OAP1300

User Manual

03-2018 / 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
3350 Scott Blvd., Bldg.15 Santa Clara, CA 95054, USA
Live Tech Support: 1(800) 652-6776
Email: support@edimax.com

CONTENTS

OVERVIEW

Your device can function in **four** different modes.

AP Mode is a regular access point for use in your wireless network. This is the default mode of the access point.

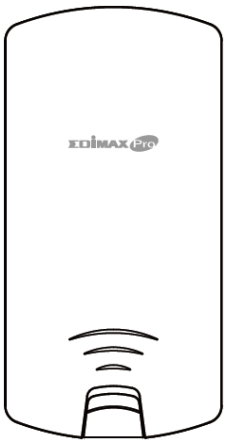
Repeater Mode is a wireless repeater (also called wireless range extender) that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network.

Managed AP Mode acts as a “slave” AP within an AP array (controlled by the AP Controller “master”).

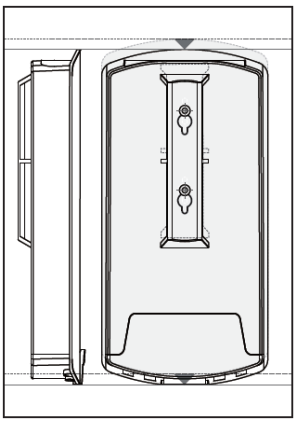
Client Bridge Mode determines the device to be a client bridge. The client bridge receives wireless signal and provides it to devices connected to the bridge via Ethernet cable.

I Product Information

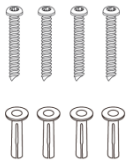
I-1 Package Contents



1



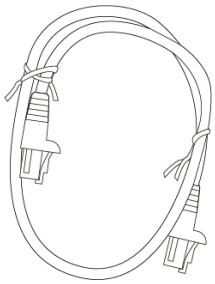
2



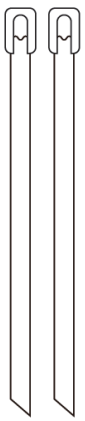
3

4

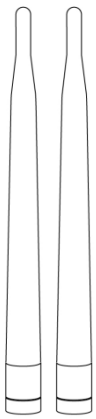
5



6



7



8

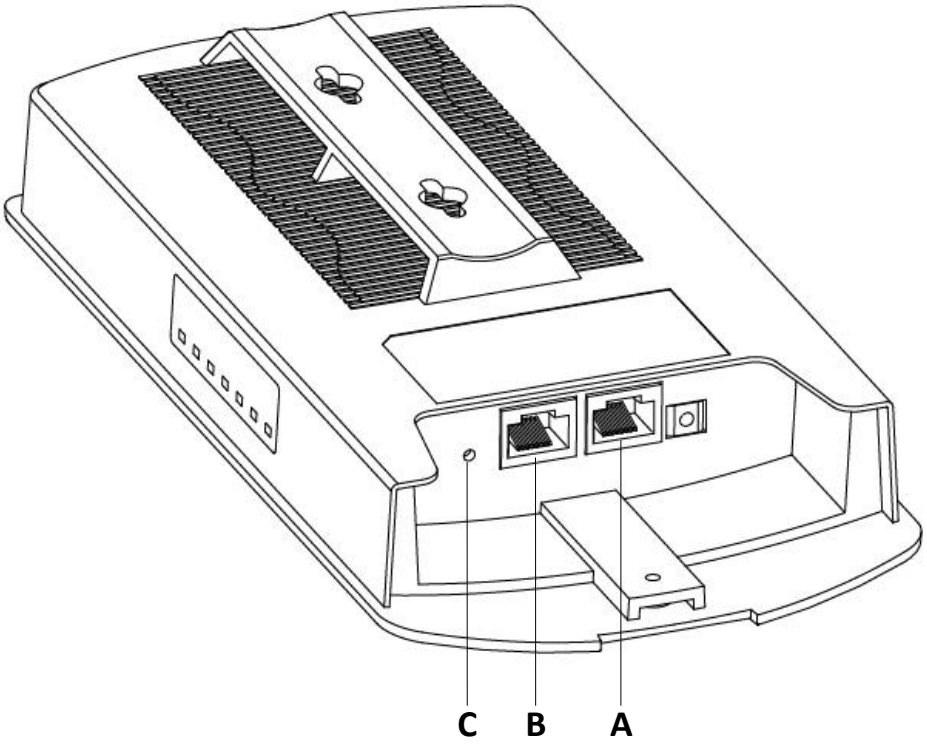
1. OAP1300 Access Point
2. Wall Mount Screw Template
3. Wall Mount Screw Set
4. CD
5. Quick Installation Guide
6. Ethernet Cable
7. Pole Mount Strap x2
8. Antenna x2

I-2 System Requirements

- Existing cable/DSL modem, PoE Switch & router
- Computer with web browser for access point configuration

