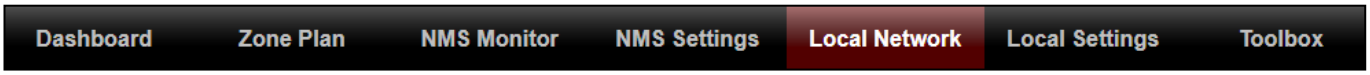
The NMS Monitor panel provides more detailed monitoring information about the AP Array than found on the Dashboard, grouped according to categories in the menu down the left side.

NMS Settings:

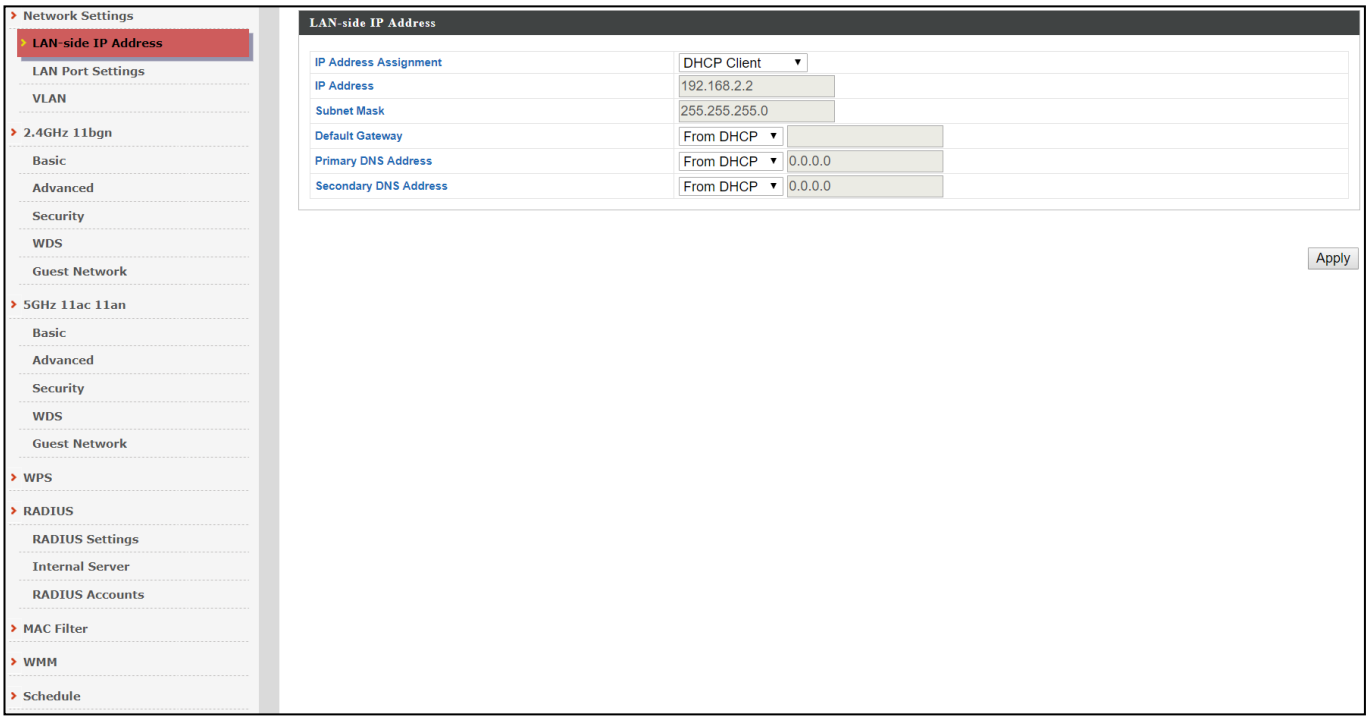
NMS Settings provides extensive configuration options for the AP Array. You can manage each AP, assign APs into groups, manage WLAN, RADIUS & guest network settings as well as upgrade firmware across multiple APs. The Zone Plan can also be configured using “Zone Edit”.



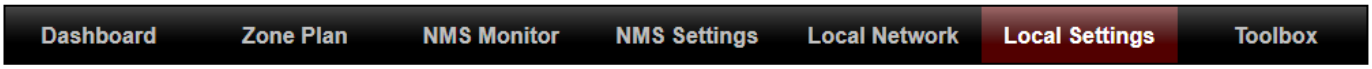
Local Network:



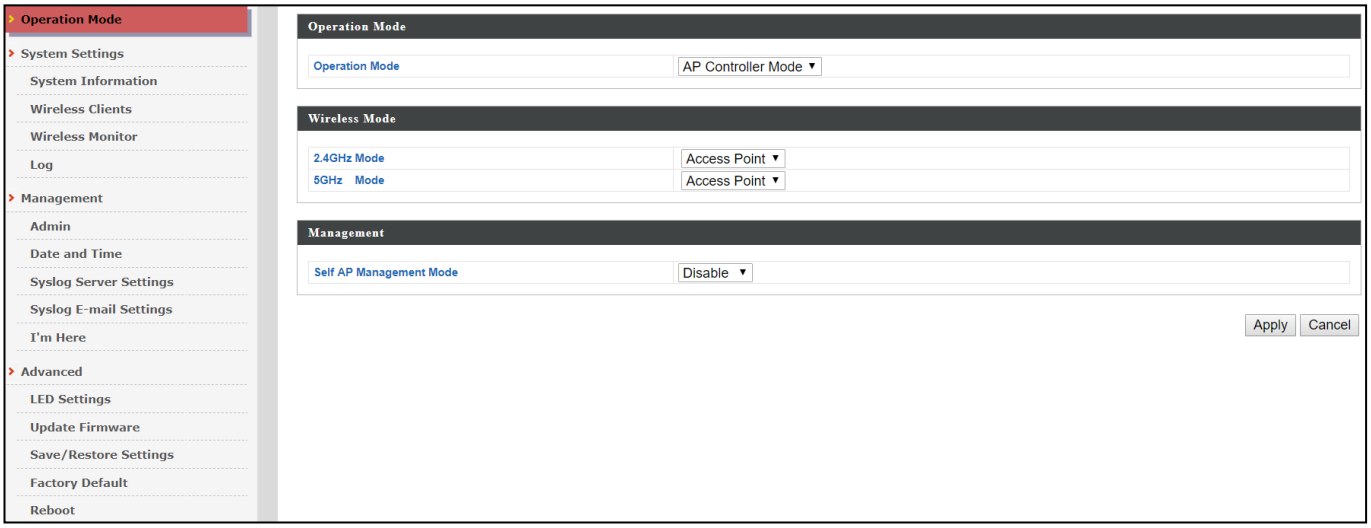
Local Network settings are for your AP Controller. You can configure the IP address and DHCP server of the AP Controller in addition to 2.4GHz & 5Ghz Wi-Fi and security, with WPS, RADIUS server, MAC filtering and WMM settings also available.



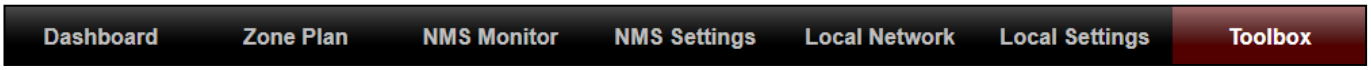
Local Settings:



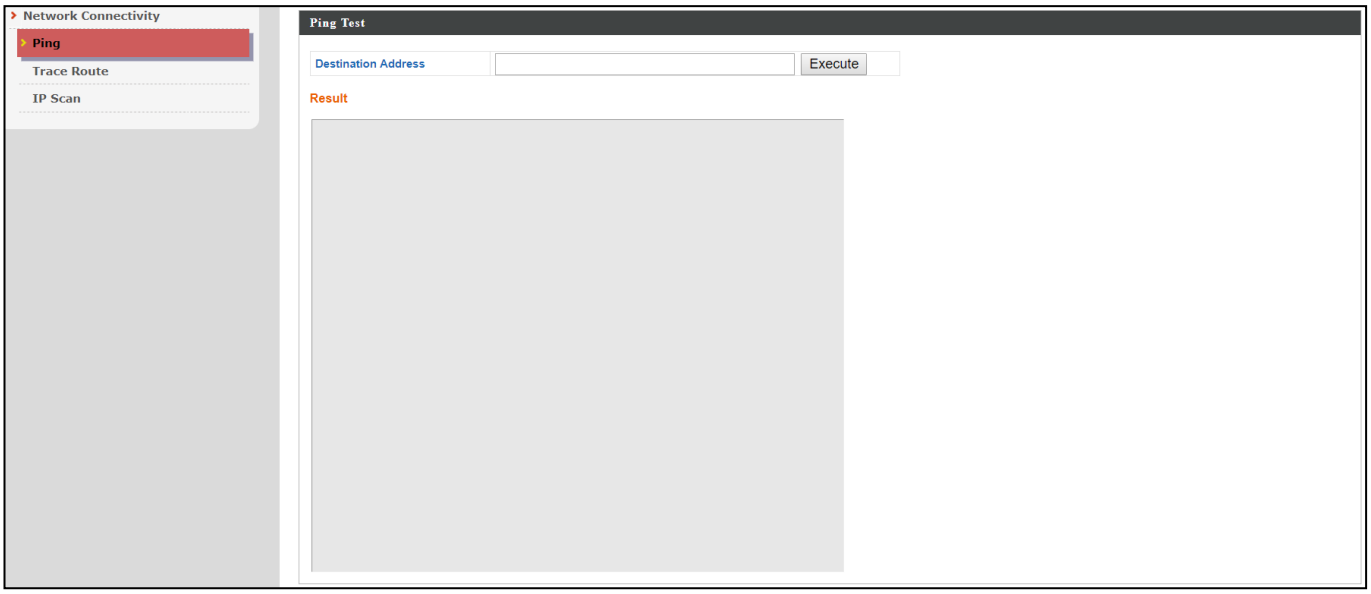
Local Settings are for your AP Controller. You can set the operation mode and view network settings (clients and logs) specifically for the AP Controller, as well as other management settings such as date/time, admin accounts, firmware and reset.



Toolbox:



The Toolbox panel provides network diagnostic tools: *Ping*, *Traceroute*, and *IP Scan*.



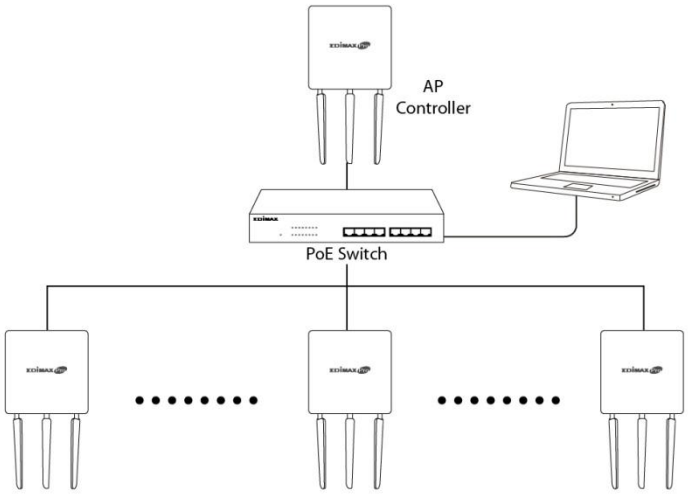
VI-3. NMS Features

Descriptions of the functions of each main panel can be found below. When using Edimax NMS, click “Apply” to save changes:

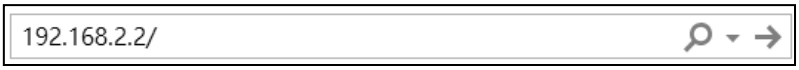
It is recommended that you login to the AP Controller to make configurations to Managed APs.

Login:

1. Connect a computer to the designated AP Controller using an Ethernet cable:



2. Open a web browser and enter the AP Controller’s IP address in the address field. The default IP address is 192.168.2.2.



Your computer’s IP address must be in the same subnet as the AP Controller.

If you changed the AP Controller's IP address, or if your gateway/router uses a DHCP server, ensure you enter the correct IP address. Refer to your gateway/router's settings.

If a DHCP server is used in the network, it is advised to use your DHCP server's settings to assign the AP Controller a static IP address.

3. Enter the username & password to login. The default username & password are admin & 1234.

Logout:

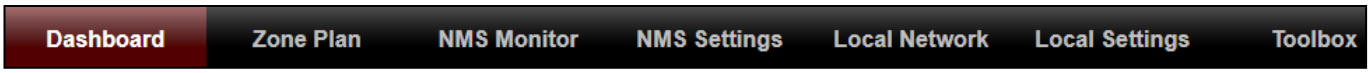
To logout from Edimax NMS, click "Logout" in the top right corner:

Restart:

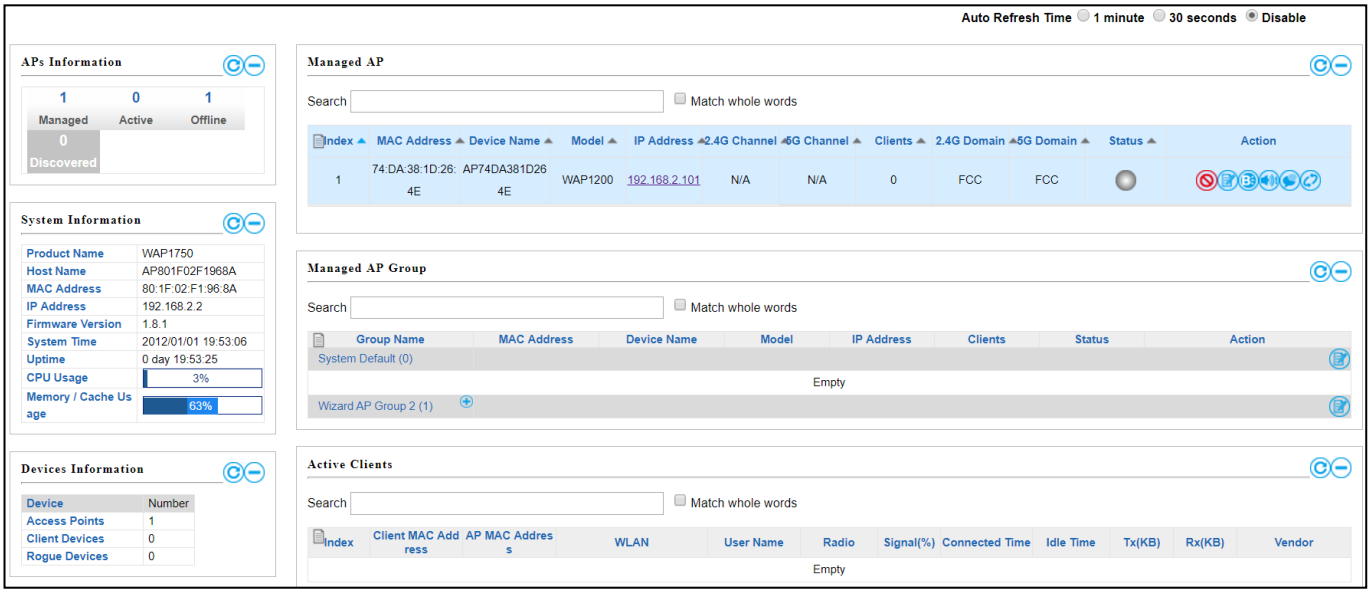
You can restart your AP Controller or any Managed AP using Edimax NMS. To restart your AP Controller go to Local Settings → Advanced → Reboot and click "Reboot".

To restart Managed APs click the Restart icon for the specified AP on the Dashboard:

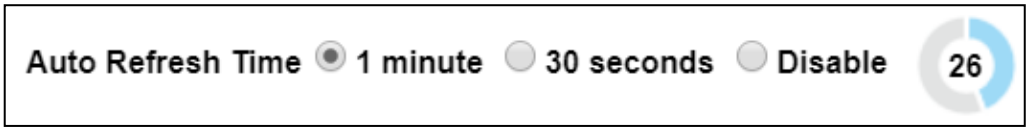
VI-4. Dashboard



The dashboard displays an overview of your AP array:

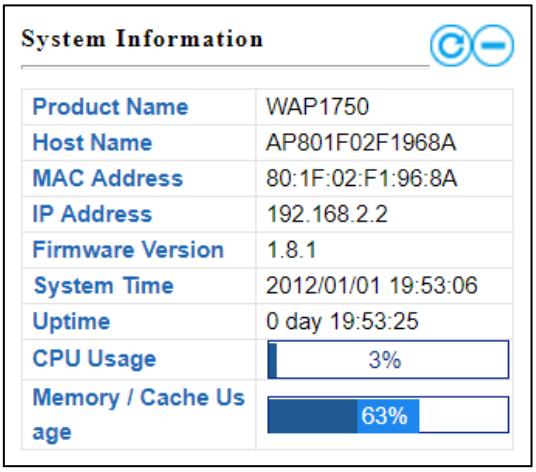


Use the blue icons above to refresh or collapse each panel in the dashboard. Click and drag to move a panel to suit your preference. You can set the dashboard to auto-refresh every 1 minute, 30 seconds or disable auto-refresh:



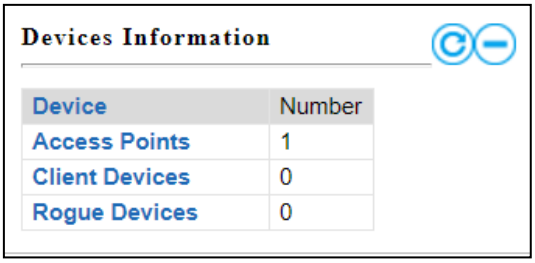
i. System Information

System Information displays information about the AP Controller: Product Name (model), Host Name, MAC Address, IP Address, Firmware Version, System Time and Uptime (time the AP has been on).



ii. Devices Information

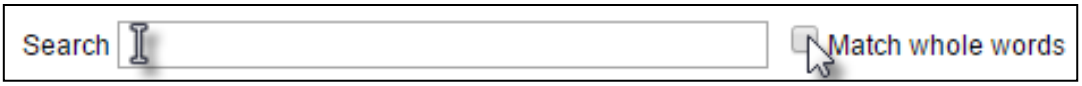
Devices Information is a summary of the number of all devices in the local network: APs, Clients Connected, and Rogue (unidentified) Devices.



iii. Managed AP

This page displays information about the Managed APs in the local network: Index (reference number), MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each AP, and Status (connected, connecting or disconnected).

The search function can be used to locate a specific Managed AP. Type in the search box and the list will update:



The Status icon displays *grey* (disconnected), *yellow* (connecting) or *green* (connected) for each Managed AP.

Each Managed AP has “Action” icons with the following functions:

1. **Disallow**
   Remove the Managed AP from the AP array and disable connectivity.

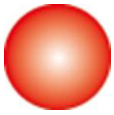
2. **Edit**
   Edit various settings for the Managed AP.

3. **Blink LED**
   The Managed AP’s LED will flash temporarily to help identify & locate the AP.

4. **Buzzer**
   The Managed AP's buzzer will sound temporarily to help identify/locate the AP.

5. **Network Connectivity**
   Go to the "Network Connectivity" panel to perform a ping or traceroute.

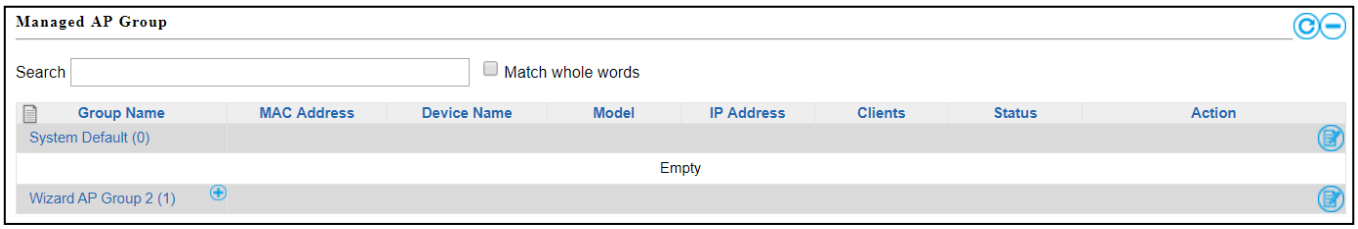
6. **Restart**
   Restarts the Managed AP.

Status Icons			
Icon	**Color**	**Status**	**Definition**
	Grey	Disconnected	Managed AP is disconnected. Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.
	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all APs in the AP array. Please check security settings. All APs must have the same firmware version. Please use the AP Controller's firmware upgrade function.
	Orange	Configuring or Upgrading	Please wait while the Managed AP makes configurations or while the firmware is upgrading.
	Yellow	Connecting	Please wait while Managed AP is connecting.
	Green	Connected	Managed AP is connected.
	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.

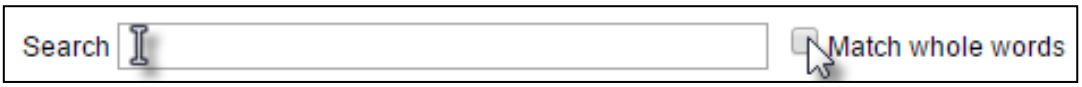
iv. Managed AP Group

Managed APs can be grouped according to your requirements. Managed AP Group displays information about each Managed AP group in the local network: Group Name, MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each AP, and Status (connected or disconnected).

To edit Managed AP Groups go to NMS Settings → AP.



The search function can be used to locate a specific Managed AP Group. Type in the search box and the list will update:



The Status icon displays grey (disconnected), yellow (connecting) or green (connected) for each individual Managed AP.

Each Managed AP Group has “Action” icons with the following functions:

1. **Disallow**
   Remove the Managed AP Group from the AP array and disable connectivity.

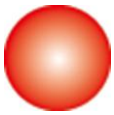
2. **Edit**
   Edit various settings for the Managed AP Group.

3. **Blink LED**
   The LED of all Managed APs in the group will flash temporarily to help identify & locate the APs.

4. **Buzzer**
   The buzzer of all Managed APs in the group will sound temporarily to help identify & locate the APs.

5. **Network Connectivity**
   Go to the “Network Connectivity” panel to perform a ping or traceroute.

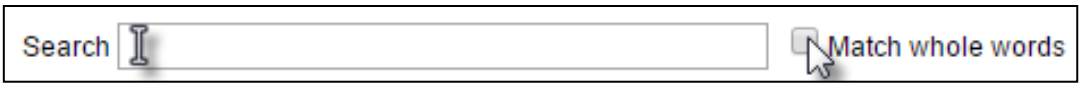
6. **Restart**
   Restarts all Managed APs in the group.

Status Icons			
Icon	**Color**	**Status**	**Definition**
	Grey	Disconnected	Managed AP is disconnected. Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.
	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all APs in the AP array. Please check security settings. All APs must have the same firmware version. Please use the AP Controller's firmware upgrade function.
	Orange	Configuring or Upgrading	Please wait while the Managed AP makes configurations or while the firmware is upgrading.
	Yellow	Connecting	Please wait while Managed AP is connecting.
	Green	Connected	Managed AP is connected.
	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.

v. Active Clients

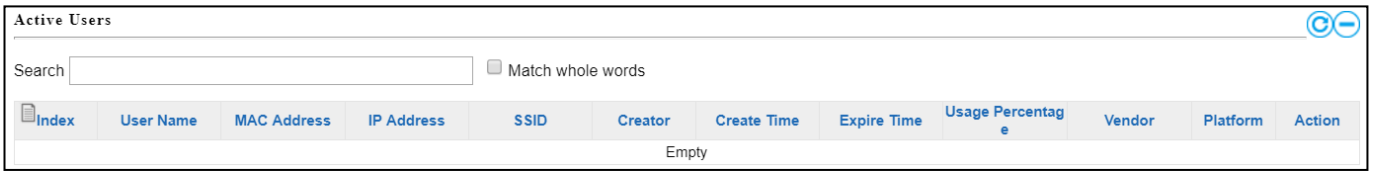
Active Clients displays information about each client in the local network: Index (reference number), Client MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each AP, and Status (on or off).

The search function can be used to locate a specific client. Type in the search box and the list will update:

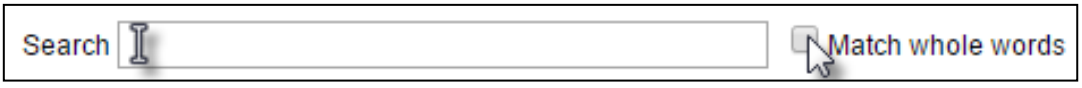


vi. Active Users

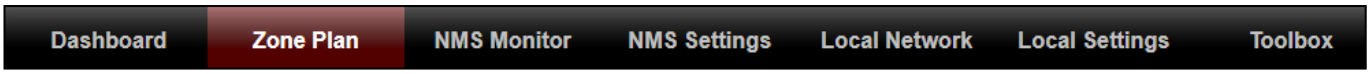
Active Users displays information about users currently connected to the AP Array: User Name, MAC Address, IP Address, SSID, Creator, Create Time, Expire Time, Usage Percentage, Vendor, Platform and Action.



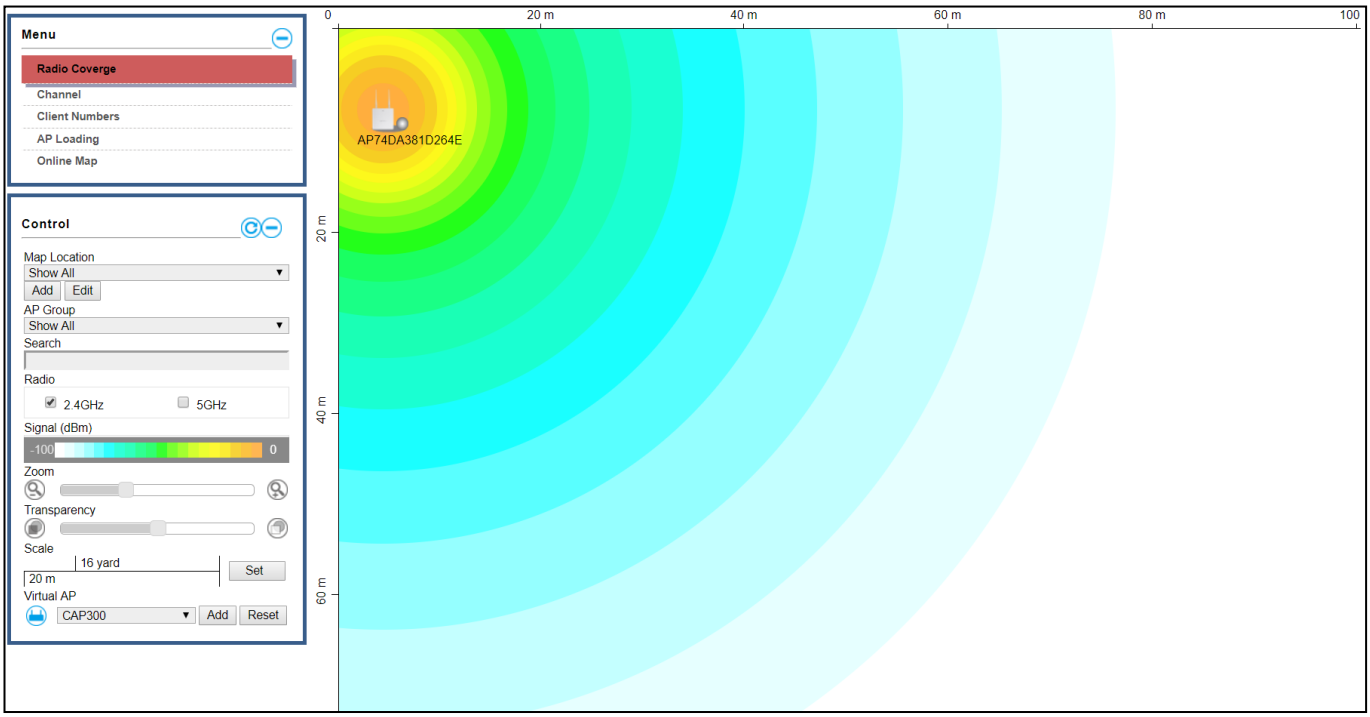
The search function can be used to locate a specific user. Type in the search box and the list will update:



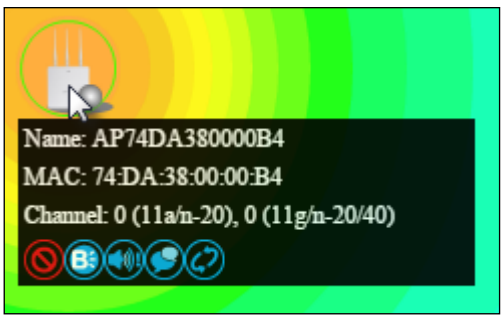
VI-5. Zone Plan



The Zone Plan can be fully customized to match your network environment. You can move the AP icons and select different location images (upload location images in NMS Settings → Zone Edit) to create a visual map of your AP array.

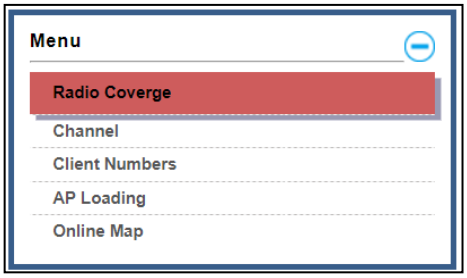


Use the menu on the left side to make adjustments and mouse-over an AP icon in the zone map to see more information. Click an AP icon in the zone map to select it and display action icons:



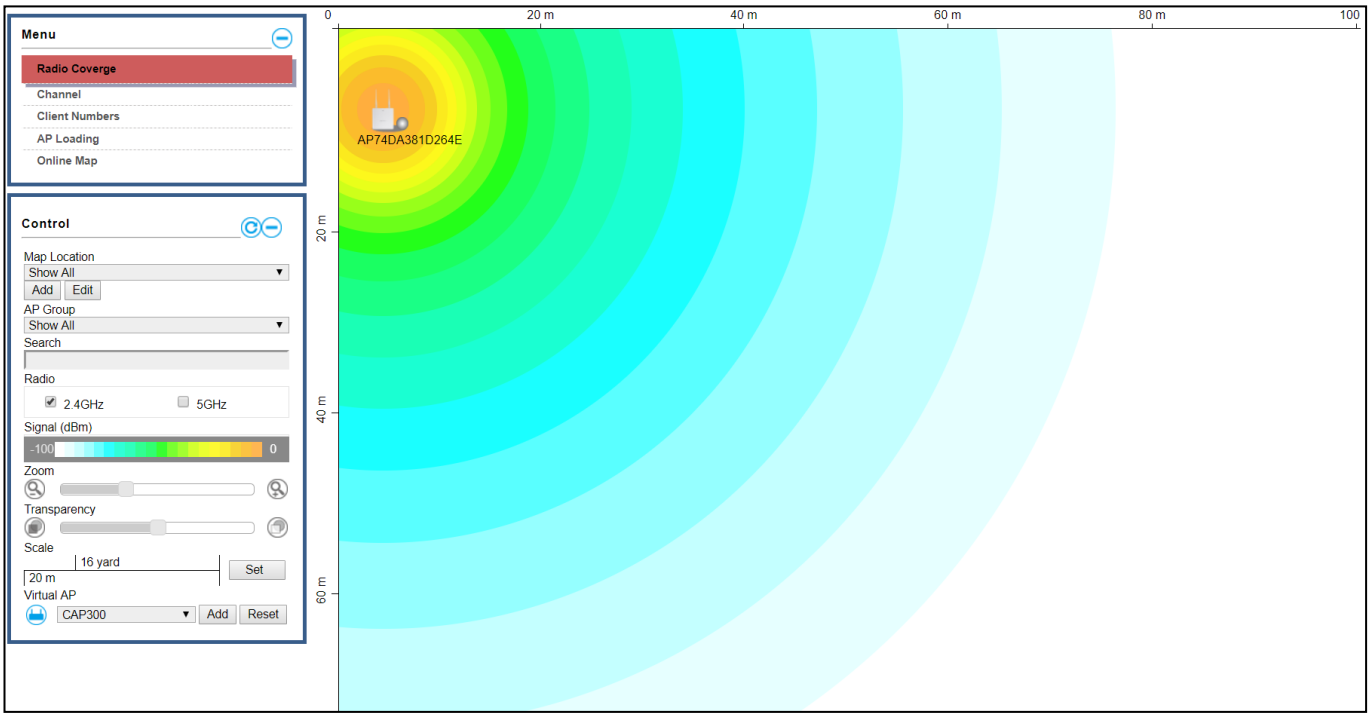
i. Menu

Menu allows you to keep track of the APs' information. Select between *Radio Coverage*, *Channel*, *Client Numbers*, *AP Loading*, and *Online Map*. When an option is selected, the zone plan and Control section will change accordingly.



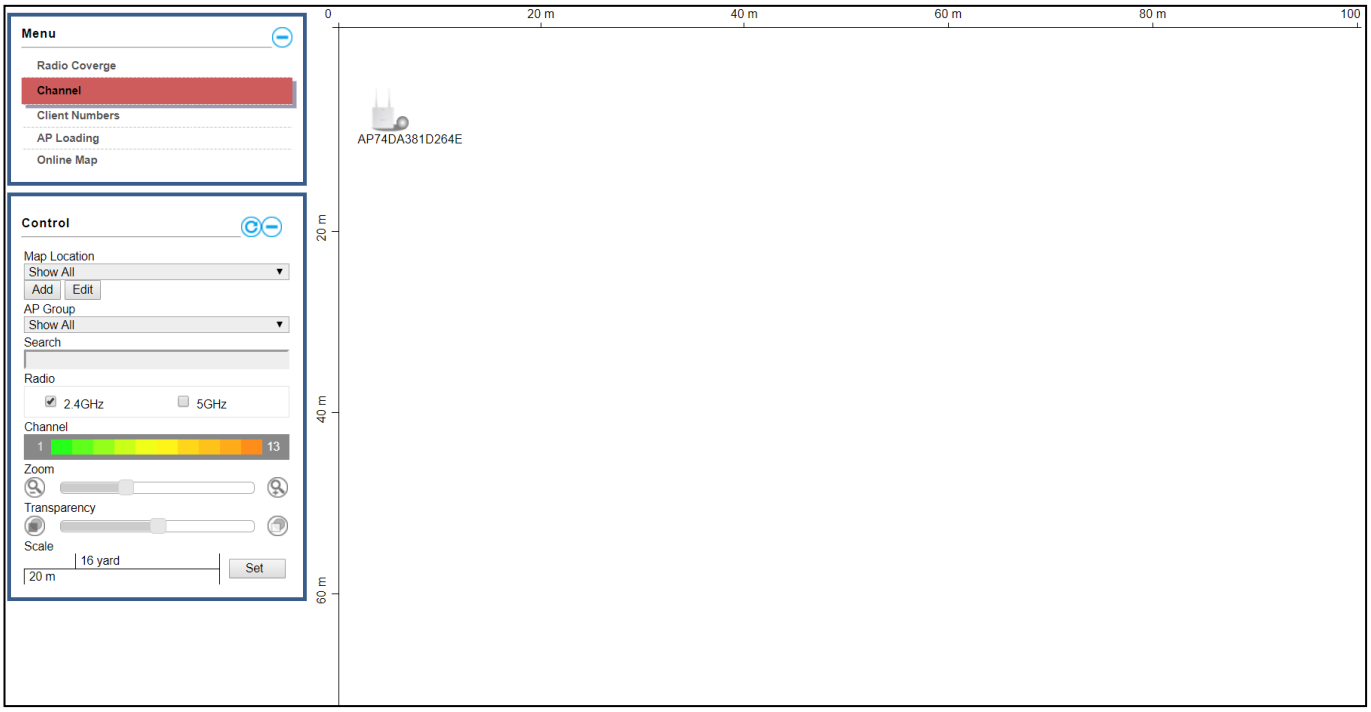
Radio Coverage:

Below is displayed as Radio Coverage is selected:



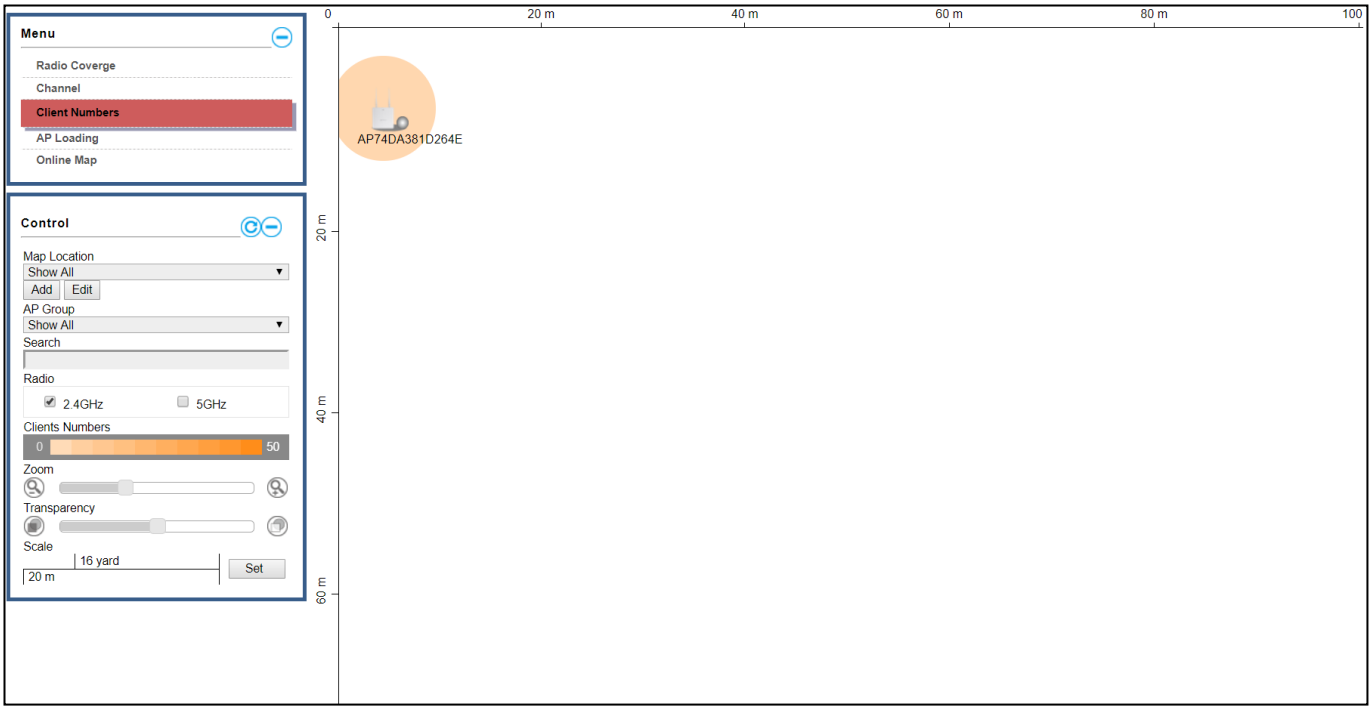
Channel:

Below is displayed as Channel is selected:



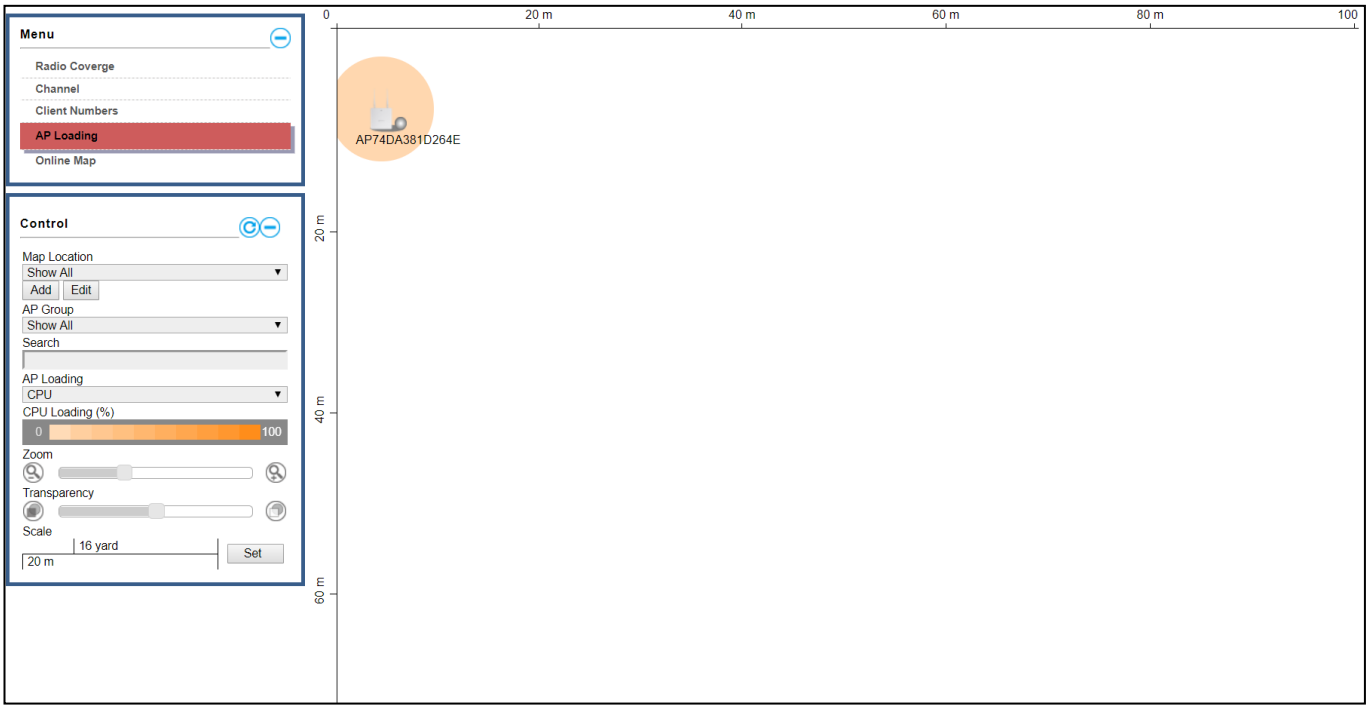
Client Numbers:

Below is displayed as Client Numbers is selected:



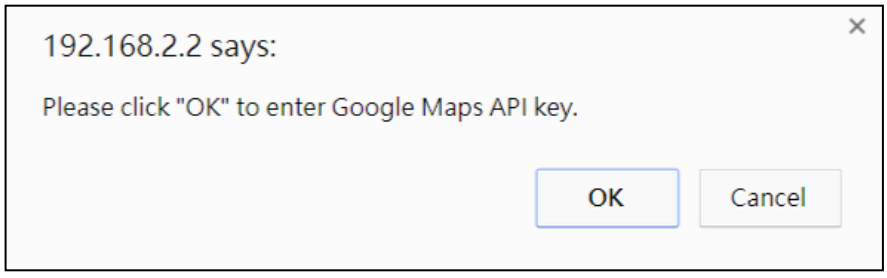
AP Loading:

Below is displayed as AP Loading is selected:

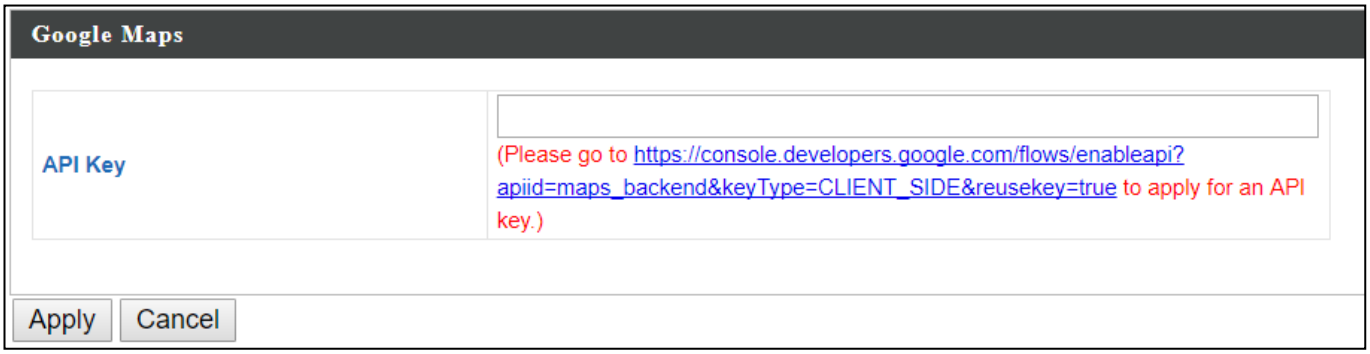


Online Map:

When Online Map is selected, the message below is displayed:



Click “OK” and the interface will bring you to the page shown below to allow API key entry:

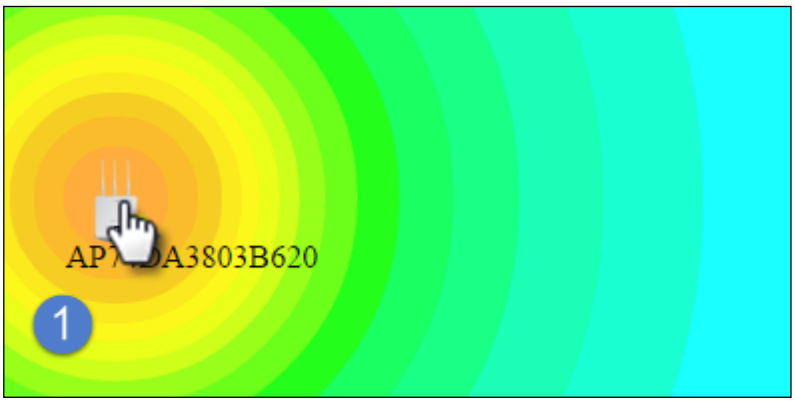


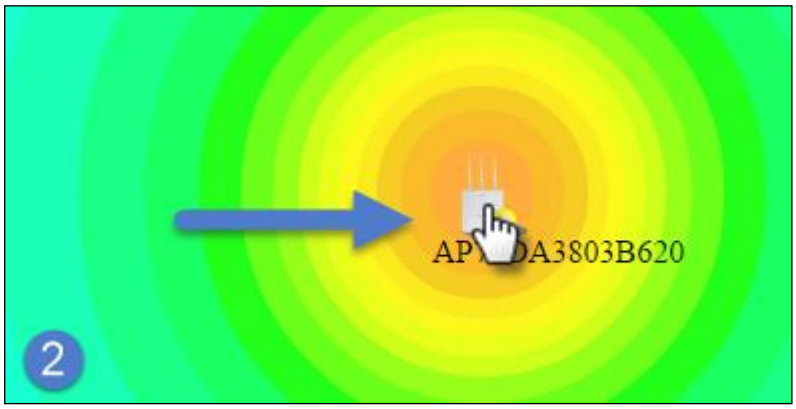
ii. Control

The Control section will change according to the selection in the Menu section.

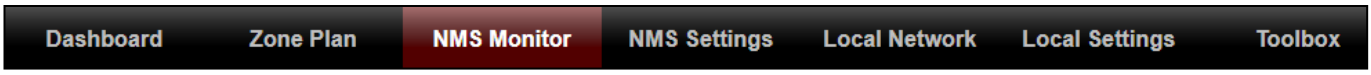
Map Location	Select a pre-defined location from the drop down menu. When you upload a location image in NMS Settings → Zone Edit, it will be available for selection here.
AP Group	You can select an AP Group to display in the zone map. Edit AP Groups in NMS Settings → AP.
Search	Use the search box to quickly locate an AP.
Radio	Use the checkboxes to display APs according to 2.4GHz or 5GHz wireless radio frequency.
Signal	When Radio Coverage is selected in Menu, signal strength is shown in the Control section below the “Radio” option. Signal strength chart displays the signal strength in dBm, and is also shown around each AP in the zone map.
Channel	When Channel is selected in Menu, channel is shown in the Control section below the “Radio” option.
Client Numbers	When Client Numbers is selected in Menu, client numbers is shown in the Control section below the “Radio” option.
AP Loading	When AP Loading is selected in Menu, AP loading is shown in the Control section below the “Search” option. Two options are available: “CPU” or “Traffic (Tx + Rx)”.
CPU Loading	This shows the CPU loading of the AP.
Traffic (Tx + Rx)	This shows the Traffic (Tx+Rx) loading.
Zoom	Use the slider to adjust the zoom level of the map.
Transparency	Use the slider to adjust the transparency of location images.
Scale	Zone map scale.
Device/Number	Displays number and type of devices in the zone map.

Click and drag an AP icon to move the icon around the zone map. The signal strength for each AP is displayed according to the “Signal” key in the menu on the right side:





VI-6. NMS Monitor

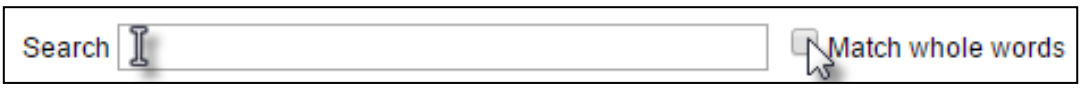


i. AP

Managed AP:

Displays information about each Managed AP in the local network: Index (reference number), MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each AP, and Status (connected, connecting or disconnected).

The search function can be used to locate a specific Managed AP. Type in the search box and the list will update:



The Status icon displays the status of each Managed AP.

Status Icons			
Icon	**Color**	**Status**	**Definition**
	Grey	Disconnected	Managed AP is disconnected. Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.
	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all APs in the AP array. Please check security settings. All APs must have the same firmware version. Please use the AP Controller's firmware upgrade function.
	Orange	Configuring or Upgrading	Please wait while the Managed AP makes configurations or while the firmware is upgrading.
	Yellow	Connecting	Please wait while Managed AP is connecting.
	Green	Connected	Managed AP is connected.
	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.

Each Managed AP has "Action" icons with the following functions:

1. **Disallow**
   Remove the Managed AP from the AP array and disable connectivity.

2. **Edit**
   Edit various settings for the Managed AP.

3. **Blink LED**
   The Managed AP's LED will flash temporarily to help identify & locate APs.

4. **Buzzer**
   The Managed AP's buzzer will sound temporarily to help identify & locate APs.

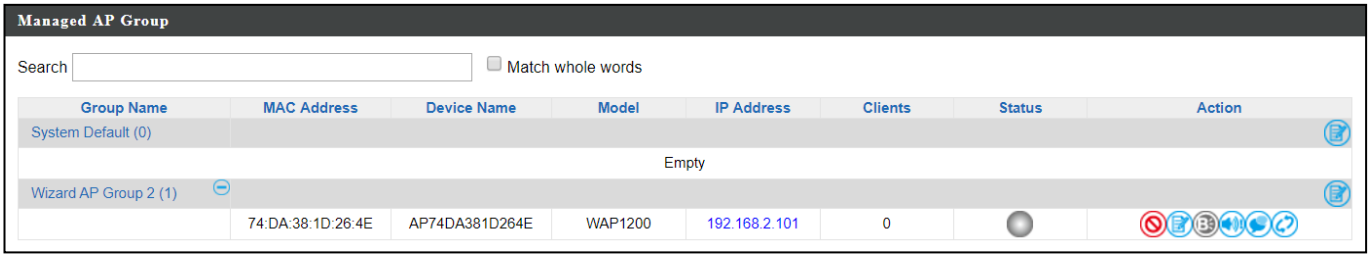
5. **Network Connectivity**
   Go to the "Network Connectivity" panel to perform a ping or traceroute.

6. **Restart**
   Restarts the Managed AP.

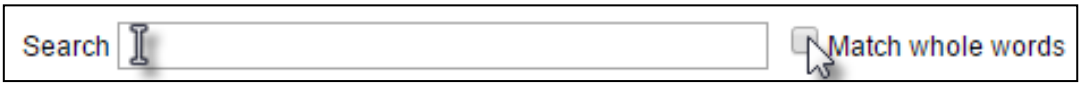
ii. Managed AP Group

Managed APs can be grouped according to your requirements. Managed AP Group displays information about each Managed AP group in the local network: Group Name, MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each AP, and Status (connected or disconnected).

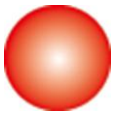
To edit Managed AP Groups go to NMS Settings → AP.



The search function can be used to locate a specific Managed AP Group. Type in the search box and the list will update:



The Status icon displays the status of each Managed AP.

Status Icons			
Icon	**Color**	**Status**	**Definition**
	Grey	Disconnected	Managed AP is disconnected. Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.
	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all APs in the AP array. Please check security settings. All APs must have the same firmware version. Please use the AP Controller's firmware upgrade function.
	Orange	Configuring or Upgrading	Please wait while the Managed AP makes configurations or while the firmware is upgrading.
	Yellow	Connecting	Please wait while Managed AP is connecting.
	Green	Connected	Managed AP is connected.
	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.

Each Managed AP has "Action" icons with the following functions:

1. **Disallow**
   Remove the Managed AP Group from the AP array and disable connectivity.

2. **Edit**
   Edit various settings for the Managed AP Group.

3. **Blink LED**
   The LED of all Managed APs in the group will flash temporarily to help identify & locate the APs.

4. **Buzzer**
   The buzzer of all Managed APs in the group will sound temporarily to help identify & locate the APs.

5. **Network Connectivity**
   Go to the “Network Connectivity” panel to perform a ping or traceroute.

6. **Restart**
   Restarts all Managed APs in the group.

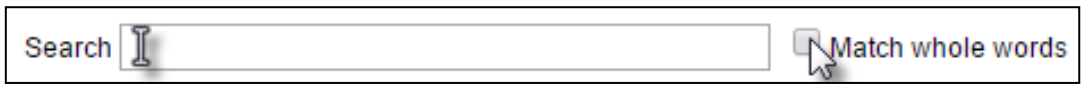
iii. WLAN

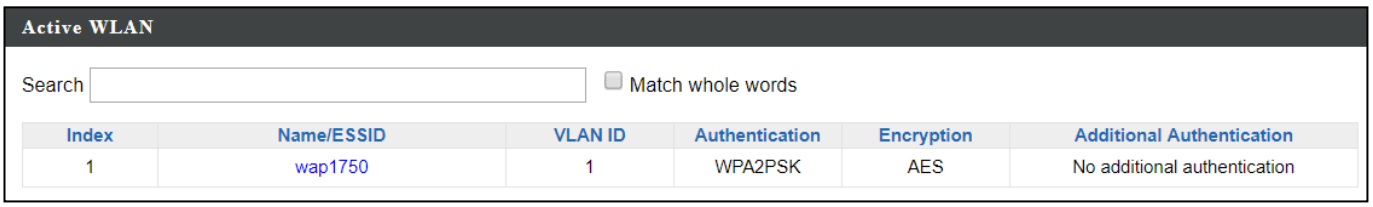
Active WLAN:

Displays information about each SSID in the AP Array: Index (reference number), Name/SSID, VLAN ID, Authentication, Encryption, IP Address and Additional Authentication.

To configure encryption and VLANs for Managed APs go to NMS Settings → WLAN.

The search function can be used to locate a specific SSID. Type in the search box and the list will update:

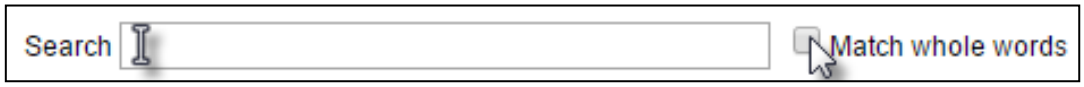




Active WLAN Group:

WLAN groups can be created according to your preference. Active WLAN Group displays information about WLAN group: *Group Name, Name/SSID, VLAN ID, Authentication, Encryption, IP Address and Additional Authentication.*

The search function can be used to locate a specific Active WLAN Group. Type in the search box and the list will update:



Active WLAN Group

Search Match whole words

Group Name	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
Wizard WLAN 2.4G Group 1 (1)					
	wap1750	1	WPA2PSK	AES	No additional authentication
Wizard WLAN 5G Group 2 (1)					
	wap1750	1	WPA2PSK	AES	No additional authentication

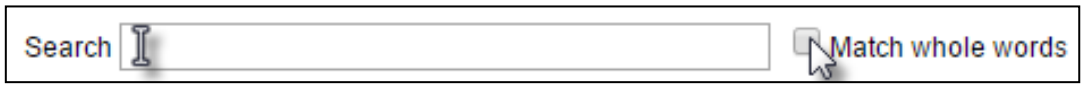
iv. Clients

Active Clients:

Displays information about clients currently connected to the AP Array: Index (reference number), Client MAC Address, AP MAC Address, WLAN (SSID), Radio (2.4GHz or 5GHz), Signal Strength received by Client, Connected Time, Idle Time, Tx & Rx (Data transmitted and received by Client in KB), and the Vendor of the client device.

You can set or disable the auto-refresh time for the client list or click “Refresh” to manually refresh.

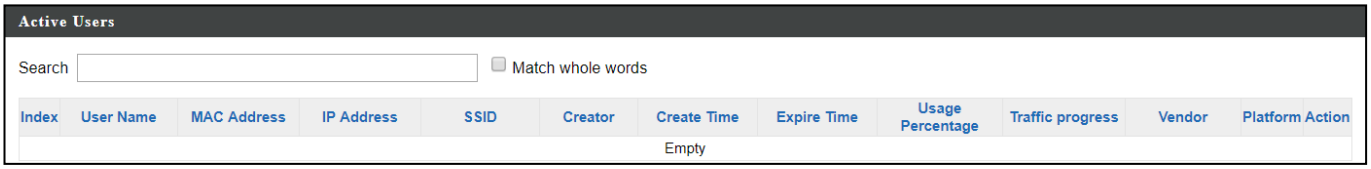
The search function can be used to locate a specific client. Type in the search box and the list will update:



v. Users

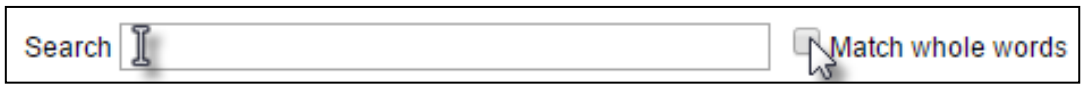
Active Users:

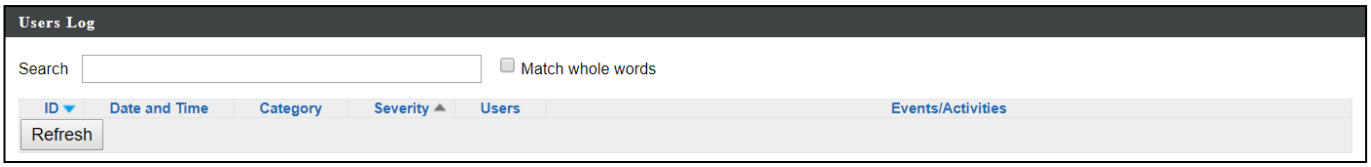
Displays information about users currently connected.



Users Log:

Displays the log information about users currently connected.





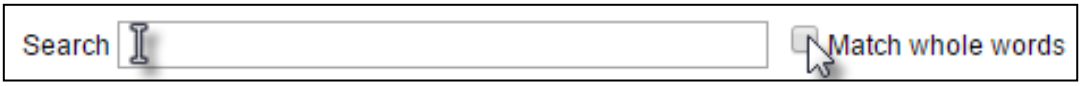
vi. Rogue Devices

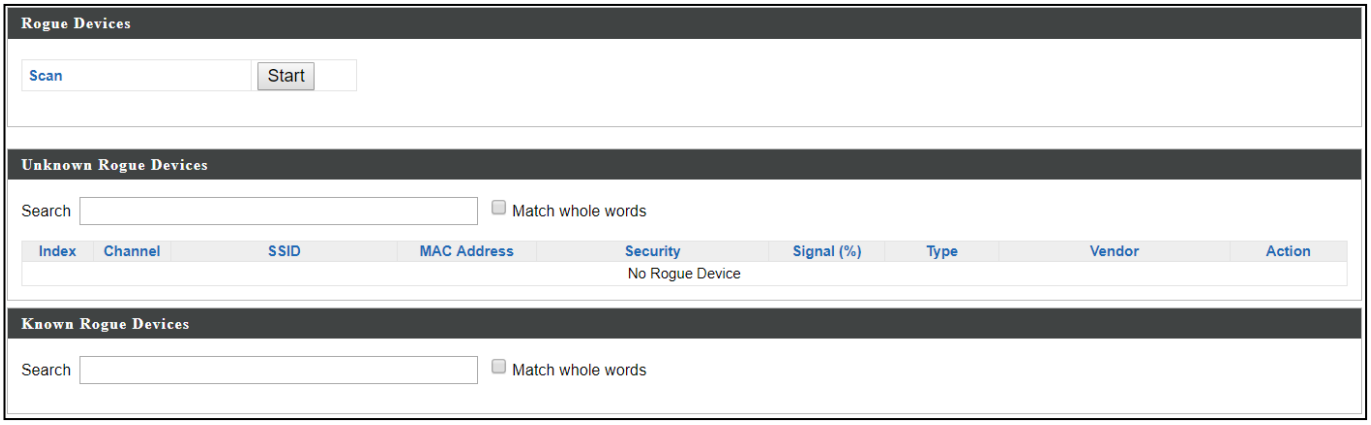
Rogue AP detection can identify any unauthorized APs which may have been installed in the network.

Click “Start” to scan for rogue devices:

Unknown Rogue Devices area displays information about rogue devices discovered during the scan: Index (reference number), Channel, SSID, MAC Address, Security, Signal Strength, Type, Vendor and Action.

The search function can be used to locate a known rogue device. Type in the search box and the list will update:

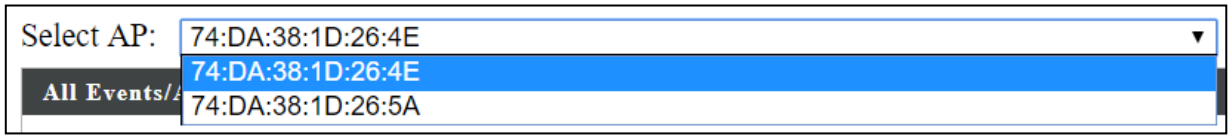




vii. Information

All Events/Activities:

Displays a log of time-stamped events for each AP in the Array – use the drop down menu to select an AP and view the log.



Select AP: 74:DA:38:1D:26:4E

All Events/Activities

Search Match whole words

ID	Date and Time	Severity	Users	Events/Activities
15	2012/01/01 00:01:10	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
14	2012/01/01 00:07:01	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
13	2012/01/01 00:00:21	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
12	2012/01/01 00:00:55	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
11	2012/01/01 00:01:05	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
10	2012/01/01 00:07:40	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
9	2012/01/01 00:09:57	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
8	2012/01/01 00:00:24	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
7	2012/01/01 00:10:31	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
6	2012/01/01 00:12:15	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
5	2012/01/01 00:13:58	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
4	2012/01/01 00:14:31	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
3	2012/01/01 00:00:22	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
2	2012/01/01 00:00:55	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully
1	2012/01/01 00:00:23	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service successfully

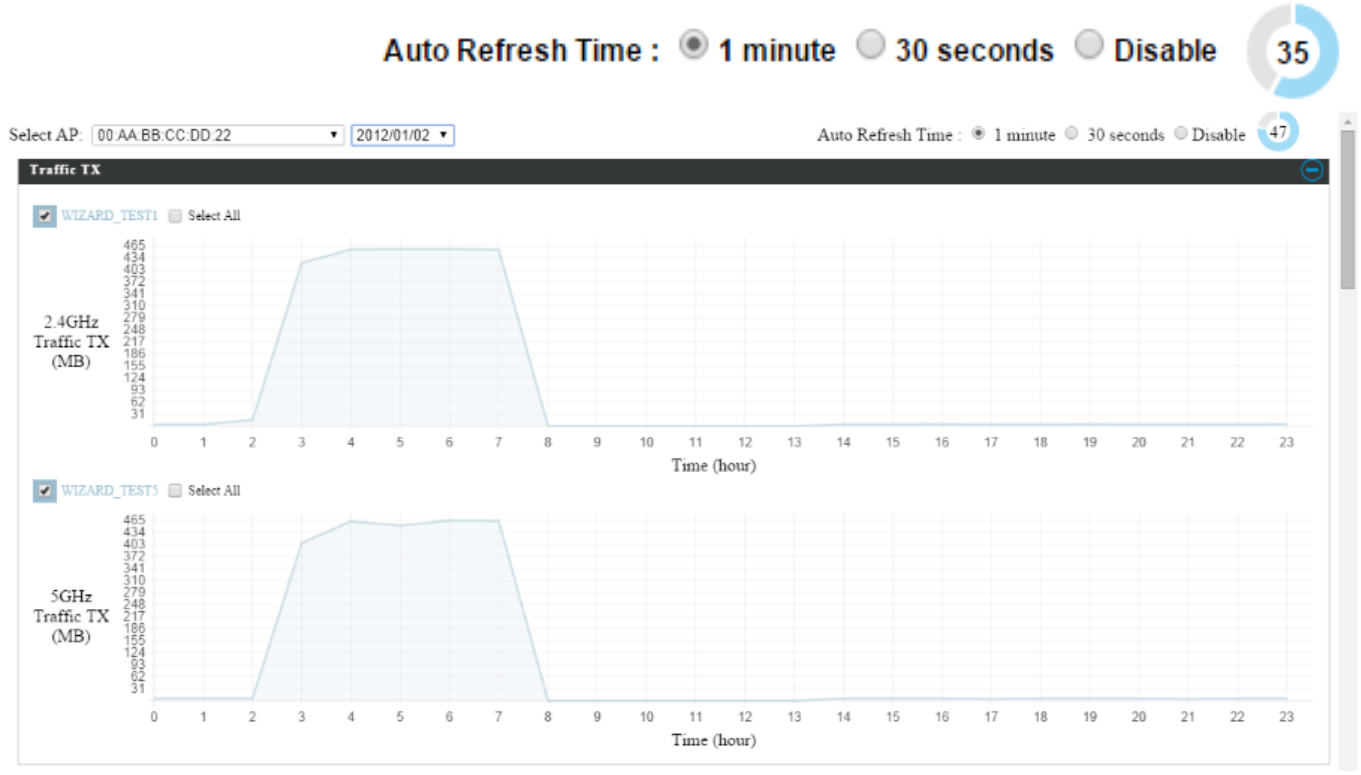
Save Refresh

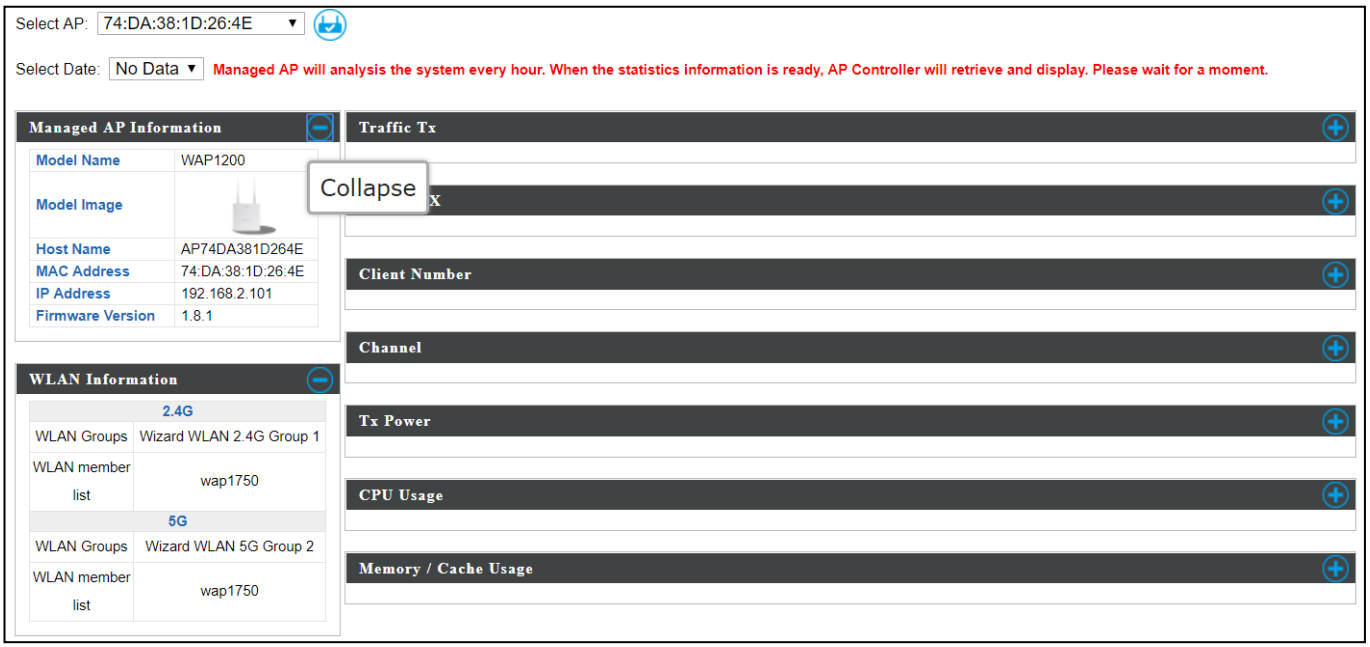
AP Monitoring:

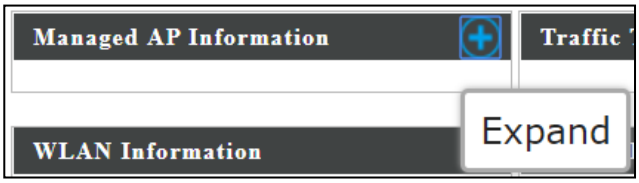
Displays graphical monitoring information about APs in the Array for 2.4GHz & 5GHz: *Traffic Tx (data transmitted in MB), Traffic Rx (data received in MB), No. of Clients, Wireless Channel, Tx Power (wireless radio power), CPU Usage and Memory Usage.*

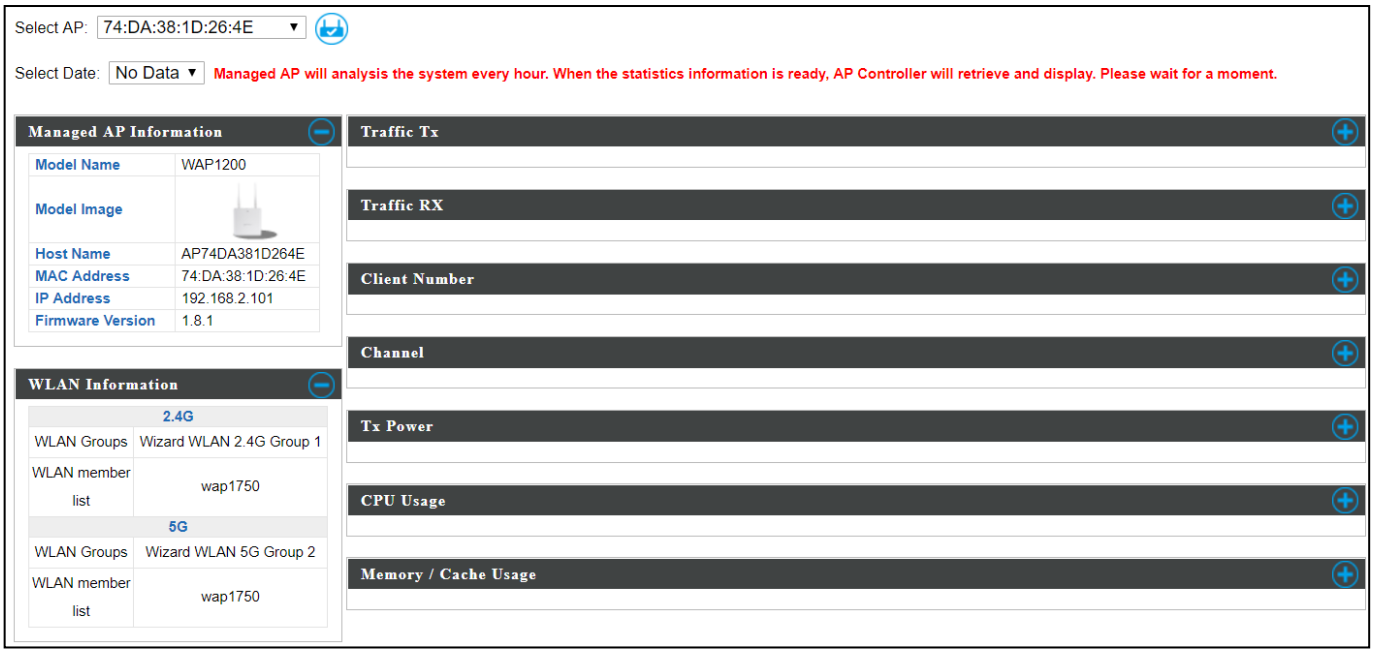
Use the drop down menus to select an AP and date.

You can set or disable the auto-refresh time for the data:



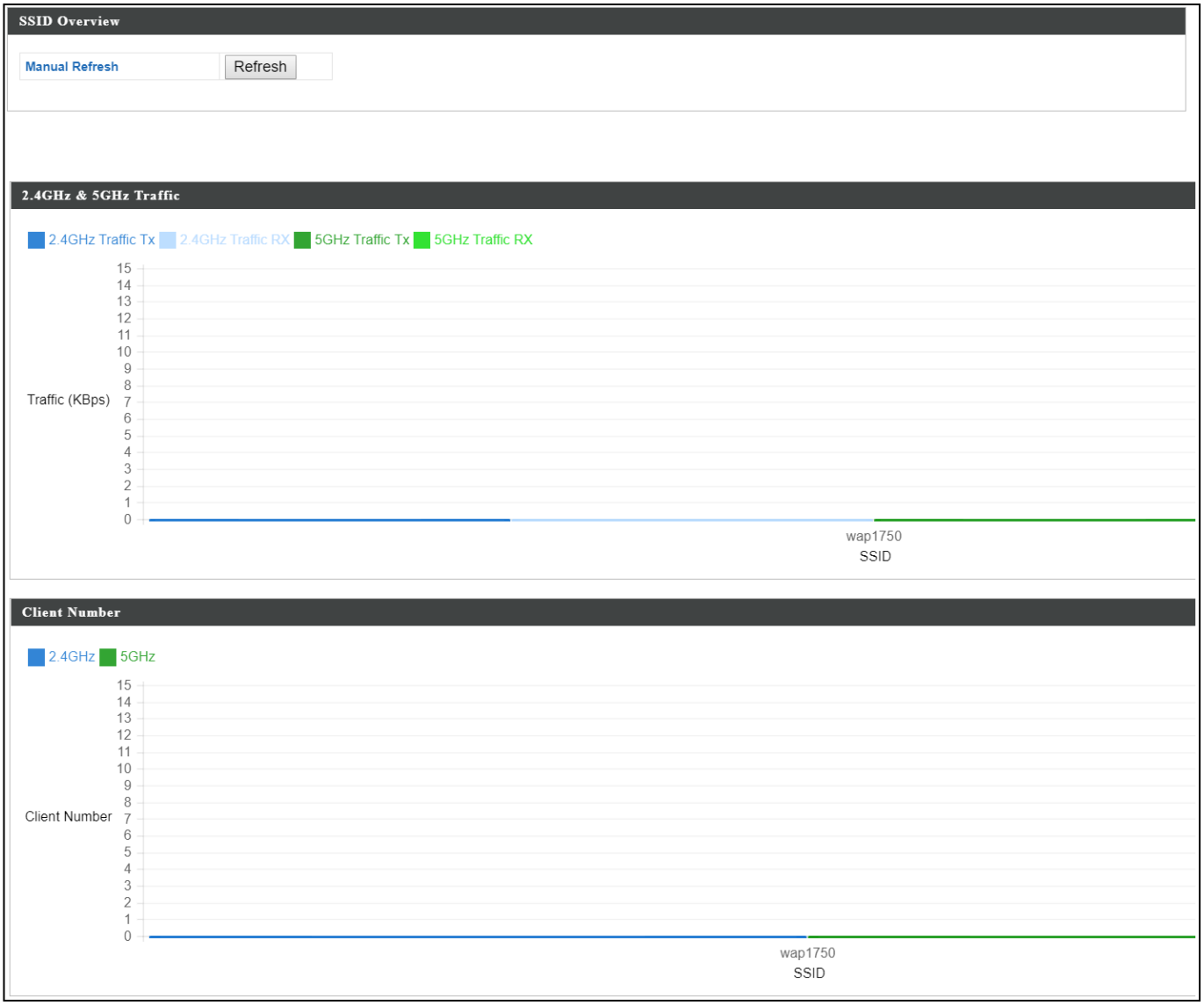



Managed AP Information
Traffic
WLAN Information
Expand


Select AP: 74:DA:38:1D:26:4E
Select Date: No Data
Managed AP will analysis the system every hour. When the statistics information is ready, AP Controller will retrieve and display. Please wait for a moment.
Managed AP Information
Model Name WAP1200
Model Image
Host Name AP74DA381D264E
MAC Address 74:DA:38:1D:26:4E
IP Address 192.168.2.101
Firmware Version 1.8.1
WLAN Information
2.4G
WLAN Groups Wizard WLAN 2.4G Group 1
WLAN member list wap1750
5G
WLAN Groups Wizard WLAN 5G Group 2
WLAN member list wap1750
Traffic Tx
Traffic RX
Client Number
Channel
Tx Power
CPU Usage
Memory / Cache Usage

SSID Overview:

Displays graphical monitoring information about APs in the Array for 2.4GHz & 5GHz.

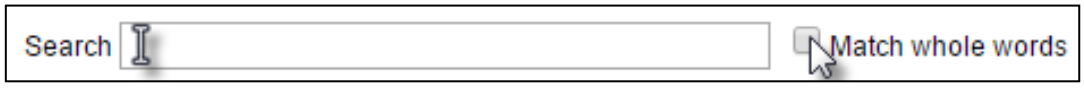


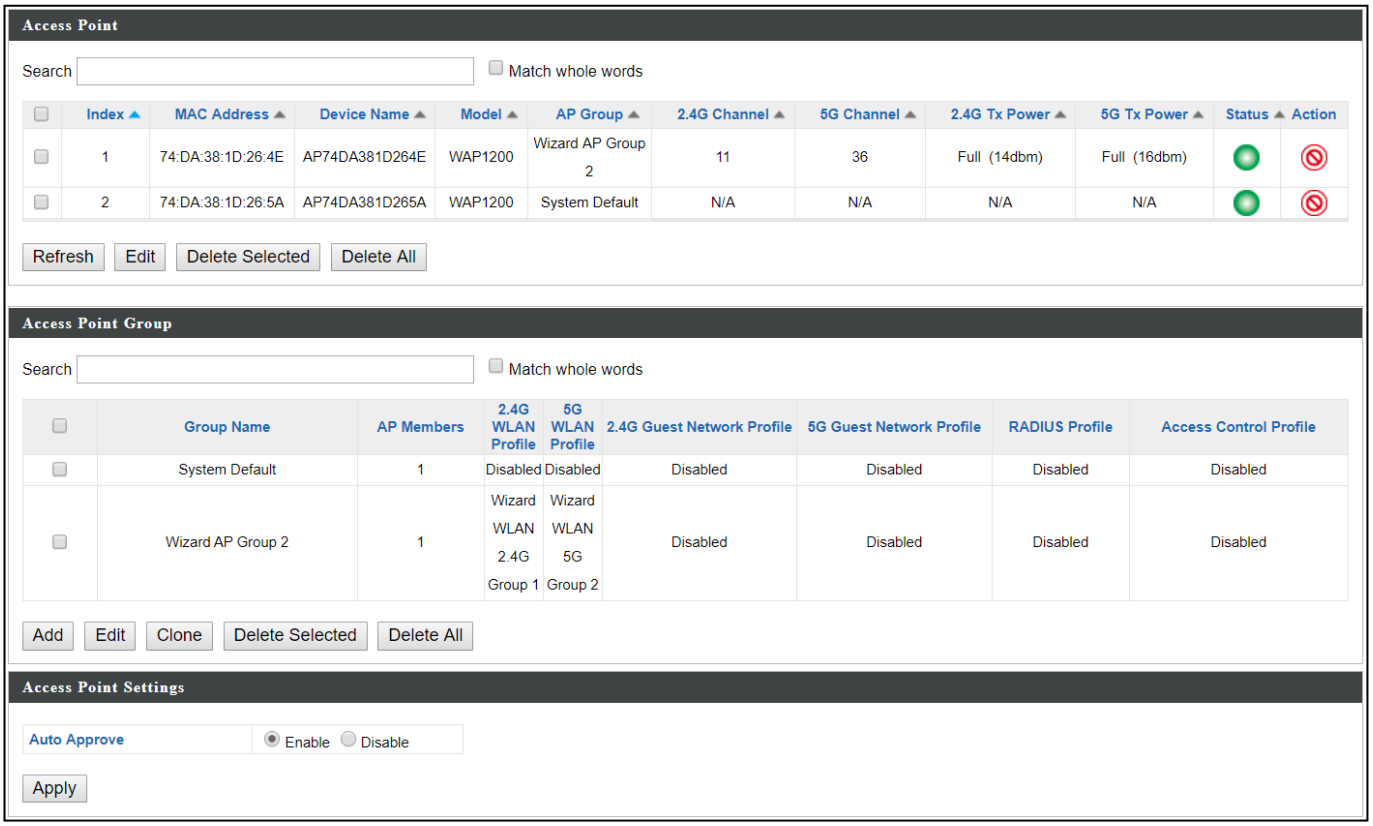
VI-7. NMS Settings

i. Access Point

Displays information about each AP and AP group in the local network and allows you to edit APs and edit or add AP groups.

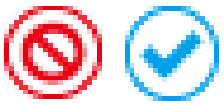
The search function can be used to locate an AP or AP group. Type in the search box and the list will update:





The Status icon displays *grey* (disconnected), *red* (authentication failed/incompatible NMS version), *orange* (upgrading firmware), *yellow* (connecting), *green* (connected) or *blue* (waiting for approval) for each individual Managed AP.

The "Action" icons enable you to allow or disallow an AP:



Select an AP or AP group using the check-boxes and click "Edit" to make configurations, or click "Add" to add a new AP group:

The AP Settings panel can enable or disable Auto Approve for all Managed APs. When enabled, Managed APs will automatically join the AP Array with the Controller AP. When disabled, Managed APs must be manually approved to join the AP Array with the Controller AP.

AP Settings	
Auto Approve	Enable or disable Auto Approve for all Managed APs.

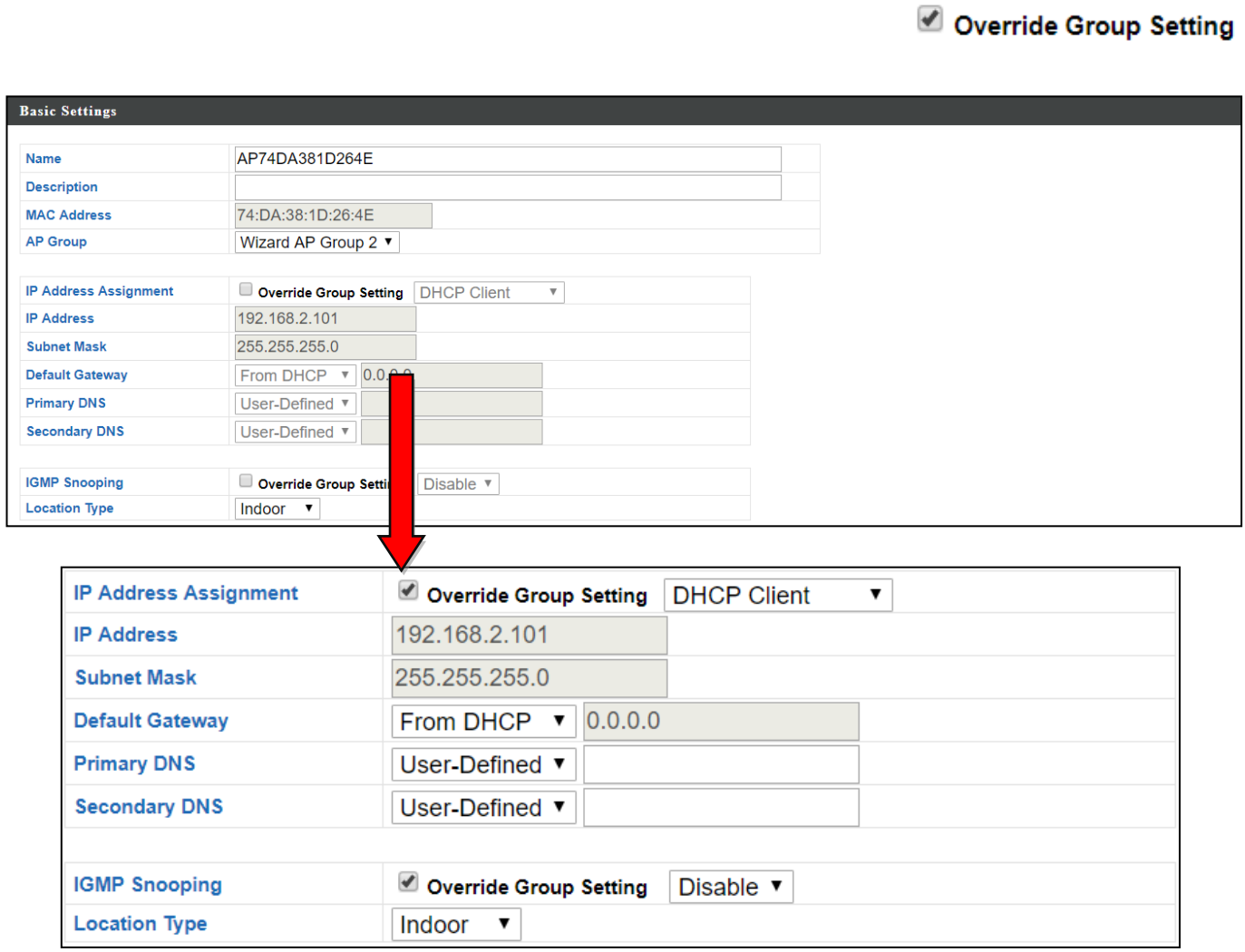
To manually approve a Managed AP, use the *allow* "Action" icon for the specified AP:

Edit AP:
Configure your selected AP on your LAN. You can set the AP as a DHCP client or specify a static IP address for your AP, and assign the AP to an AP group, as well as edit 2.4GHz & 5GHz wireless radio settings. Event log is displayed at the bottom of the page.

You can also use Profile Settings to assign the AP to WLAN, Guest Network, RADIUS and Access Control groups independently from AP Group settings. Click "Save" to save the settings. Click "Cancel" to forfeit the changes. Click "Save and Apply" to save and apply the settings.

Edit Basic Settings:

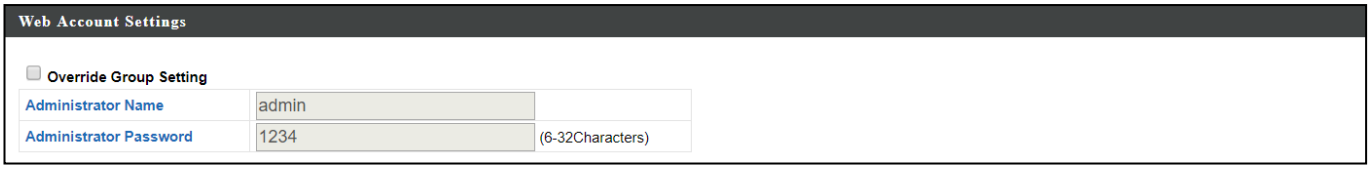
When “Override Group Setting” is checked, options/fields will turn white to allow adjustments.



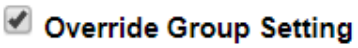
Basic Settings	
Name	Edit the AP name. The default name is AP + MAC address.
Description	Enter a description of the AP for reference e.g. 2nd Floor Office.
MAC Address	Displays MAC address.
AP Group	Use the drop down menu to assign the AP to an AP Group.
IP Address Assignment	Select “DHCP Client” for your AP to be assigned a dynamic IP address from your router’s DHCP server, or select “Static IP” to manually specify a static/fixed IP address for your AP (below). Check the box “Override Group Setting” if the AP is a member of an AP Group and you wish to use a different setting than the AP Group setting.
IP Address	Specify the IP address here. This IP address will be assigned to

	your AP and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank.
Primary DNS	DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.
Secondary DNS	DHCP users can select “From DHCP” to get secondary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.
IGMP Snooping	Enable / Disable the IGMP Snooping function. IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic.
Location Type	Select the location of the AP (indoor or outdoor).

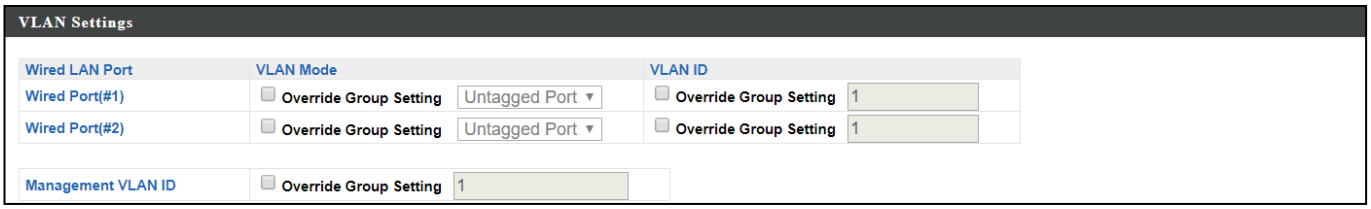
Edit Web Account Settings:



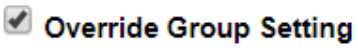
When “Override Group Setting” is checked, options/fields will turn white to allow adjustments.



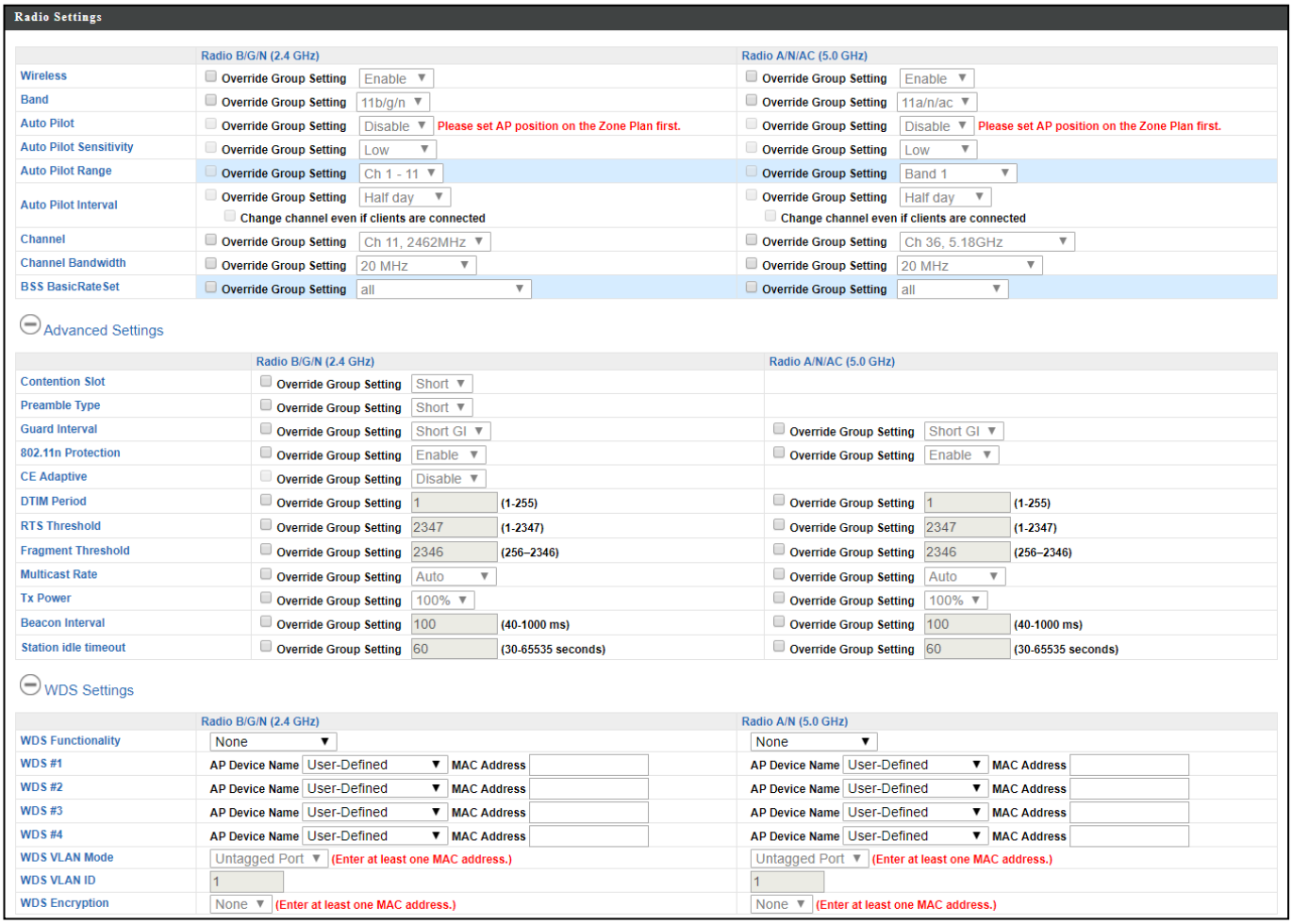
Edit VLAN Settings:



When “Override Group Setting” is checked, options/fields will turn white to allow adjustments.



Edit Radio Settings:



Radio Settings	
Wireless	Enable or disable the AP's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the AP. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the AP's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot Sensitivity	Select sensitivity of Auto Pilot.
Auto Pilot Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Pilot Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according

	to your preference.
Channel	When Auto Pilot is disabled, select a channel (1-11) manually.
Channel Bandwidth	Set the channel bandwidth or use Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

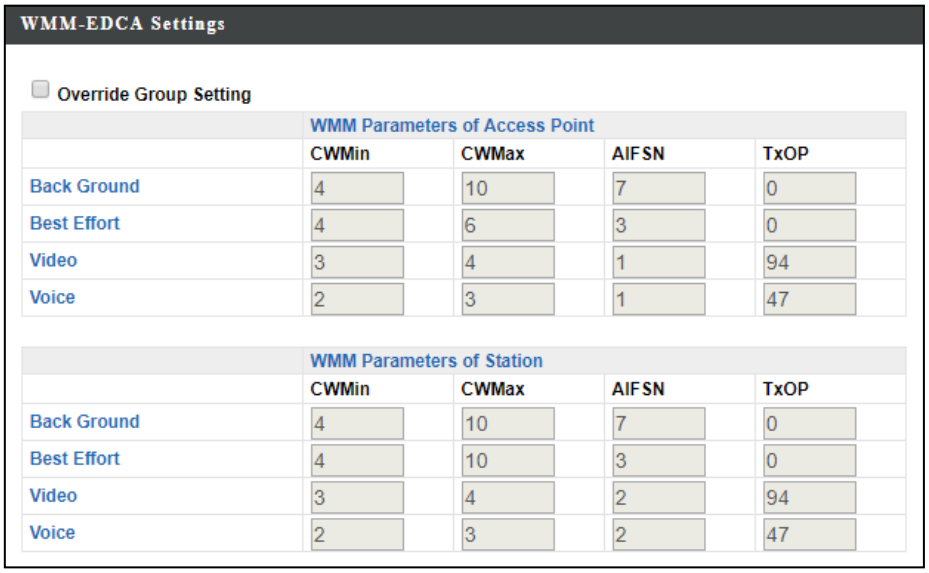
Changing these settings can adversely affect the performance of your AP.

Advanced Settings	
Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM.
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the AP and roaming wireless adapters. The default value is “Short Preamble”.
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to AP, and AP will broadcast Clear to Send (CTS), before a packet is sent from client.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. (The default value is 1)
RTS Threshold	Set the RTS threshold of the wireless radio. (The default value is 2347)
Fragment Threshold	Set the fragment threshold of the wireless radio. (The default value is 2346)

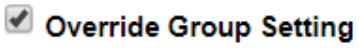
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the AP to a wireless client to verify if the station is still alive / active.

WDS Settings	
WDS Functionality	A wireless distribution system (WDS) is a system enabling the wireless interconnection of APs in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple APs without the traditional requirement for a wired backbone to link them.
AP Device Name	Set AP Device Name.
MAC Address	Set MAC Address of AP.
WDS VLAN Mode	Enable / Disable VLAN function.
WDS VLAN ID	Set VLAN ID of WDS.
WDS Encryption	Set WDS Encryption.