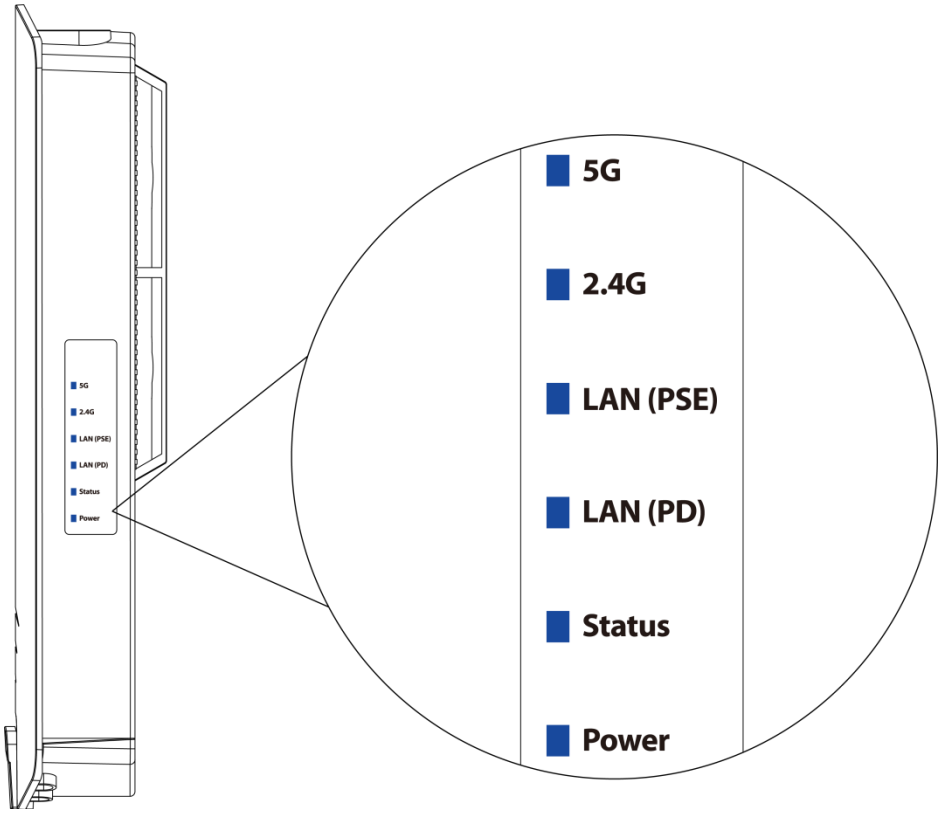
I-3 Hardware Overview

Ports and Button



A	LAN 1 POE-IN	LAN port with Power over Ethernet (PoE) IN
B	LAN 2 POE-OUT	LAN port with PoE OUT
C	Reset	Reset Button

I-4 LED Status



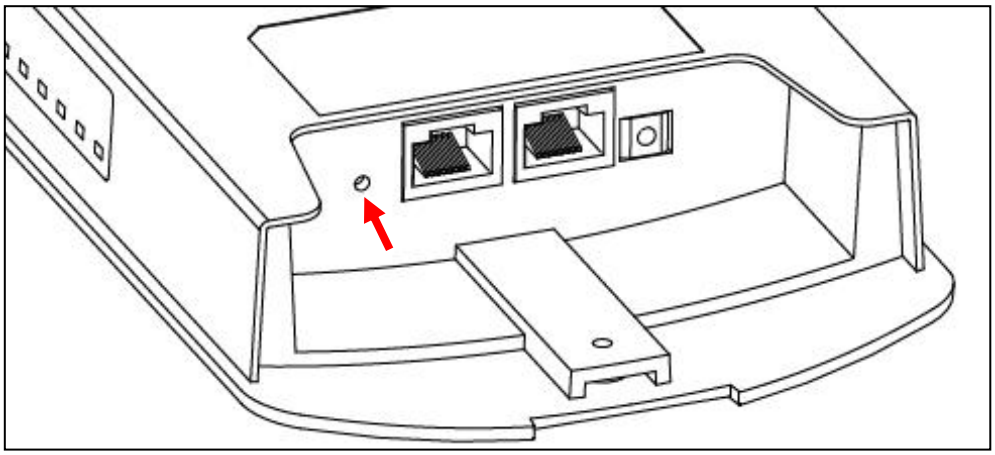
LED	LED Status	Description
5G (WLAN)	On	Wireless enabled.
	Off	Wireless disabled.
2.4G (WLAN)	On	Wireless enabled.
	Off	Wireless disabled.
LAN (PSE)	On	LAN port connected.
	Flashing	Activity (transmitting and receiving).
	Off	LAN port not connected.
LAN (PD)	On	LAN port connected.
	Flashing	Activity (transmitting and receiving).
	Off	LAN port not connected.
Status	On	Access point booting up.
	Off	No occurred error.
Power	On	The access point is on.
	Flashing	Upgrading firmware.
	Off	The access point is off.

I-5 Reset

If you experience problems with your access point, you can reset the device back to its factory settings. This resets all settings back to default.

1. Press and hold the reset button on the access point 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 access point to restart. The access point is ready for setup when the Power LED is turned on.

II Quick Setup & Mode Selection

The unit can function as a standalone access point (**AP Mode**), as a repeater (**Repeater Mode**), as part of an AP array (**Managed AP Mode**), or as a client bridge (**Client Bridge Mode**).

Follow the default mode steps below and select the desired operation mode.

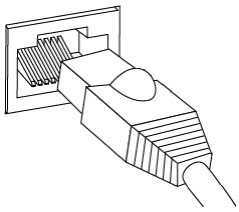
II-1 Default Mode: Access Point Mode

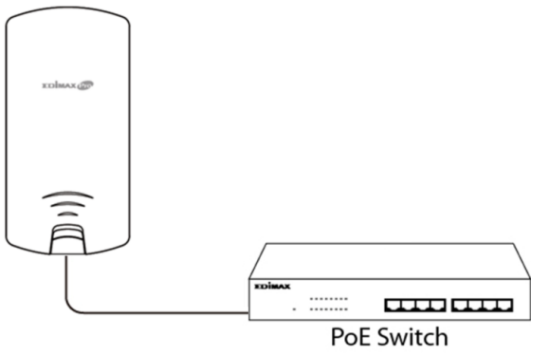
1. Set your computer's IP address to **192.168.2.x** where **x** is a number in the range **3 – 100**. If you are unsure how to do this, please refer to ***V-1 Configuring your IP address*** for more information.

Please ensure there are no other active network connections on your computer by disabling Wi-Fi and other Ethernet connections.

2. Wire an Ethernet cable to the **LAN 1 (PoE-In)** port of the access point and the PoE switch to power up the access point.

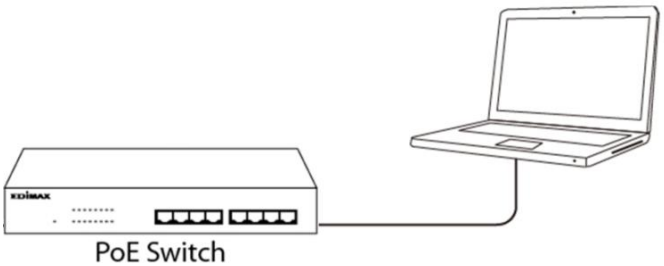
LAN 1 (PoE-In) Port



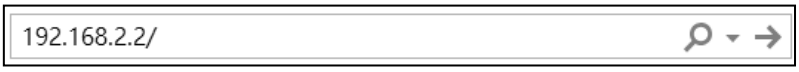


3. Please wait a moment for the device to start up. The device is ready when the Power LED is turned on.

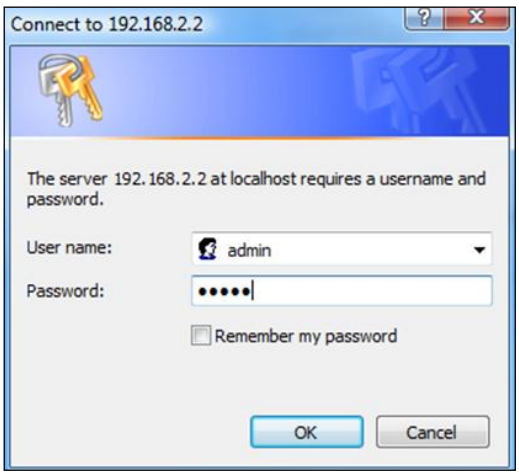
4. Connect a computer to the switch using an Ethernet cable.