Edit WMM-EDCA Settings:

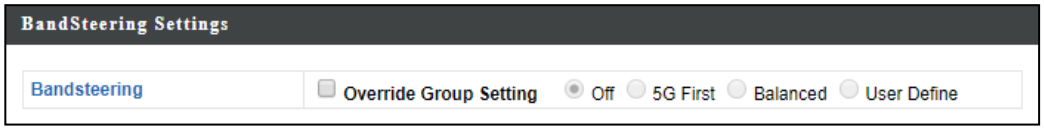


When “Override Group Setting” is checked, options/fields will turn white to allow adjustments.



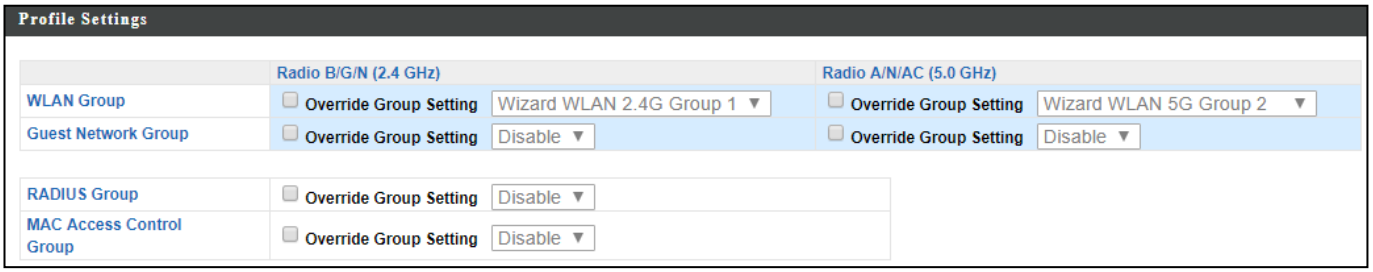
WMM-EDCA Settings:	
Back Ground	Access Category (AC) is Back Ground
Best Effort	Access Category (AC) is Best Effort
Video	Access Category (AC) is video
Voice	Access Category (AC) is voice

Edit BandSteering Settings:

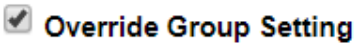


When “Override Group Setting” is checked, options/fields will turn white to allow adjustments.

Edit Profile Settings:



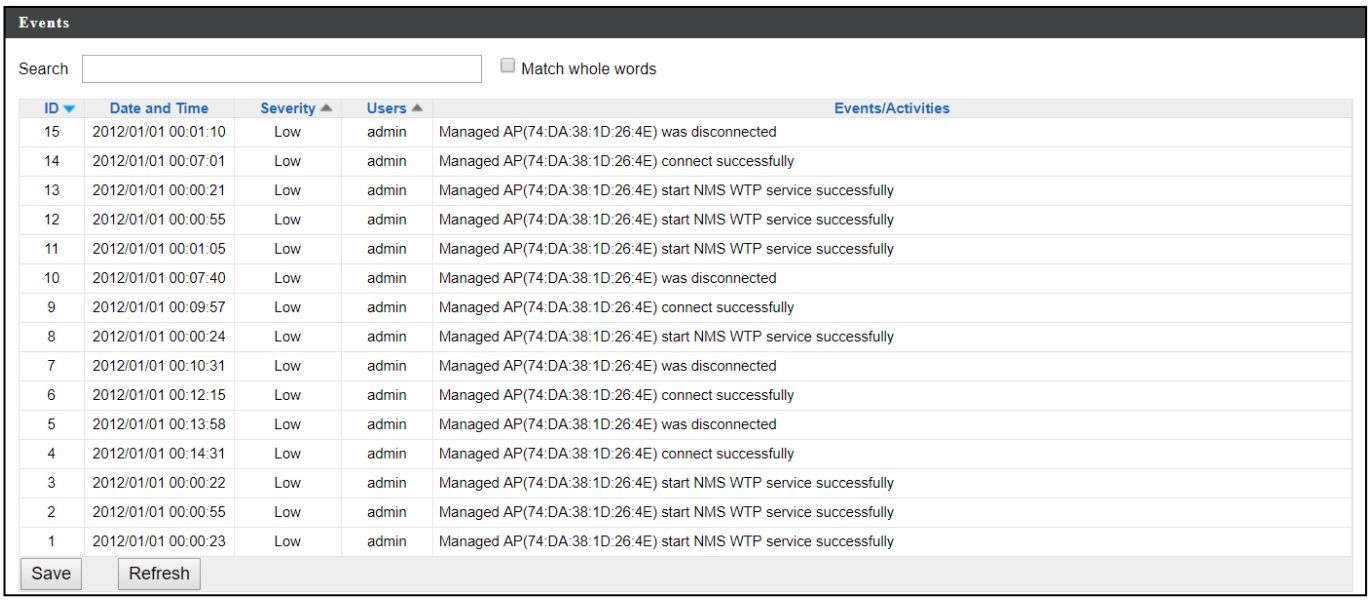
When “Override Group Setting” is checked, options/fields will turn white to allow adjustments.



Profile Settings	
WLAN Group	Assign the AP’s 2.4GHz or 5GHz SSID(s) to a WLAN Group.
Guest Network Group	Assign the AP’s 2.4GHz or 5GHz SSID(s) to a Guest Network Group.
RADIUS Group	Assign the AP’s 2.4GHz SSID(s) to a RADIUS group. Y
MAC Access Control Group	Assign the AP’s 2.4GHz SSID(s) to a RADIUS group.

Events:

Press “Refresh” to refresh the event log
Press “Save” to save the event log as .log file.



Add/Edit AP Group:

Configure your selected AP group. AP group settings apply to all APs in the group, unless individually set to override group settings.

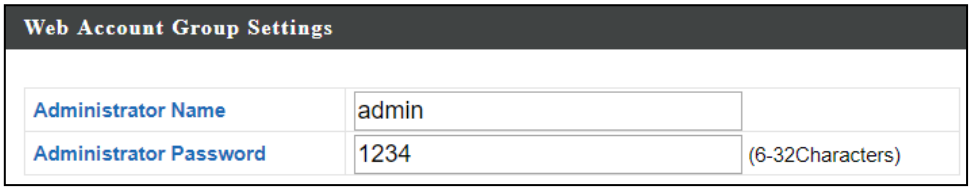
You can use Profile Group Setting**s** to assign the AP group to WLAN, Guest Network, RADIUS and Access Control groups.

Edit Basic Group Settings:

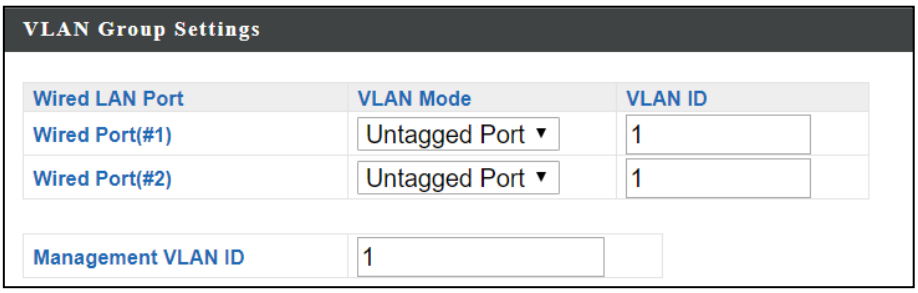
The Group Settings panel can be used to quickly move APs between existing groups: select an AP and use the drop down menu or search to select AP groups and use << and >> arrows to move APs between groups.

Basic Group Settings	
Name	Edit the AP group name.
Description	Enter a description of the AP group for reference e.g. 2nd Floor Office Group.
IGMP Snooping	Enable / Disable the IGMP Snooping function. IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic.

Edit Web Account Group Settings:



Edit VLAN Group Settings:



Edit Radio Group Settings:

Radio Group Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Wireless	Enable	Enable
Band	11b/g/n	11a/n/ac
Auto Pilot	Disable	Disable
Auto Pilot Sensitivity	Low	Low
Auto Pilot Range	Ch 1 - 11	Band 1
Auto Pilot Interval	Half day Change channel even if clients are connected	Half day Change channel even if clients are connected
Channel	Ch 11, 2462MHz	Ch 36, 5.18GHz
Channel Bandwidth	20 MHz	20 MHz
BSS BasicRateSet	all	all

Advanced Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Contention Slot	Short	
Preamble Type	Short	
Guard Interval	Short GI	Short GI
802.11n Protection	Enable	Enable
CE Adaptive	Disable	
DTIM Period	1 (1-255)	1 (1-255)
RTS Threshold	2347 (1-2347)	2347 (1-2347)
Fragment Threshold	2346 (256–2346)	2346 (256–2346)
Multicast Rate	Auto	Auto
Tx Power	100%	100%
Beacon Interval	100 (40-1000 ms)	100 (40-1000 ms)
Station idle timeout	60 (30-65535 seconds)	60 (30-65535 seconds)

Radio Group Settings	
Wireless	Enable or disable the AP group's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the AP group. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the AP group's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot Sensitivity	Select sensitivity of Auto Pilot.
Auto Pilot Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Pilot Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel	When Auto Pilot is disabled, select a channel (1-11) manually.
Channel Bandwidth	Set the channel bandwidth or use Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

Changing these settings can adversely affect the performance of your APs.

Advanced Settings	
Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM.
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the AP and roaming wireless adapters. The default value is “Short Preamble”.
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to AP, and AP will broadcast Clear to Send (CTS), before a packet is sent from client.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the AP to a wireless client to verify if the station is still alive/active.

Edit WMM-EDCA Settings:

WMM-EDCA Settings

	WMM Parameters of Access Point			
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	6	3	0
Video	3	4	1	94
Voice	2	3	1	47

	WMM Parameters of Station			
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	10	3	0
Video	3	4	2	94
Voice	2	3	2	47

Edit BandSteering Settings:

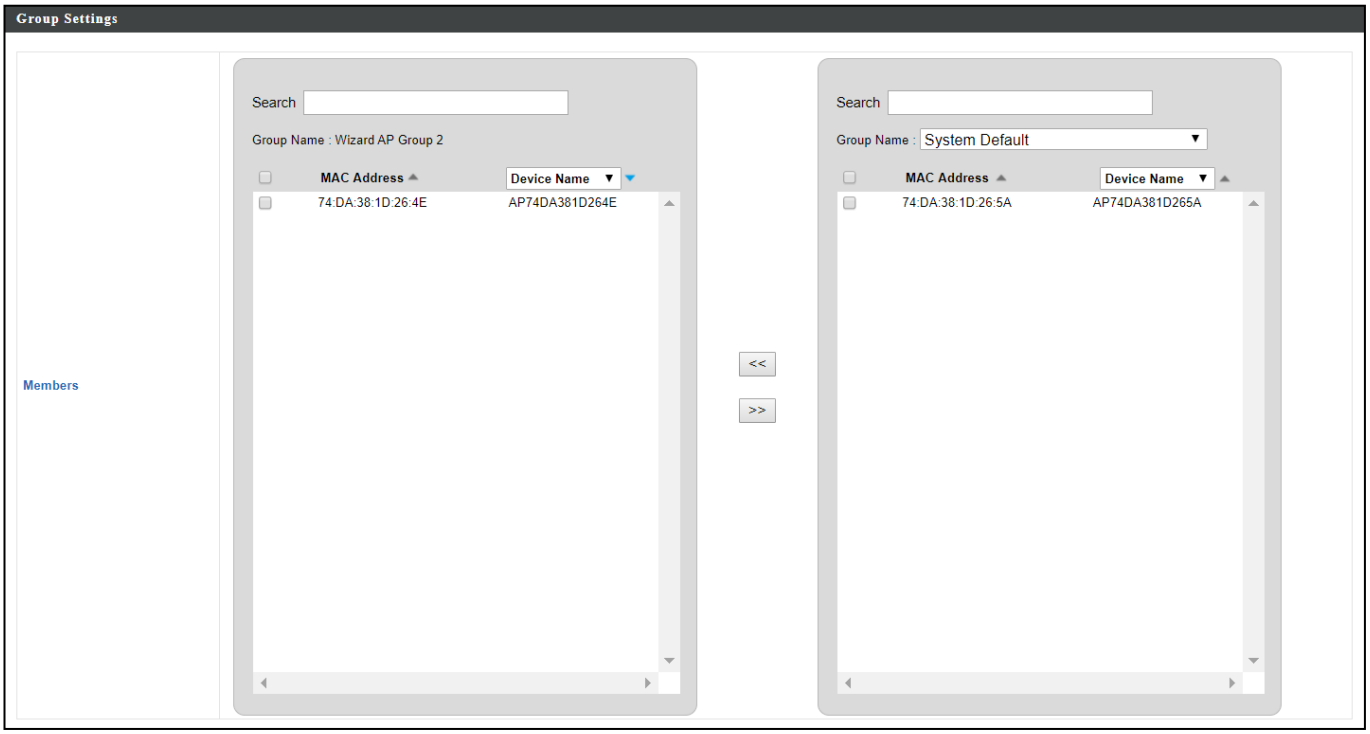
BandSteering Group Settings

Bandsteering	(•) Off ( ) 5G First ( ) Balanced ( ) User Define

Edit Profile Settings:

Profile Group Settings	
WLAN Group	Assign the AP group's 2.4GHz or 5GHz SSIDs to a WLAN Group.
Guest Network Group	Assign the AP group's 2.4GHz or 5GHz SSIDs to a Guest Network Group.
RADIUS Group	Assign the AP group's 2.4GHz SSIDs to a RADIUS group. You can edit RADIUS groups in NMS Settings → RADIUS.
MAC Access Control Group	Assign the AP's 2.4GHz SSIDs to a RADIUS group. You can edit RADIUS groups in NMS Settings → Access Control**.**

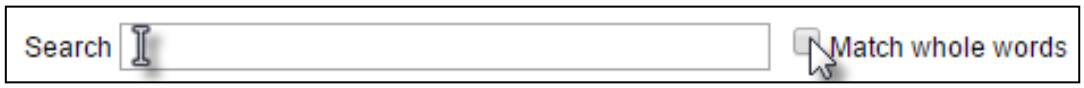
Edit Group Settings:

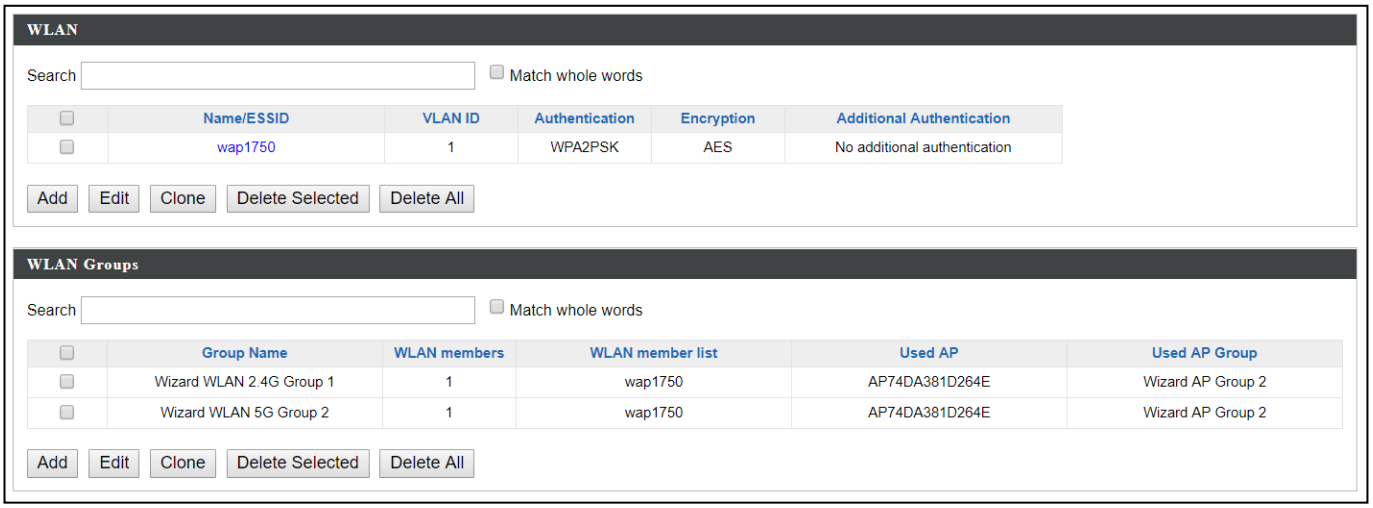


ii. WLAN

Displays information about each WLAN and WLAN group in the local network and allows you to add or edit WLANs & WLAN Groups.

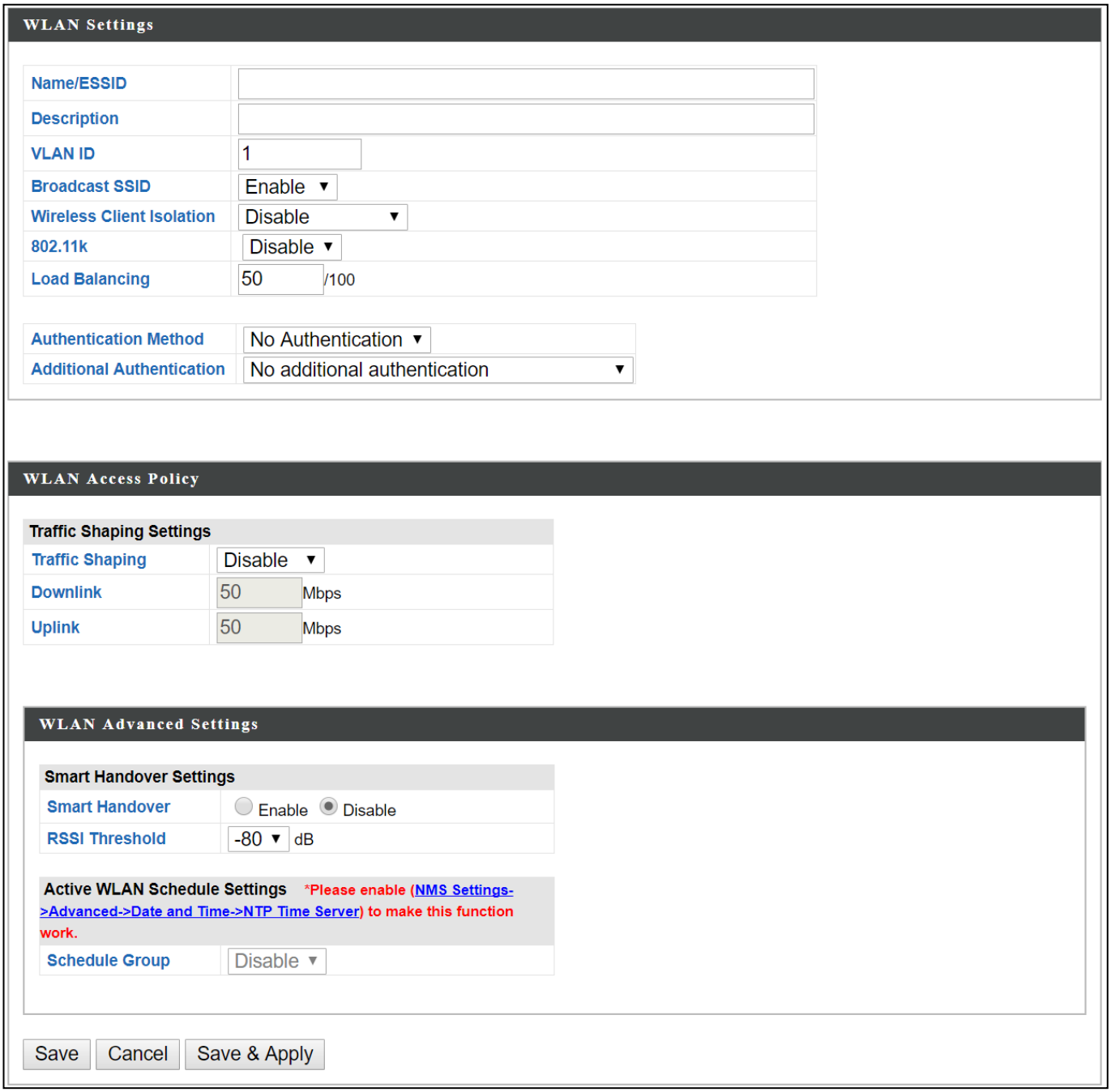
The search function can be used to locate a WLAN or WLAN Group. Type in the search box and the list will update:





Select a WLAN or WLAN Group using the check-boxes and click “Edit” or click “Add” to add a new WLAN or WLAN Group:

Add/Edit WLAN:



WLAN Settings	
Name/ESSID	Edit the WLAN name (SSID).
Description	Enter a description of the SSID for reference e.g. 2nd Floor Office HR.
VLAN ID	Specify the VLAN ID.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the AP from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
802.11k	Enable / Disable to define and expose radio and network information (helps facilitate the management and maintenance of a mobile wireless LAN).
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu.
WPA Type	It can select WPA only or WPA2 only or WPA/WPA2 Mixed Mode-PSK
Encryption Type	It can select TKIP/AES Mixed Mode or AES
Key Renewal Interval	It can set renewal internal time
Pre-Shared Key Type	It can set Passphrase or Hex (64 characters)
Pre-Shared Key	It can set 8-64 characters
Additional Authentication	Select an additional authentication method from the drop down menu.

Various security options (wireless data encryption) are available. When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

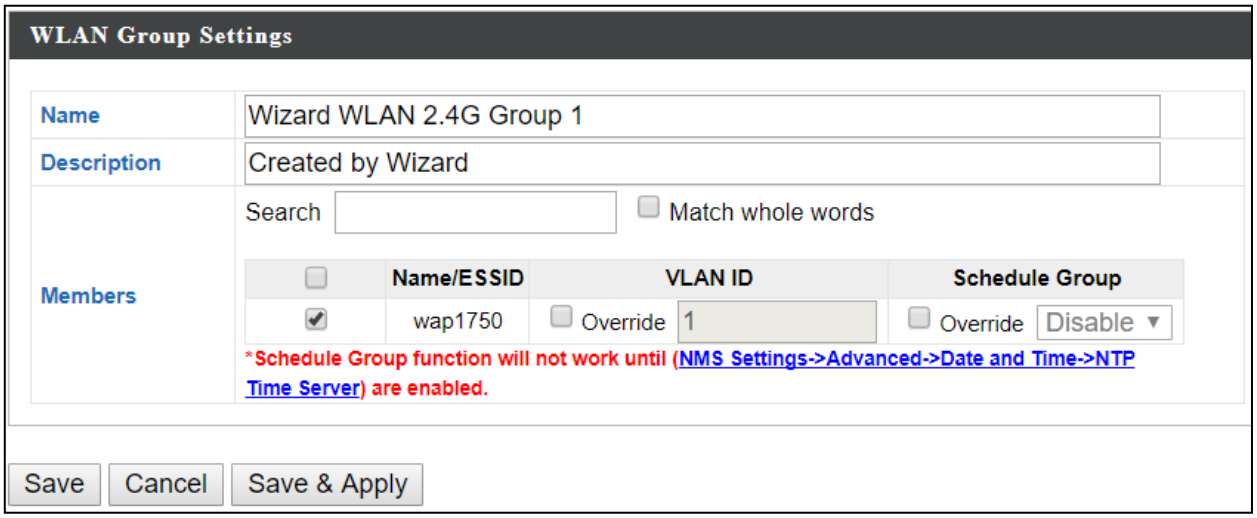
It is essential to configure wireless security in order to prevent unauthorised access to your network.

Select hard-to-guess passwords which include combinations of numbers, letters and symbols, and change your password regularly.

WLAN Access Policy	
Traffic Shaping	Enable / Disable traffic shaping.
Downlink	Set downlink between 1-200Mbps
Uplink	Set uplink between 1-200Mbps

WLAN Advanced Settings	
Smart Handover	Enable or disable Smart Handover.
RSSI Threshold	Set a RSSI Threshold level.

Add/Edit WLAN Group:

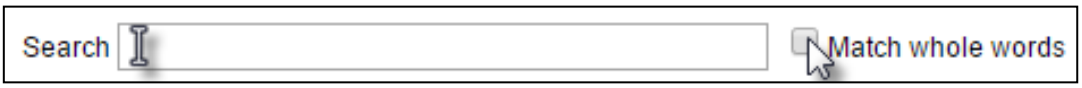


WLAN Group Settings	
Name	Edit the WLAN Group name.
Description	Enter a description of the WLAN Group for reference e.g. 2nd Floor Office HR Group.
Members	Select SSIDs to include in the group using the checkboxes and assign VLAN IDs.

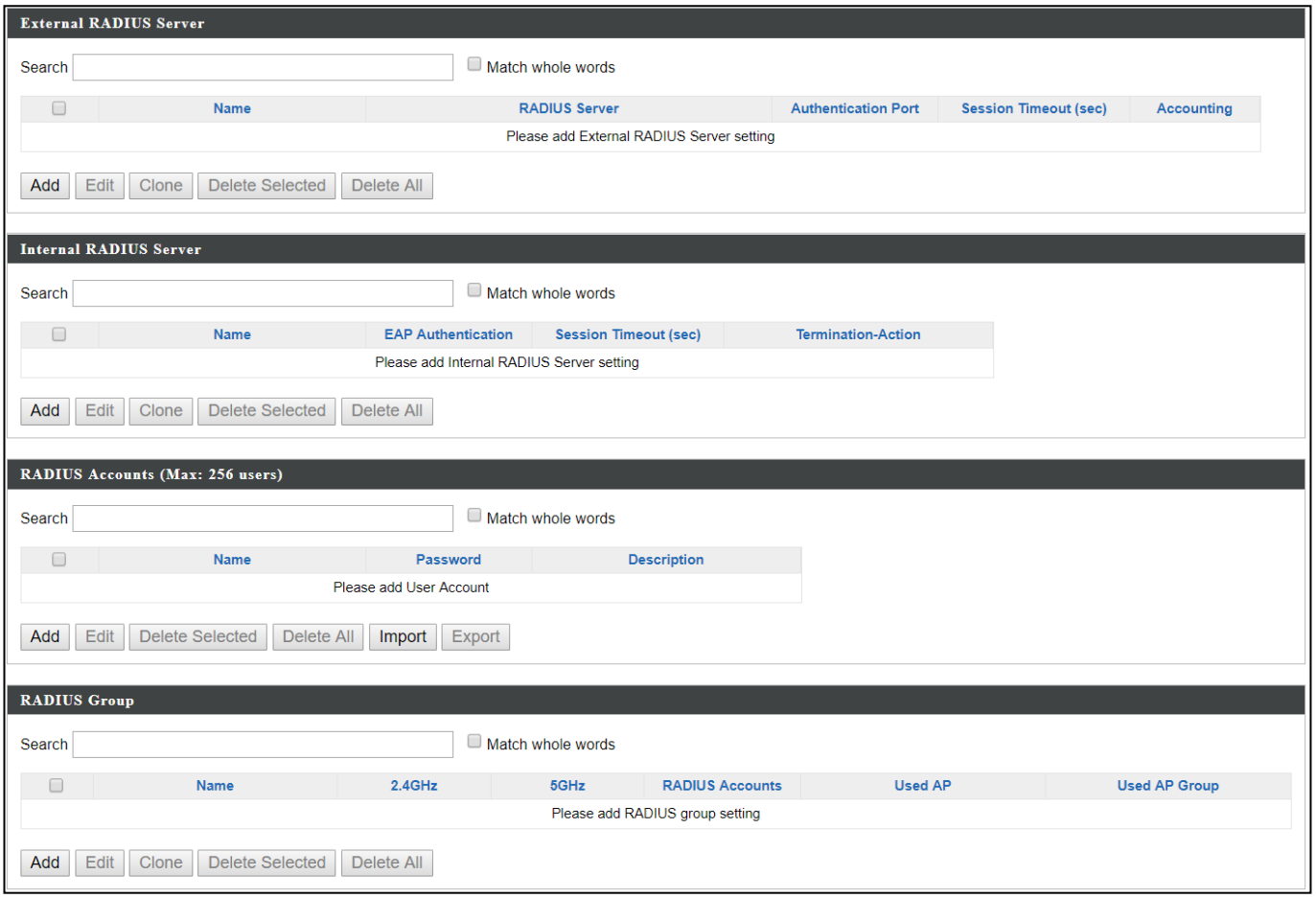
iii. RADIUS

Displays information about External & Internal RADIUS Servers, Accounts and Groups and allows you to add or edit RADIUS Servers, Accounts & Groups.

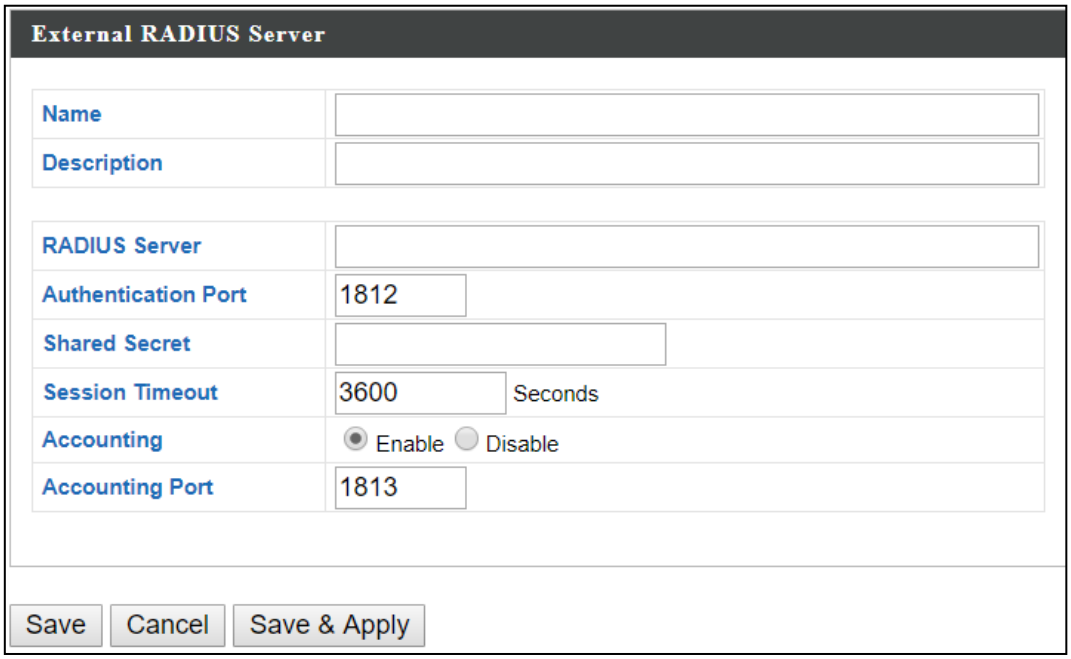
The search function can be used to locate a RADIUS Server, Account or Group. Type in the search box and the list will update:



Make a selection using the check-boxes and click “Edit” or click “Add” to add a new WLAN or WLAN Group:

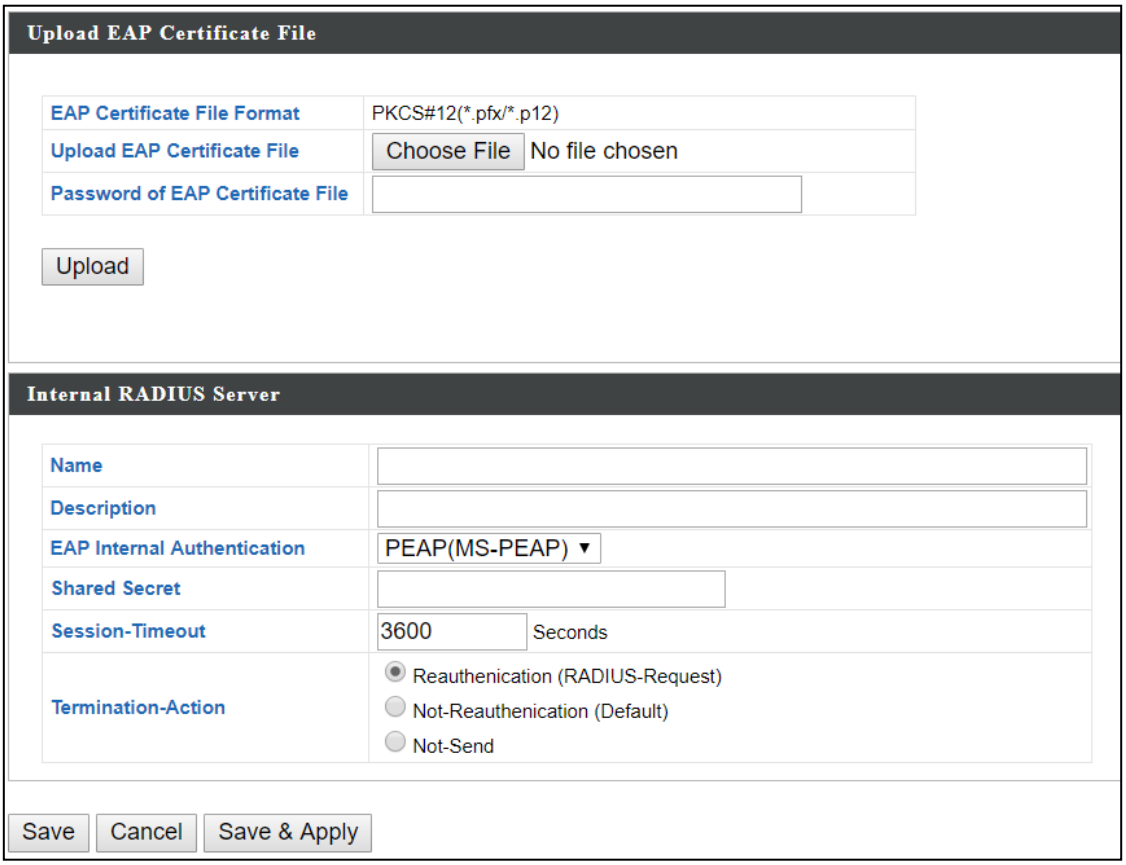


Add/Edit External RADIUS Server:



Name	Enter a name for the RADIUS Server.
Description	Enter a description of the RADIUS Server for reference.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. (Value must be between 1 – 65535)
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Accounting	Enable or disable RADIUS accounting.
Accounting Port	When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. (Value must be between 1 – 65535)

Add/Edit Internal RADIUS Server:

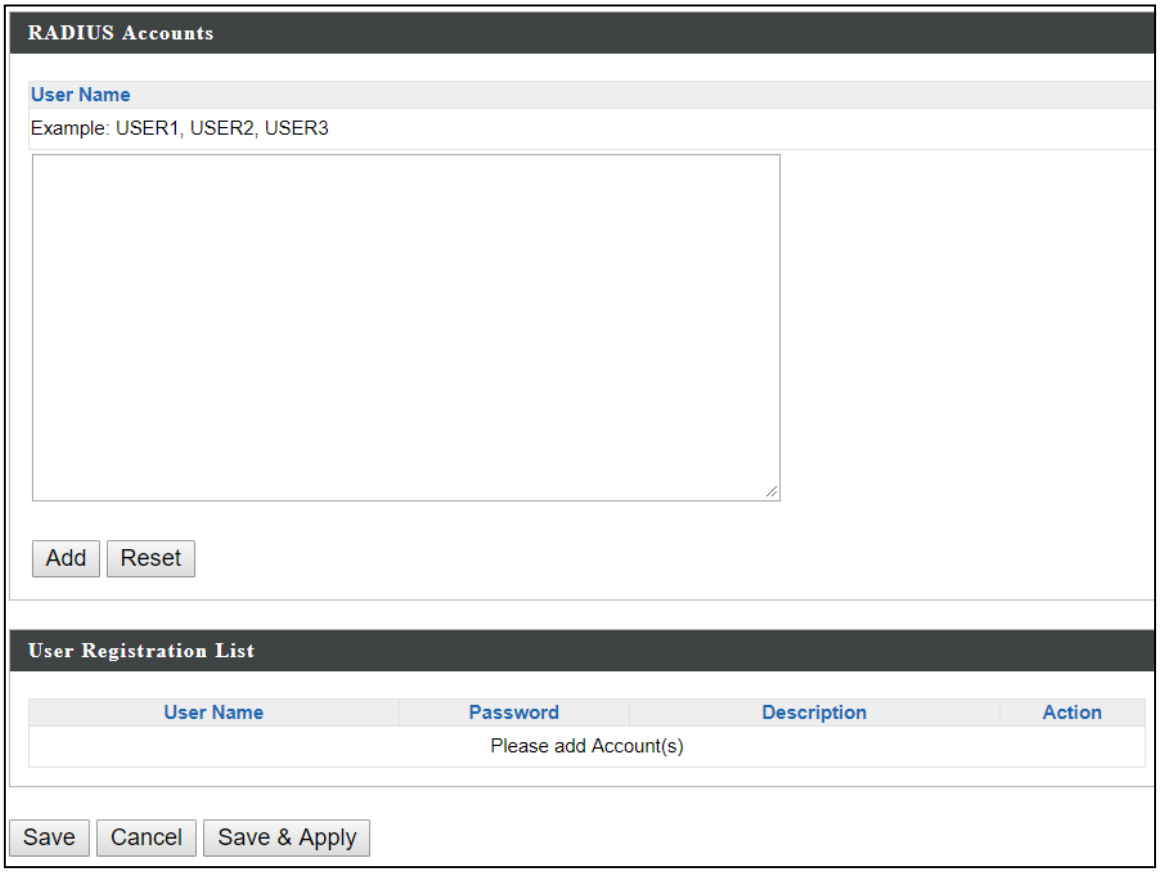


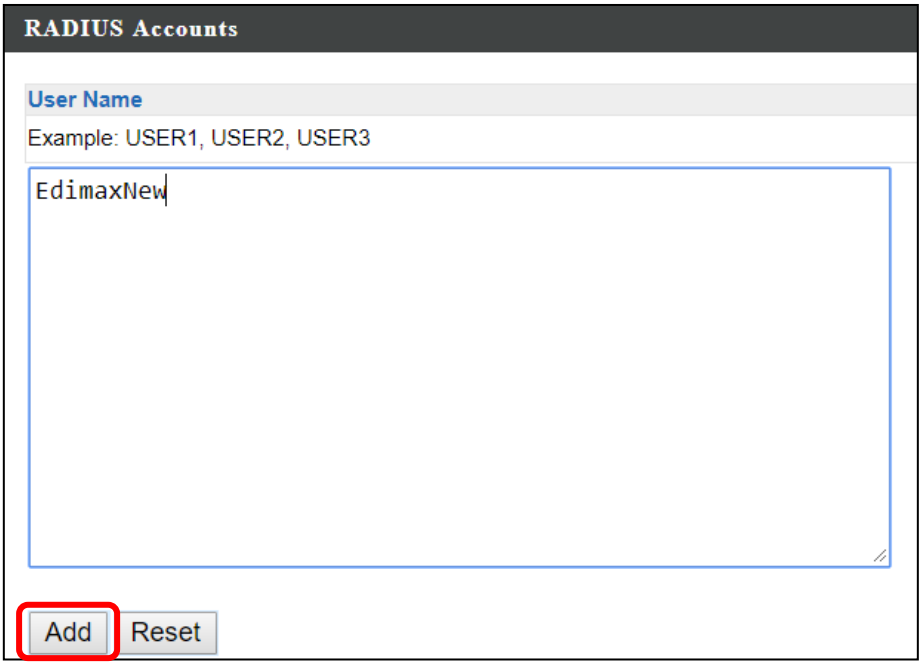
Upload EAP Certificate File	
EAP Certificate File Format	Displays the EAP certificate file format: PKCS#12(*.pfx/*.p12)
EAP Certificate File	Click “Upload” to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.

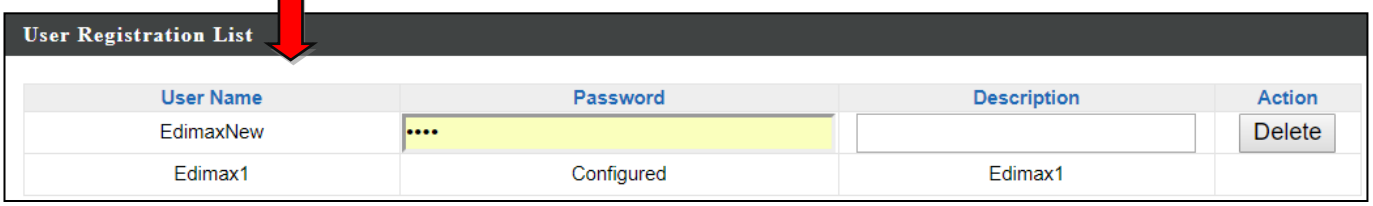
Internal RADIUS Server	
Name	Enter a name for the Internal RADIUS Server.
Description	Enter a description of the Internal RADIUS Server for reference.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click “Upload” to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
Shared Secret	Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Termination Action	Select a termination-action attribute: “Reauthentication” sends a RADIUS request to the AP, “Not-Reauthentication” sends a default termination-action attribute to the AP, “Not-Send” no termination-action attribute is sent to the AP.

Add/Edit/Import/Export RADIUS Accounts:

The internal RADIUS server can authenticate up to 256 user accounts. The “RADIUS Accounts” page allows you to configure and manage users.

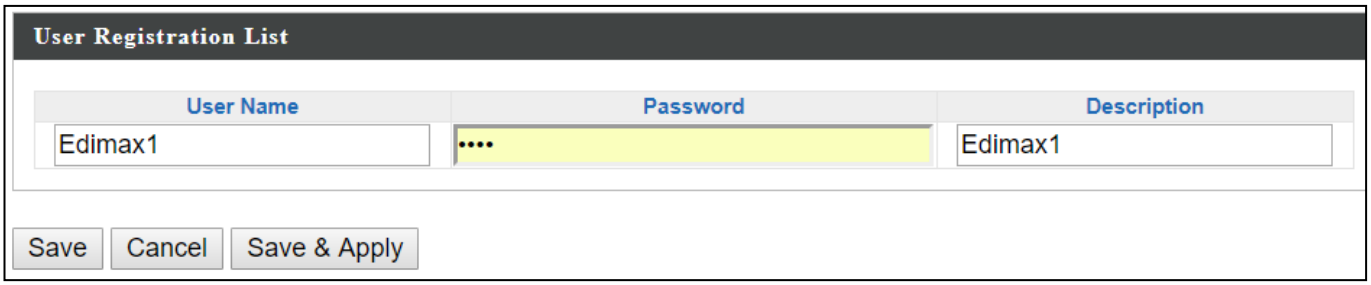

RADIUS Accounts
User Name
Example: USER1, USER2, USER3
Add
Reset
User Registration List
User Name
Password
Description
Action
Please add Account(s)
Save
Cancel
Save & Apply


RADIUS Accounts
User Name
Example: USER1, USER2, USER3
EdimaxNew
Add
Reset


User Registration List
User Name
Password
Description
Action
EdimaxNew
Delete
Edimax1
Configured
Edimax1

RADIUS Accounts	
User Name	Enter the user names here, separated by commas.
Add	Click “Add” to add the user to the user registration list.
Reset	Clear text from the user name box.

User Registration List	
User Name	Displays the user name.
Password	Enter a password.
Description	Enter a description of the user.
Delete	Delete the user.

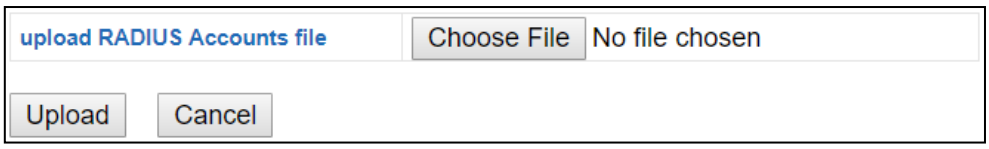


Edit User Registration List	
User Name	Existing user name is displayed here and can be edited according to your preference.
Password	Enter or edit a password for the specified user.
Description	Displays current description of the user and can be edited.

Delete Selected	Delete selected user from the user registration list.
Delete All	Delete all users from the user registration list.

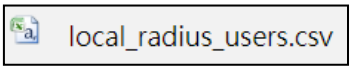
Import:

If you wish to import RADIUS accounts, press “Import”. The following page is displayed below. Choose a file from a file and press “Upload” to import RADIUS accounts.

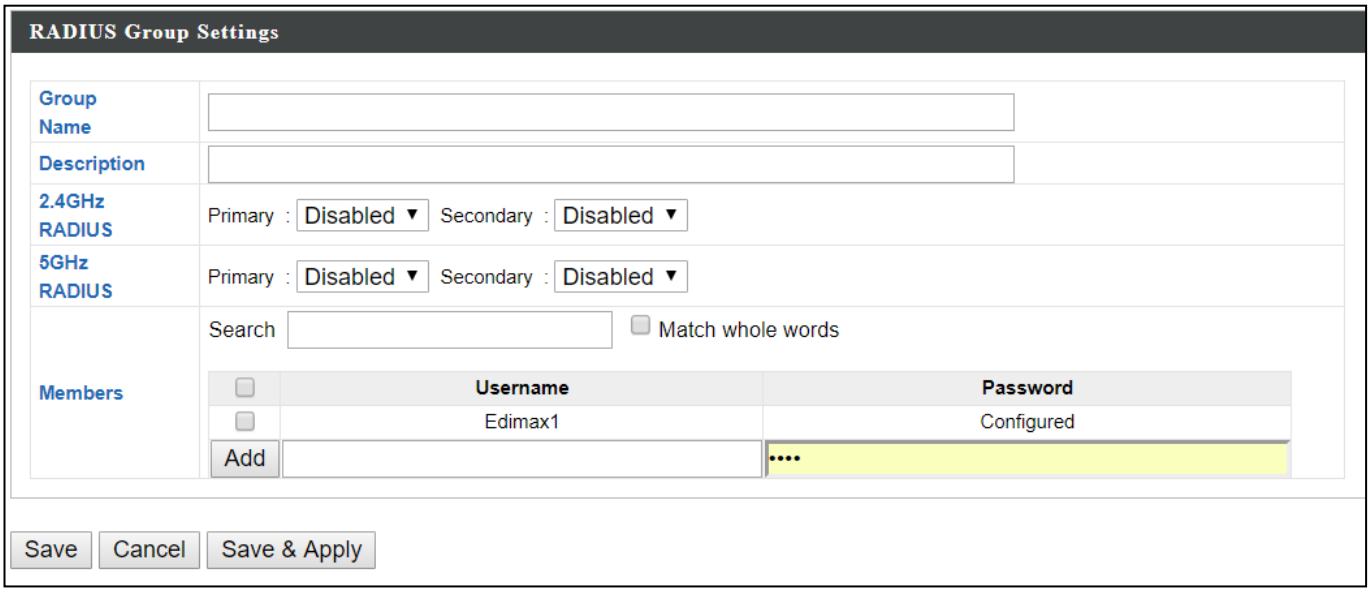


Export:

If you wish to export your current list of RADIUS accounts, press “Export”. Your list will be saved in a format similar to the one below:



Add/Edit RADIUS Group:



RADIUS Group Settings	
Group Name	Edit the RADIUS Group name.
Description	Enter a description of the RADIUS Group for reference.
2.4GHz RADIUS	Enable/Disable primary & secondary RADIUS servers for 2.4GHz.
5GHz RADIUS	Enable/Disable primary & secondary RADIUS servers for 5GHz.
Members	Add RADIUS user accounts to the RADIUS group.

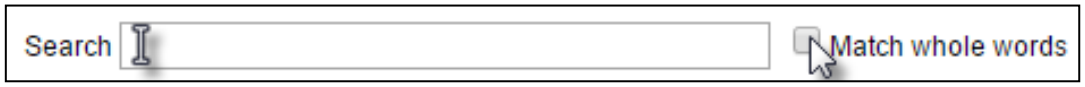
iv. Access Control

MAC Access Control is a security feature that can help to prevent unauthorized users from connecting to your AP.

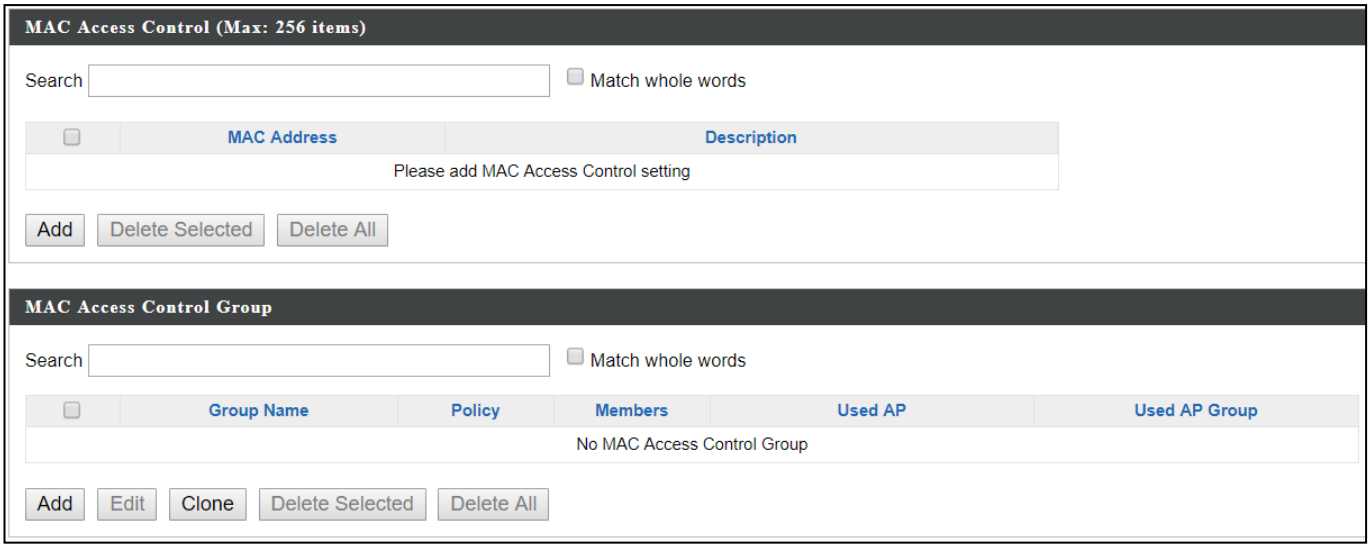
This function allows you to define a list of network devices permitted to connect to the AP. Devices are each identified by their unique MAC address. If a device not on the list of permitted MAC addresses attempts to connect to the AP, it will be denied.

The Access Control panel displays information about MAC Access Control & MAC Access Control Groups and Groups and allows you to add or edit MAC Access Control & MAC Access Control Group settings.

The search function can be used to locate a MAC address or MAC Access Control Group. Type in the search box and the list will update:



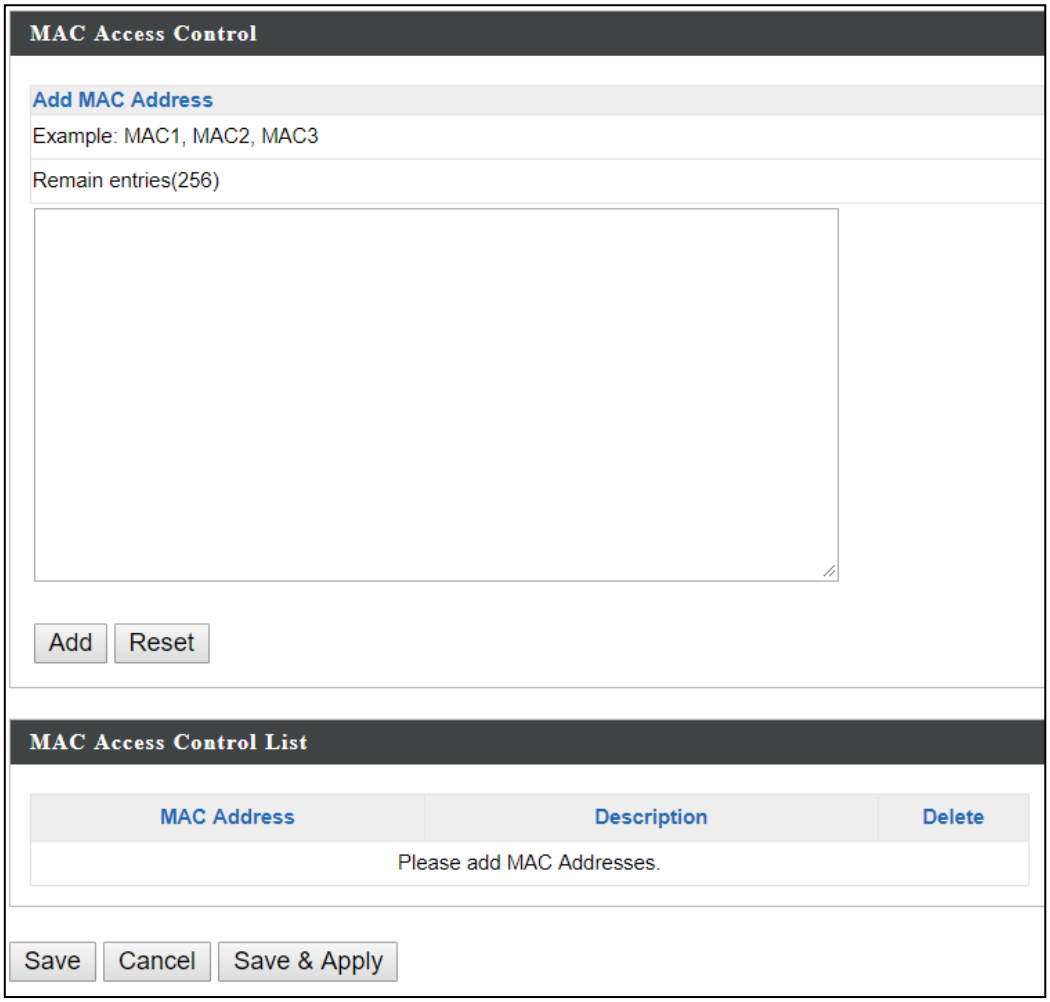
Make a selection using the check-boxes and click “Edit” or click “Add” to add a new MAC Address or MAC Access Control Group:



Delete Selected	Delete the selected entry(s) from the list.
Delete All	Delete all entries from the table.

Add/Edit MAC Access Control:

Click “Add” to enter the page shown below:

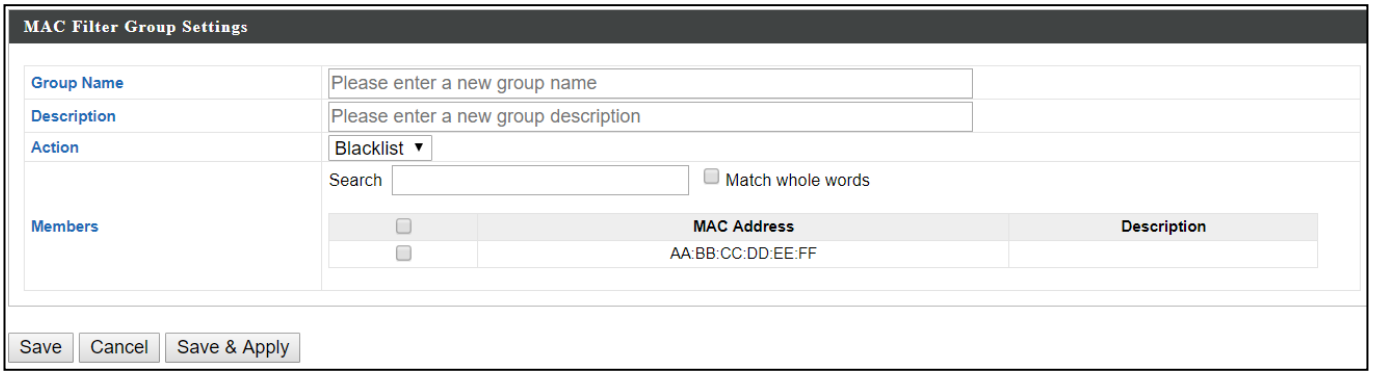


Add MAC Address	Enter a MAC address of computer or network device manually e.g. ‘aa-bb-cc-dd-ee-ff’ or enter multiple MAC addresses separated with commas, e.g. ‘aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg’
Add	Click “Add” to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

MAC address entries will be listed in the “MAC Address Filtering Table”. Select an entry using the “Select” checkbox.

Add/Edit/Clone MAC Access Control Group:

Click “Add” to enter the page shown below:



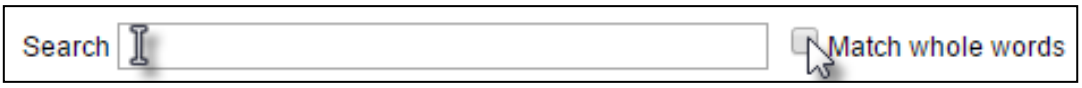
MAC Filter Group Settings	
Group Name	Edit the MAC Access Control Group name.
Description	Enter a description of the MAC Access Control Group for reference.
Action	Select “Blacklist” to deny access to specified MAC addresses in the group, and select “Whitelist” to permit access to specified MAC address in the group.
Members	Check the checkbox to add MAC addresses to the group.

v. Guest Network

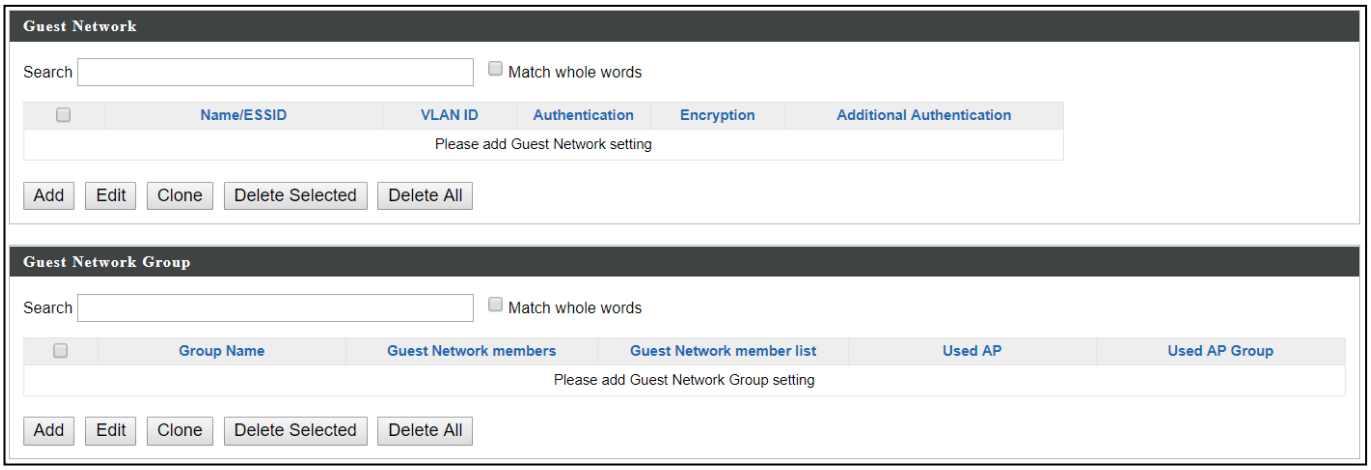
You can setup an additional “Guest” Wi-Fi network so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. The “Guest” screen displays settings for your guest Wi-Fi network.

The Guest Network panel displays information about Guest Networks and Guest Network Groups and allows you to add or edit Guest Network and Guest Network Group settings.

The search function can be used to locate a Guest Network or Guest Network Group. Type in the search box and the list will update:



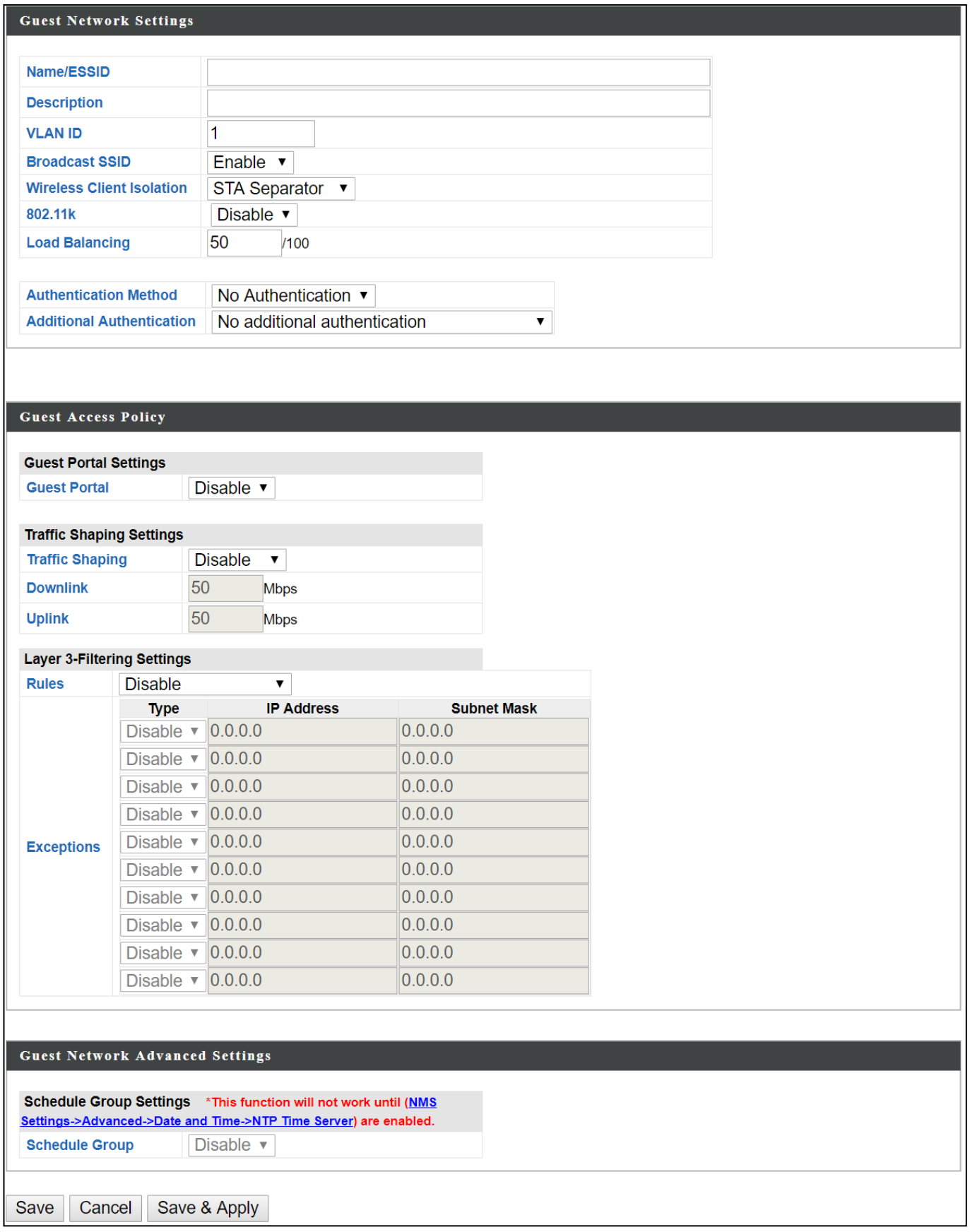
Make a selection using the check-boxes and click “Edit” or click “Add” to add a new Guest Network or Guest Network Group.



Delete Selected	Delete the selected entry(s) from the list.
Delete All	Delete all entries from the table.

Add/Edit Guest Network:

Click “Add” to enter the page shown below:



Guest Network Settings	
Name/ESSID	Edit the Guest Network name (SSID).
Description	Enter a description of the Guest Network for reference e.g. 2nd Floor Office HR.
VLAN ID	Specify the VLAN ID.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the AP from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
802.11k	Enable / Disable to define and expose radio and network information. (Helps facilitate the management and maintenance of a mobile wireless LAN)
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu.
Additional Authentication	Select an additional authentication method from the drop down menu.

Various security options (wireless data encryption) are available. When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It is essential to configure wireless security in order to prevent unauthorised access to your network.

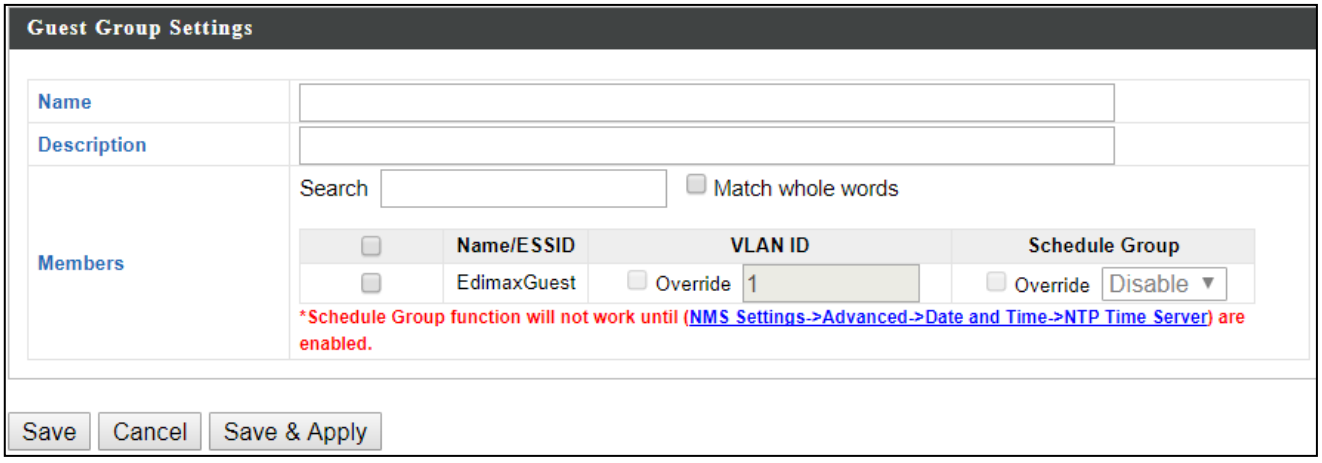
Select hard-to-guess passwords which may include combinations of numbers, letters and symbols, and change your passwords regularly.

Guest Access Policy	
Guest Portal	Enable or disable guest portal for the guest network.
Traffic Shaping	Enable or disable traffic shaping for the guest network.
Downlink	Enter a downlink limit in MB.
Uplink	Enter an uplink limit in MB.
Rules	Enter IP addresses to be filtered according to the drop down menu: “Allow all by Default”, “Deny all by Default”, “Internet Only” and “Disable”
Exceptions	After selecting the rule above, exceptions can be setup to allow / deny guest access.

Guest Network Advanced Settings	
Schedule Group	Select a schedule group.

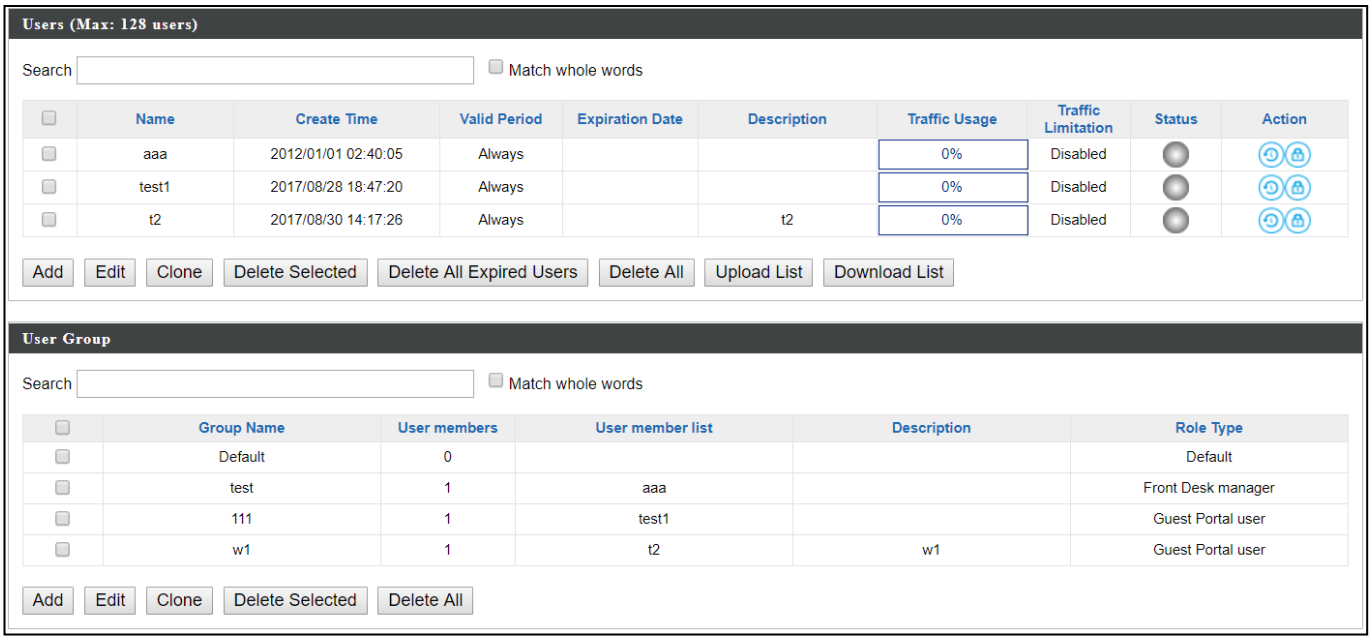
Clone	Select an entry and clone its settings. You will be taken to the add guest network settings page shown above. Enter / edit the fields and save your selection.

Add/Edit Guest Network Group:



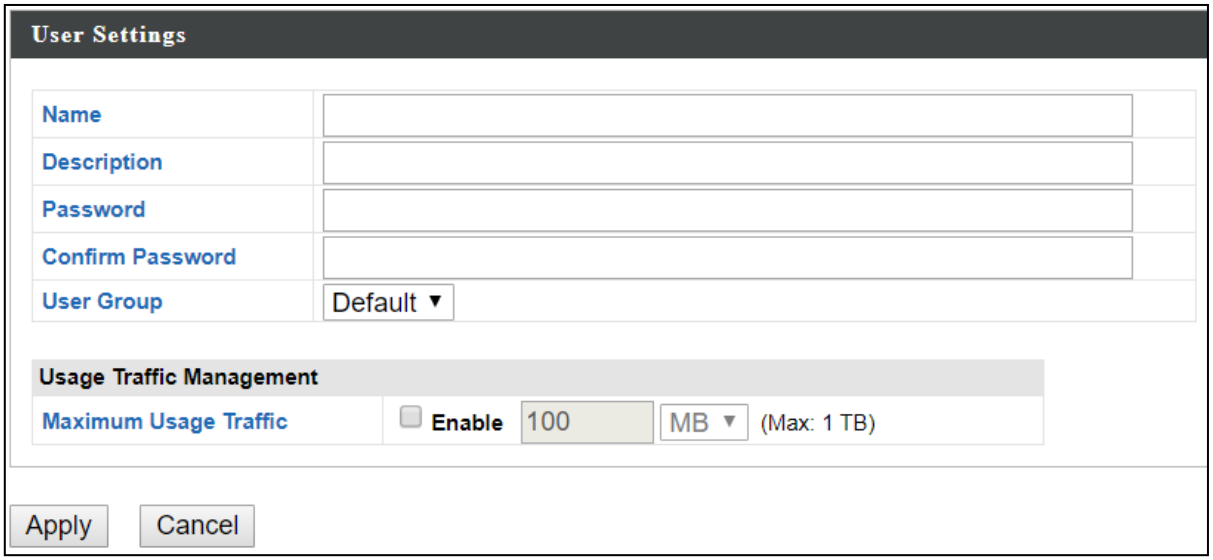
Guest Network Group Settings	
Group Name	Edit the Guest Network Group name.
Description	Enter a description of the Guest Network for reference.
Members	Add SSIDs to the Guest Network group.

vi. Users



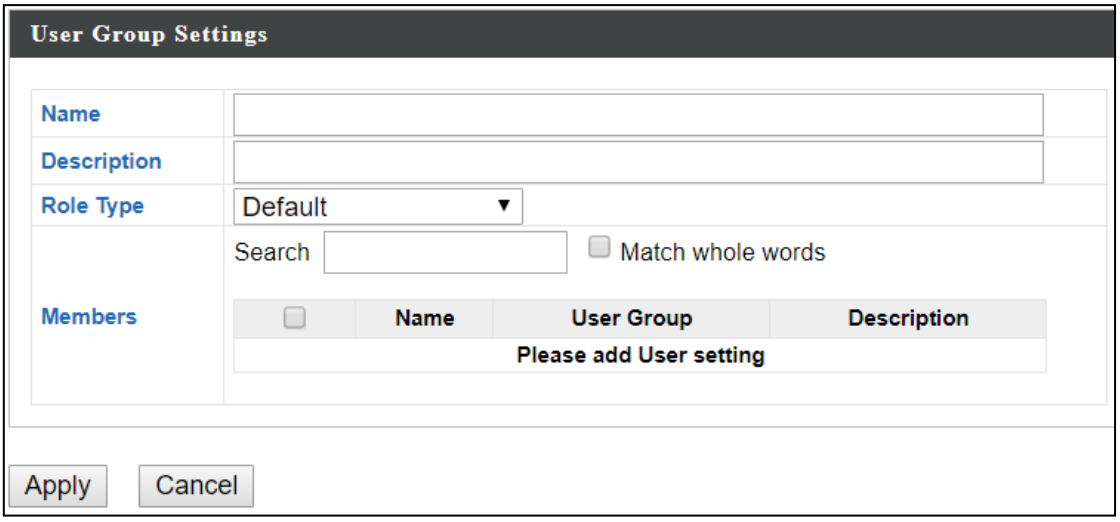
User Panel:

Press “Add” to add a new user, or “Edit” to edit an existing user, or “Clone” to clone an existing user’s settings. For the 3 options specified above, enter the fields below:



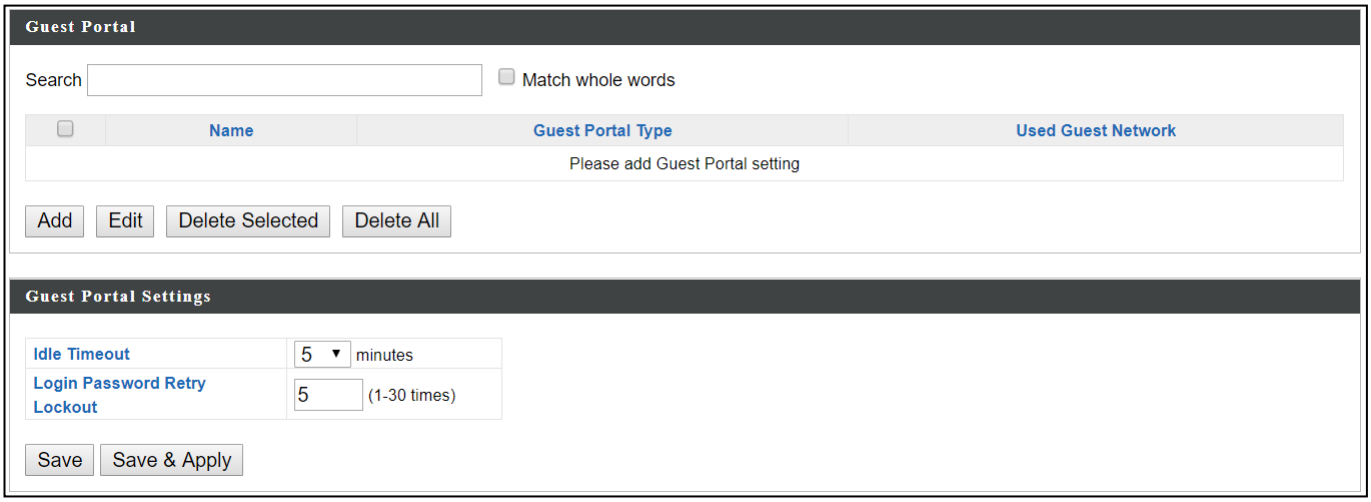
User Group Panel:

Click “Add” to add a new user group, or “Edit” to edit an existing user group, or “Clone” to clone an existing user group’s settings. For the 3 options specified above, enter the fields below:



vii. Guest Portal

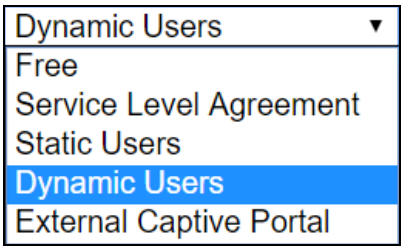
A guest portal is a web page which is displayed to newly connected users before they are granted broader access to network resources.



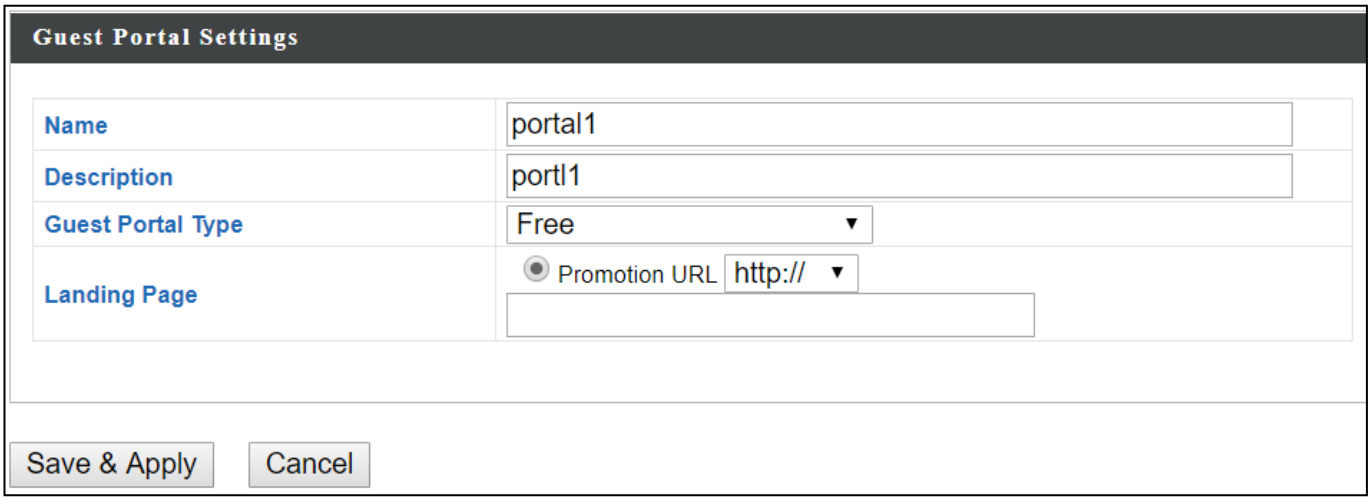
Guest Portal Settings	
Idle Timeout	Select an idle timeout time from the drop down menu.
Login Password Retry Lockout	Enter a number (between 1 and 30) for the number of login password retry. If login password has been entered incorrectly for the number entered here, it will be locked.

Add / Edit:

Enter the fields according to the selected “Guest Portal Type” below:

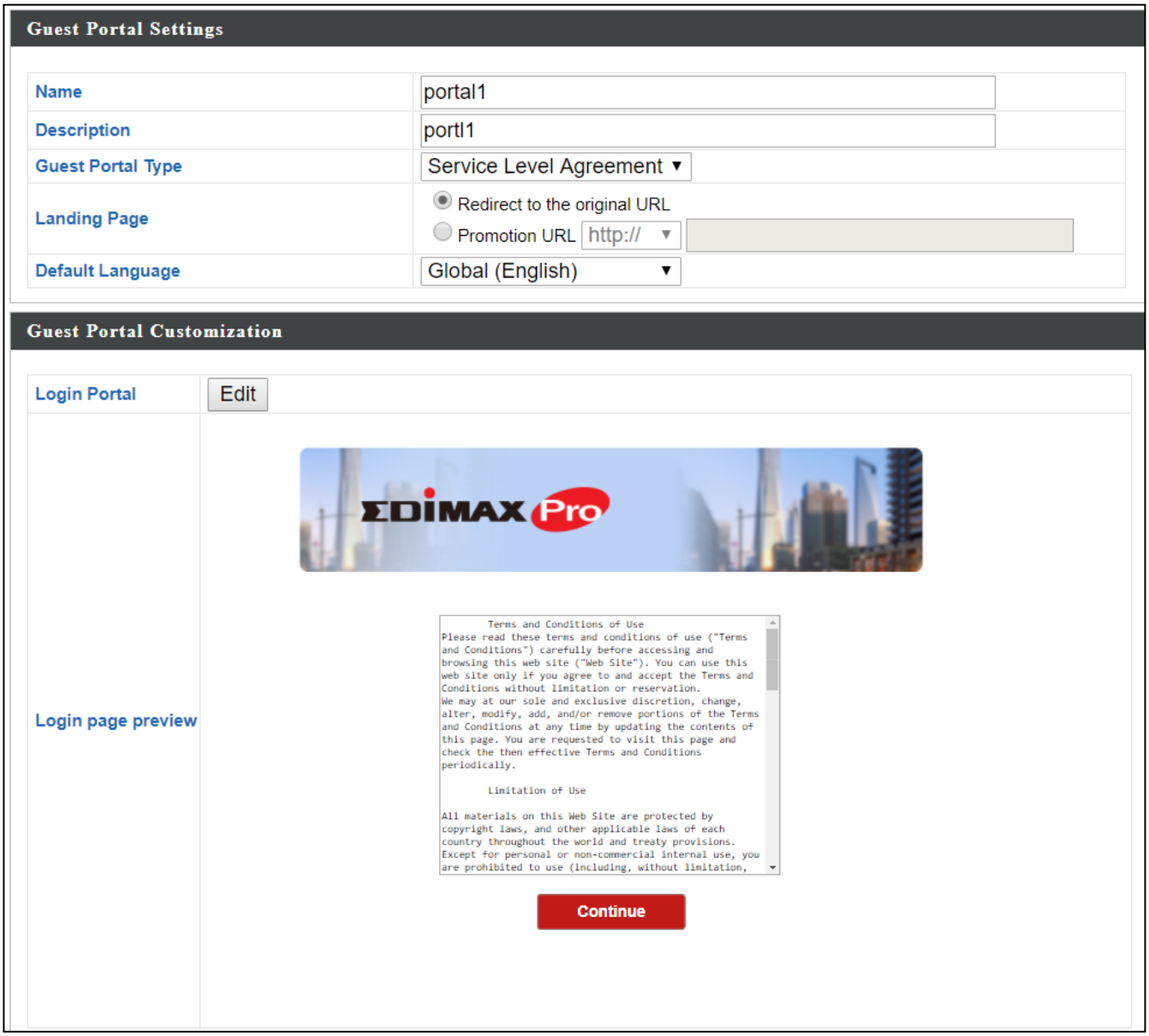


Free Guest Portal Type:



Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Landing Page	Enter a “Promotion URL”.

User Level Agreement Guest Portal Type:



Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Landing Page	Select between “Redirect to the original URL” or “Promotion URL” (enter the promotion URL).
Default Language	Choose a default language.

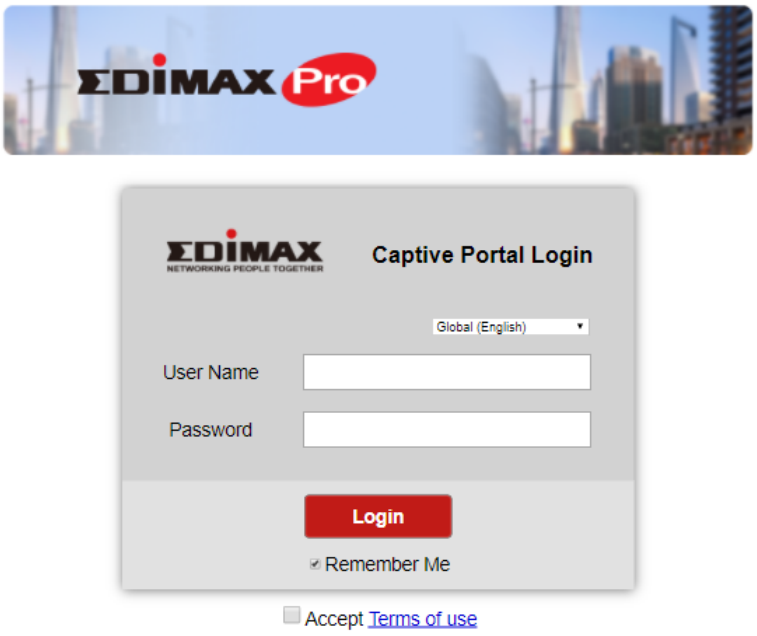
For Login Portal, click “Edit” and see below to edit the login portal.

Static Users Guest Portal Type:

Guest Portal Settings

Name	portal1
Description	portl1
Guest Portal Type	Static Users
Authentication Server	Local Database
Authentication User Group	111
Landing Page	Redirect to the original URL Promotion URL http://
Default Language	Global (English)

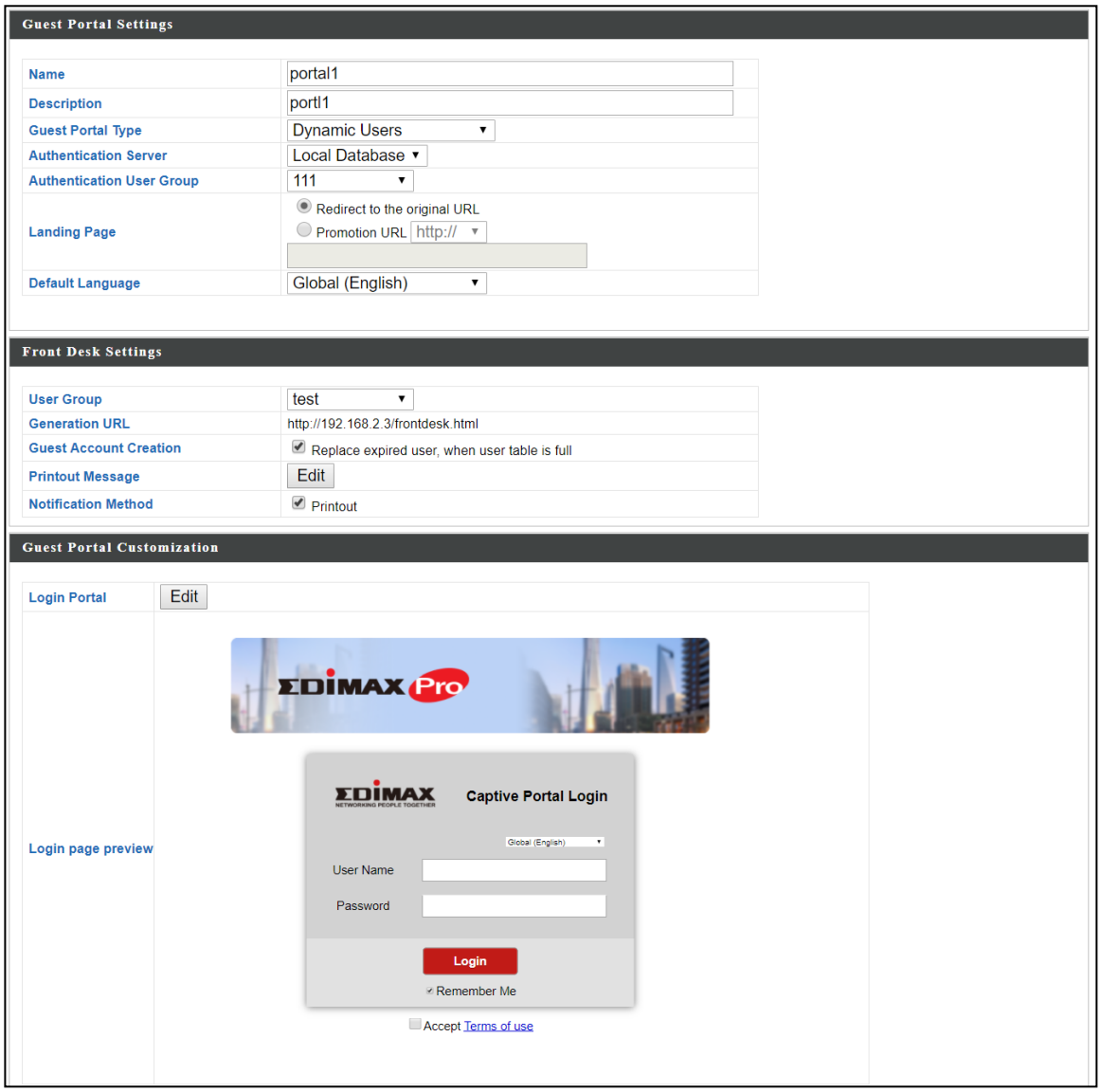
Guest Portal Customization

Login Portal	Edit
Login page preview	

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Authentication Server	Select an authentication server.
Authentication User Group	Select an authentication user group.
Landing Page	Select between “Redirect to the original URL” or “Promotion URL” (enter the promotion URL).
Default Language	Choose a default language.

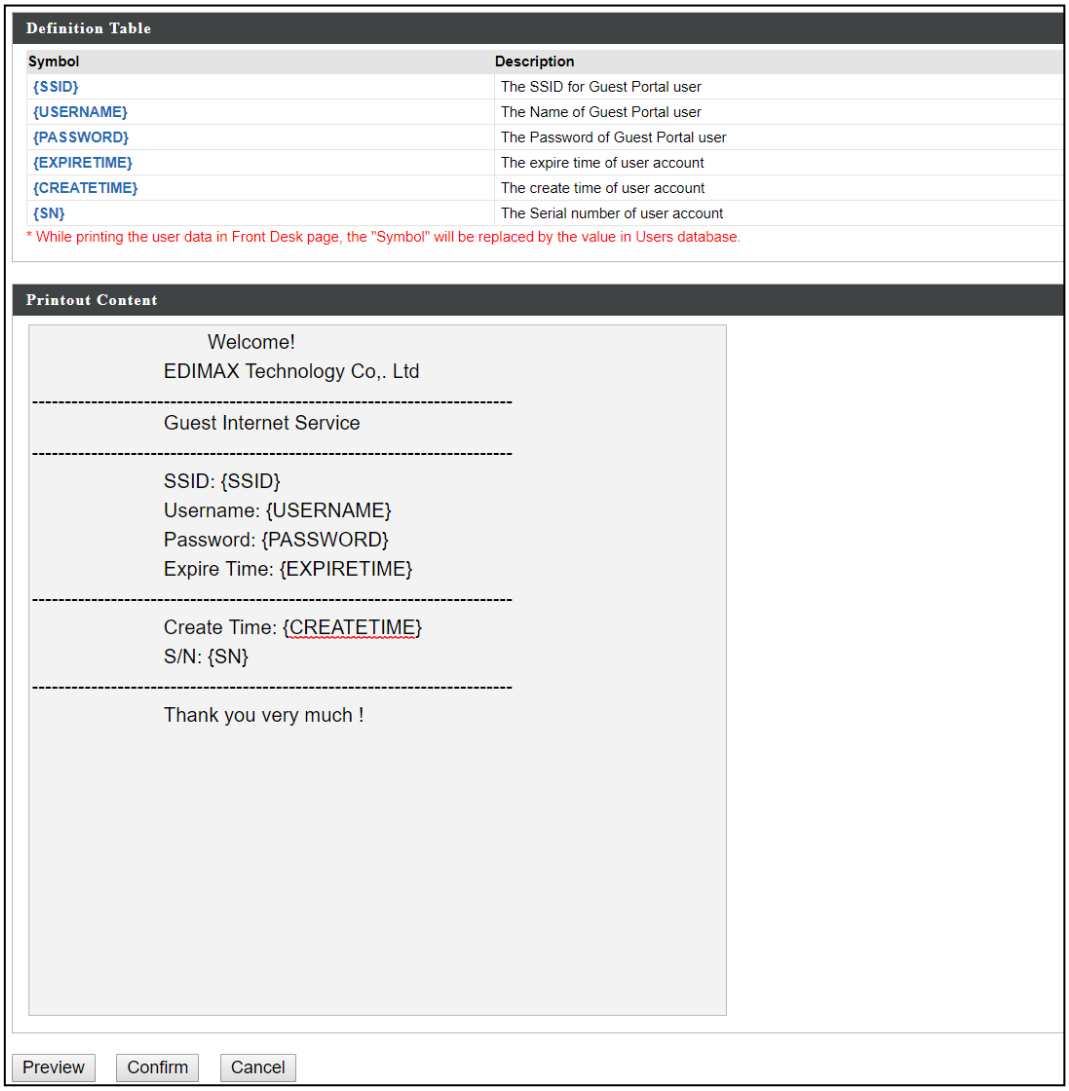
For Login Portal, click “Edit” and see below to edit the login portal.

Dynamic Users Guest Portal Type:



Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Authentication Server	Select an authentication server.
Authentication User Group	Select an authentication user group.
Landing Page	Select between “Redirect to the original URL” or “Promotion URL” (enter the promotion URL).
Default Language	Choose a default language.

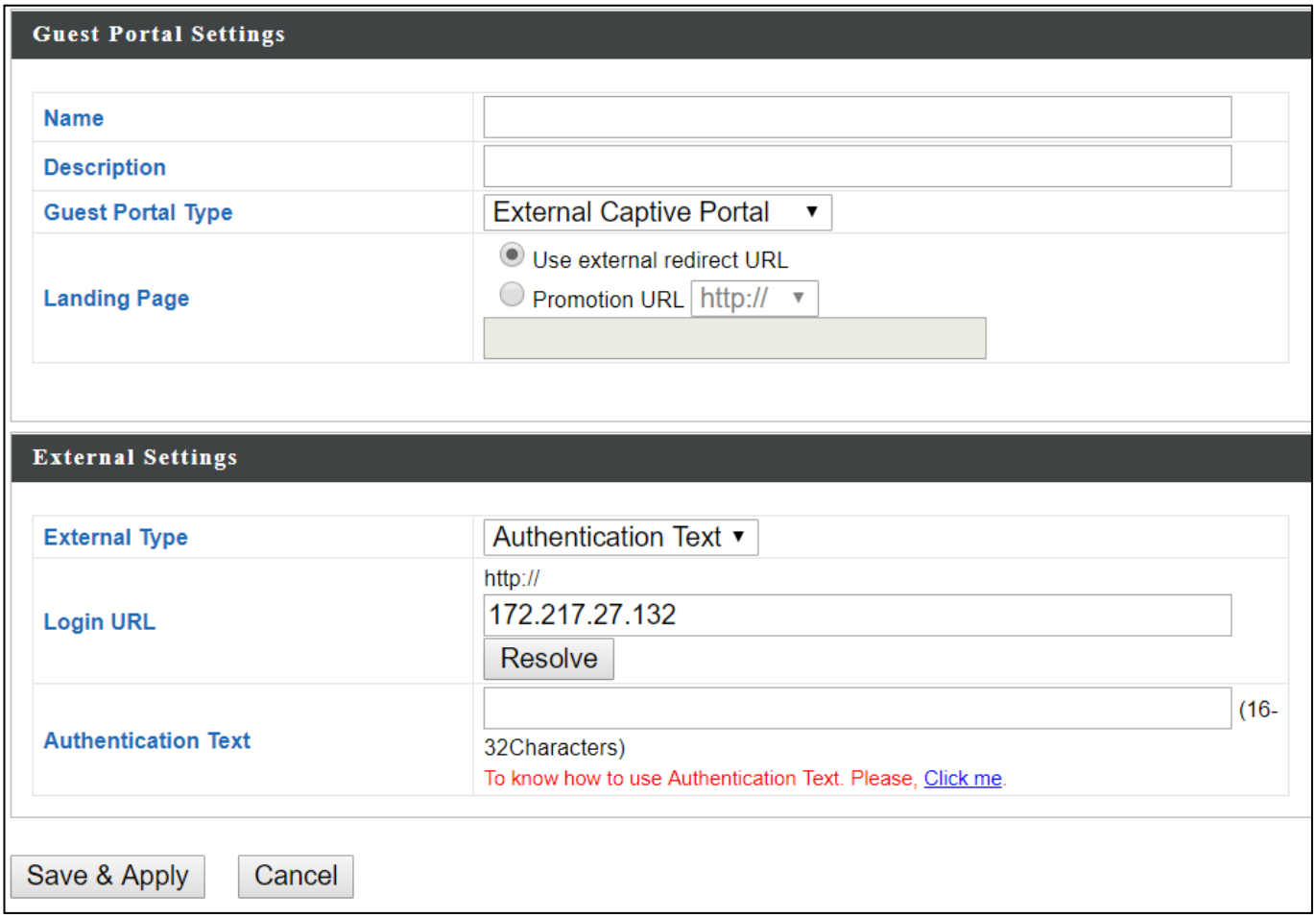
Front Desk Settings	
User Group	Select a user group.
Generation URL	Go to this URL to create dynamic account (and password) for a user.
Guest Account Creation	Check / uncheck to enable / disable “Replace expired user when user table is full”.
Printout Message	Click “Edit” to edit printout message, please see below.
Notification Method	Check / uncheck to enable / disable notification by printout.