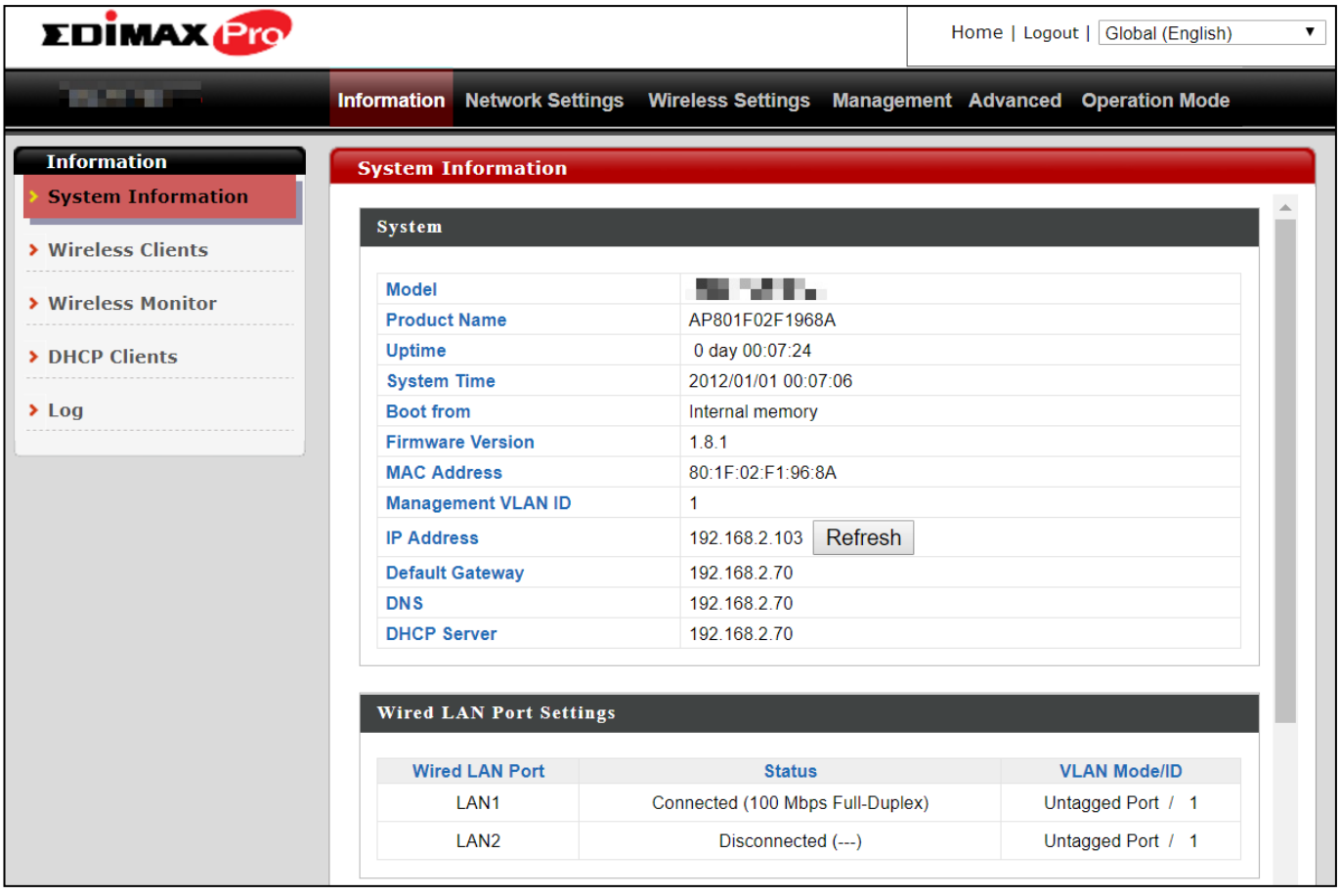
5. Enter the device's default IP address 192.168.2.2 into the URL bar of a web browser.



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

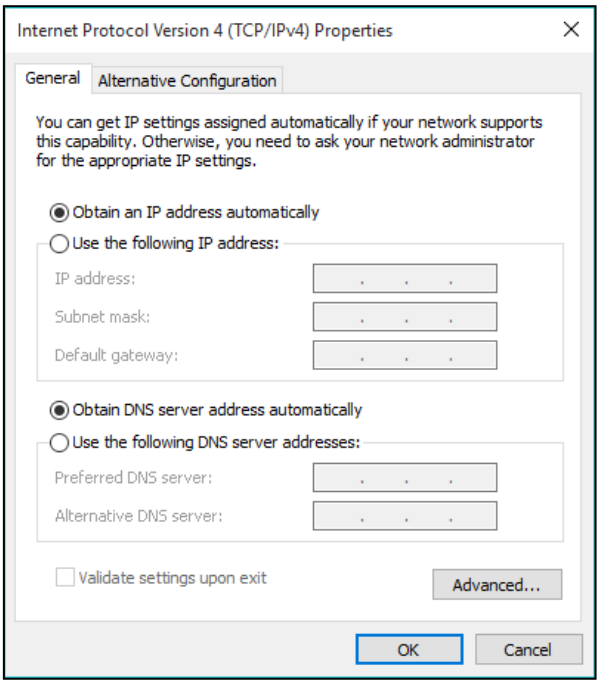


7. "System Information" home screen will be shown:

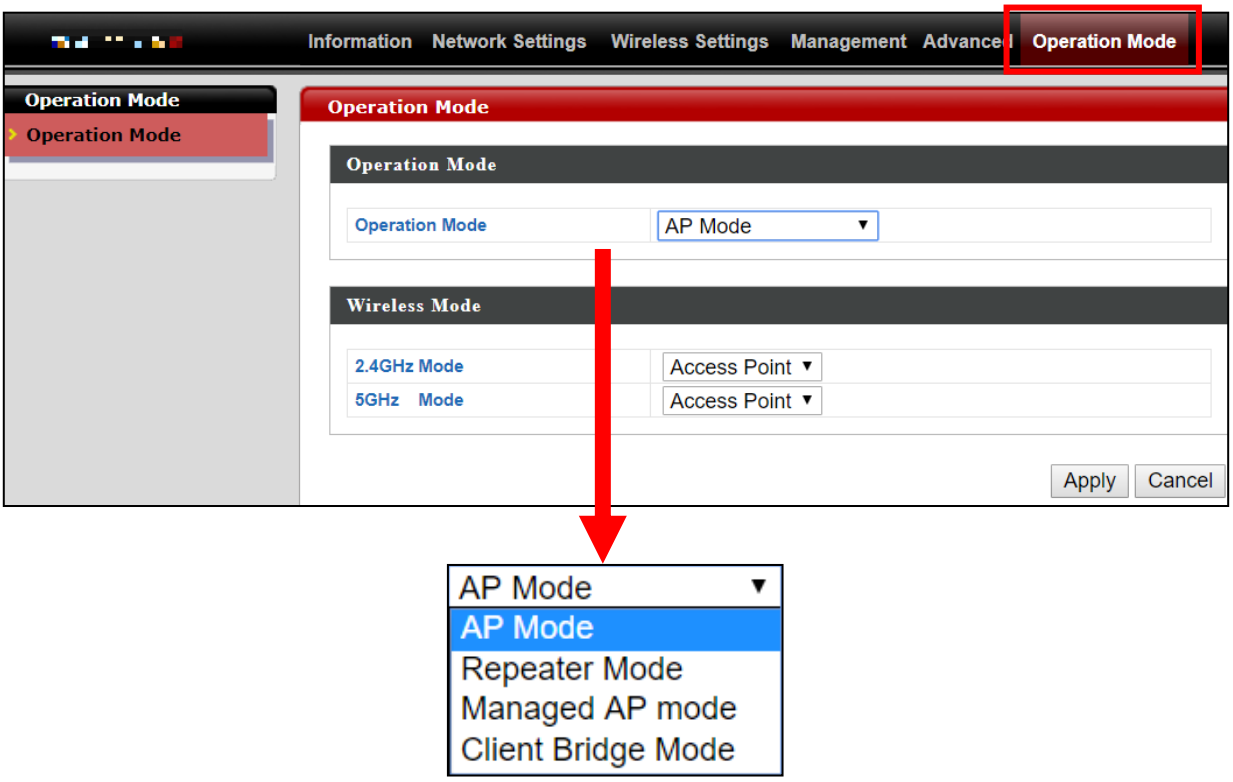


8. By default, the device is in AP Mode.

If you do not wish to change the operation mode, switch your computer back to dynamic IP address now.



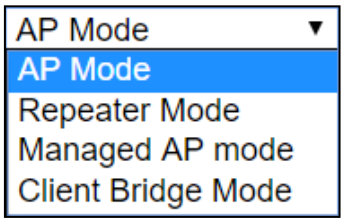
9. If you wish to change to a different operation mode, go to "Operation Mode" tab to select the desired operation mode. Follow the steps in the following sections to change the operation mode.