Click “Preview” to preview the printout, “Confirm” to confirm the message, or “Cancel” to cancel the changes.

For Login Portal, click “Edit” and see below to edit the login portal.

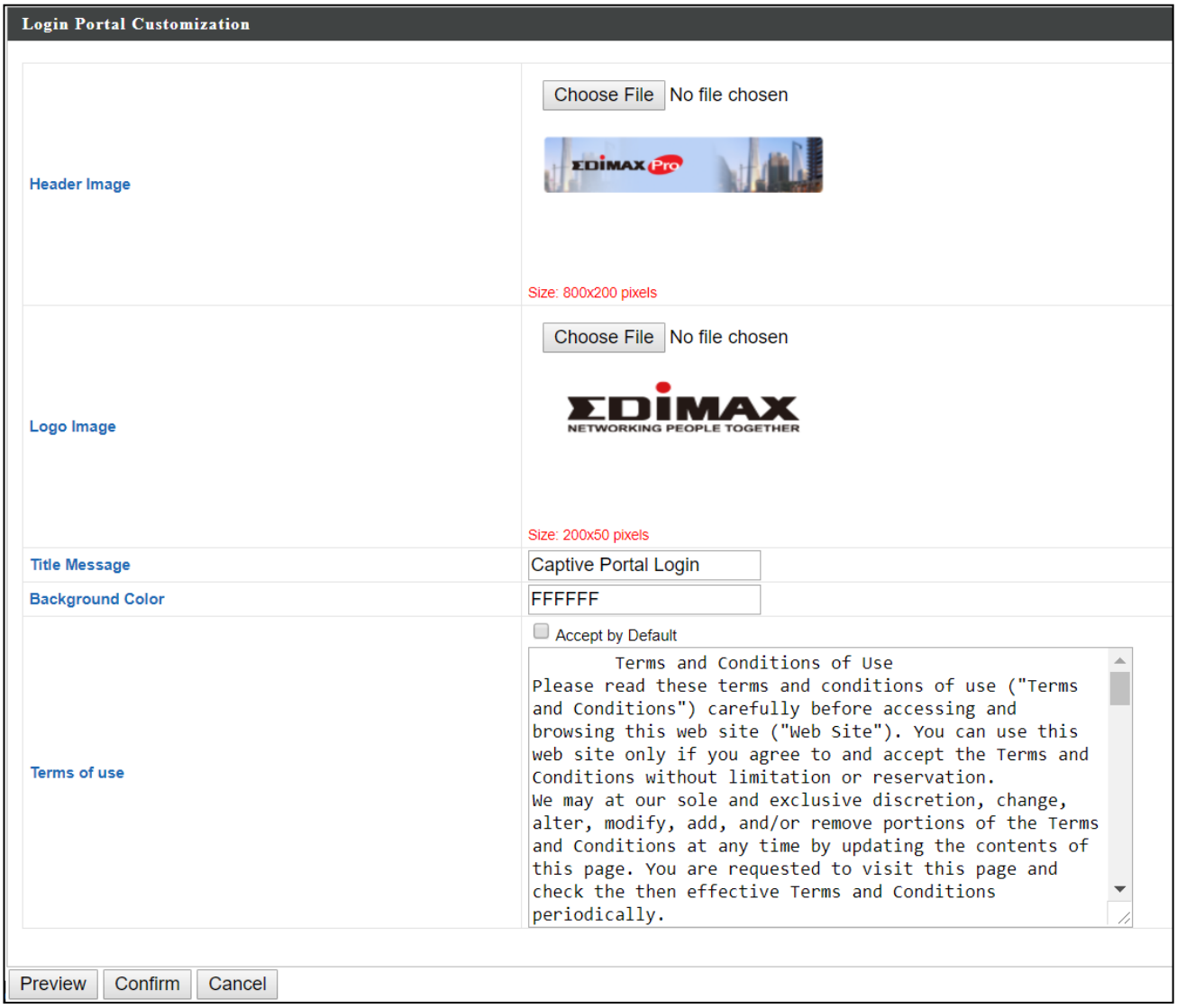
External Captive Portal Guest Portal Type:

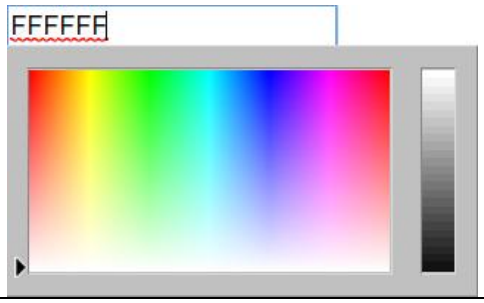


Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Landing Page	Select between “Use external redirect URL” or “Promotion URL” (enter the promotion URL).

External Settings	
Login URL	Enter / edit a login URL.
Authentication Text	Enter an authentication text. Click “Click me” for help.

Editing “Login Portal”:



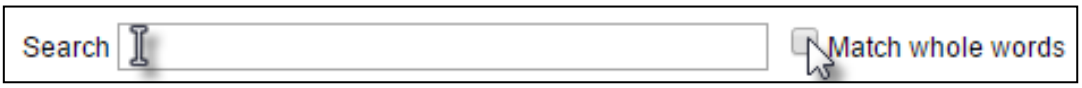
Header Image	Click “Choose File” to select a file as the header image.
Logo Image	Click “Choose File” to select a file as the logo image. (Only for Static and Dynamic users guest portal type)
Title Message	Enter / edit a title message. (Only for Static and Dynamic users guest portal type)
Background Color	Click on the field where color selection will be available. Select a desired color. 
Terms of use	Enter / edit the terms of use message

Click “Preview” to preview the printout, “Confirm” to confirm the message, or “Cancel” to cancel the changes.

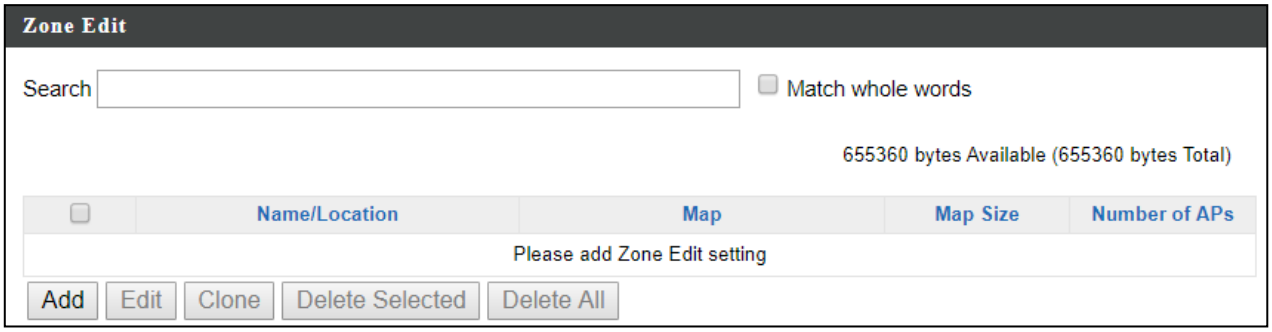
viii. Zone Edit

Zone Edit displays information about zones for use with the Zone Plan feature and allows you to add or edit zones.

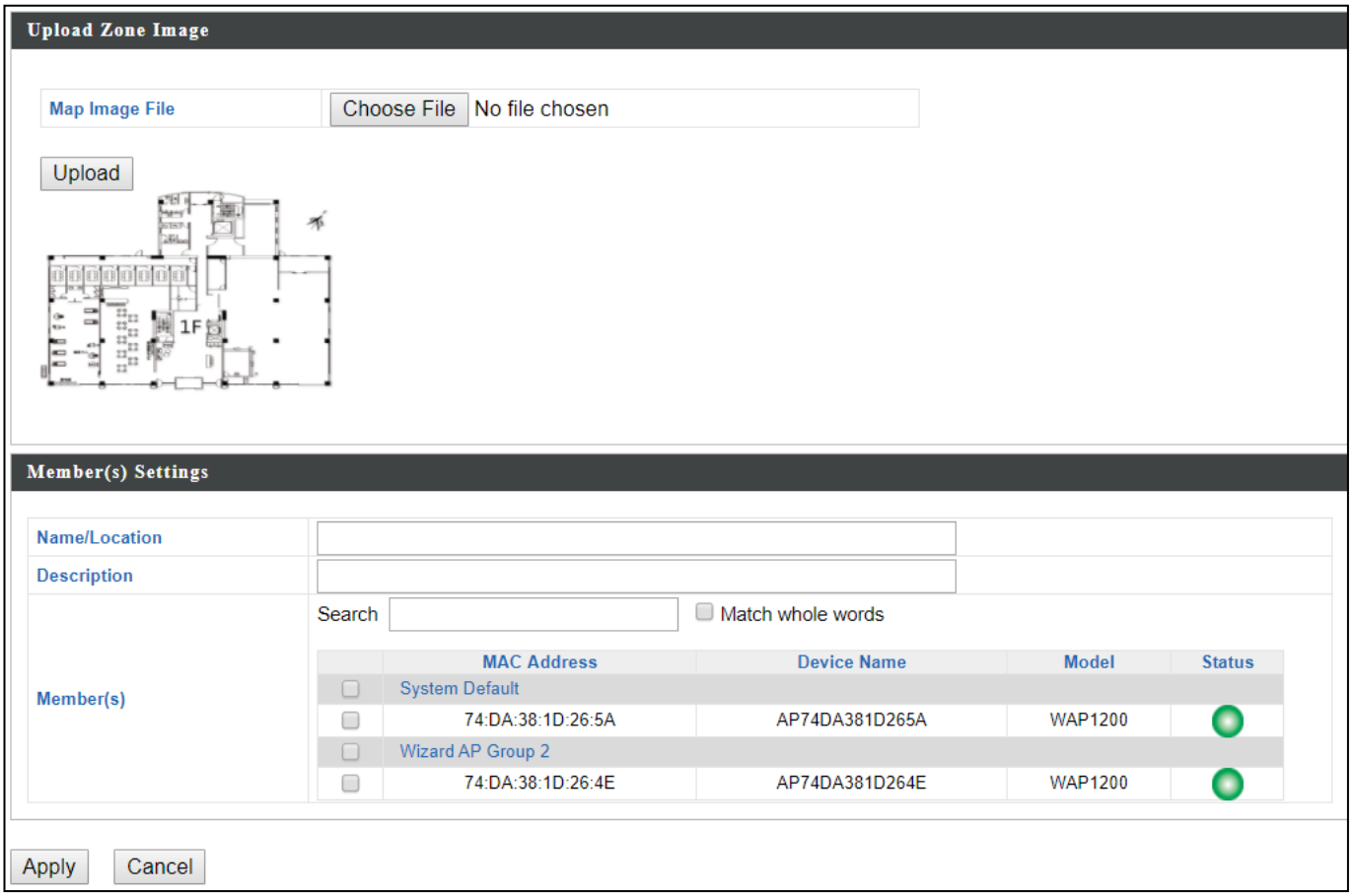
The search function can be used to find existing zones. Type in the search box and the list will update:



Make a selection using the check-boxes and click “Edit” or click “Add” to add a new zone.



Add/Edit Zone:

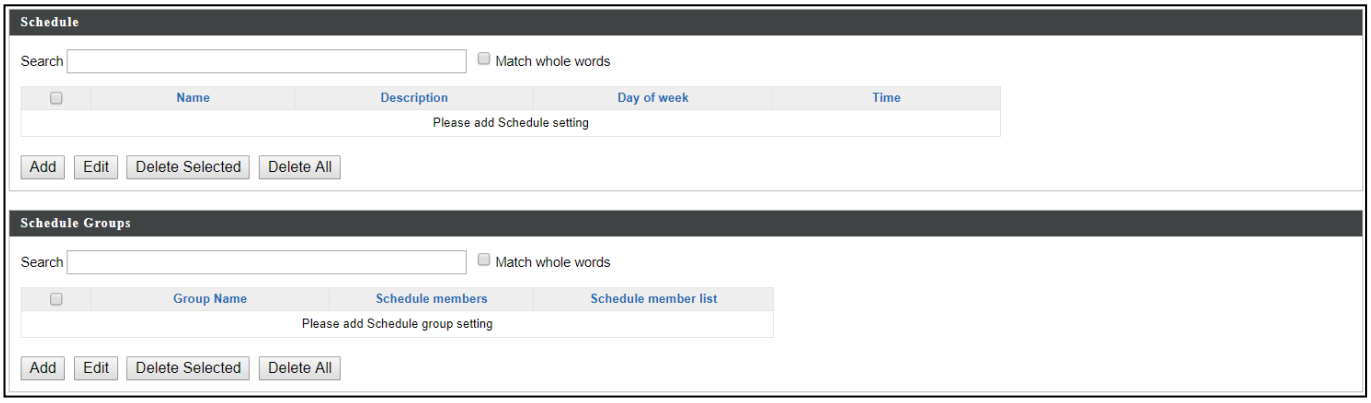


Upload Zone Image	
Choose File	Click to locate an image file to be displayed as a map in the Zone Plan feature. Typically a floor plan image is useful.

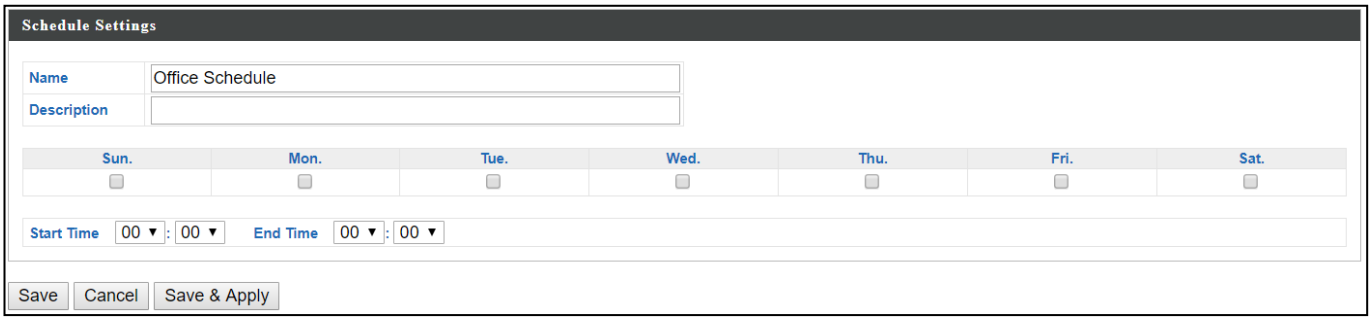
Member(s) Setting	
Name/Location	Name the location or simply enter the name of the location.
Description	Enter a description of the zone/location for reference.
Members	Assign APs to the specified zone/location for use with the Zone Plan feature.

ix. Schedule

Setup schedule start time/end time in Active WLAN Schedule Settings or Guest Network Advanced Settings.

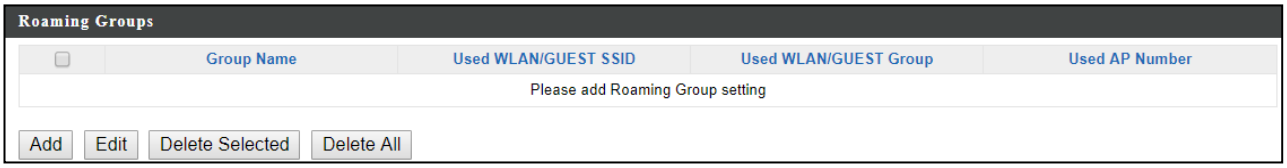


Add / Edit:

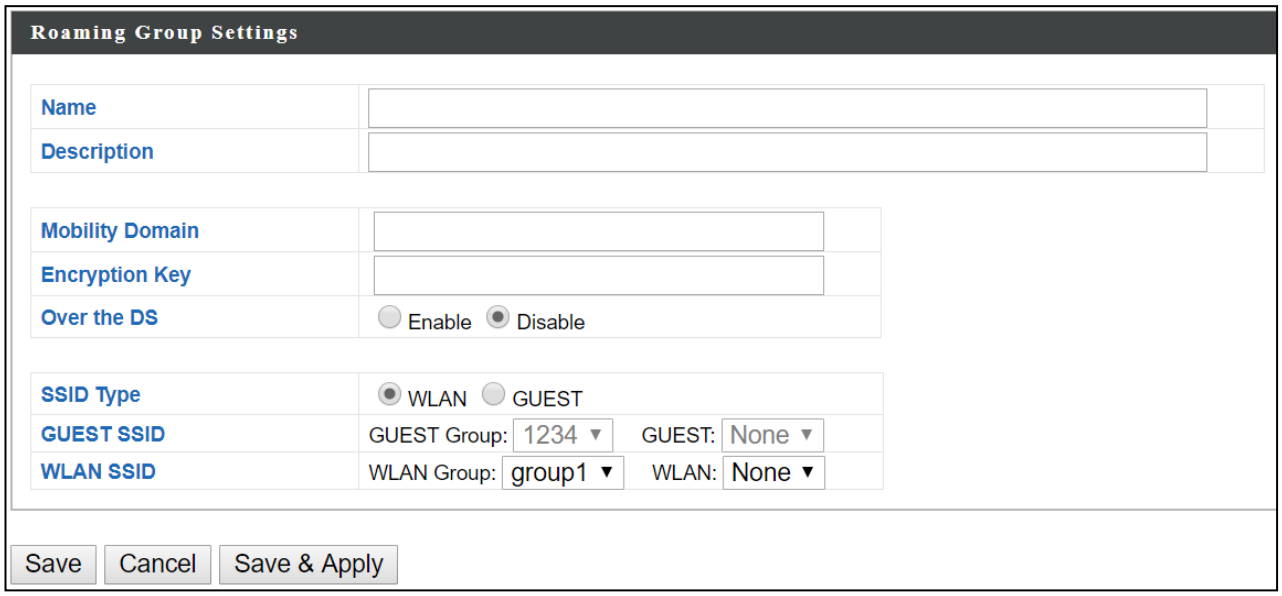


x. Smart Roaming

Smart roaming permits continuous connectivity on wireless devices that are moving. The handoffs from one station to another are fast and secure, and are managed seamlessly.



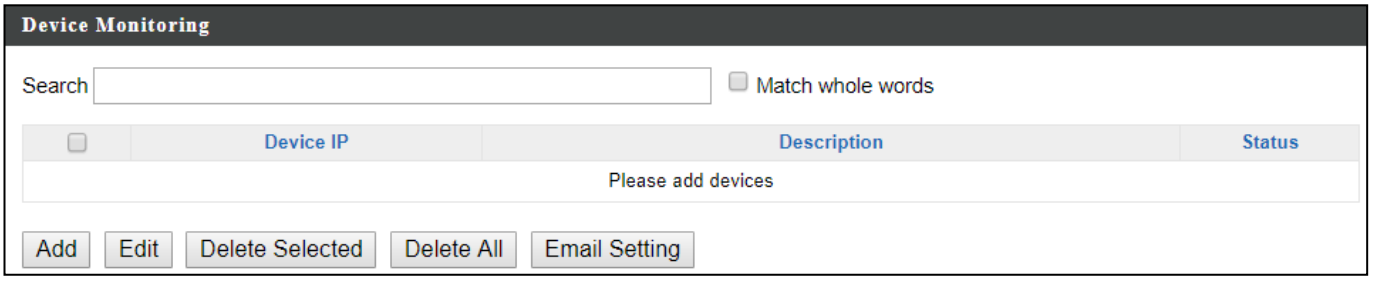
Add / Edit:



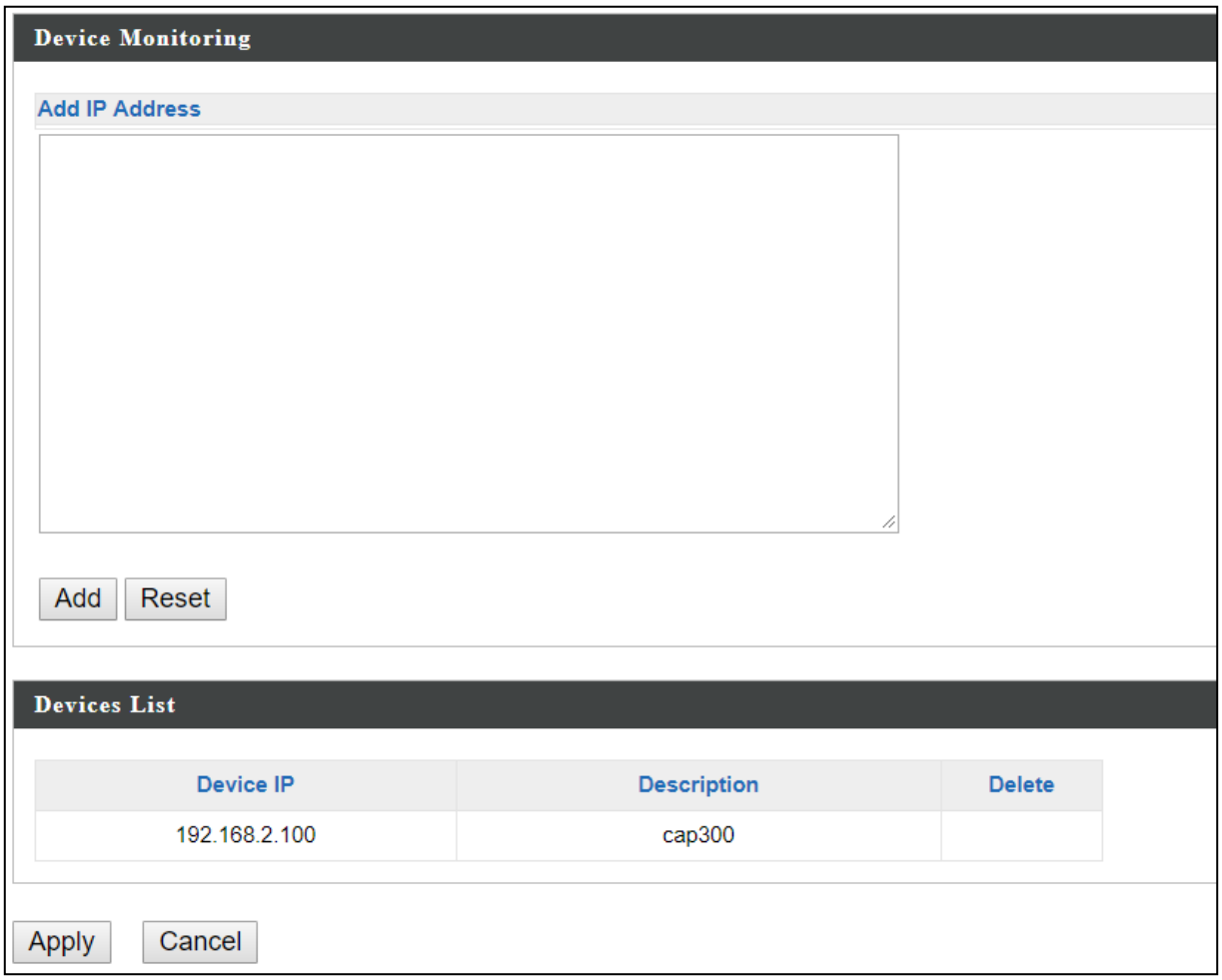
Roaming Group Settings	
Name	Enter / edit the name of roaming group.
Description	Enter / edit a description for reference.
Mobility Domain	Enter / edit a mobility domain.
Encryption Key	Enter / edit an encryption key.
Over the DS	Check to enable / disable this function.
SSID Type	Select the SSID type.
Guest SSID	Select the Guest Group from the drop down menu. Select a Guest from the drop down menu.
WLAN SSID	Select the WLAN Group from the drop down menu. Select a WLAN from the drop down menu.

xi. Device Monitoring

This page monitors the device's status (alive or not alive) after you set the Device IP.



Add / Edit:

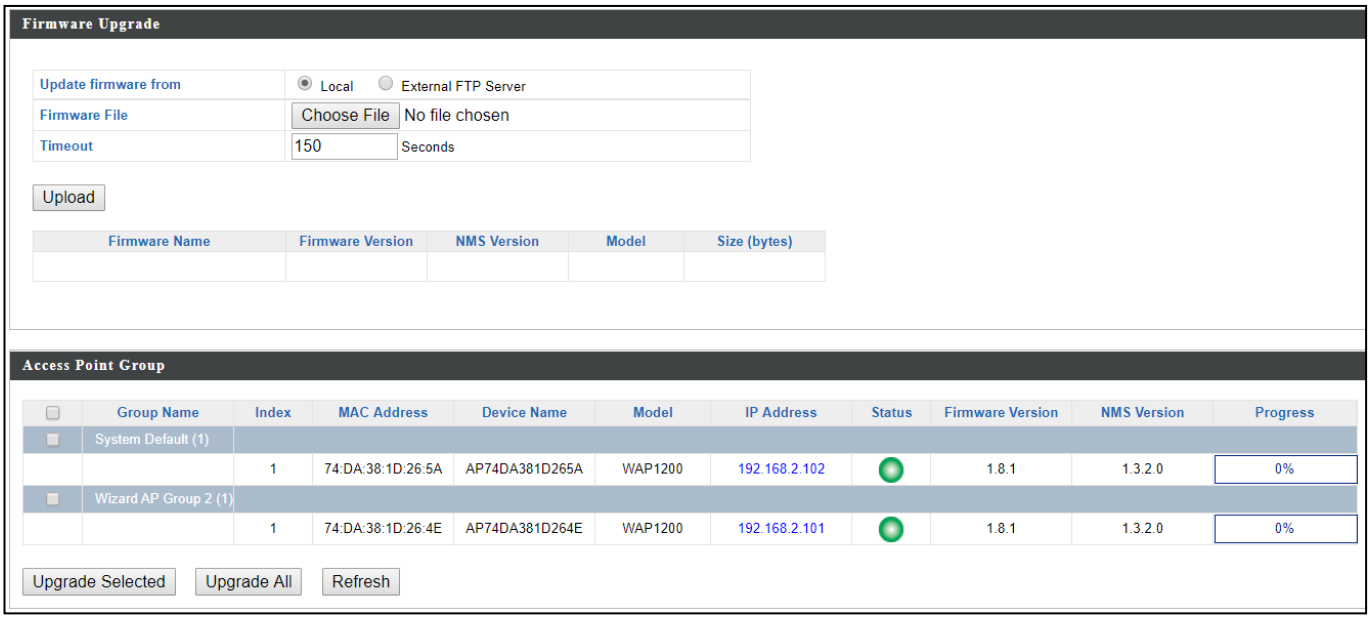


Enter an IP Address and click "Add" to add the device(s). Click "Reset" to clear the field.

xii. Firmware Upgrade

Firmware Upgrade allows you to upgrade firmware to AP Groups. First, upload the firmware file from a local disk or external FTP server: locate the file and click “Upload” or “Check”. The table below will display the Firmware Name, Firmware Version, NMS Version, Model and Size.

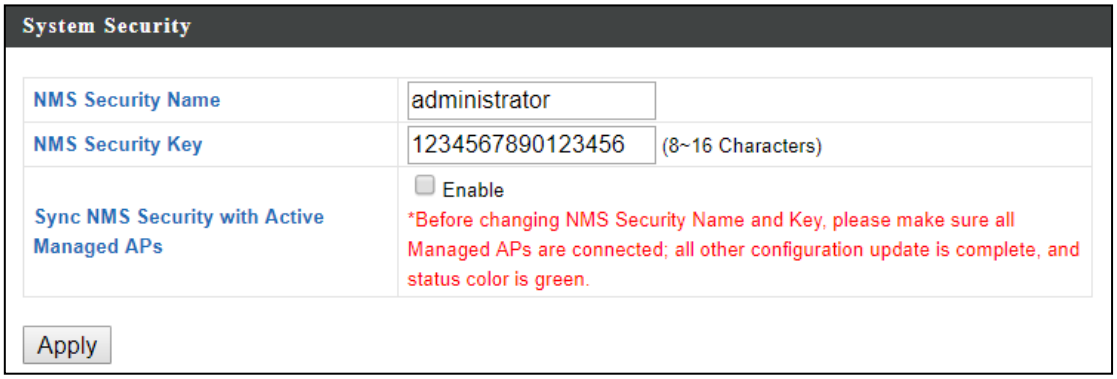
Then click “Upgrade All” to upgrade all APs in the Array or select AP groups from the list using check-boxes and click “Upgrade Selected” to upgrade only selected APs.



xiii. Advanced

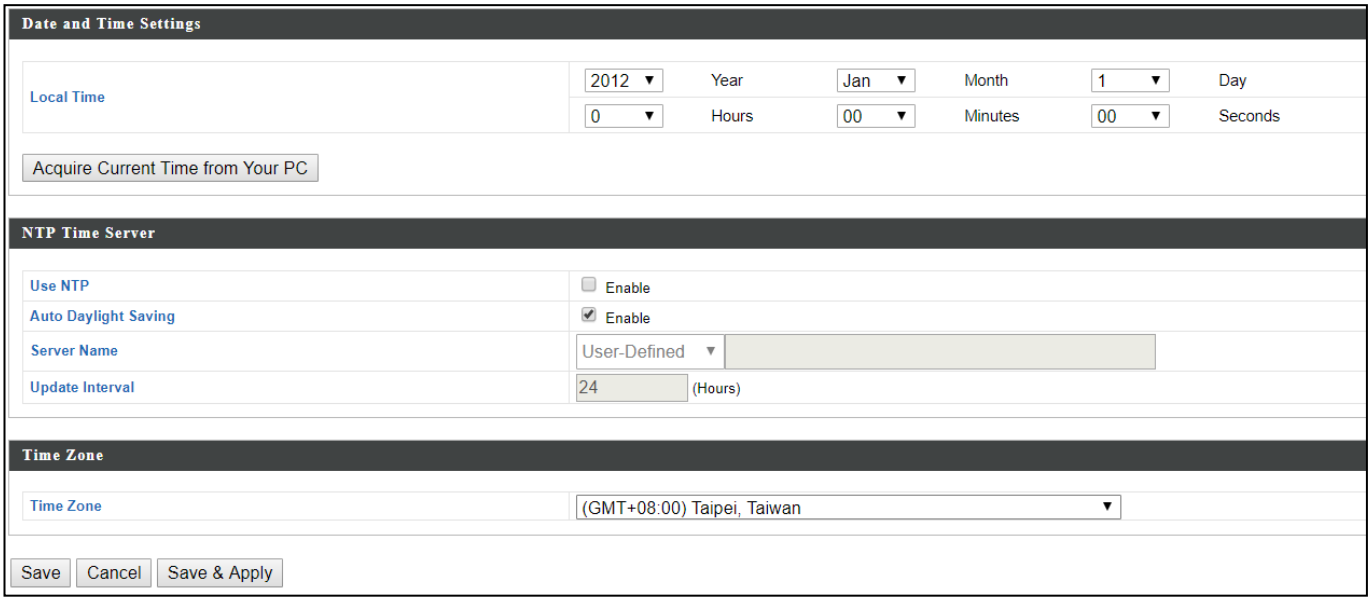
System Security:

Configure the NMS system login name and password.



Date & Time:

Configure the date & time settings of the AP Array. The date and time of the APs can be configured manually or can be synchronized with a time server.



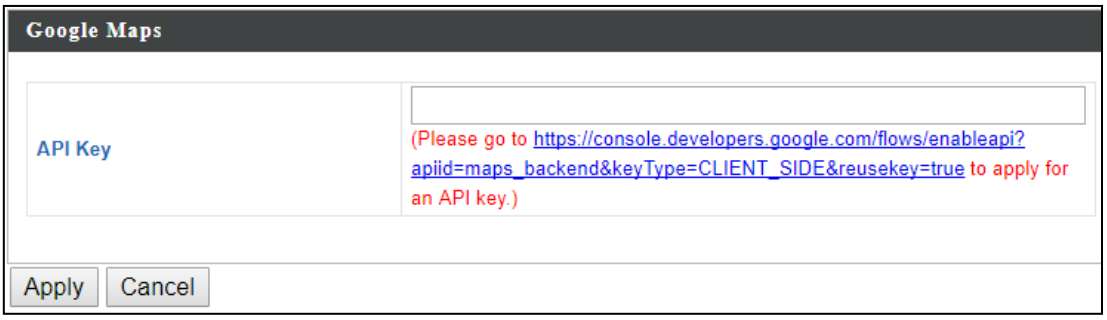
Date and Time Settings	
Local Time	Set the AP's date and time manually using the drop down menus.
Acquire Current Time from your PC	Click "Acquire Current Time from Your PC" to enter the required values automatically according to your computer's current time and date.

NTP Time Server	
Use NTP	The AP also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the AP to update/synchronize with the NTP server.

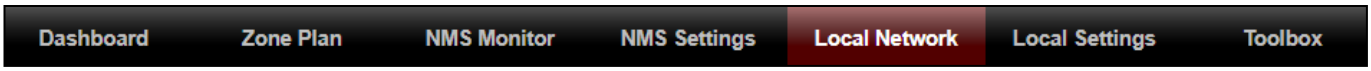
Time Zone	
Time Zone	Select the time zone of your country/ region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.

Google Maps:

Click on the link below the entry field and follow Google's instructions to obtain an API key. Enter the key into the entry field.



VI-8. Local Network



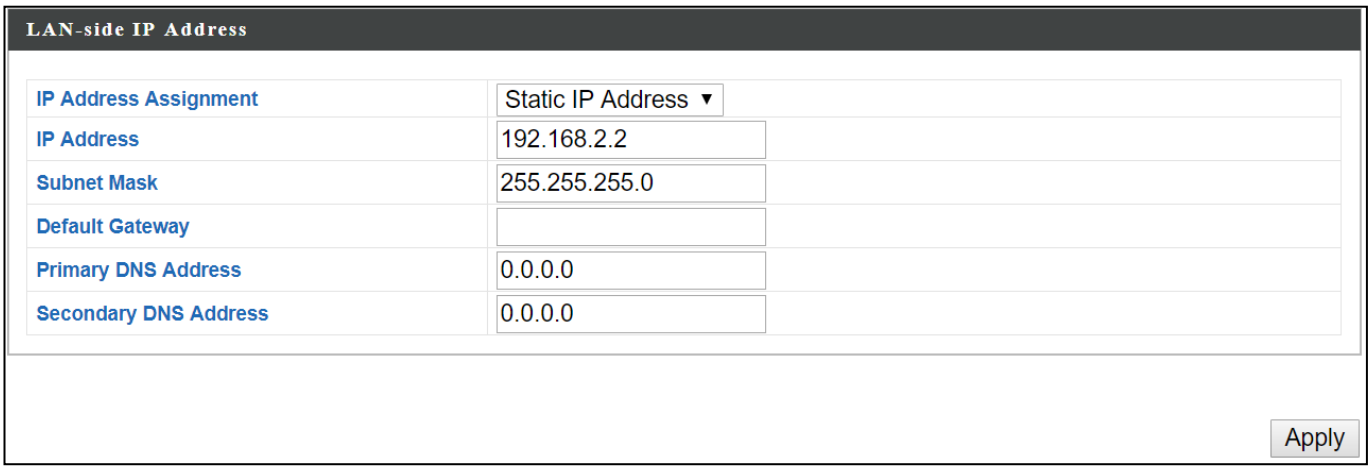
i. Network Settings

LAN-Side IP Address:

The “LAN-side IP address” page allows you to configure your AP Controller on your Local Area Network (LAN). You can enable the AP to dynamically receive an IP address from your router’s DHCP server or you can specify a static IP address for your AP, as well as configure DNS servers. You can also set your AP Controller as a DHCP server to assign IP addresses to other devices on your LAN.

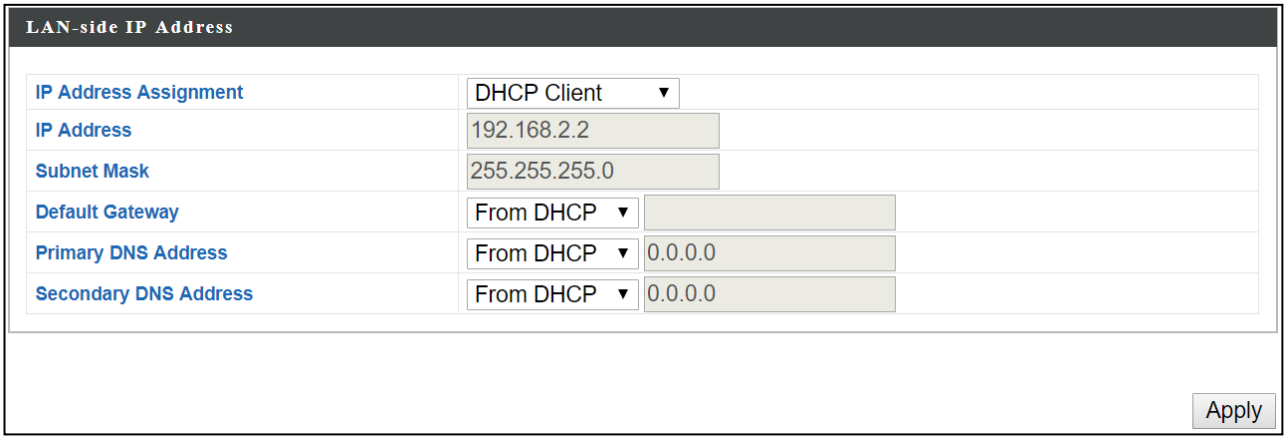
The AP’s default IP address is 192.168.2.2

Disable other DHCP servers on the LAN if using AP Controllers DHCP Server.

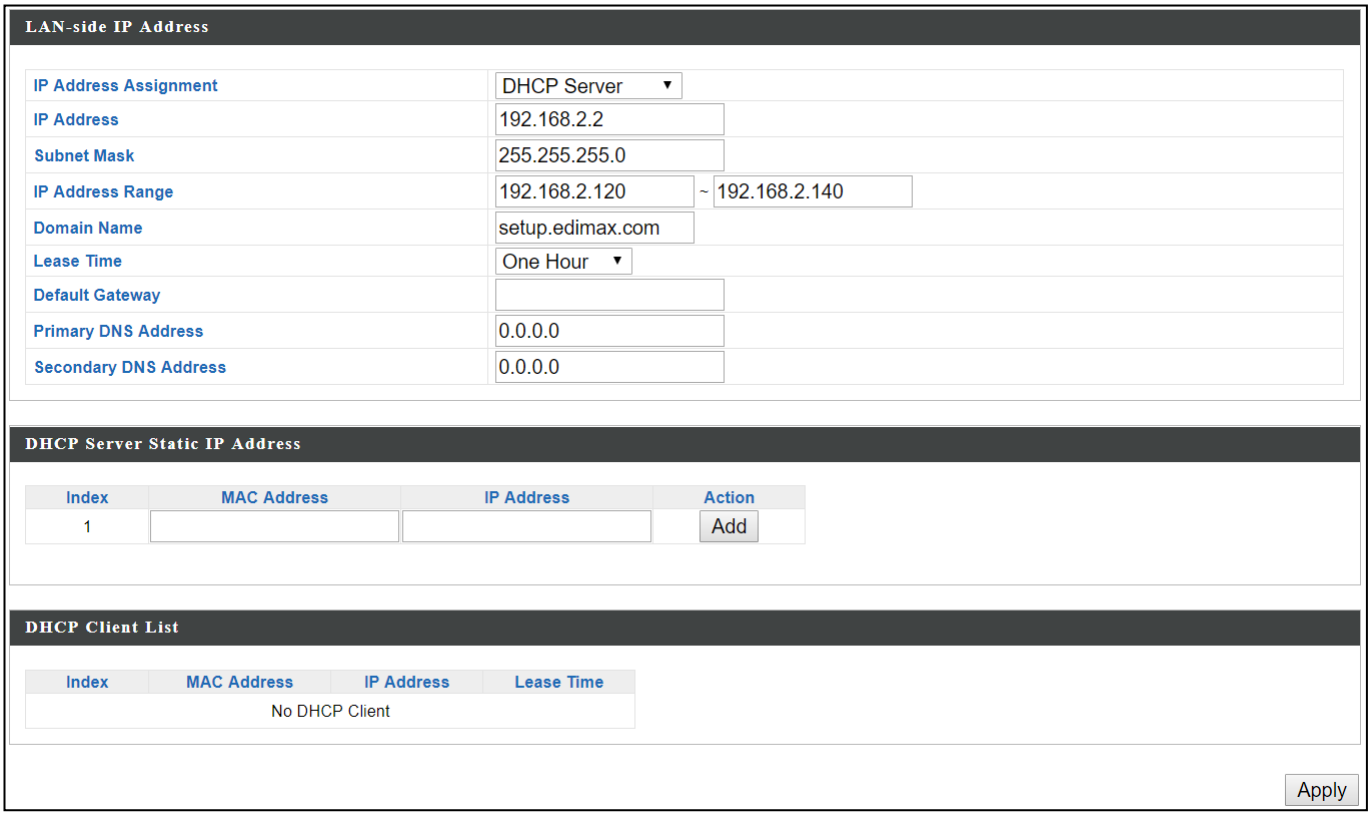


LAN-side IP Address	
IP Address Assignment	Select “Static IP” to manually specify a static/fixed IP address for your AP. Select “DHCP Client” for your AP to be assigned a dynamic IP address from your router’s DHCP server, or select “DHCP Server” for your AP to act as a DHCP server and assign IP addresses on your LAN.

Static IP Address	
IP Address	Specify the IP address here. This IP address will be assigned to your AP and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank.
Primary DNS Address	For static IP users, the default value is blank.
Secondary DNS Address	For static IP users, the default value is blank.



DHCP Client	
IP Address	When “DHCP Client” is selected this value cannot be modified.
Subnet Mask	When “DHCP Client” is selected this value cannot be modified.
Default Gateway	Select “From DHCP” or select “User-Defined” and enter a default gateway.
Primary DNS Address	Select “From DHCP” or select “User-Defined” and enter a primary DNS address.
Secondary DNS Address	Select “From DHCP” or select “User-Defined” and enter a secondary DNS address.



DHCP Server	
IP Address	Specify the IP address here. This IP address will be assigned to your AP and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
IP Address Range	Enter the start and end IP address of the IP address range which your AP's DHCP server will assign to devices on the network.
Domain Name	Enter a domain name.
Lease Time	Select a lease time from the drop down menu. IP addresses will be assigned for this period of time.
Default Gateway	Enter a default gateway.
Primary DNS Address	Enter a primary DNS address.
Secondary DNS Address	Enter a secondary DNS address.

Your AP's DHCP server can be configured to assign static (fixed) IP addresses to specified network devices, identified by their unique MAC address:

DHCP Server Static IP Address	
MAC Address	Enter the MAC address of the network device to be assigned a static IP address.
IP Address	Specify the IP address to assign the device.
Add	Click to assign the IP address to the device.

LAN Port Settings:

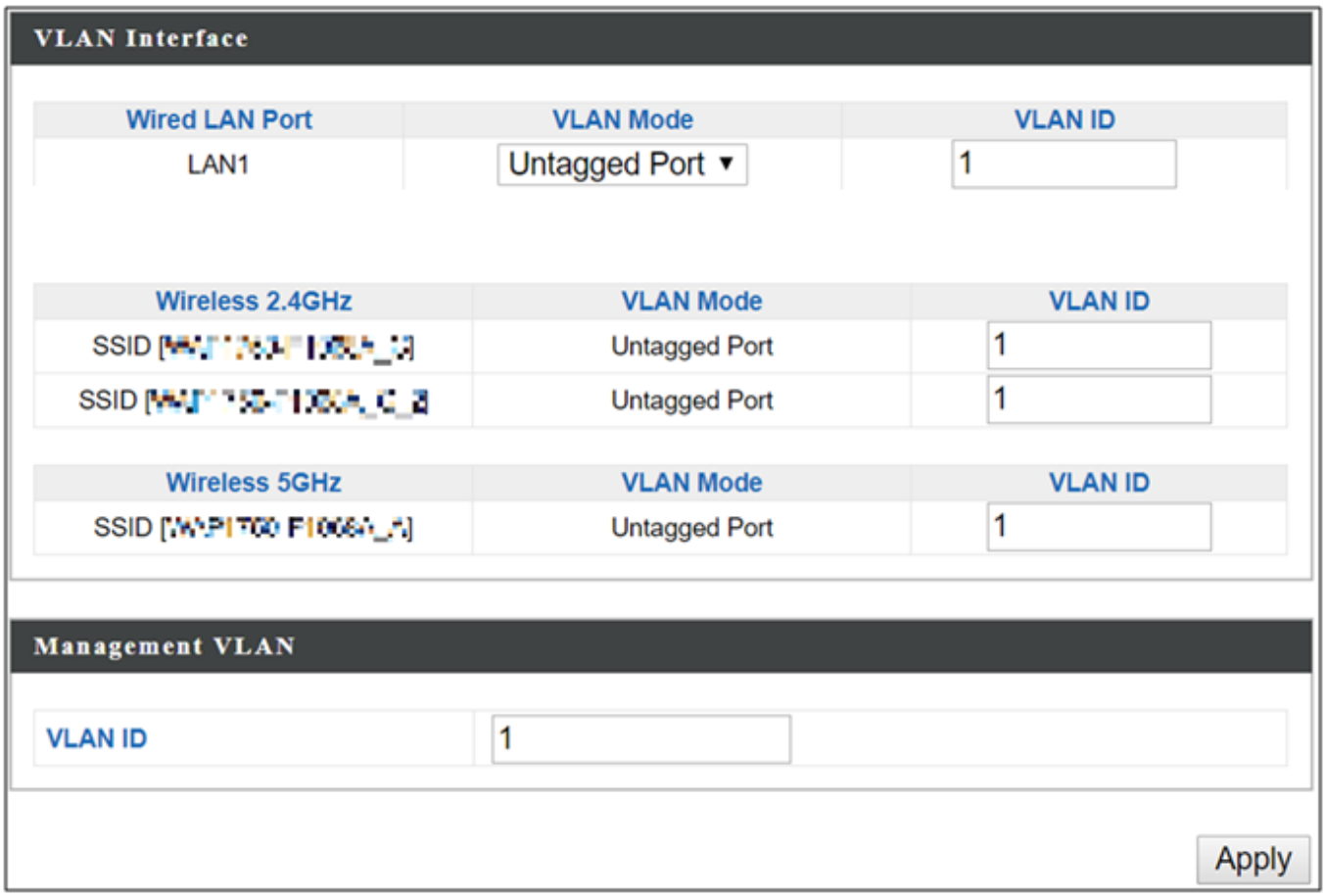
The “LAN Port” page allows you to configure the settings for your AP Controllers wired LAN (Ethernet) ports.

Wired LAN Port	Identifies LAN port 1.
Enable	Enable/disable specified LAN port.
Speed & Duplex	Select a speed & duplex type for specified LAN port, or use the “Auto” value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packets transfer/receive.
Flow Control	Enable/disable flow control. Flow control can pause new session request until current data processing is complete, in order to avoid device overloads under heavy traffic.
802.3az	Enable/disable 802.3az. 802.3az is an Energy Efficient Ethernet feature which disables unused interfaces to reduce power usage.

VLAN:

"VLAN" (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other.

VLAN IDs in the range 1 – 4095 are supported.



VLAN Interface	
Wired LAN Port/Wireless	Identifies LAN port 1 and wireless SSIDs.
VLAN Mode	Select "Tagged Port" or "Untagged Port" for specified LAN interface.
VLAN ID	Set a VLAN ID for specified interface, if "Untagged Port" is selected.