II-2 Repeater Mode

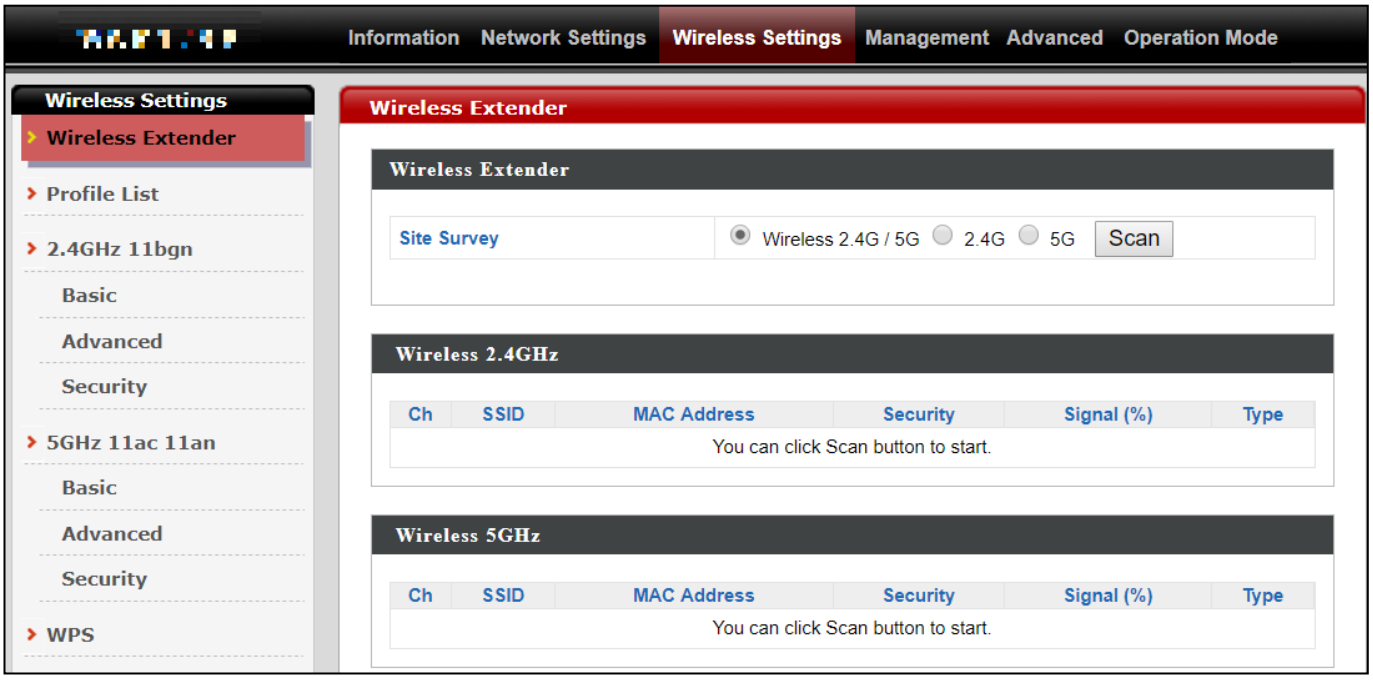
From the default mode above,

1. Select Repeater Mode from the operation mode drop down menu:

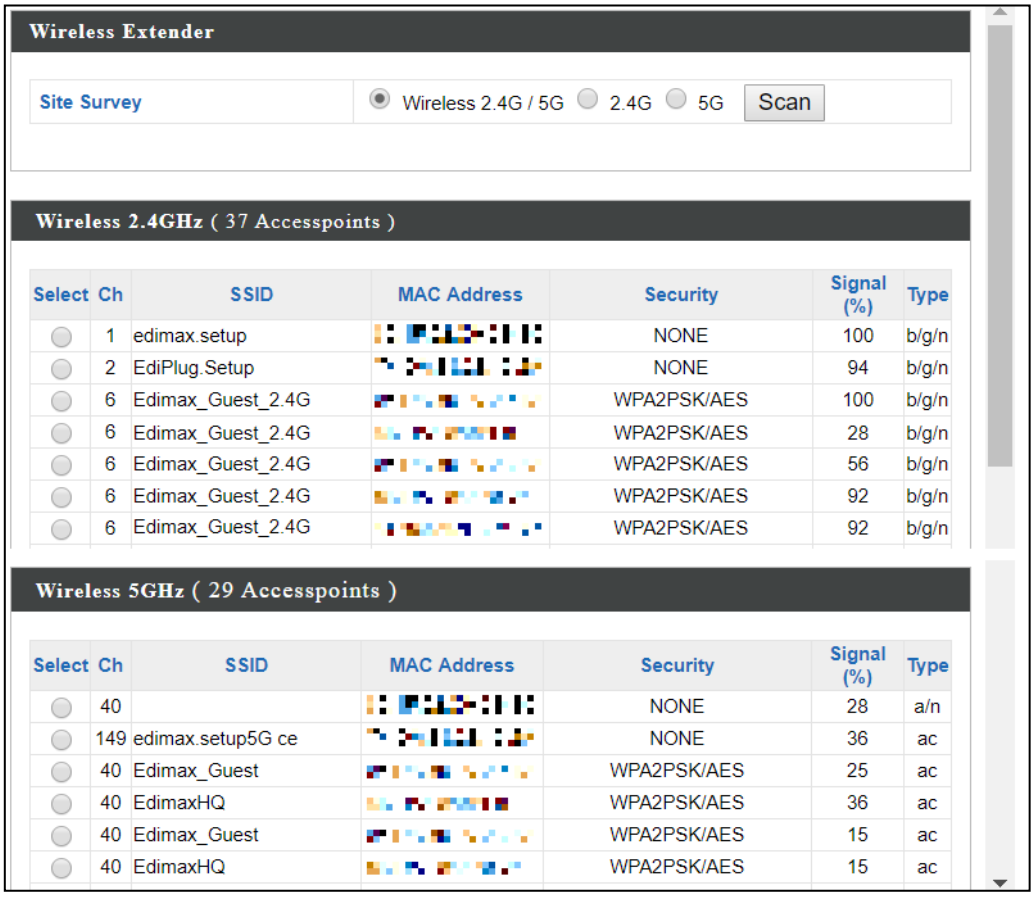


2. Press “Apply” and wait for the device to reboot into Repeater Mode:

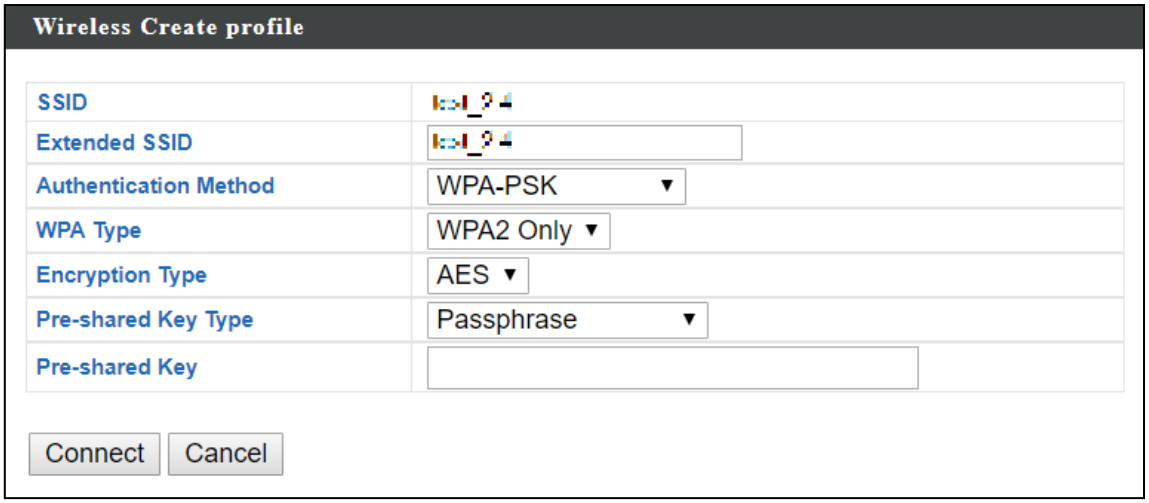
3. When system page is displayed, go to **Wireless Settings → Wireless Extender**.



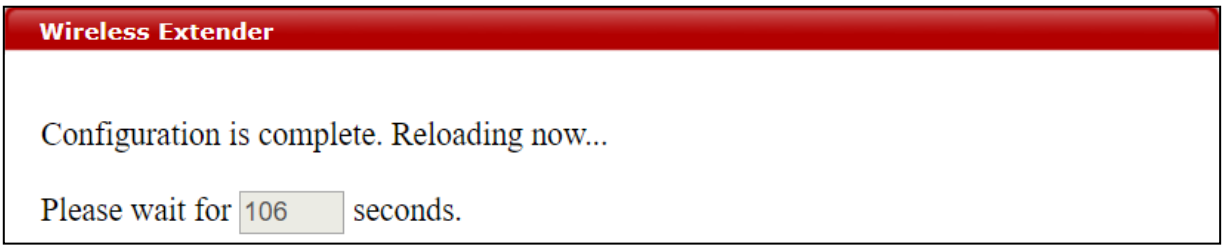
4. Click Scan to search for and display available SSIDs