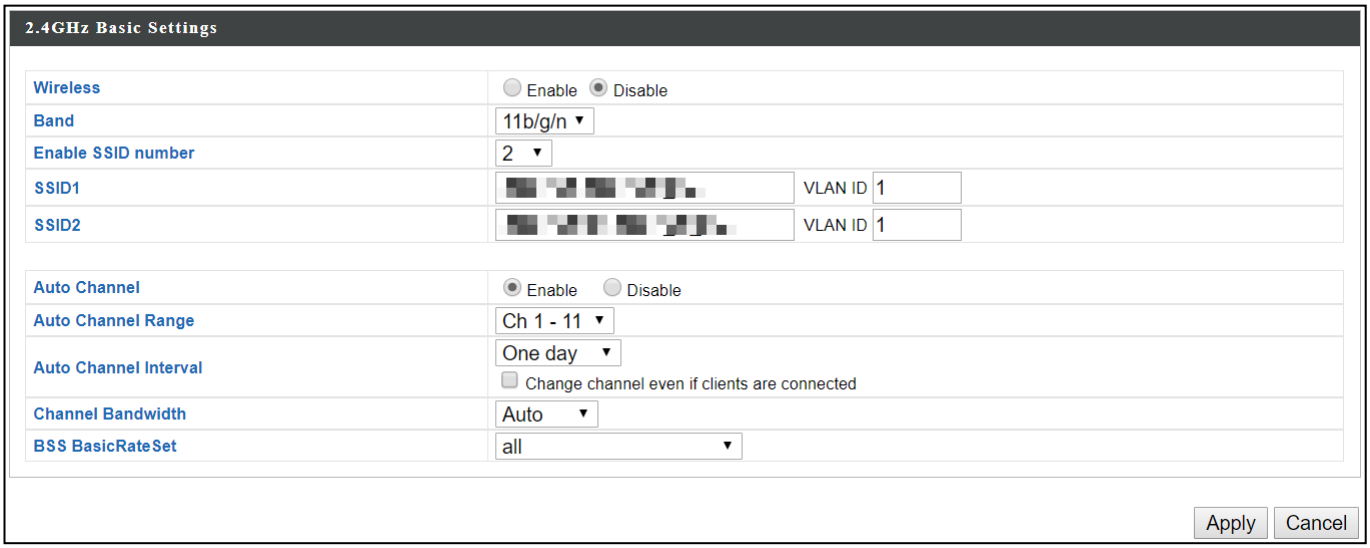
Management VLAN	
VLAN ID	Specify the VLAN ID of the management VLAN. Only the hosts belonging to the same VLAN can manage the device.

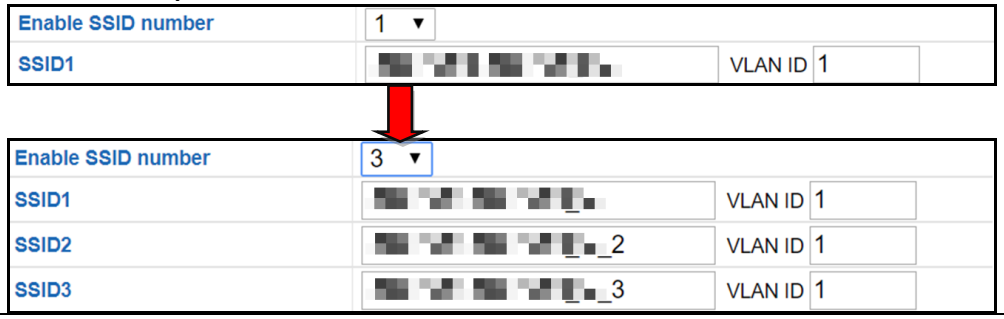
ii. 2.4GHz 11bgn

The “2.4GHz 11bgn” menu allows you to view and configure information for your AP’s 2.4GHz wireless network across five categories: Basic, Advanced, Security, WDS & Guest Network.

Basic:

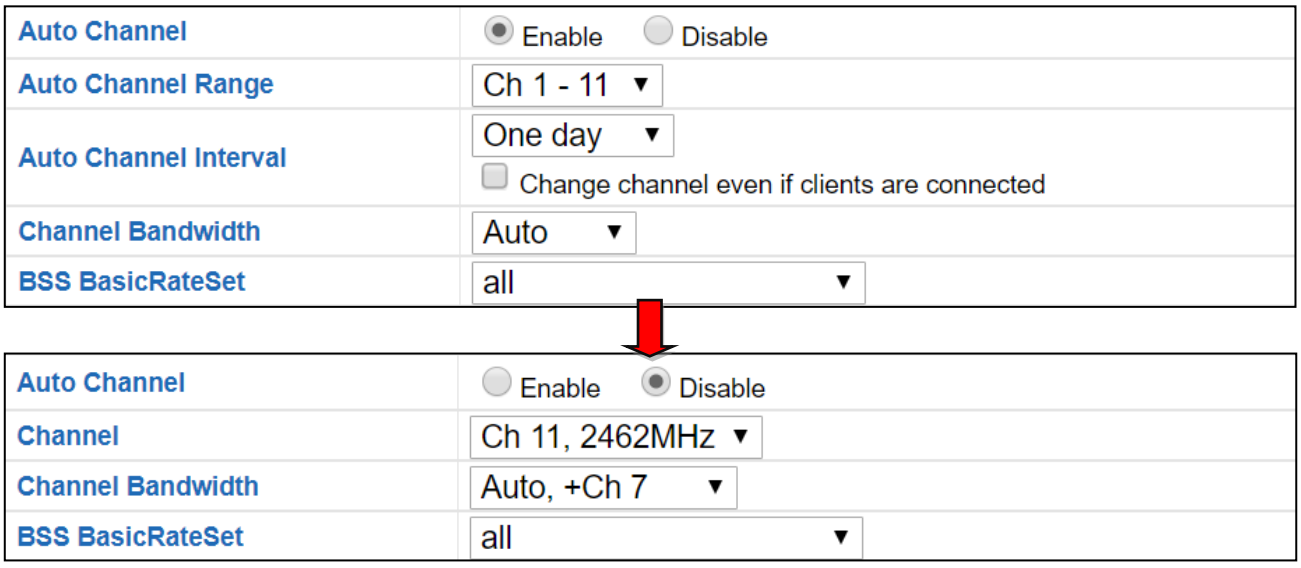
The “Basic” screen displays basic settings for your AP’s 2.4GHz Wi-Fi network.



Wireless	Enable or disable the AP’s 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active.
Band	Wireless standard used for the AP. Combinations of 802.11b, 802.11g & 802.11n can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of 16 can be enabled. 
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.

VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Enable: Auto channel selection will automatically set the wireless channel for the AP's 2.4GHz frequency based on availability and potential interference. Disable: Select a channel manually as shown in the next table.
Auto Channel Range	Select a range to which auto channel selection can choose from.
Auto Channel Interval	Select a time interval for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Select the channel bandwidth: 20MHz (lower performance but less interference); or 40MHz (higher performance but potentially higher interference); or Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

When auto channel is disabled, configurable fields will change. Select a wireless channel manually:

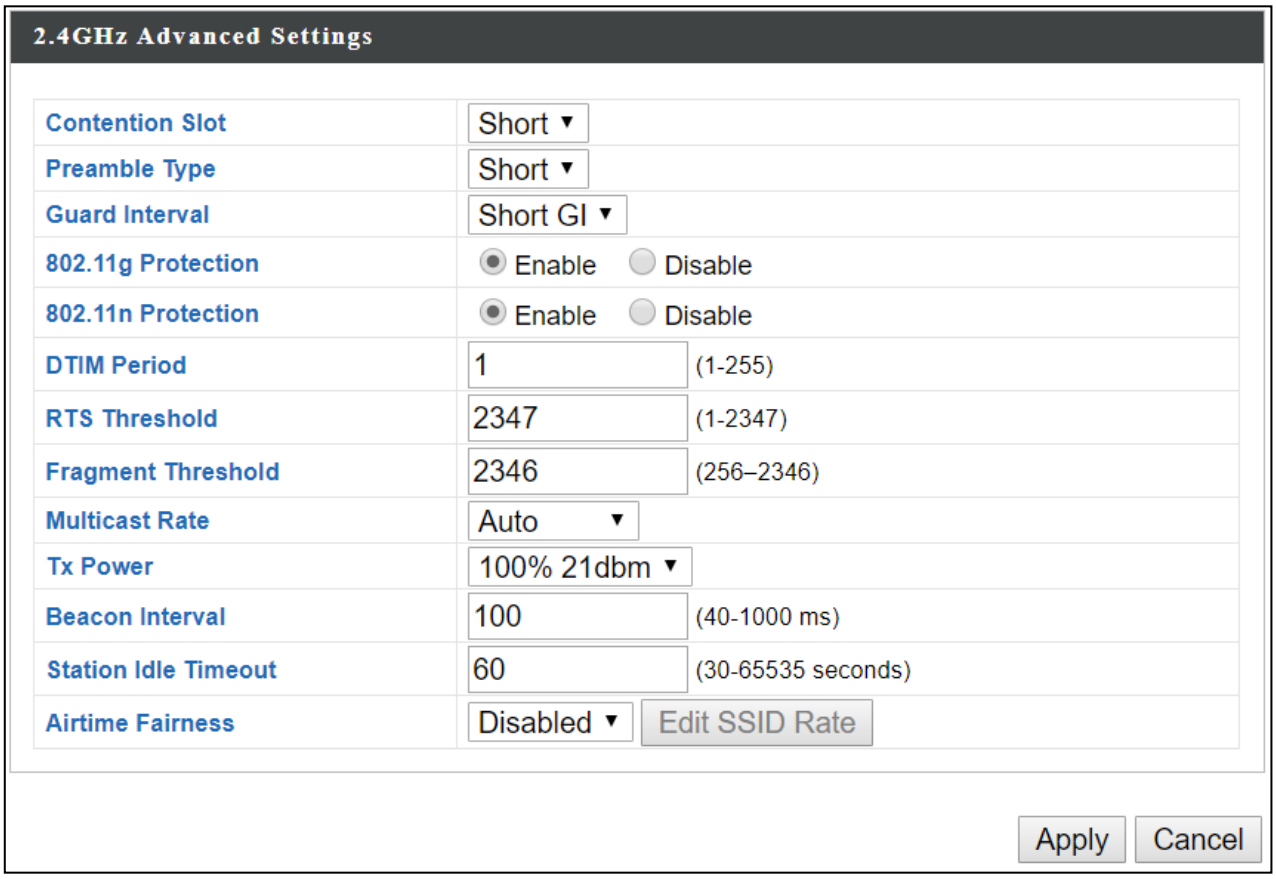


Channel	Select a wireless channel from 1 – 11.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference); or 40MHz (higher performance but potentially higher interference); or Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

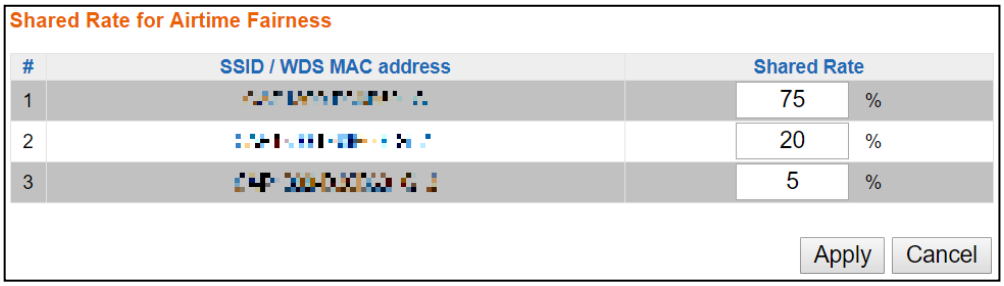
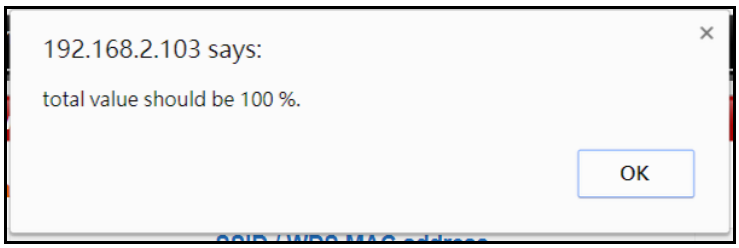
Advanced:

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

Changing these settings can adversely affect the performance of your AP.



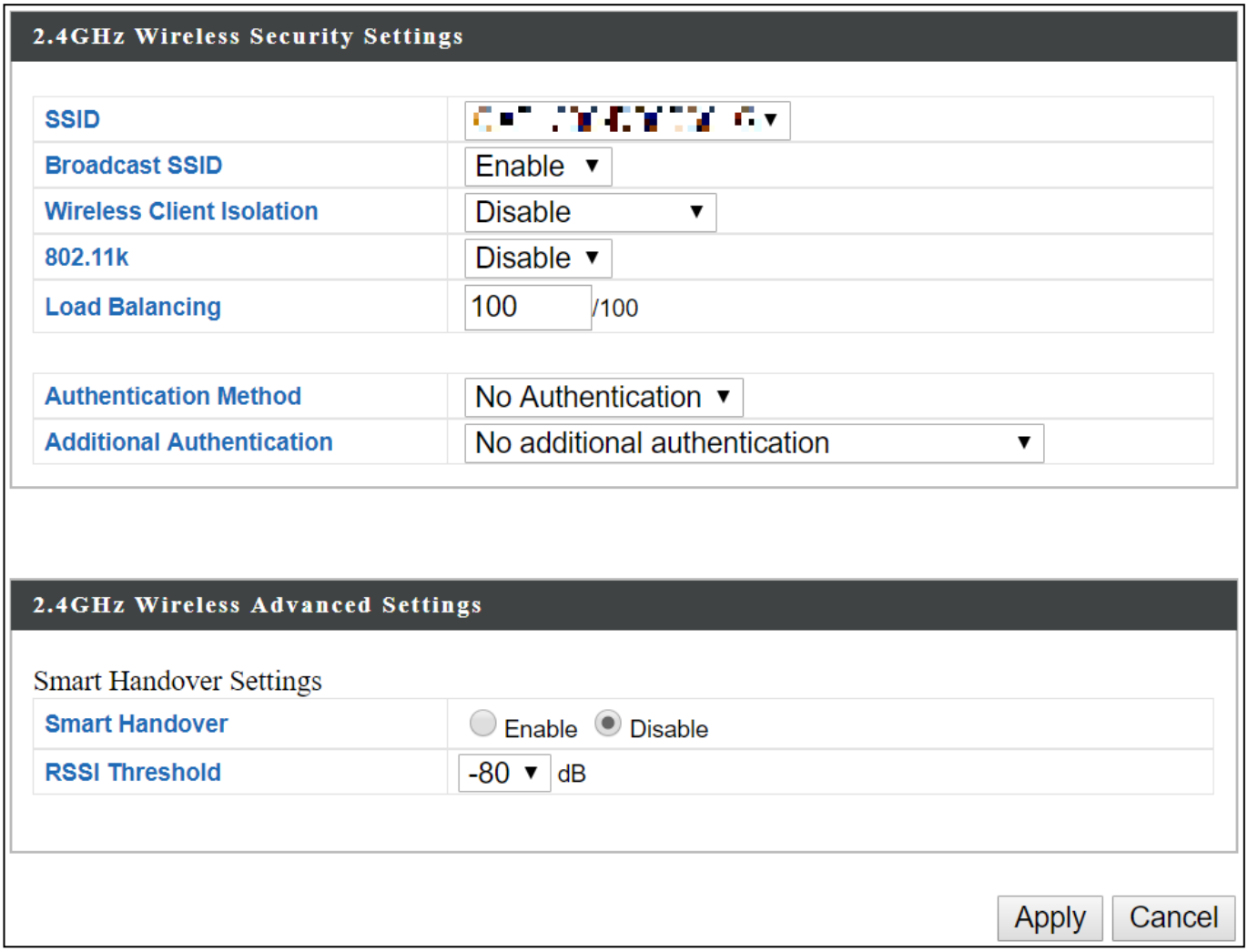
Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM.
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communications defines the length of the CRC (Cyclic Redundancy Check) block for communication between the AP and roaming wireless adapters. The default value is “Short Preamble”.
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11g Protection	Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to AP, and AP will broadcast Clear to Send (CTS), before a packet is sent from client).
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to AP, and AP will broadcast Clear to Send (CTS), before a packet is sent from client).
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting. The range of the transfer rate is between 1Mbps to 54Mbps
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output may enhance security since access to your signal can be potentially prevented from malicious/unknown users in distant areas.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for the AP to send keepalive messages to a wireless client to check if the station is still alive / active.

Airtime Fairness	Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate. Set airtime fairness to “Auto”, “Static” or “Disable”. When “Auto” is selected, the share rate is automatically managed. When “Static” is selected, press “Edit SSID Rate” to enter a % for each SSID’s share rate as shown below:  The % field has to add up to 100% or the system will display a message:  Airtime fairness is disabled if “Disable” is selected.

Security:

The AP provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It is essential to configure wireless security in order to prevent unauthorised access to your network.



SSID Selection	Select a SSID to configure its security settings.
Broadcast SSID	Enable or disable SSID broadcast. Enable: the SSID will be visible to clients as an available Wi-Fi network. Disable: the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the AP from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu and refer to the appropriate information below for your method.

No Authentication / Additional Authentication:

When "No Authentication" is selected in "Authentication Method", extra options are made available in the next line:

Additional Authentication	Select an additional authentication method from the drop down menu or select "No additional authentication" for no authentication, where no password/key is required to connect to the AP. For other options, refer to the information below.

"No additional authentication" is not recommended as anyone can connect to your device's SSID.

Additional wireless authentication methods can be applied to all authentication methods:

WPS must be disabled to use additional authentication.

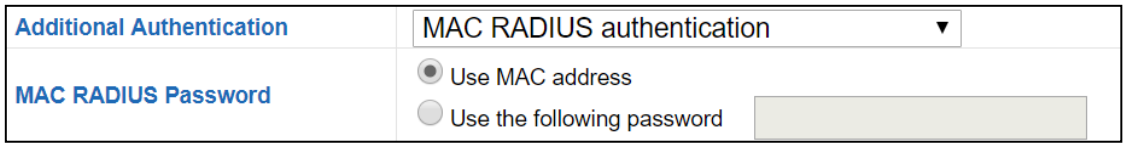
MAC Address Filter:

Restrict wireless clients access based on MAC address specified in the MAC filter table.

MAC-RADIUS Authentication:

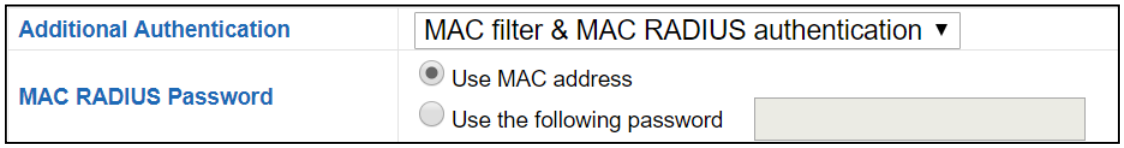
Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.

WPS must be disabled to use MAC-RADIUS authentication.



MAC Filter & MAC-RADIUS Authentication:

Restrict wireless clients access using both of the above MAC filtering & RADIUS authentication methods.

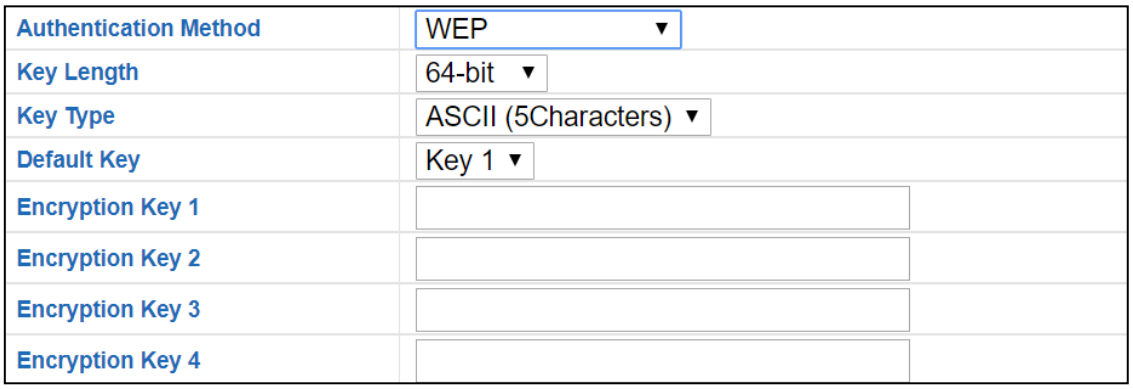


MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select “Use the following password”, enter the password in the field below.

WEP:

WEP (Wired Equivalent Privacy) is a basic encryption type.
When selected, a notice will pop-up as exemplified below:

Below is a figure showing the configurable fields:

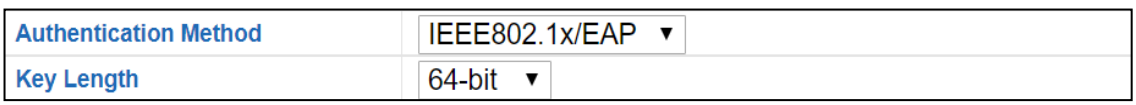


Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
Key Type	Choose from “ASCII” (any alphanumerical character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key (1 – 4 below) is the default key. For security purposes, you can set up to four keys (below) and change which is the default key.
Encryption Key 1 – 4	Enter your encryption key/password according to the format you selected above.

For a higher level of security, please consider using WPA encryption.

IEEE802.1x/EAP:

Below s a figure showing the configurable fields:

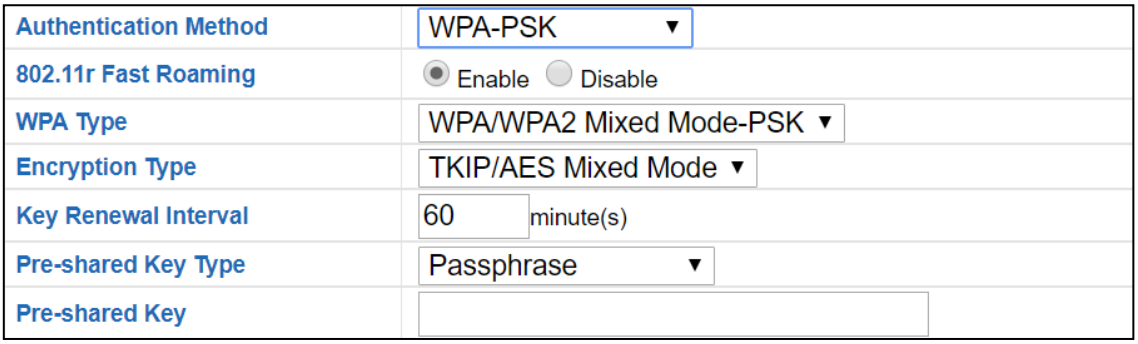


Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.

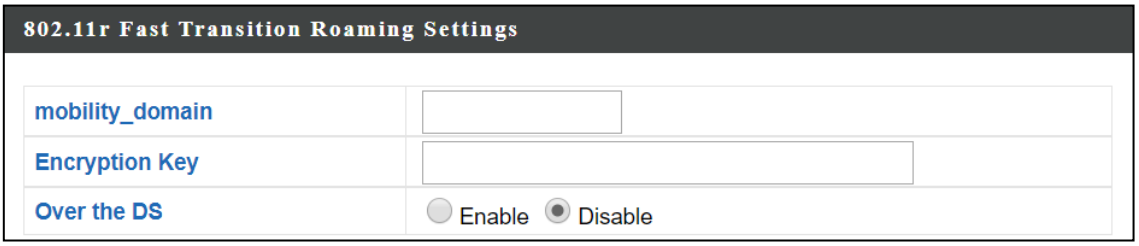
WPA-PSK:

WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

Below is a figure showing the configurable fields:



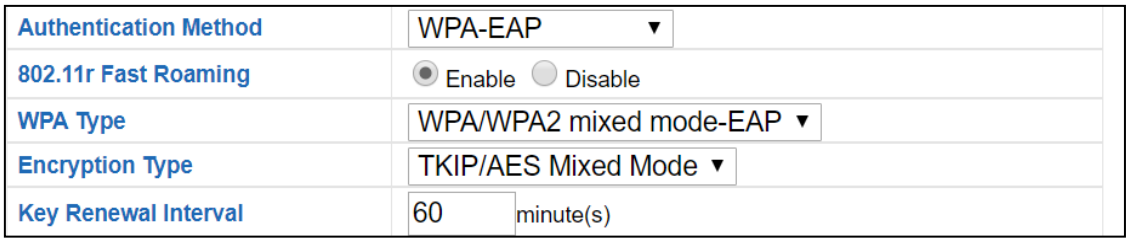
Fast Roaming Settings will also be shown:



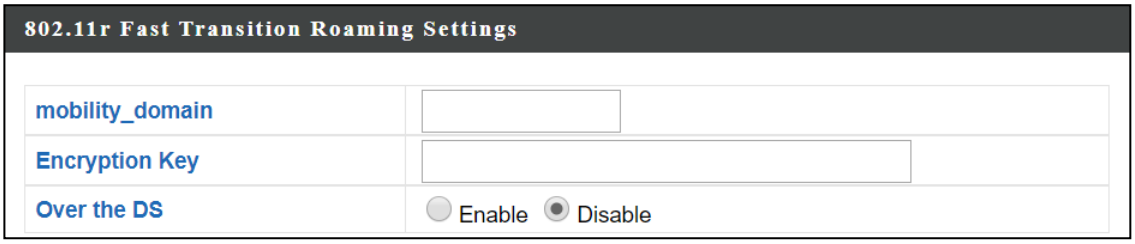
802.11r Fast Roaming	When your device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both preshared key (PSK) and 802.1X authentication methods.
WPA Type	Select from WPA/WPA2 Mixed Mode-PSK, WPA2 or WPA only. WPA2 is safer than WPA, but is not supported by all wireless clients. Please make sure your wireless client supports your selection.
Encryption	Select “TKIP/AES Mixed Mode” or “AES” encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.
Pre-Shared Key Type	Choose from “Passphrase” (8 – 63 alphanumeric characters) or “Hex” (up to 64 characters from 0-9, a-f and A-F).
Pre-Shared Key	Please enter a security key/password according to the format you selected above.

802.11r Fast Transition Roaming Settings	
Mobility_domain	Specify the mobility domain (2.4GHz or 5GHz)
Encryption Key	Specify the encryption key
Over the DS	Enable or disable this function.

WPA-EAP:



Fast Roaming Settings will also be shown:



WPA Type	Select from WPA/WPA2 Mixed Mode-EAP, WPA2-EAP or WPA-EAP.
Encryption Type	Select “TKIP/AES Mixed Mode” or “AES” encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.

WPA-EAP must be disabled to use MAC-RADIUS authentication.

802.11r Fast Transition Roaming Settings	
Mobility_domain	Specify the mobility domain (2.4GHz or 5GHz)
Encryption Key	Specify the encryption key
Over the DS	Enable or disable this function.

WDS:

Wireless Distribution System (WDS) can bridge/repeat APs together in an extended network. WDS settings can be configured as shown below.

When using WDS, configure the IP address of each AP to be in the same subnet and ensure there is only one active DHCP server among connected APs, preferably on the WAN side.

WDS must be configured on each AP, using correct MAC addresses. All APs should use the same wireless channel and encryption method.

2.4GHz

WDS Functionality	Disabled ▼
Local MAC Address	80:1F:02:F1:96:8A

WDS Peer Settings

WDS #1	MAC Address
WDS #2	MAC Address
WDS #3	MAC Address
WDS #4	MAC Address

WDS VLAN

VLAN Mode	Untagged Port ▼ (Enter at least one MAC address.)
VLAN ID	1

WDS Encryption method

Encryption	None ▼ (Enter at least one MAC address.)

Apply Reset

2.4GHz	
WDS Functionality	Select “WDS with AP” to use WDS with AP or “WDS Dedicated Mode” to use WDS and also block communication with regular wireless clients. When WDS is used, each AP should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your AP.

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDS devices you wish to connect.

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

WDS Encryption method	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES consisting of 8-63 alphanumeric characters.

Guest Network:

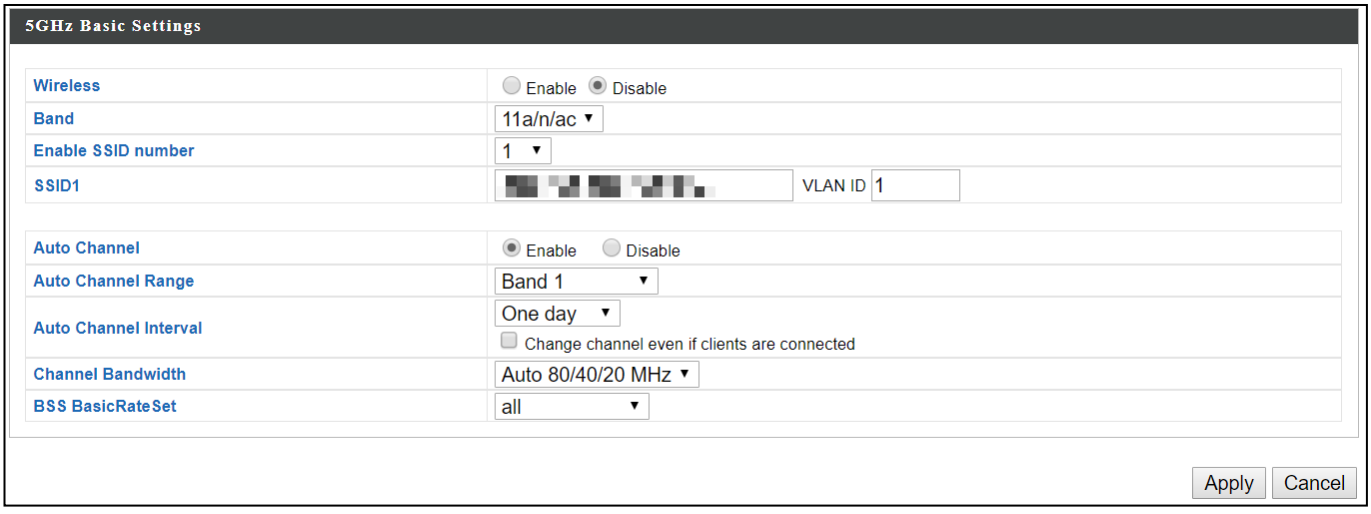
Enable / disable guest network to allow clients to connect as guests.

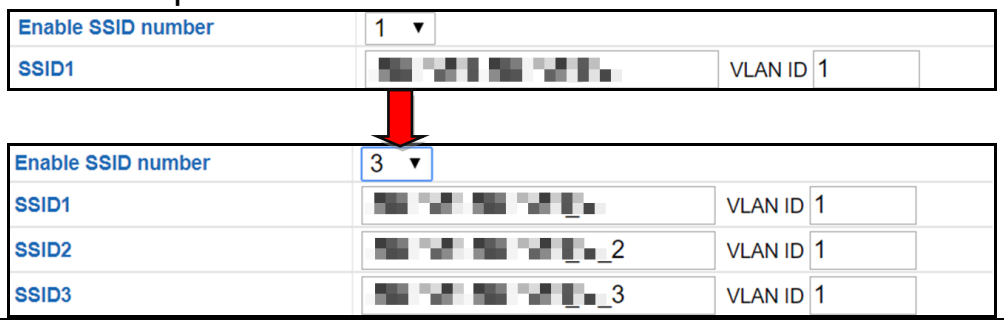
iii. 5GHz 11ac 11an

The “5GHz 11ac 11an” menu allows you to view and configure information for your AP’s 5GHz wireless network across five categories: Basic, Advanced, Security, WDS & Guest Network.

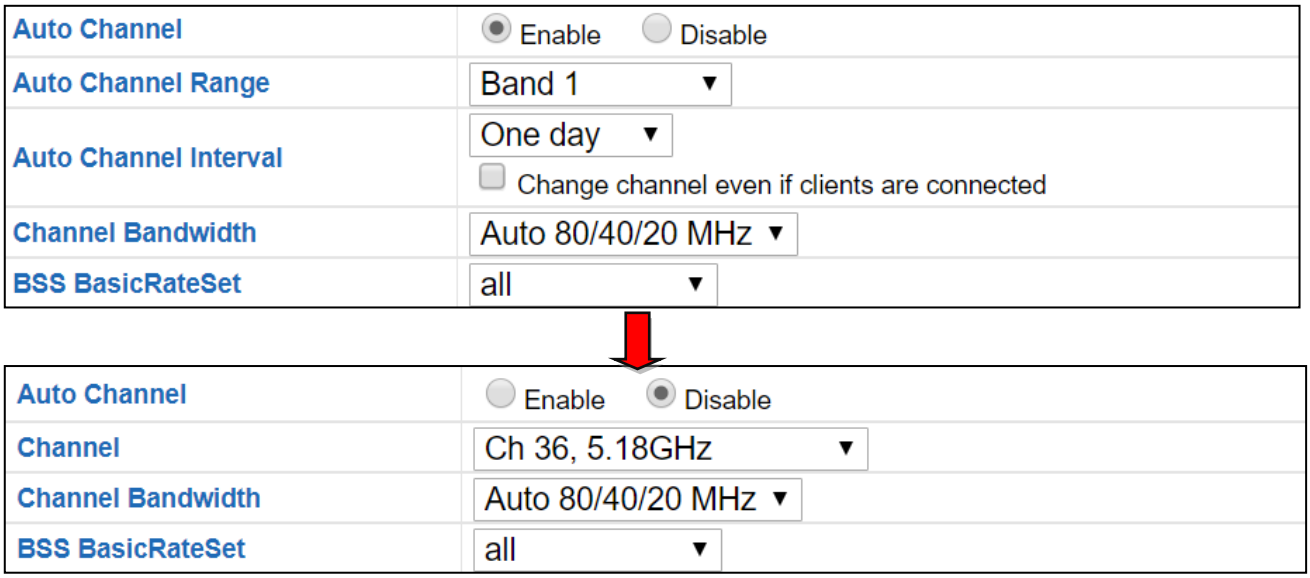
Basic:

The “Basic” screen displays basic settings for your AP’s 5GHz Wi-Fi network (s).



Wireless	Enable or disable the AP's 5GHz wireless radio. When disabled, no 5GHz SSIDs will be active.
Band	Wireless standard used for the AP. Combinations of 802.11a, 802.11n & 802.11ac can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of 16 can be enabled. 
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the AP's 5GHz frequency based on availability and potential interference. When disabled, configurable fields will change as shown below:
Auto Channel Range	Select a range to which auto channel selection can choose from.
Auto Channel Interval	Select a time interval for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Select the channel bandwidth: 20MHz (lower performance but less interference); or Auto 40/20 MHz; or Auto 80/40/20 MHz (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

When auto channel is disabled, configurable fields will change. Select a wireless channel manually:

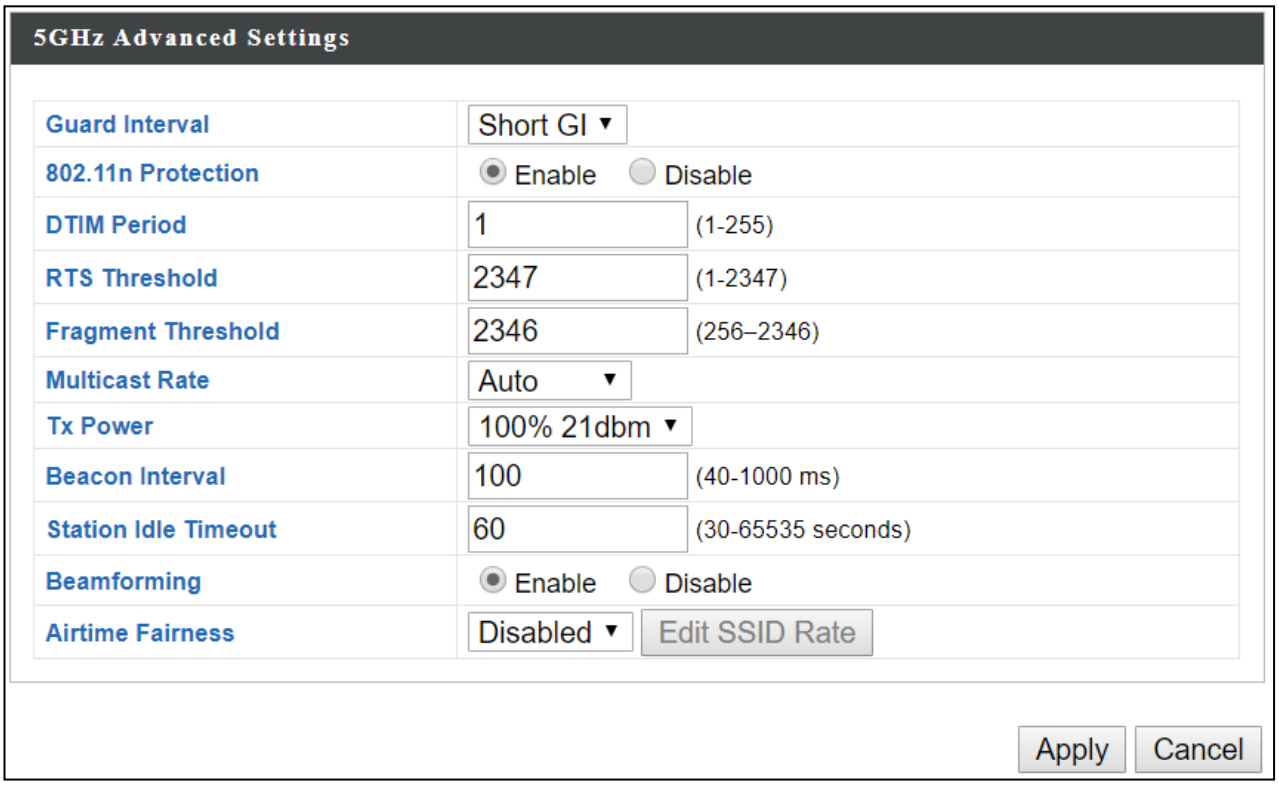


Channel	Select a wireless channel.
Channel Bandwidth	Select the channel bandwidth: - 20MHz (lower performance but less interference) - Auto 40/20 MHz - Auto 80/40/20 MHz (automatically select based on interference level)
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

Advanced:

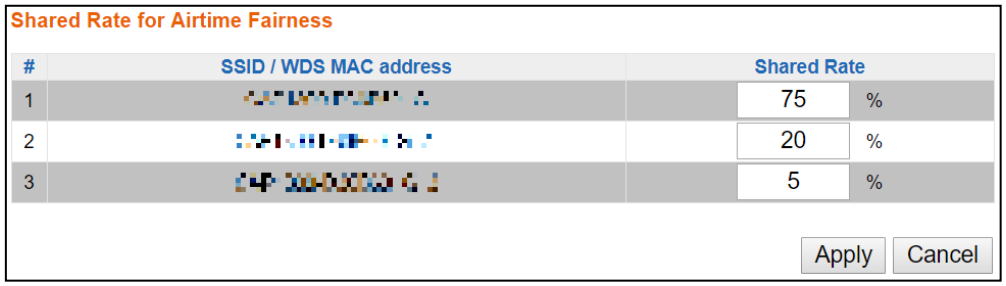
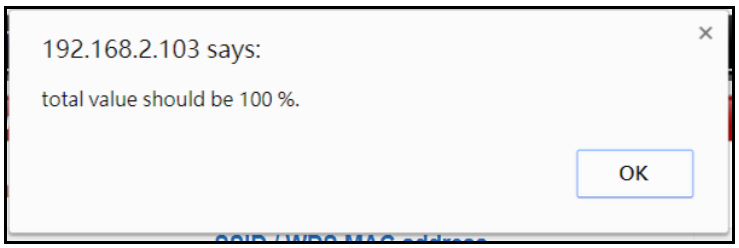
These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

Changing these settings can adversely affect the performance of your AP.



Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to AP, and AP will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. (The default value is 1)
RTS Threshold	Set the RTS threshold of the wireless radio. (The default value is 2347)
Fragment Threshold	Set the fragment threshold of the wireless radio. (The default value is 2346)

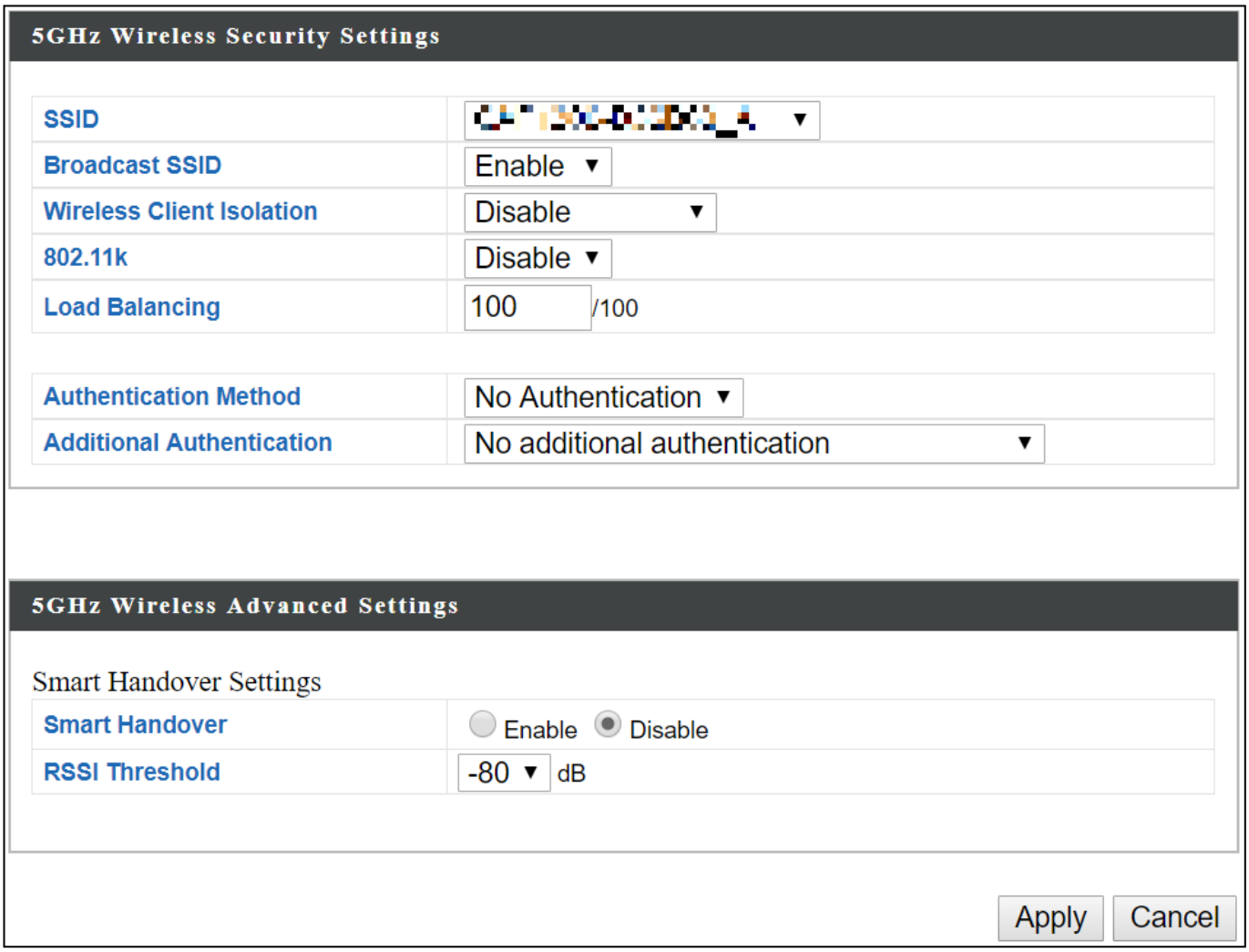
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the AP to a wireless client to verify if the station is still alive/active.
Beamforming	Beamforming is a signal processing technique used in sensor arrays for directional signal transmission or reception. This is achieved by combining elements in an antenna array in such a way that signals at particular angles experience constructive interference while others experience destructive interference. Beamforming can be used at both the transmitting and receiving ends in order to achieve spatial selectivity. The improvement compared with omnidirectional reception / transmission is known as the directivity of the array.

Airtime Fairness	Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate. Set airtime fairness to “Auto”, “Static” or “Disable”. When “Auto” is selected, the share rate is automatically managed. When “Static” is selected, press “Edit SSID Rate” to enter a % for each SSID’s share rate as shown below:  The % field has to add up to 100% or the system will display a message:  Airtime fairness is disabled if “Disable” is selected.

Security:

The AP provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

It's essential to configure wireless security in order to prevent unauthorised access to your network.



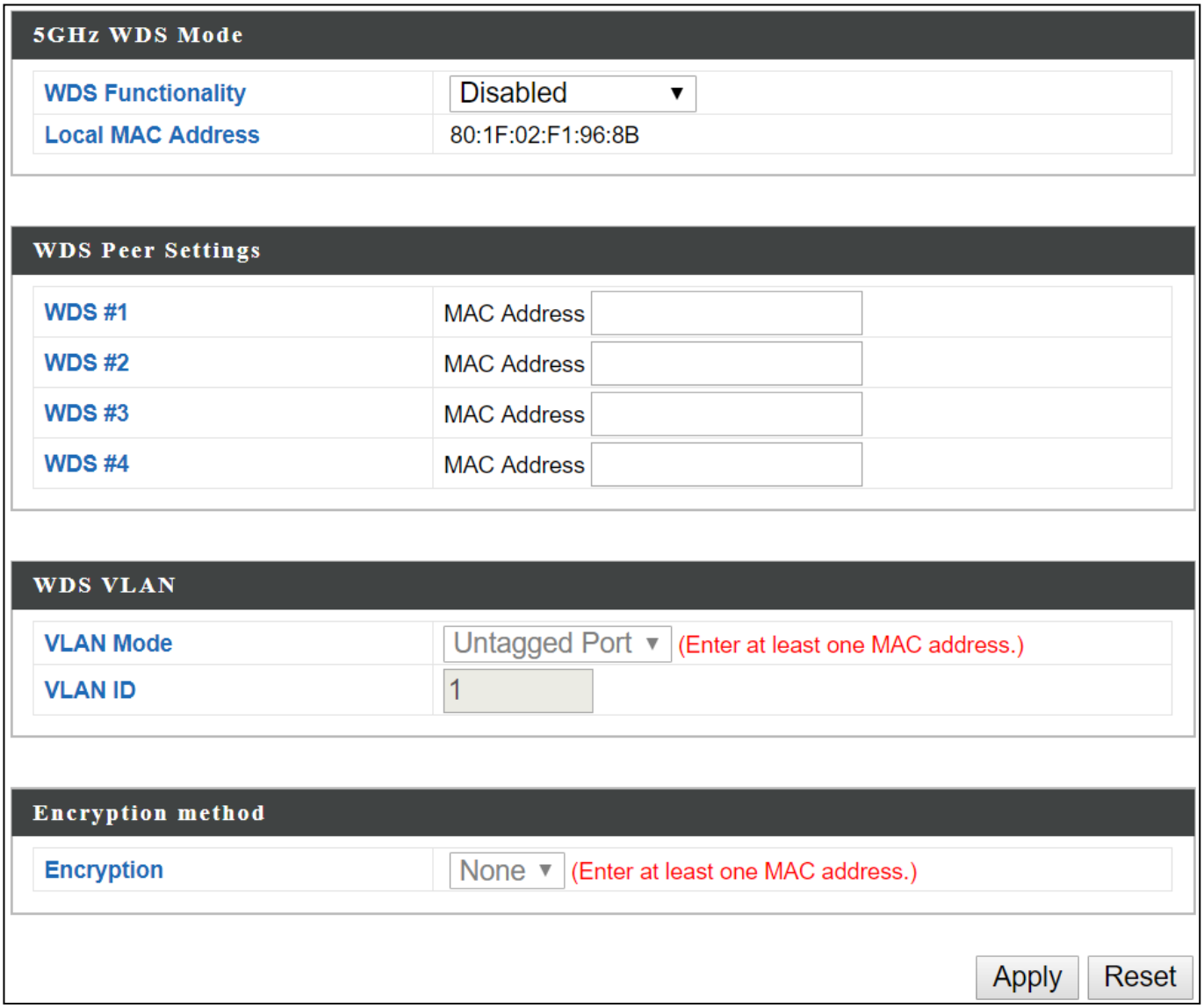
SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the AP from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu.

WDS:

Wireless Distribution System (WDS) can bridge/repeat APs together in an extended network. WDS settings can be configured as shown below.

When using WDS, configure the IP address of each AP to be in the same subnet and ensure there is only one active DHCP server among connected APs, preferably on the WAN side.

WDS must be configured on each AP, using correct MAC addresses. All APs should use the same wireless channel and encryption method.



5GHz WDS Mode	
WDS Functionality	Select “WDS with AP” to use WDS with AP or “WDS Dedicated Mode” to use WDS and also block communication with regular wireless clients. When WDS is used, each AP should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your AP.

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDA devices you wish to connect.

WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

WDS Encryption	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES with 8-63 alphanumeric characters.

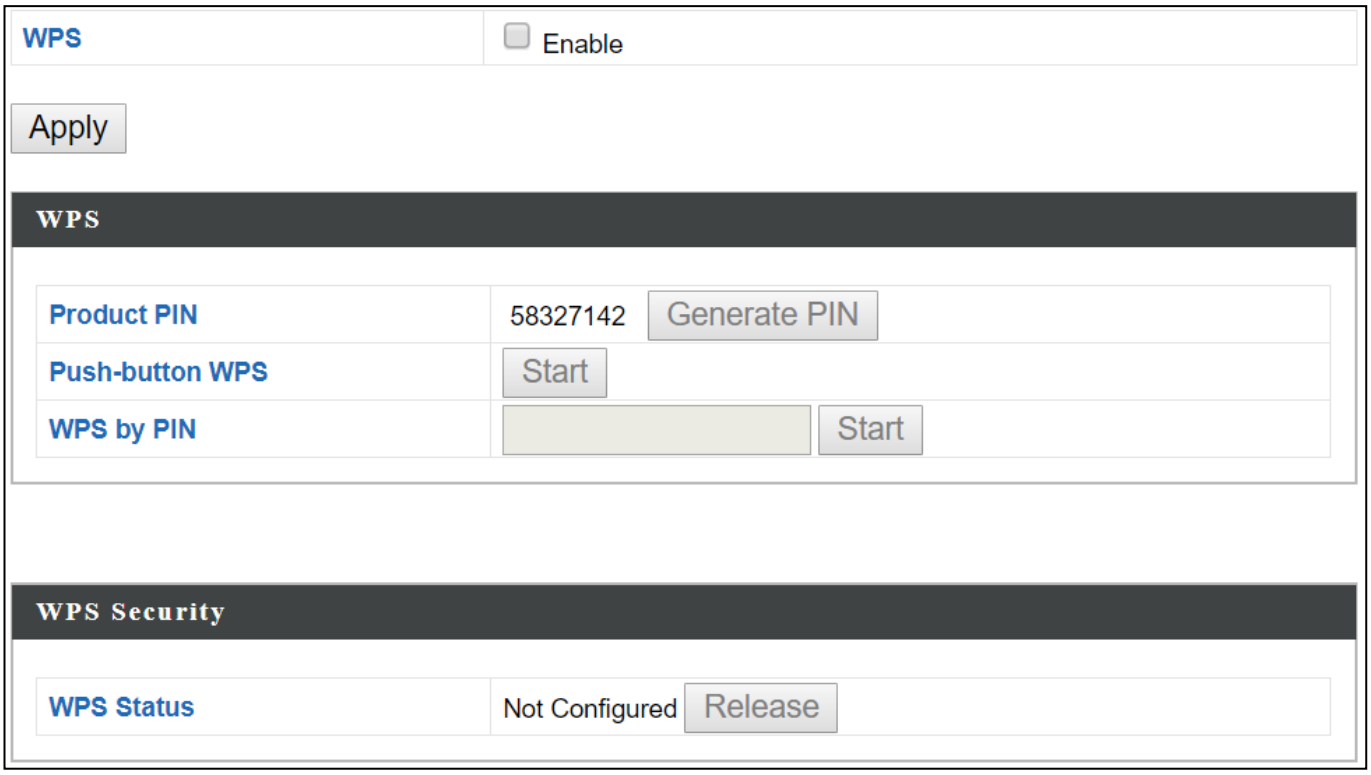
Guest Network:

Enable / disable guest network to allow clients to connect as guests.

iv. WPS

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the compatible device or from within the compatible device's firmware / configuration interface (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

Please refer to the manufacturer's instructions of your WPS device.



WPS	Check/uncheck this box to enable/disable WPS functionality. WPS must be disabled when using MAC-RADIUS authentication.

WPS	
Product PIN	Displays the WPS PIN code of the device, used for PIN code WPS. You will be required to enter this PIN code into another WPS device for PIN code WPS. Click “Generate PIN” to generate a new WPS PIN code.
Push-Button WPS	Click “Start” to activate WPS on the AP for approximately 2 minutes.
WPS by PIN	Enter the PIN code of another WPS device and click “Start” to attempt to establish a WPS connection. WPS function will last for approximately 2 minutes.

WPS Security	
WPS Status	WPS security status is displayed here. Click “Release” to clear the existing status.

v. RADIUS

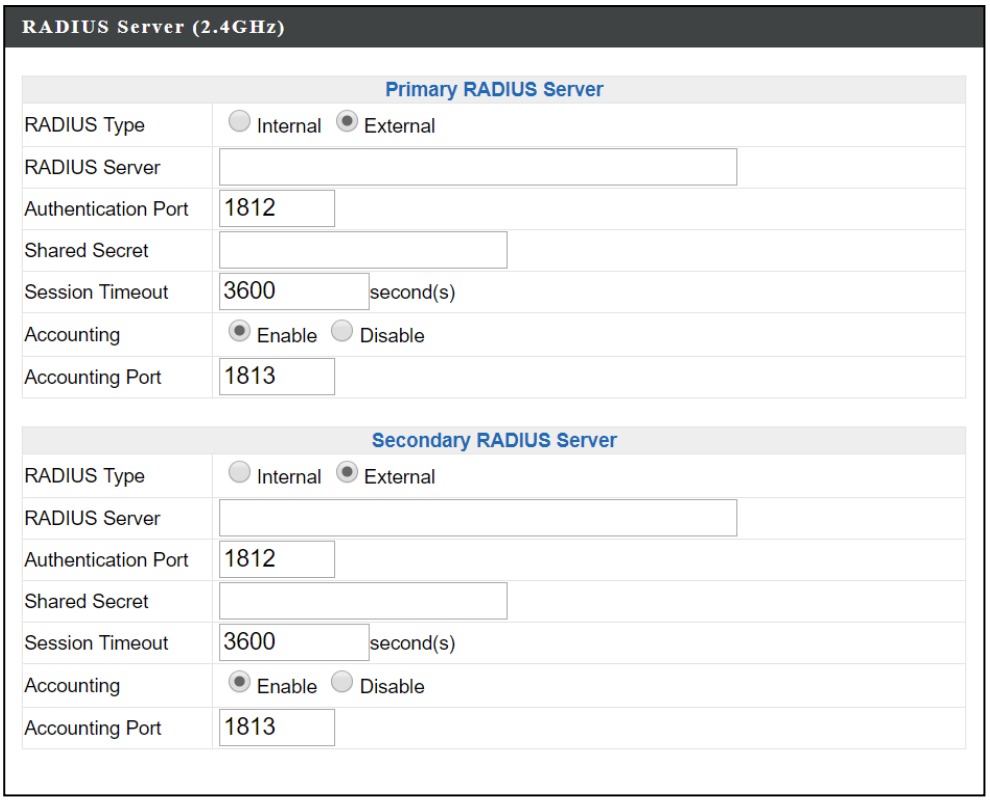
The RADIUS menu allows you to configure the AP's external RADIUS server settings.

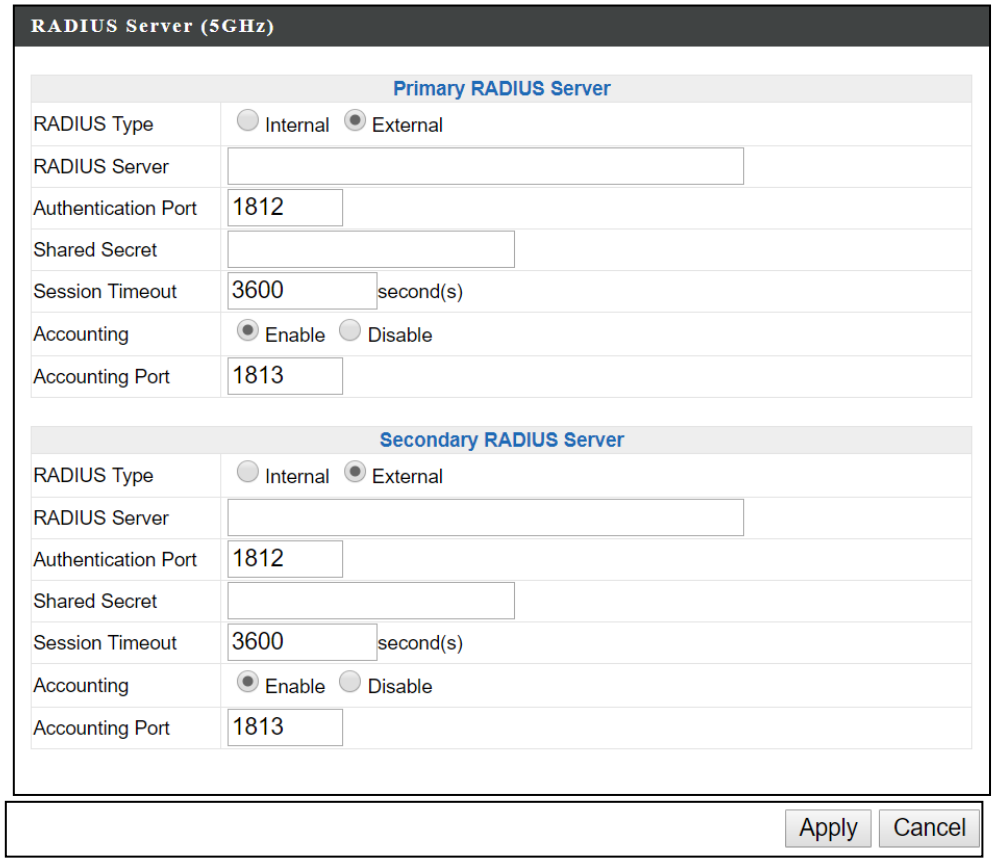
A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The AP can utilize a primary and a secondary (backup) external RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz).

RADIUS Settings:

Configure the RADIUS server settings for 2.4GHz and 5GHz. Each frequency can use an internal or external RADIUS server.

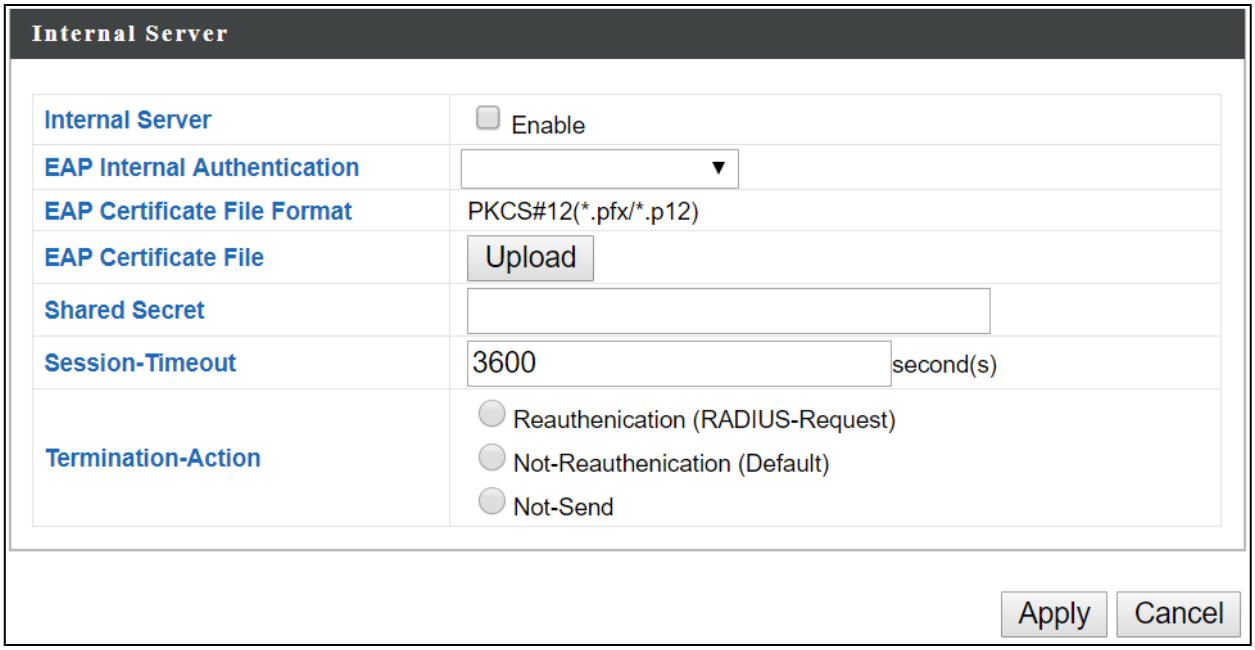




RADIUS Type	Select “Internal” to use the AP’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Accounting	Enable or disable RADIUS accounting.
Accounting Port	When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between 1 – 65535.

Internal Server:

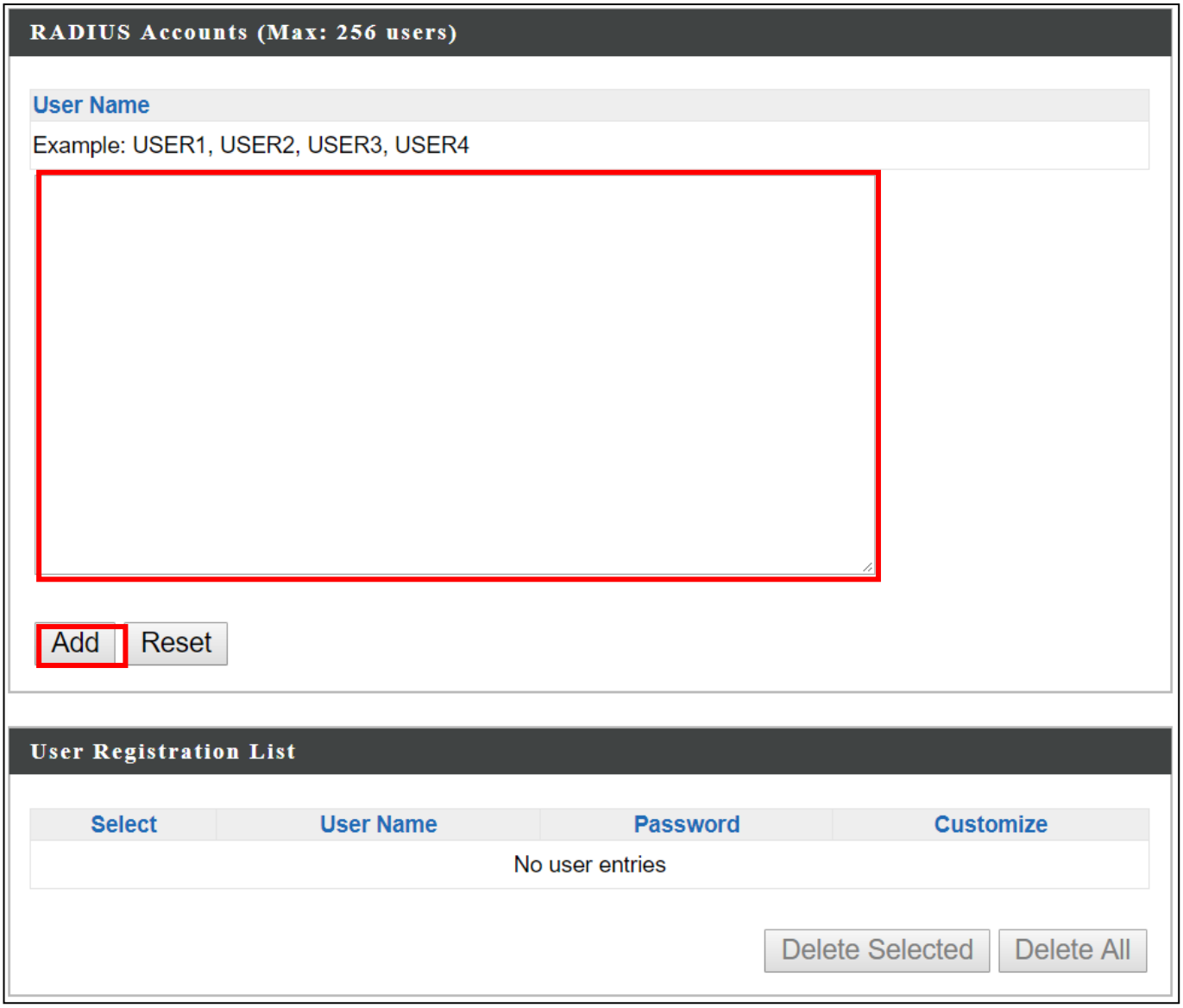
The AP features a built-in RADIUS server which can be configured as shown below.



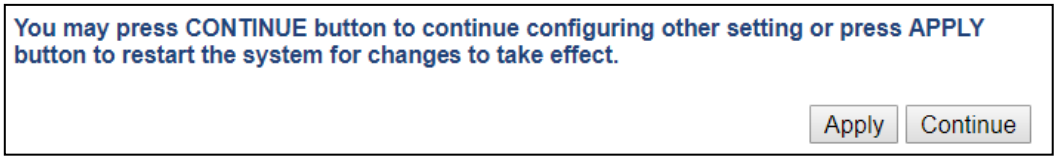
Internal Server	Check/uncheck to enable/disable the AP's internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click "Upload" to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.
Shared Secret	Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Termination Action	Select a termination-action attribute: Reauthentication: sends a RADIUS request to the AP Not-Reauthentication: sends a default termination-action attribute to the AP Not-Send: no termination-action attribute is sent to the AP.

RADIUS Accounts:

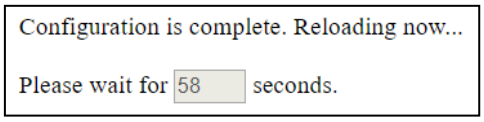
The internal RADIUS server can authenticate up to 256 user accounts. The "RADIUS Accounts" page allows you to configure and manage users.



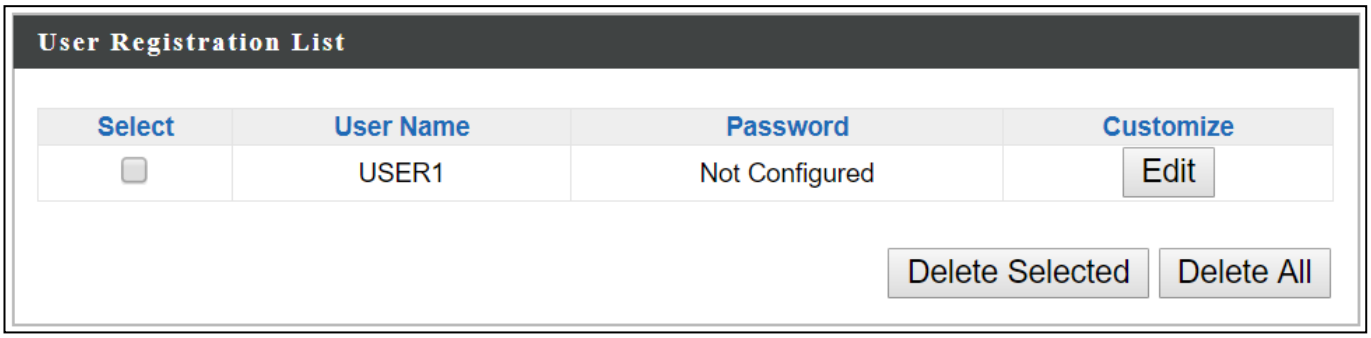
Enter a username in the box below and click "Add" to add the username. The webpage will display the message below:



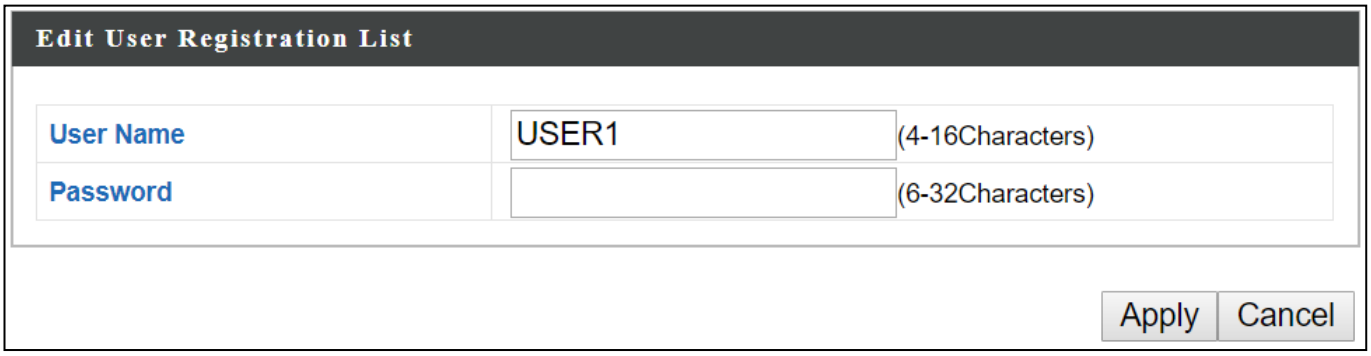
If you choose to apply the settings (by clicking “Apply”), your system will restart the system with a message shown below:



Press “Continue” to see the new user registration list.



Select “Edit” to edit the username and password of the RADIUS account:



User Name	Enter the user names here, separated by commas.
Add	Click “Add” to add the user to the user registration list.
Reset	Clear text from the user name box.

Select	Check the box to select a user.
User Name	Displays the user name.
Password	Displays if specified user name has a password (configured) or not (not configured).
Customize	Click “Edit” to open a new field to set/edit a password for the specified user name (below).

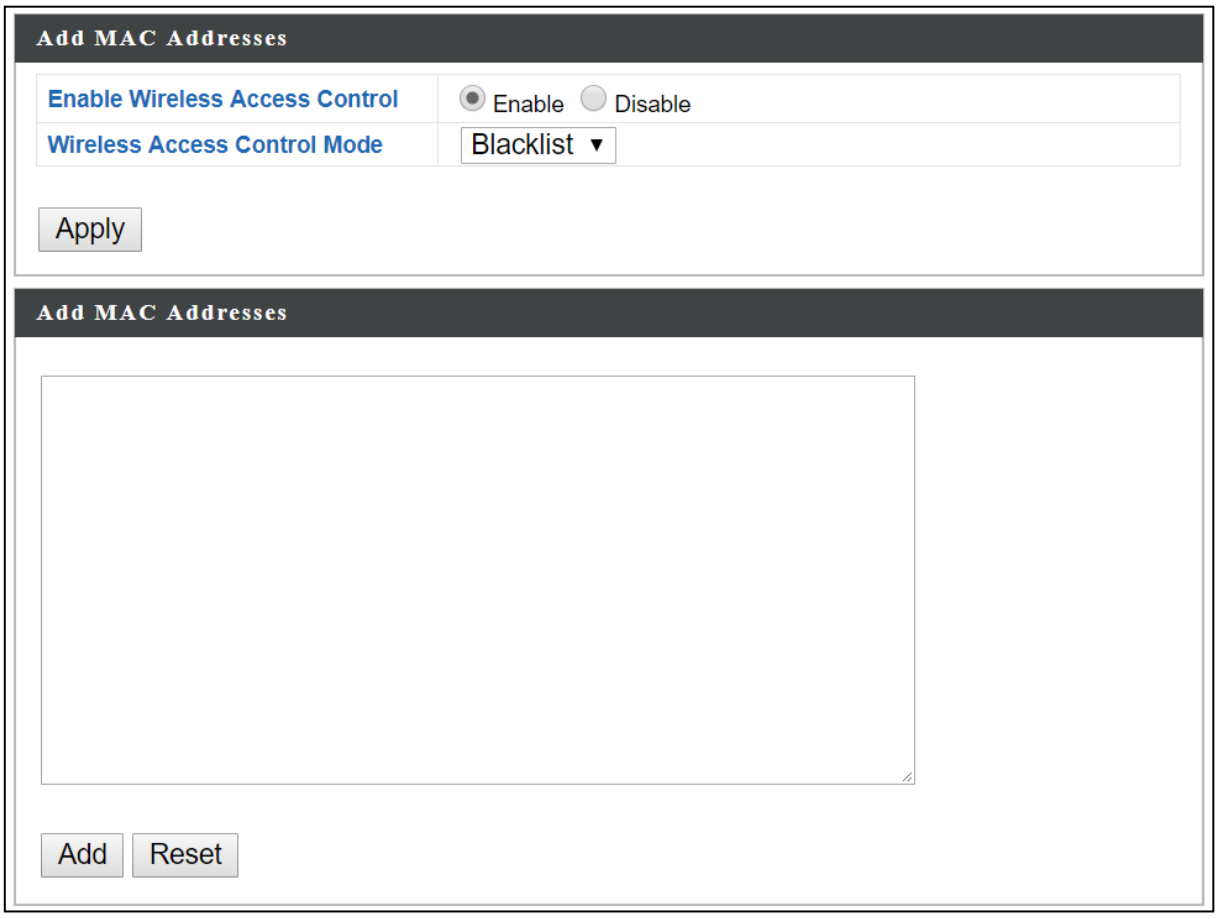
Delete Selected	Delete selected user from the user registration list.
Delete All	Delete all users from the user registration list.

vi. MAC Filter

MAC filtering is a security feature that can help to prevent unauthorized users from connecting to your AP.

This function allows you to define a list of network devices permitted to connect to the AP. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the AP, it will be denied.

The MAC address filtering table is displayed below:



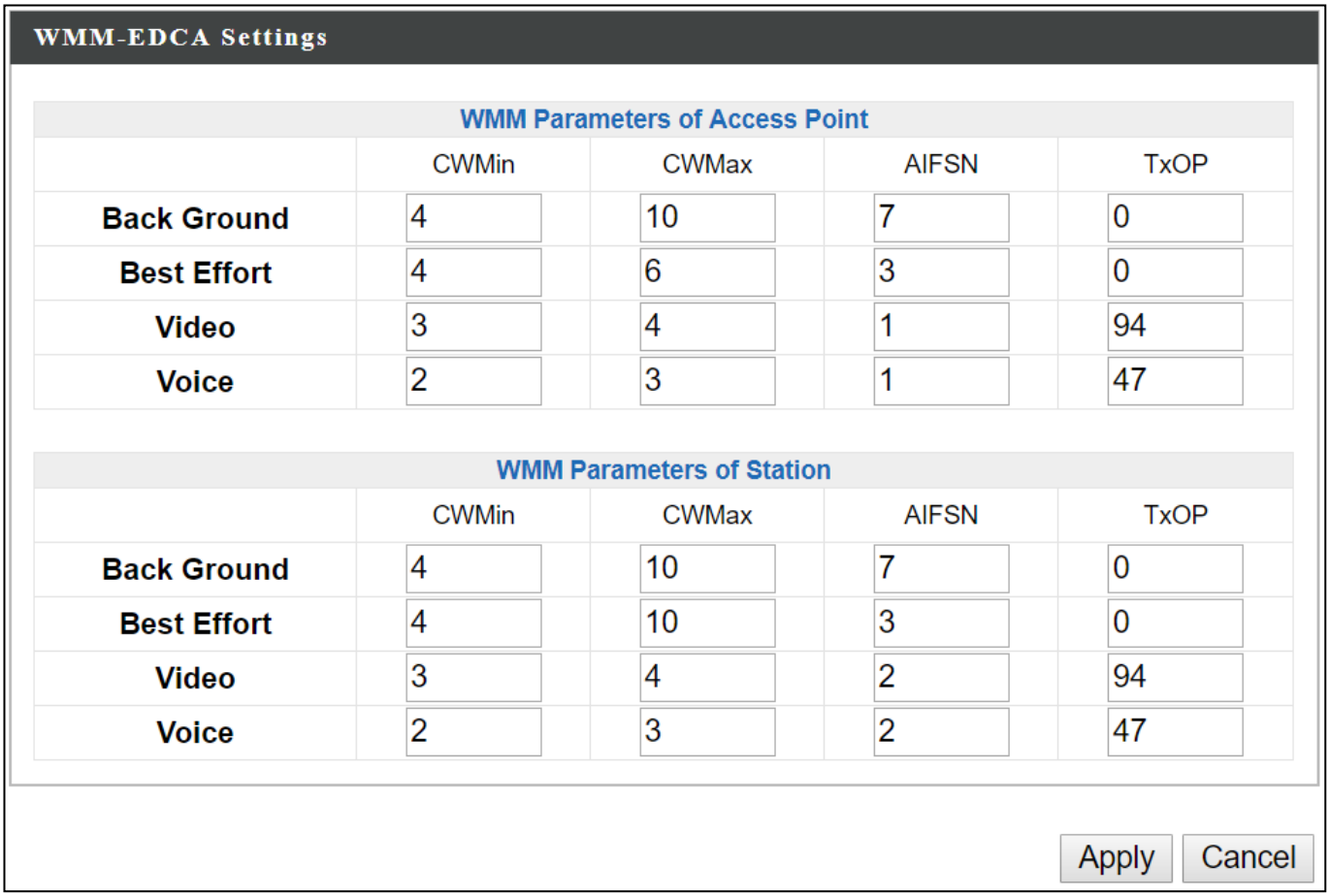
Add MAC Address	Enter a MAC address of computer or network device manually e.g. ‘aa-bb-cc-dd-ee-ff’ or enter multiple MAC addresses separated with commas, e.g. ‘aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg’
Add	Click “Add” to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

MAC address entries will be listed in the “MAC Address Filtering Table”. Select an entry using the “Select” checkbox.

Select	Delete selected or all entries from the table.
MAC Address	The MAC address is listed here.
Delete Selected	Delete the selected MAC address from the list.
Delete All	Delete all entries from the MAC address filtering table.
Export	Click “Export” to save a copy of the MAC filtering table. A new window will pop up for you to select a location to save the file.

vii. WMM

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.



Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

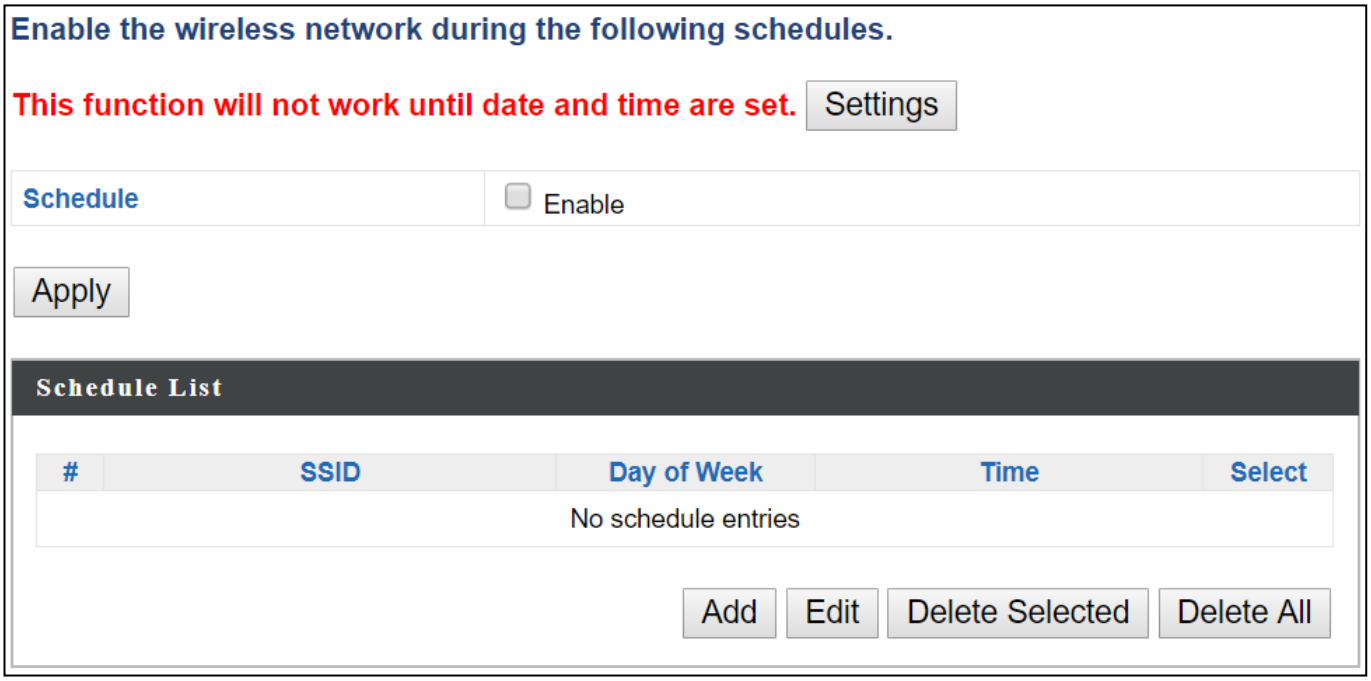
Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
Best Effort	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP and streaming media with minimum time delay.

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can be adjusted further manually:

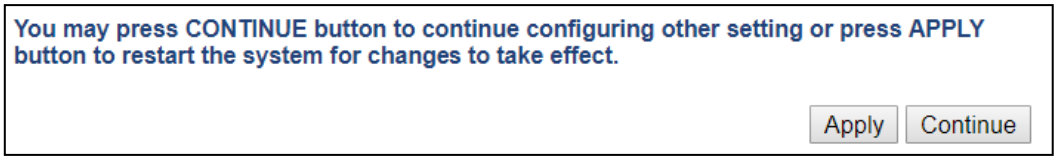
CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value reaches the number defined by CWMax (below). The CWMin value must be lower than the CWMax value. The contention window scheme helps to avoid frame collisions and determine priority of frame transmission. A shorter window has a higher probability (priority) of transmission.
CWMax	Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above).
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
TxOP	Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized. A value of 0 means only one frame per transmission. A greater value means higher priority.

viii. Schedule

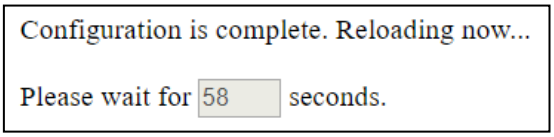
The schedule feature allows you to automate the wireless network for the specified time ranges. Wireless scheduling can save energy and increase the security of your network.



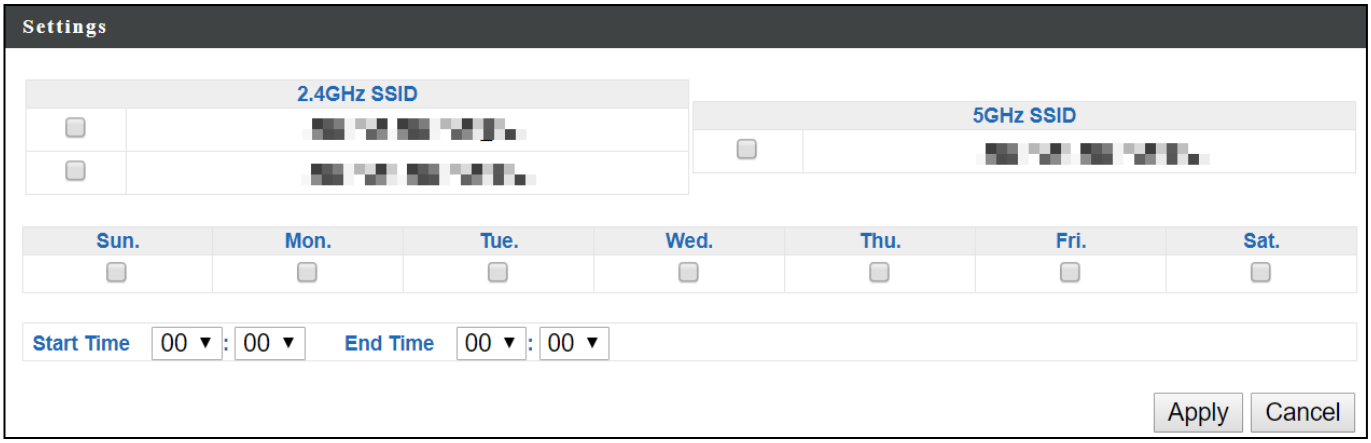
1. Select “Add” to add a schedule.
   The webpage will display the message below:



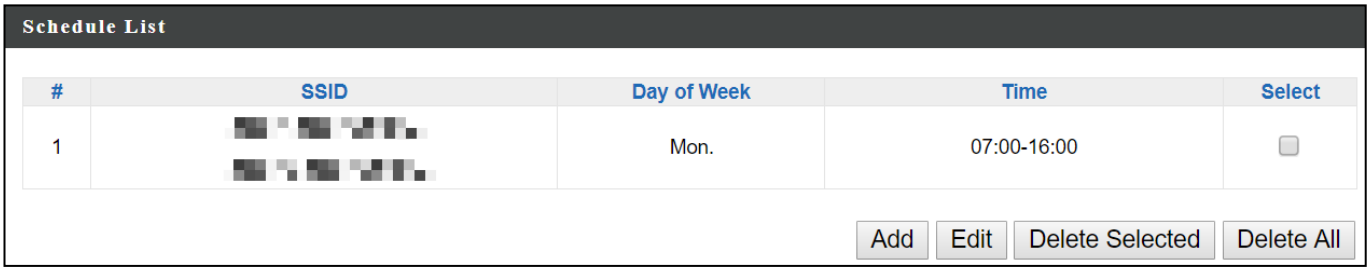
   If you choose to apply the settings (by clicking “Apply”), your system will restart the system with a message shown below:



2. Settings page will be shown if “Continue” is selected:
Check/uncheck the box of the desired SSID network, day of schedule and select the Start Time and End Time (using the dropdown menu).
Select “Apply” to apply the settings, or “Cancel” to forfeit the schedule.



Schedules will be shown in the Schedule List as exemplified below:



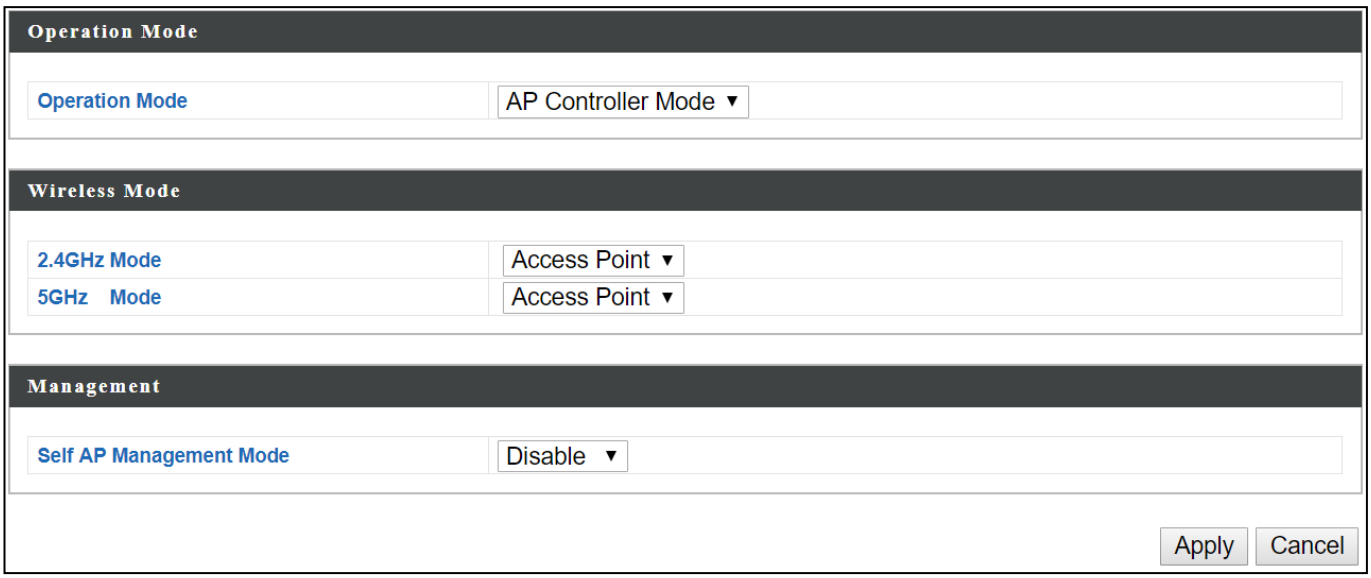
VI-9. Local Settings

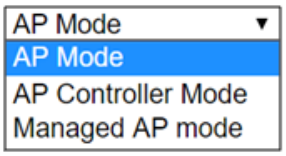
i. Operation Mode

The AP can function in five different modes. Set the operation mode of the AP here.

1. AP Mode: The device acts as a standalone AP

2. AP controller Mode: The device acts as the designated master of the AP array
3. Managed AP Mode: The device acts as a slave AP within the AP array.



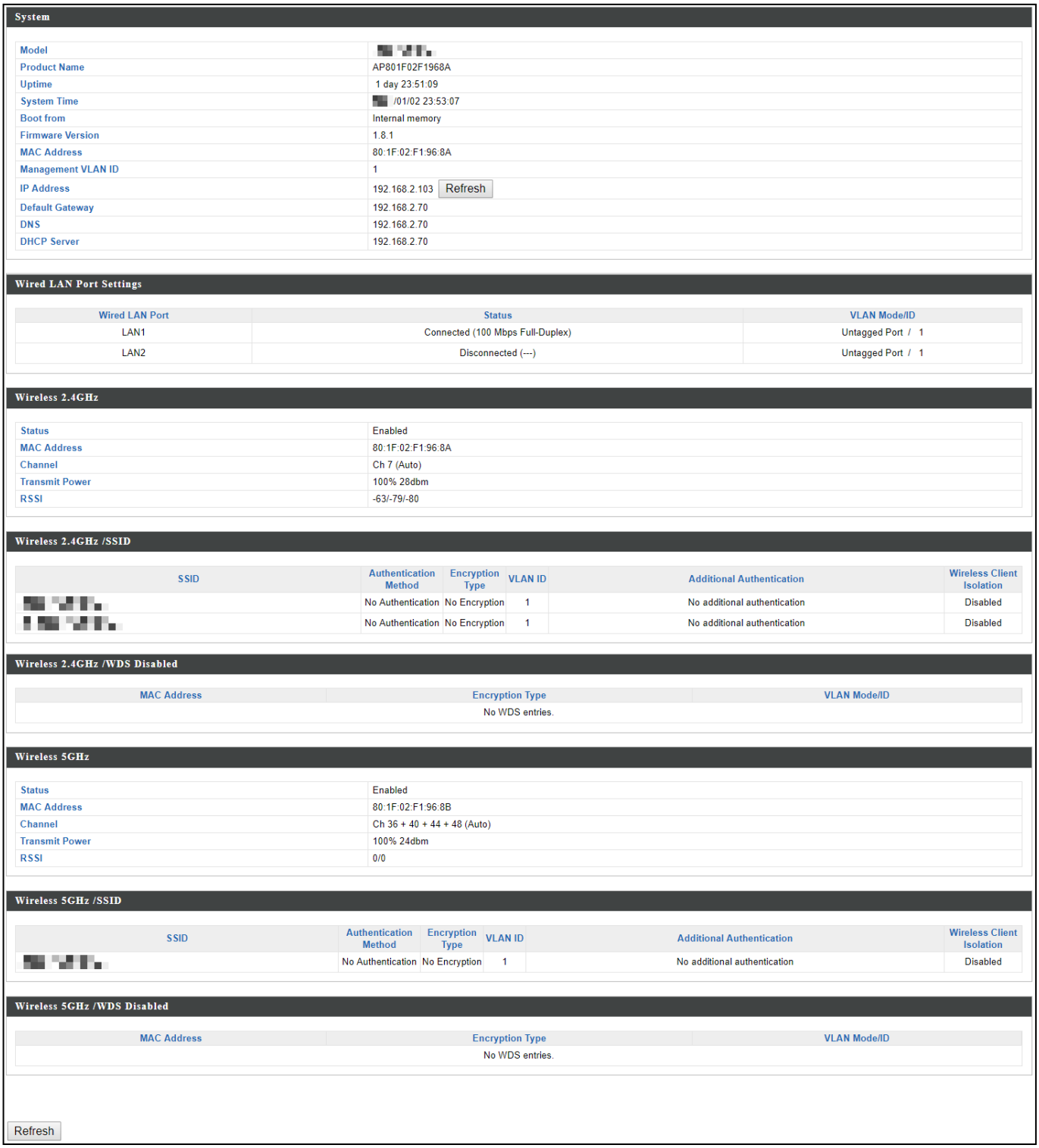


In Managed AP mode some functions of the AP will be disabled in this user interface and must be set using Edimax Pro NMS on the AP Controller.

In AP Controller Mode the AP will switch to the Edimax Pro NMS user interface.

System Information:

“System Information” page displays basic system information.



System

Model	[redacted]
Product Name	AP801F02F1968A
Uptime	1 day 23:51:09
System Time	[redacted] /01/02 23:53:07
Boot from	Internal memory
Firmware Version	1.8.1
MAC Address	80:1F:02:F1:96:8A
Management VLAN ID	1
IP Address	192.168.2.103 Refresh
Default Gateway	192.168.2.70
DNS	192.168.2.70
DHCP Server	192.168.2.70

Wired LAN Port Settings

Wired LAN Port	Status	VLAN Mode/ID
LAN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1

Wireless 2.4GHz

Status	Enabled
MAC Address	80:1F:02:F1:96:8A
Channel	Ch 7 (Auto)
Transmit Power	100% 28dbm
RSSI	-63/-79/-80

Wireless 2.4GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
[redacted]	No Authentication	No Encryption	1	No additional authentication	Disabled
[redacted]	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 2.4GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

Wireless 5GHz

Status	Enabled
MAC Address	80:1F:02:F1:96:8B
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Transmit Power	100% 24dbm
RSSI	0/0

Wireless 5GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
[redacted]	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 5GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

Refresh

System	
Model	Displays the model number of the AP.
Product Name	Displays the product name for reference, which consists of “AP” plus the MAC address.
Uptime	Displays the total time since the device was turned on.
System Time	Displays the system time.
Boot From	Displays information for the booted hardware, booted from internal memory.
Firmware Version	Displays the firmware version.
MAC Address	Displays the AP’s MAC address.
Management VLAN ID	Displays the management VLAN ID.
IP Address	Displays the IP address of this device. Click “Refresh” to update this value.
Default Gateway	Displays the IP address of the default gateway.
DNS	IP address of DNS (Domain Name Server)
DHCP Server	IP address of DHCP Server.

Wired LAN Port Settings	
Wired LAN Port	Specifies which LAN port (1 or 2).
Status	Displays the status of the specified LAN port (connected or disconnected).
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port.