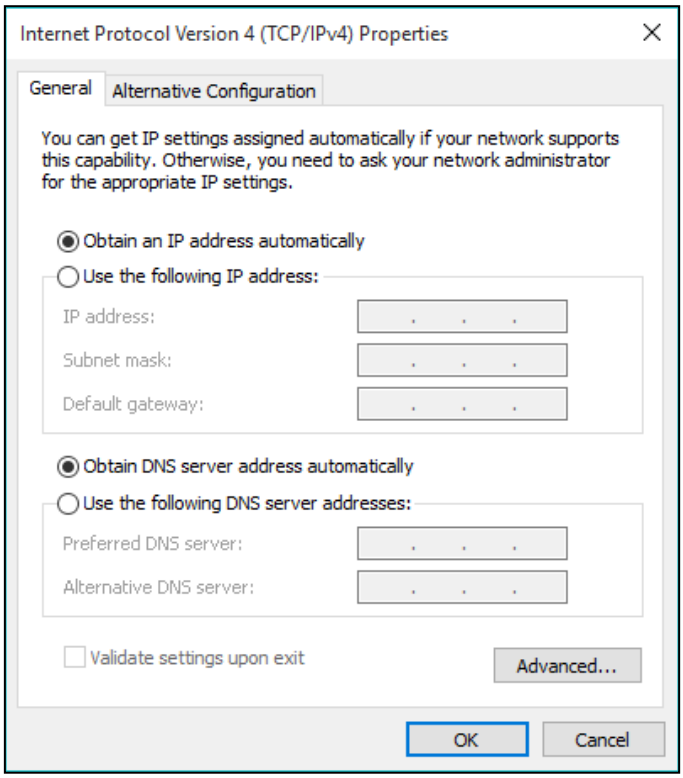
5. Click the circle icon to connect to an available source SSID. SSIDs can be configured independently for each frequency 2.4GHz & 5GHz.



6. Edit the new extended SSID according to your preference and enter the security details for the source SSID (e.g. Pre-shared Key). Click “Connect” to proceed.
Wait for the configuration to take effect:



7. The device (now in Repeater Mode) will establish a connection to the source SSID and repeat the extended SSID. The device will become a DHCP client of the router/root AP. Switch your computer back to dynamic IP address.



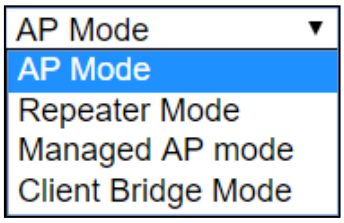
8. To access the web user interface, check your router/root AP’s settings to determine the device’s new IP address. Enter the new IP address into the browser for the web user interface.

If you wish to switch the operation mode, please reset the device to factory default (via web user interface or hardware reset).

II-3 Client Bridge Mode

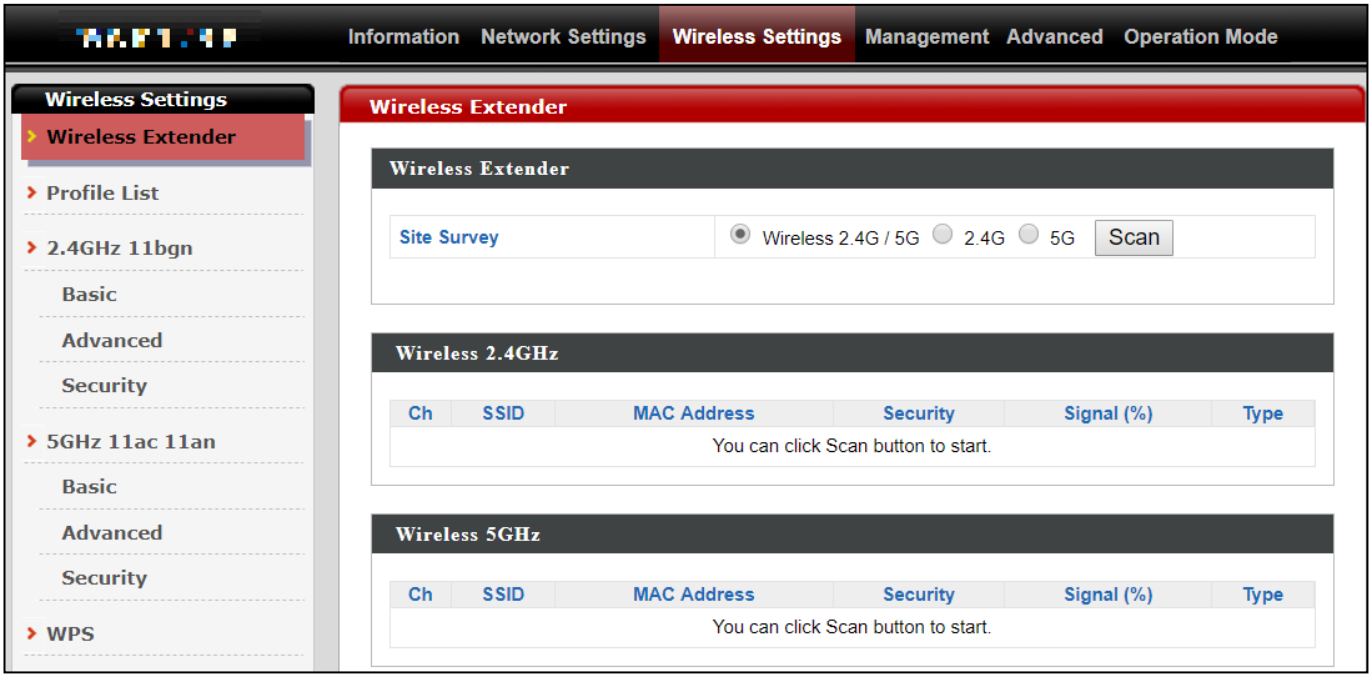
From the default mode above,

1. Select Client Bridge Mode from the operation mode drop down menu:

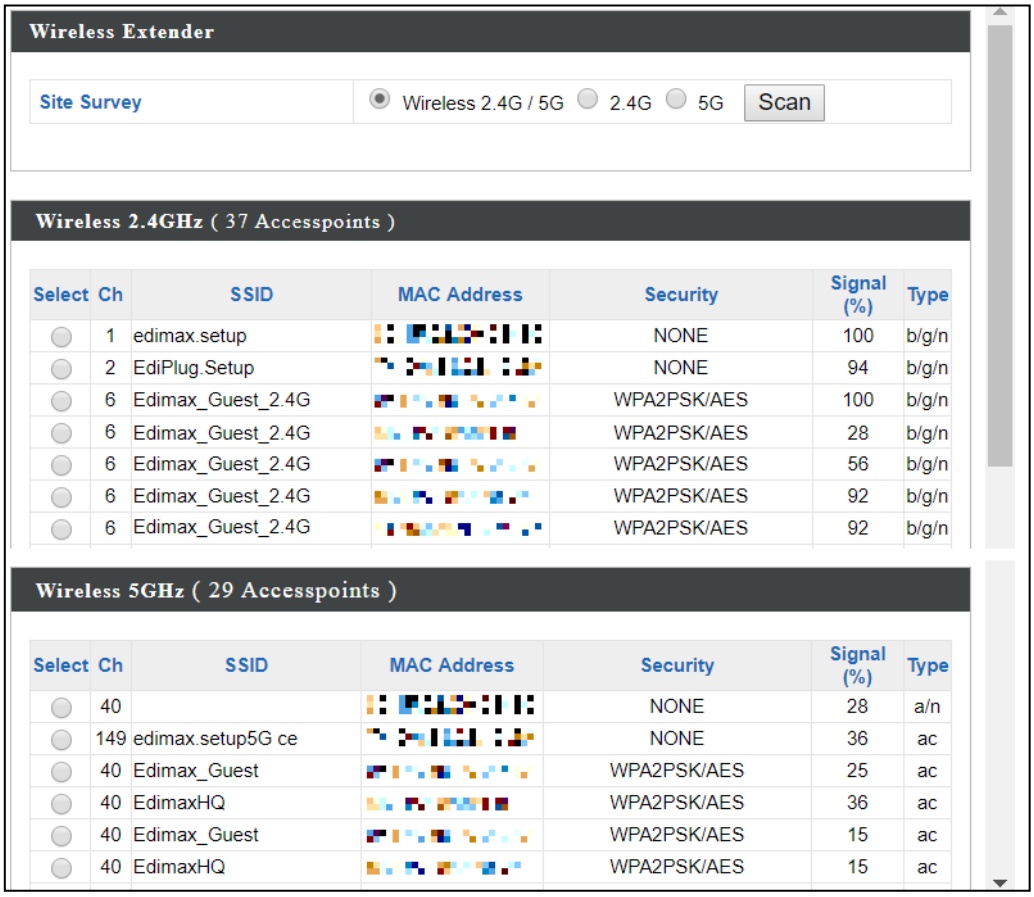


2. Press “Apply” and wait for the device to reboot into Client Bridge Mode:

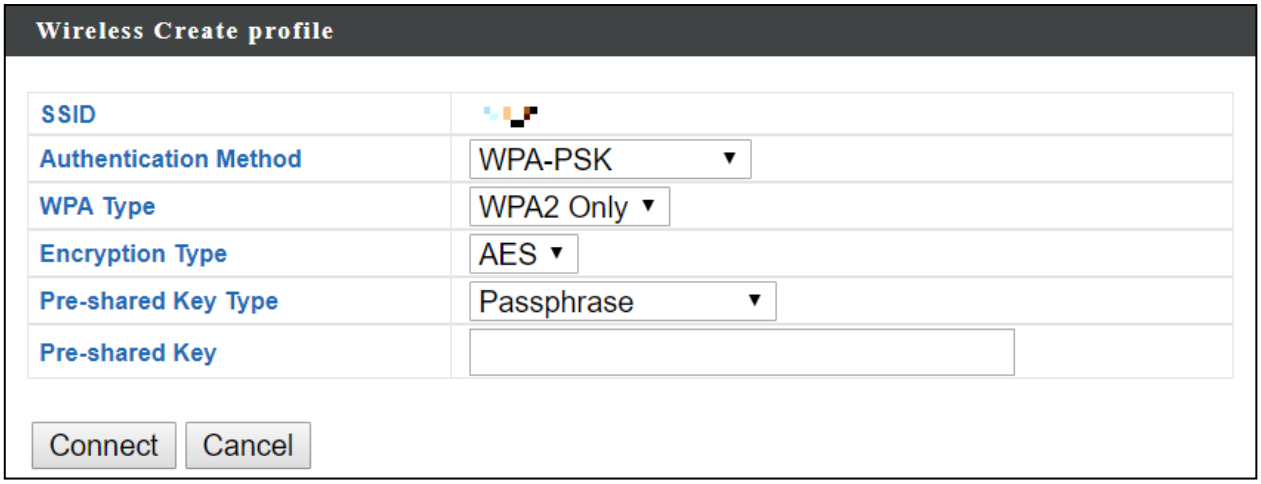
3. When system page is displayed, go to **Wireless Settings → Wireless Extender**.



4. Click Scan to search for and display available SSIDs

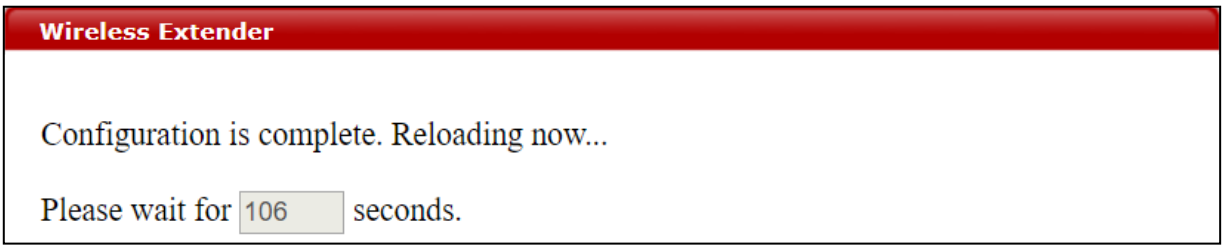


5. Click the circle icon to connect to an available source SSID. SSIDs can be configured independently for each frequency 2.4GHz & 5GHz.

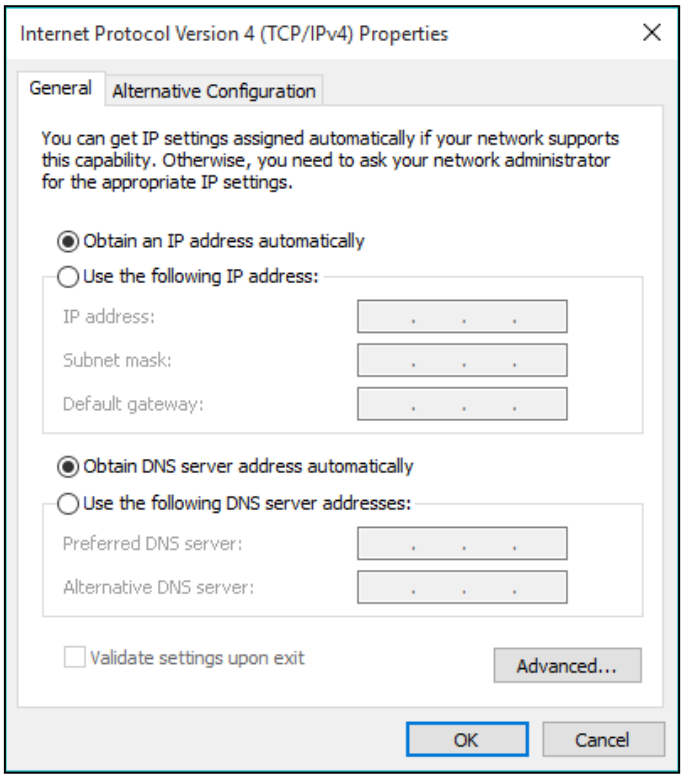


6. Edit according to your preference and enter the security details for the source SSID (e.g. Pre-shared Key). Click “Connect” to proceed.

Wait for the configuration to take effect:



7. The device (now in Client Bridge Mode) will receive wireless signal and provides it to devices connected to the bridge via Ethernet cable. The device will become a DHCP client of the router/root AP. Switch your computer back to dynamic IP address.



8. To access the web user interface, check your router/root AP’s settings to determine the device’s new IP address. Enter the new IP address into the browser for the web user interface.

If you wish to switch the operation mode, please reset the device to factory default (via web user interface or hardware reset).

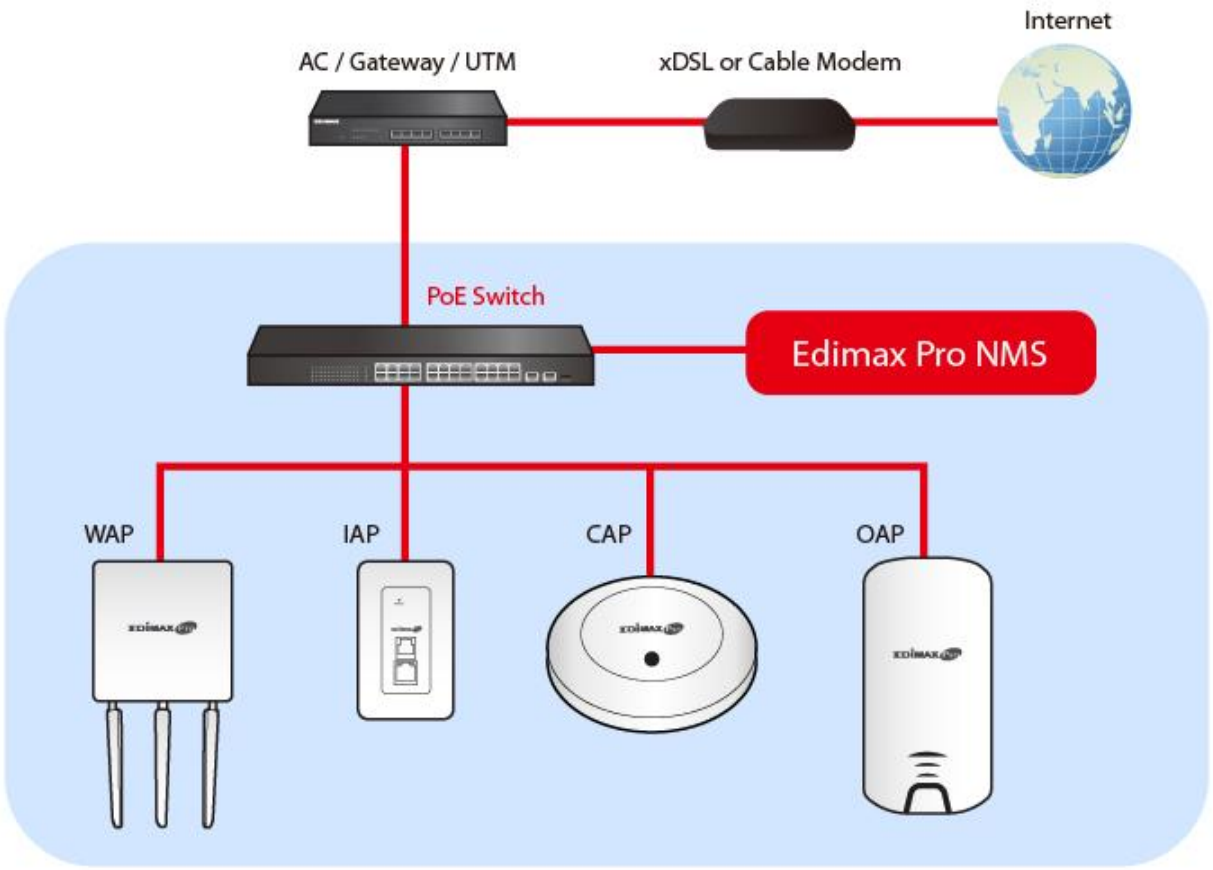
II-4 Managed AP Mode

Scenario: The Unit being managed by an AP Controller

The access point can be part of an AP Array by switching to “Managed AP Mode”.

An AP Array is a *group of access points* centrally managed by an *AP Controller*, where it can monitor, configure and manage all Managed APs.

An overview of the system is shown below:

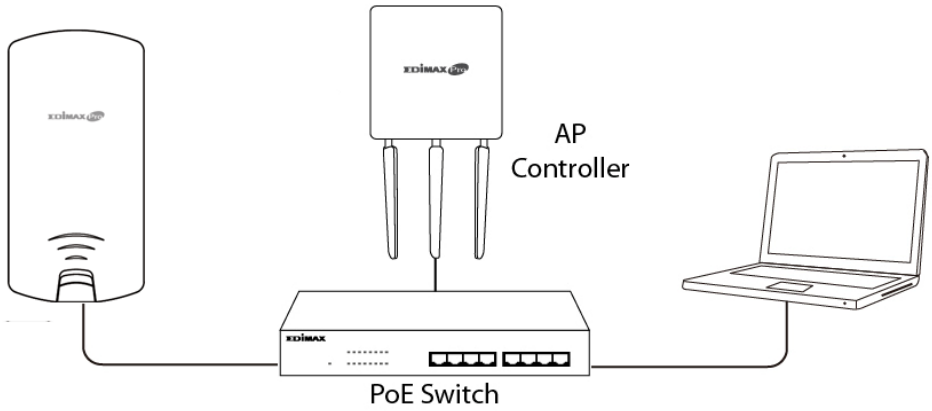


By default, the access point will automatically switch mode if an AP Controller is present in the network.