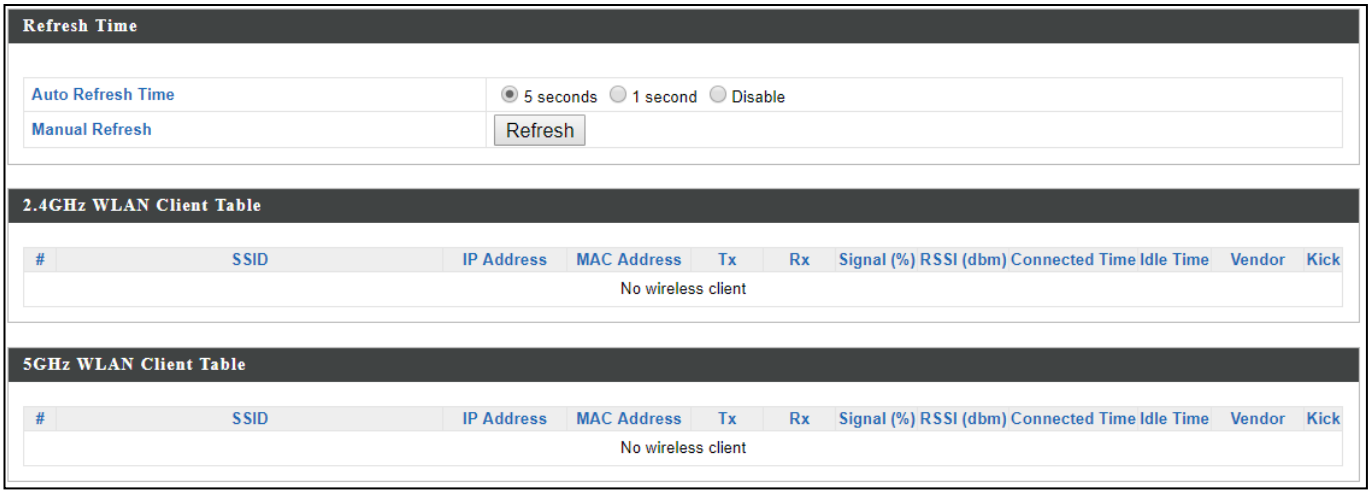
Wireless 2.4GHz (5GHz)	
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or disabled).
MAC Address	Displays the AP's MAC address.
Channel	Displays the channel number the specified wireless frequency is using for broadcast.
Transmit Power	Displays the wireless radio transmit power level as a percentage.
RSSI	Received signal strength indicator (RSSI) is a measurement of the power present in a received radio signal.

Wireless 2.4GHZ (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID.
Encryption Type	Displays the encryption type for the specified SSID.
VLAN ID	Displays the VLAN ID for the specified SSID.
Additional Authentication	Displays the additional authentication type for the specified SSID.
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID.

Wireless 2.4GHZ (5GHz) / WDS Status	
MAC Address	Displays the peer AP's MAC address.
Encryption Type	Displays the encryption type for the specified WDS.
VLAN Mode/ID	Displays the VLAN ID for the specified WDS.

Wireless Clients:

"Wireless Clients" page displays information about all wireless clients connected to the AP on the 2.4GHz or 5GHz frequency.

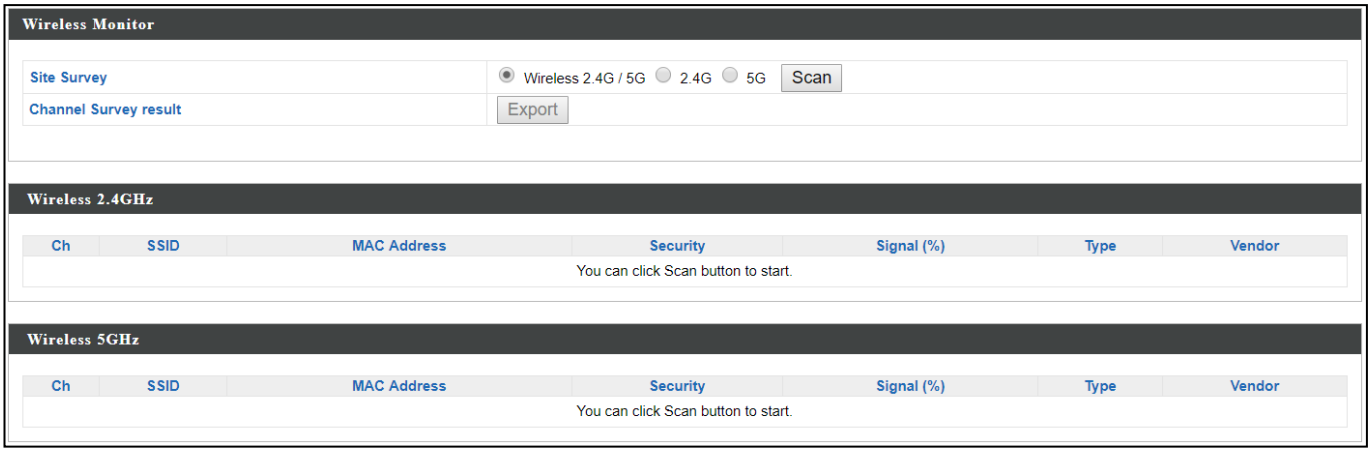


Refresh time	
Auto Refresh Time	Select a time interval for the client table list to automatically refresh.
Manual Refresh	Click refresh to manually refresh the client table.

2.4GHz (5GHz) WLAN Client Table	
SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.
Signal (%)	Displays the wireless signal strength for the specified client.
Connected Time	Displays the total time the wireless client has been connected to the AP.
Idle Time	Client idle time is the time for which the client has not transmitted any data packets i.e. is idle.
Vendor	The vendor of the client's wireless adapter is displayed here.

Wireless Monitor:

“Wireless Monitor” is a tool built into the AP to scan and monitor the surrounding wireless environment. Select a frequency and click “Scan” to display a list of all SSIDs within range along with relevant details for each SSID.



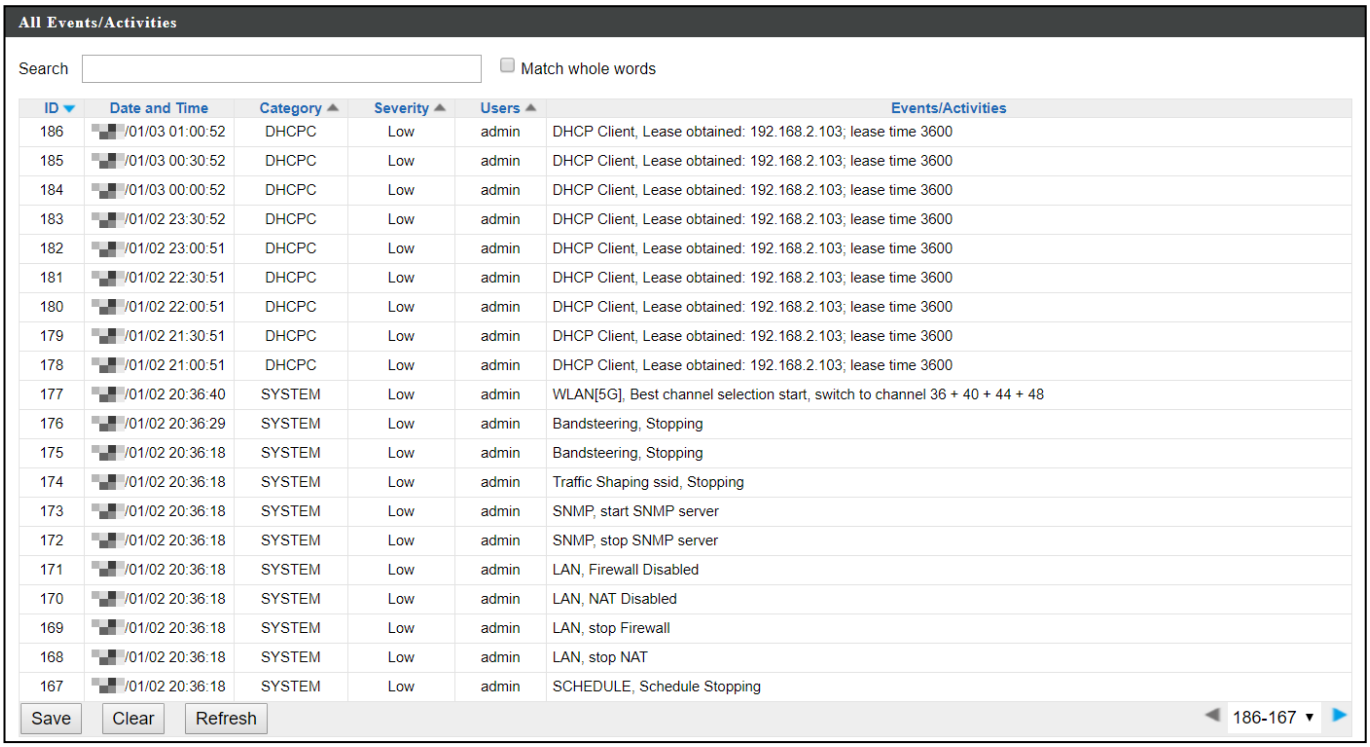
Wireless Monitor	
Site Survey	Select which frequency (or both) to scan, and click “Scan” to begin.
Channel Survey Result	After a scan is complete, click “Export” to save the results to local storage.

Site Survey Results	
Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/AP for the specified SSID.
Security	Displays the authentication/encryption type of the specified SSID.
Signal (%)	Displays the current signal strength of the SSID.
Type	Displays the 802.11 wireless networking standard(s) of the specified SSID.
Vendor	Displays the vendor of the wireless router/AP for the specified SSID.

Log:

“System log” displays system operation information such as up time and connection processes. This information is useful for network administrators.

Older entries will be overwritten when the log is full



Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

The following information/events are recorded by the log:

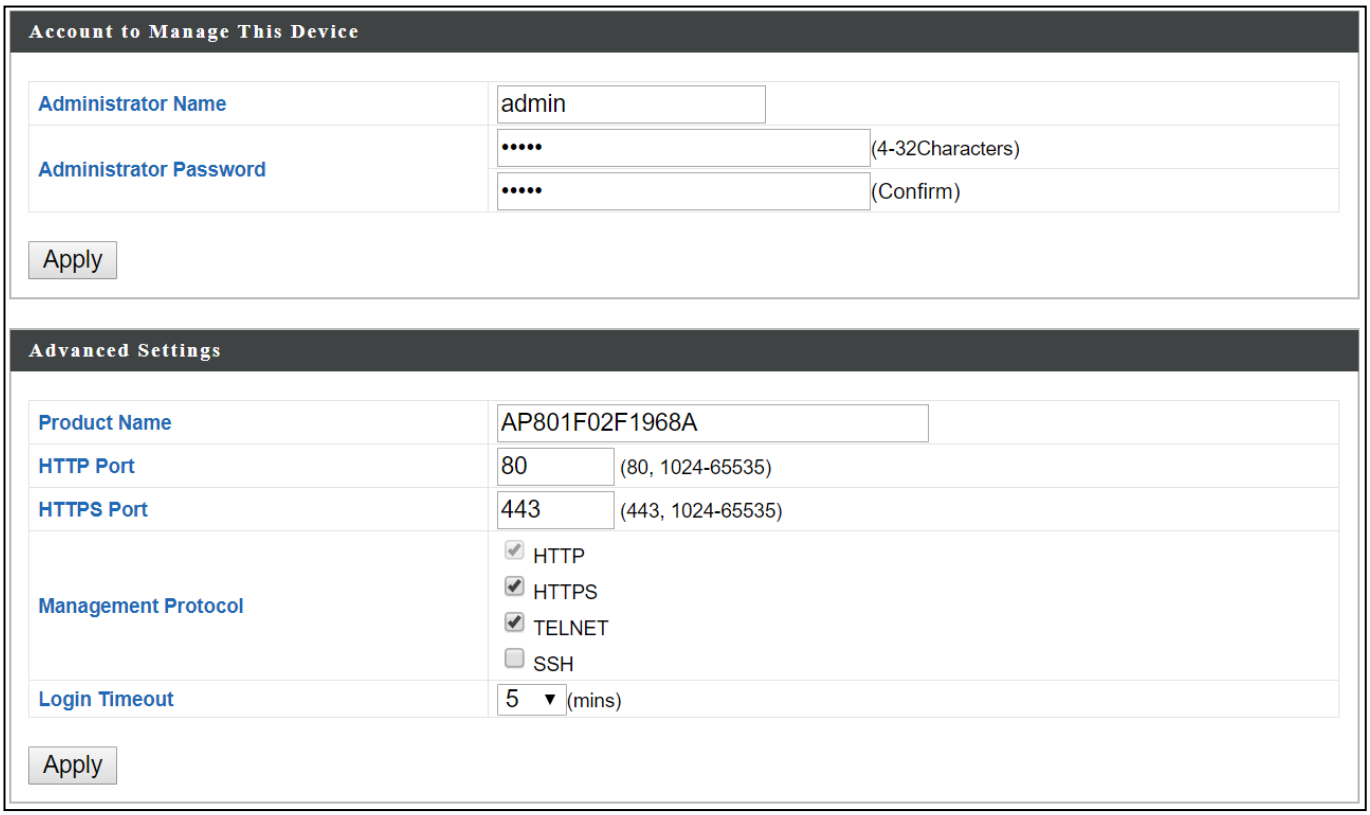
Log (Category)	
USB	Mount & un-mount
Wireless Client	Connected & disconnected Key exchange success & fail
Authentication	Authentication fail or successful
Association	Success or fail
WPS	M1 - M8 messages WPS success
Change Settings	Displays the total time the wireless client has been connected to the AP
System Boot	Displays current model name
Vendor	The vendor of the client's wireless adapter is displayed here
NTP Client	Syncing time with NTP server
Wired Link	LAN Port link status and speed status
Proxy ARP	Proxy ARP module start & stop
Bridge	Bridge start & stop
SNMP	SNMP server start & stop
HTTP	HTTP start & stop
HTTPS	HTTPS start & stop
SSH	SSH-client server start & stop
Telnet	Telnet-client server start or stop
WLAN (2.4G) and (5G)	WLAN (2.4G) and (5G) channel status and country/region status

ii. Management

Admin:

You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface.

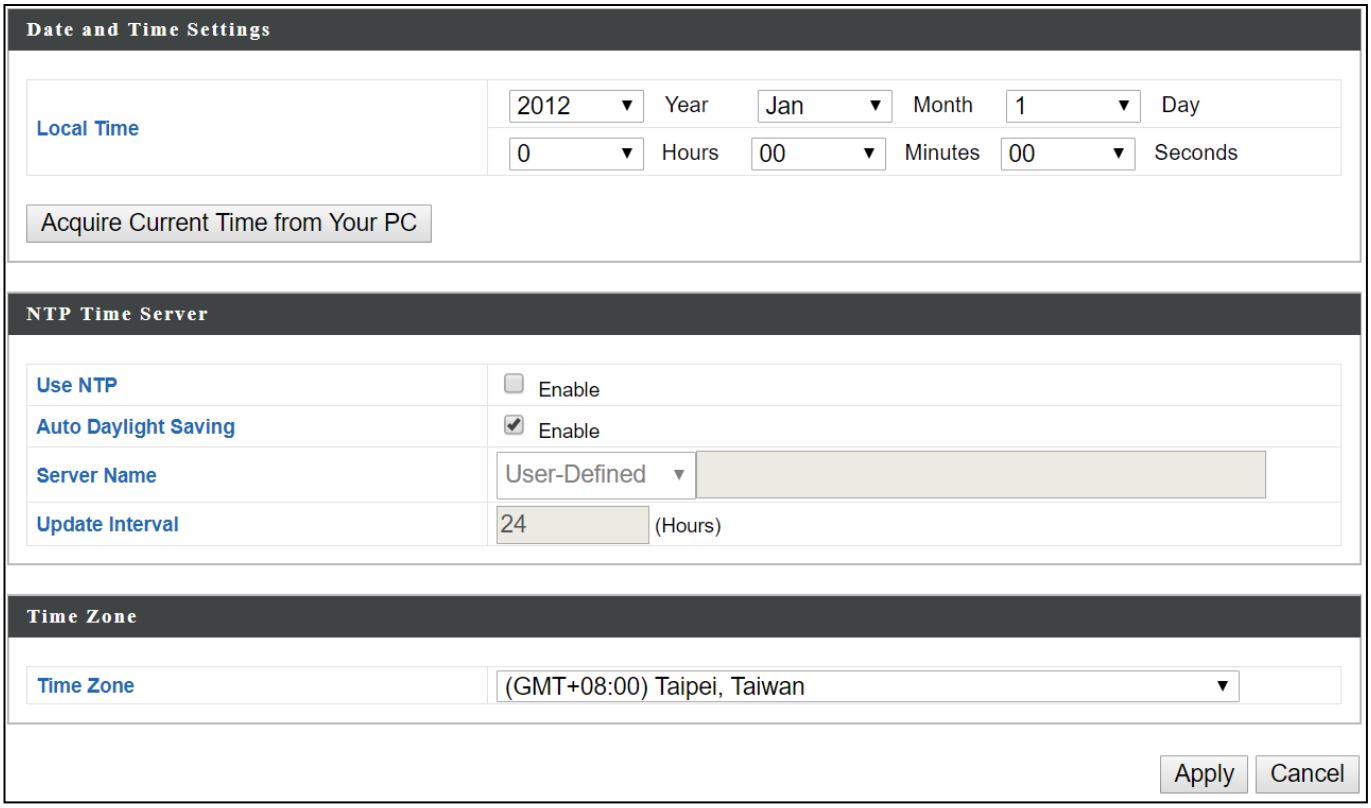


Account to Manage This Device	
Administrator Name	Set the AP's administrator name. This is used to log in to the browser based configuration interface and must be between 4-16 alphanumeric characters (case sensitive).
Administrator Password	Set the AP's administrator password. This is used to log in to the browser based configuration interface and must be between 4-32 alphanumeric characters (case sensitive).

Advanced Settings	
Product Name	Edit the product name according to your preference consisting of 1-32 alphanumeric characters. This name is used for reference purposes.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below). When SNMP is enabled, complete the SNMP fields below.
SNMP Version	Select SNMP version appropriate for your SNMP manager.
SNMP Get Community	Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests.
SNMP Set Community	Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests.
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of network errors.
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (2-128 alphanumeric characters) of the SNMP manager.

Date and Time:

Configure the date and time settings of the AP here. The date and time of the device can be configured manually or can be synchronized with a time server.



Date and Time Settings	
Local Time	Set the AP's date and time manually using the drop down menus.
Acquire Current Time from your PC	Click "Acquire Current Time from Your PC" to enter the required values automatically according to your computer's current time and date.

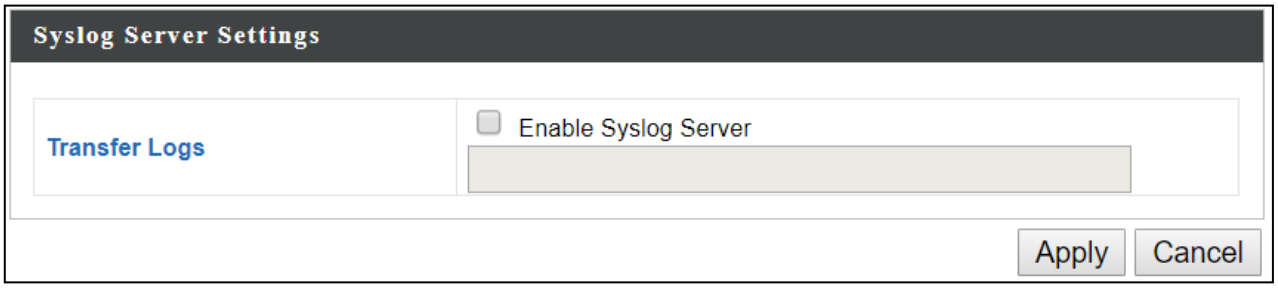
NTP Time Server	
Use NTP	The AP also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the AP to update/synchronize with the NTP server.

Time Zone	
Time Zone	Select the time zone of your country/region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.

Press “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

Syslog Server Settings:

The system log can be sent to a server.



Syslog Server Settings	
Transfer Logs	Check the box to enable the use of a syslog server. Enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.

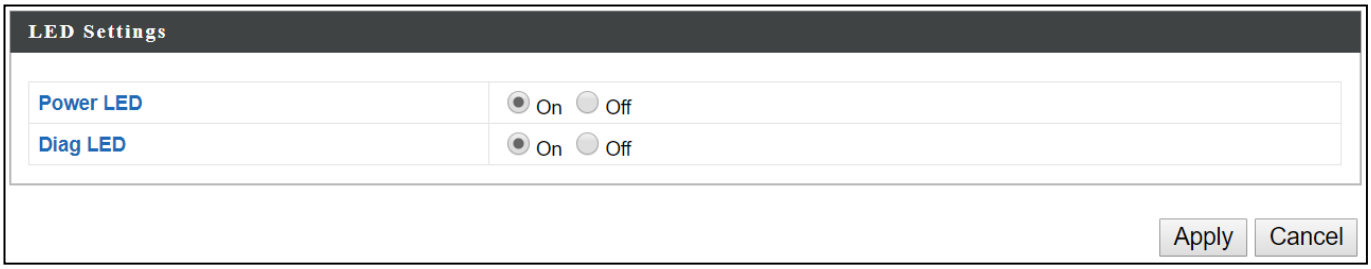
Syslog E-mail Settings:

Syslog E-mail Settings	
E-mail Logs	Check the box to enable/disable e-mail logs.
E-mail Subject	Specify the subject line of log emails.
SMTP Server Address	Specify the SMTP server address used to send log emails.
SMTP Server Port	Specify the SMTP server port used to send log emails.
Sender E-mail	Specify the sender email address.
Receiver E-mail	Specify the email to receive log emails.
Authentication	Disable or select authentication type: SSL or TLS. When using SSL or TLS, enter the username and password.

iv. Advanced

LED Settings:

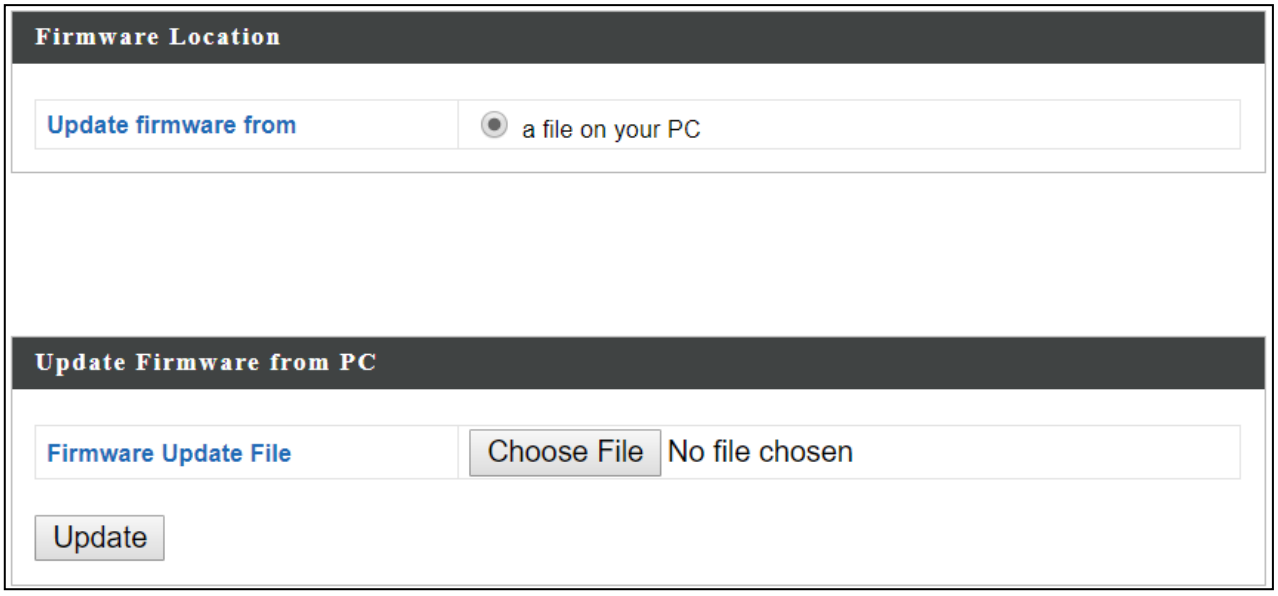
The AP's LEDs can be manually enabled or disabled according to your preference.



Power LED	Select on or off.
Diag LED	Select on or off.

Update Firmware:

The “Firmware” page allows you to update the firmware of the system. Updated firmware versions often offer increased performance and security, as well as bug fixes. Download the latest firmware from the Edimax website.

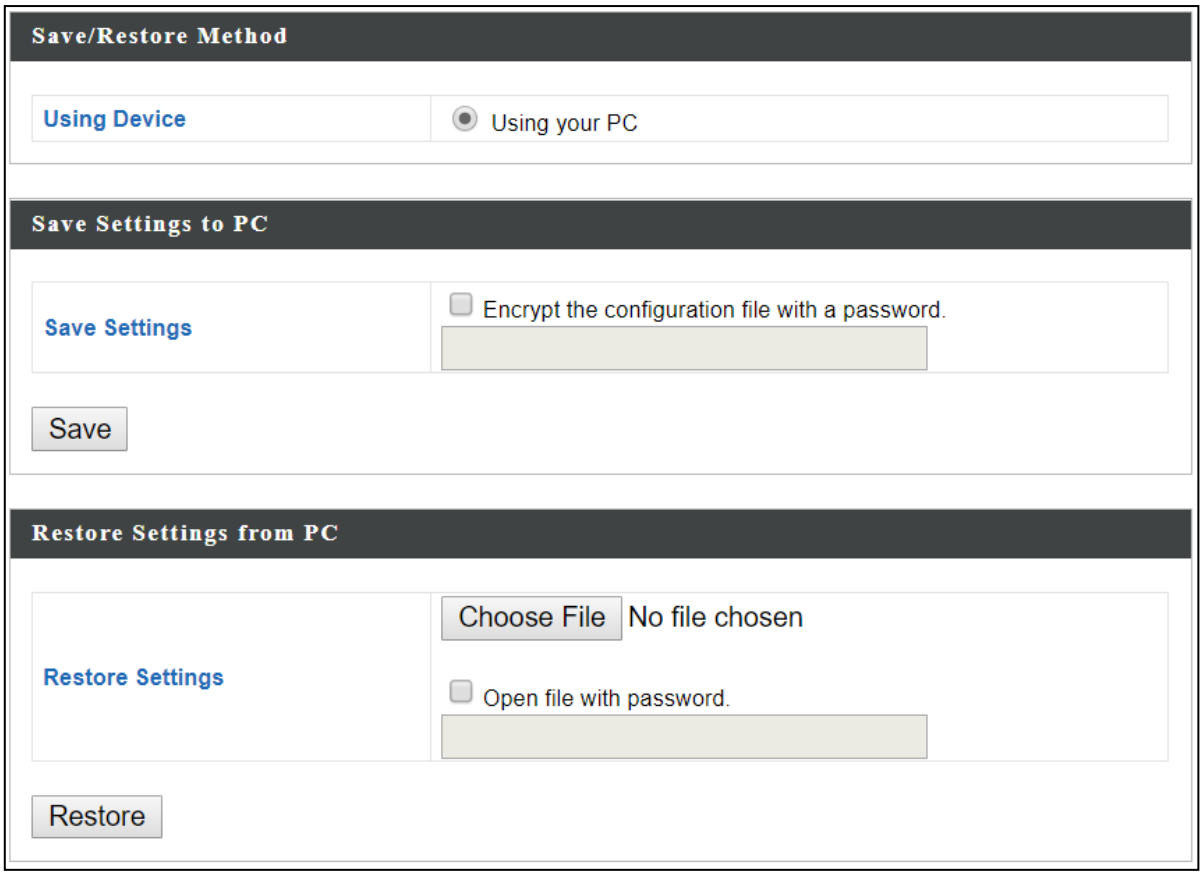


Do not switch off or disconnect the AP during a firmware upgrade, as this could damage the device.

Firmware Location	Click “Choose File” to upload firmware from your local computer.

Save/Restore Settings:

The device's "Save / Restore Settings" page enables you to save / backup the device's current settings as a file to your local computer, and restore the AP to previously saved settings.



Save Settings to PC	
Save Settings	Encryption: If you wish to encrypt the configuration file with a password, check the "Encrypt the configuration file with a password" box and enter a password. Click "Save" to save current settings. A new window will open to allow you to specify a location to save to.

Restore Settings from PC	
Restore Settings	Click the "Choose File" button to find a previously saved settings file on your computer. If your settings file is encrypted with a password, check the "Open file with password" box and enter the password in the following field. Click "Restore" to replace your current settings.

Factory Default:

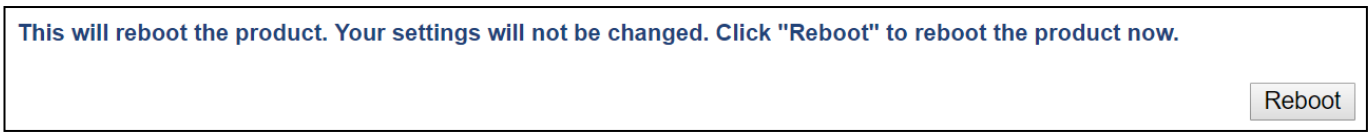
If the AP malfunctions or is not responding, rebooting the device maybe an option to consider. If rebooting does not work, try resetting the device back to its factory default settings. You can reset the AP back to its default settings using this feature if the reset button is not accessible.

Factory Default	Click “Factory Default” to restore settings to the factory default. A pop-up window will appear and ask you to confirm.

After resetting to factory defaults, please wait for the AP to reset and restart.

Reboot:

If the AP malfunctions or is not responding, rebooting the device may be an option to consider. You can reboot the AP remotely using this feature.



Reboot	Click “Reboot” to reboot the device. A countdown will indicate the progress of the reboot.

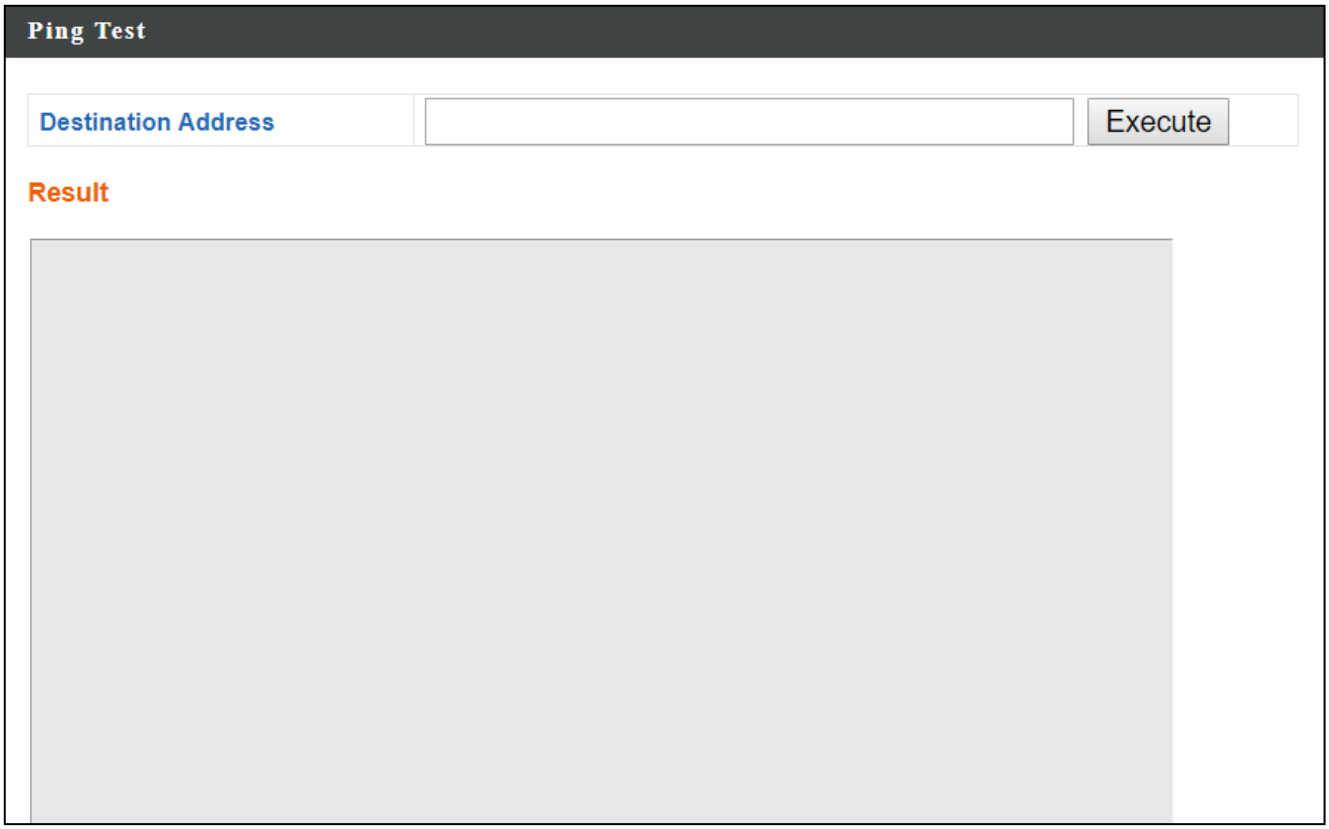
VI-10. Toolbox

The Toolbox panel provides network diagnostic tools: Ping, Traceroute, and IP Scan.

i. Network Connectivity

Ping:

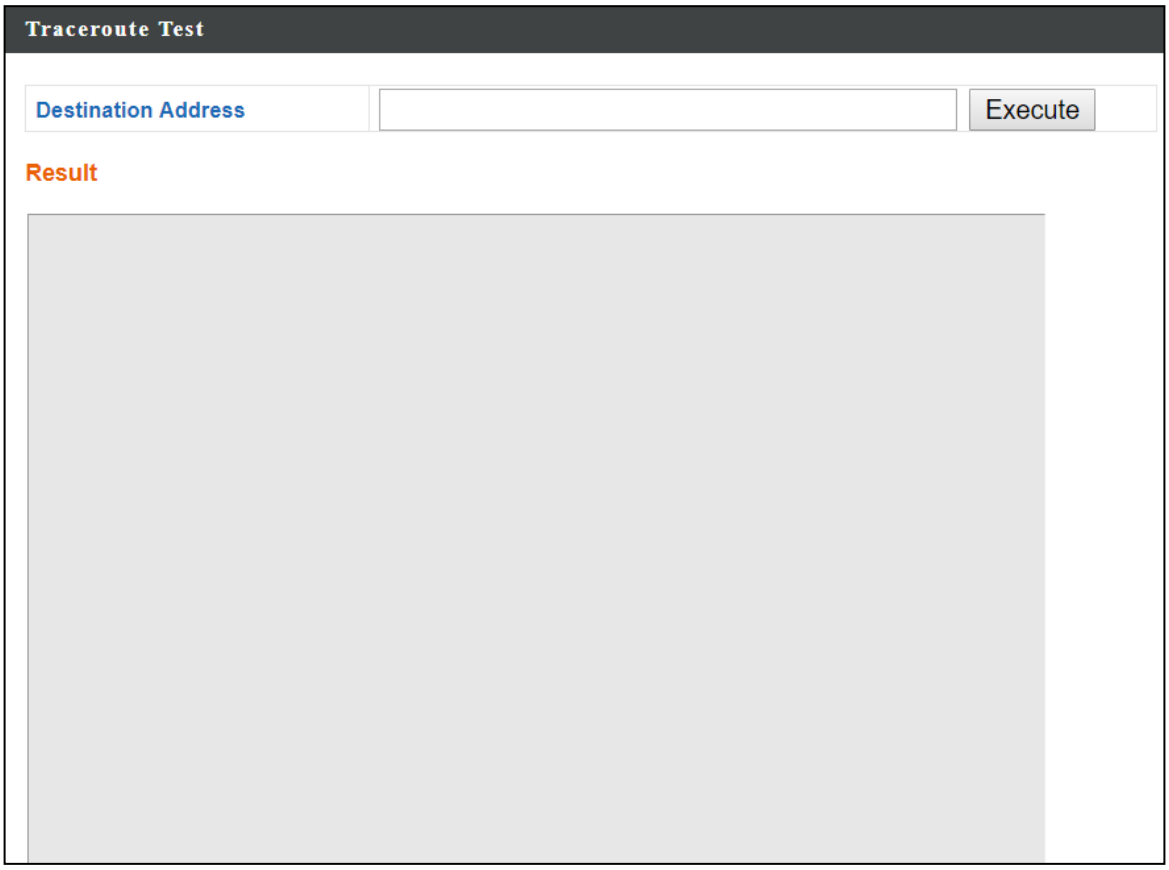
Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.



Destination Address	Enter the address of the host.
Execute	Click “Execute” to ping the host.

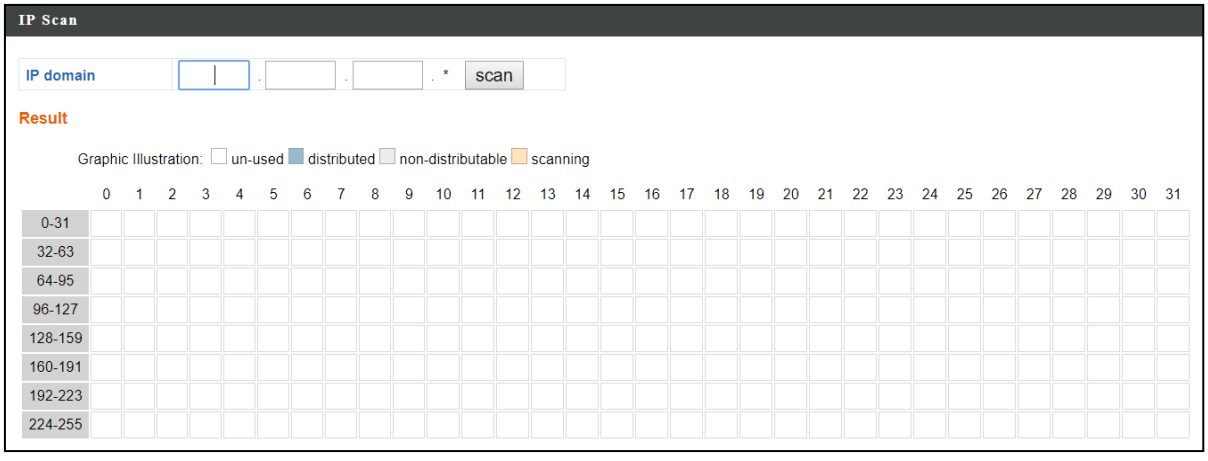
Trace Route:

Traceroute is a diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network.



Destination Address	Enter the address of the host.
Execute	Click “Execute” to execute the traceroute command.

IP Scan:



VII. WPS

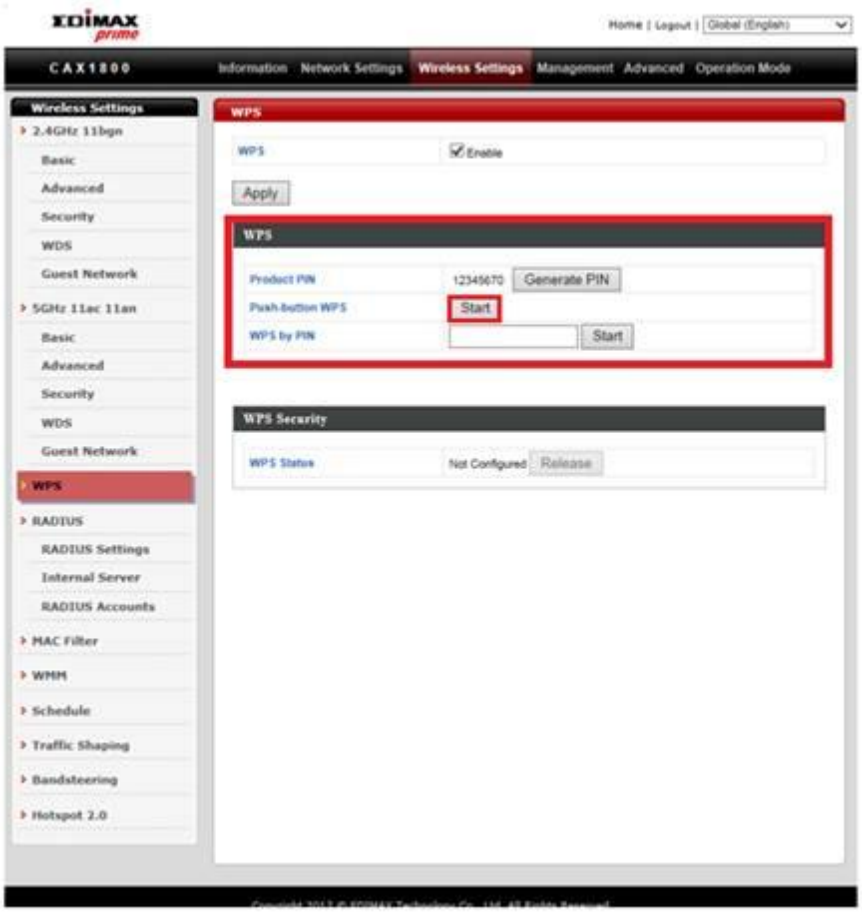
WPS is a simple way to establish connections between WPS compatible devices. You can use the WPS button on CAX1800 webpage to activate the AP's WPS function.

1. Go to "Wireless Settings".

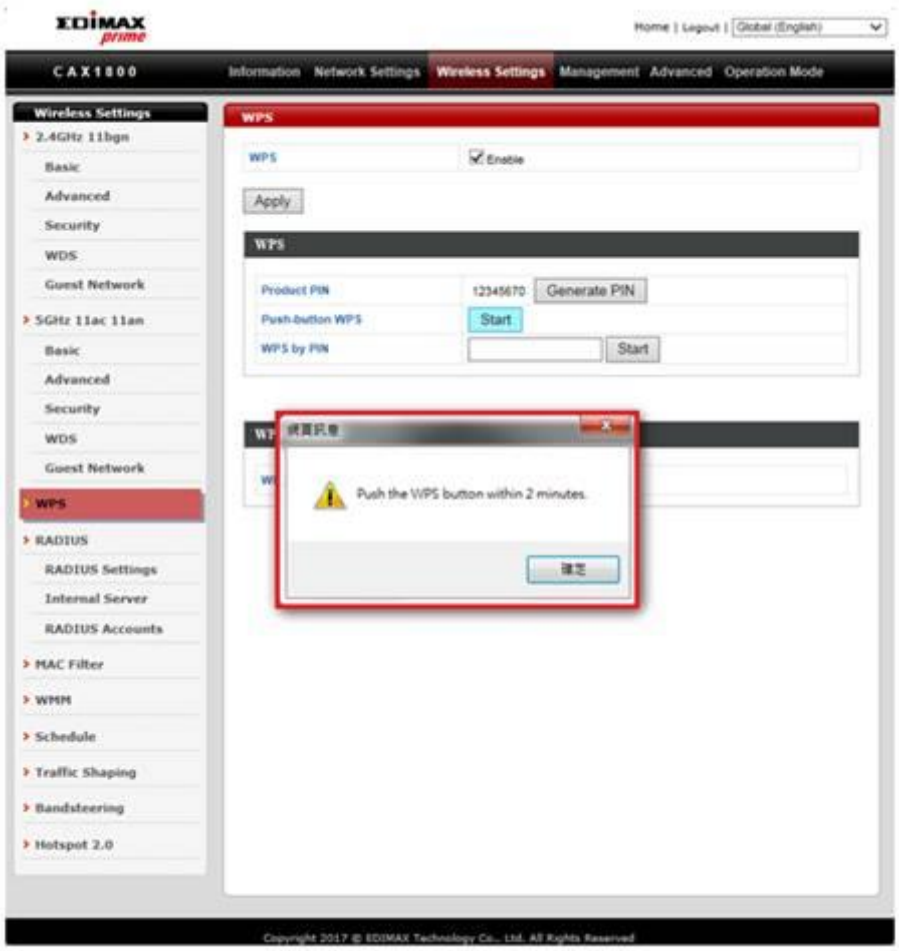
2. Tap "WPS".

3. Check the checkbox of "Enable" and click "Apply" to turn on WPS function.

4. Click Start to establish connections between WPS compatible devices.



5. Within two minutes, press the WPS button to activate WPS on your WPS-compatible wireless device.



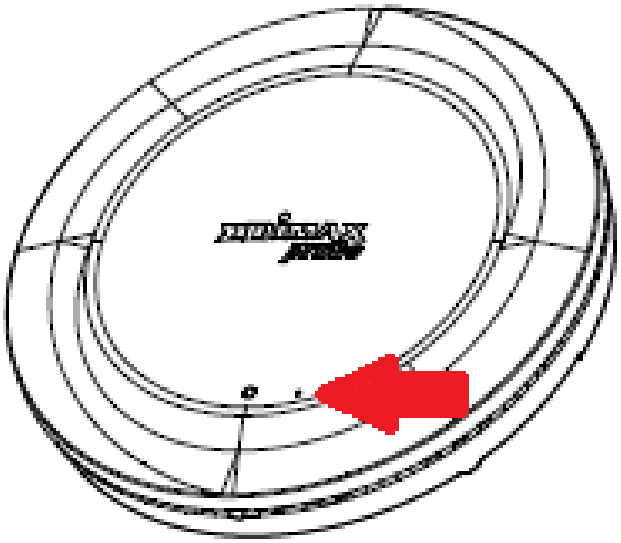
VIII. Reset

If you experience problems with your AP, you can reset the device back to its factory settings.

1. Press and hold the reset button on the AP for at least 10 seconds then release the button.

You may need to use a pin or similar sharp object to push the reset button.

2. Wait for the AP to restart. The AP is ready for setup when the LED is **Blue**.



COPYRIGHT

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

	AT	BE	BG	HR	CY	CZ	DK
	EE	FI	FR	DE	EL	HU	IE
	IT	LV	LT	LU	MT	NL	PL
	PT	RO	SK	SI	ES	SE	UK

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is restricted to indoor use.

Federal Radiation Exposure Statement

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body or nearby persons.

This device is restricted to indoor use.

RED Compliance Statement

Compliance with 2014/53/EU Radio Equipment Directive (RED)

In accordance with Article 10.8(a) and 10.8(b) of the RED, the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

Frequency range (MHz)	Max. Transmit Power (dBm)
2400-2483.5	19.95
5150-5250	22.84

A simplified DoC shall be provided as follows: Article 10(9)

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type AX1800 Dual-Band Ceiling Mount PoE AP is in compliance with Directive 2014/53/EU

The full text of the EU declaration of conformity is available at the following internet address: http://www.edimax.com/edimax/global/

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Safety
This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use
The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use
None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU, 2014/35/EU.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/53/EU, 2014/35/EU.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/53/EU, 2014/35/EU.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/53/EU, 2014/35/EU.

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/53/UE, 2014/35/UE.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 2014/53/EU, 2014/35/EU.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/53/EU, 2014/35/EU).

Türkçe: Bu cihaz 2014/53/EU, 2014/35/EU direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 2014/53/EU, 2014/35/EU.

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/53/EU, 2014/35/EU.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/53/EU, 2014/35/EU.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 2014/53/EU, 2014/35/EU.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/53/EU, 2014/35/UE.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/53/EU, 2014/35/EU.

Português: Este equipamento cumpre os requesitos essênciais da Directiva 2014/53/EU, 2014/35/EU.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/53/EU, 2014/35/EU.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/53/EU, 2014/35/EU.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/53/EU, 2014/35/EU.

suomen kieli: Tämä laite täyttää direktiivien 2014/53/EU, 2014/35/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN AT BE CY CZ DK EE FI FR RU DE GR HU IE IT LV LT LU MT NL PL PT UA SK SI ES SE GB IS LI NO CH BG RO TR

WEEE Directive & Product Disposal

At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European Radio Equipment Directive.

Equipment: AX1800 Dual-Band Ceiling Mount PoE AP
Model No.: CAX1800

The following European standards for essential requirements have been followed:

Directives 2014/53/EU

Spectrum : EN 300 328 V2.1.1 (2016-11)
EN 301 893 V2.1.1 (2017-05)
EMC : EN 301 489-1 V2.2.0 (2017-03)
EN 301 489-17 V3.2.0 (2017-03)
EN 55032:2015/AC:2016 Class B
EN 61000-3-2:2014
EN 61000-3-3:2013
EN 55035:2017
EMF : EN 62311:2008 and EN 50665:2017
Safety (LVD) : IEC 62368-1:2014 (2nd Edition) and/or EN 62368-1:2014+A11:2017

Edimax Technology Europe B.V.
Fijenhof 2,
5652 AE Eindhoven,
The Netherlands

a company of :
Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd.,
Neihu Dist., Taipei City,
Taiwan

Signature:

Printed Name: David Huang
Title: Director
Edimax Technology Europe B.V.

Date of Signature: Nov., 2019
Signature:

Printed Name: Albert Chang
Title: Director
Edimax Technology Co., Ltd.

CE

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The ‘“Program”“, below, refers to any such program or work, and a ‘“work based on the Program”“ means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term ‘“modification”“.) Each licensee is addressed as ‘“you”“.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep

intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and '"any later version'", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM '"AS IS'" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES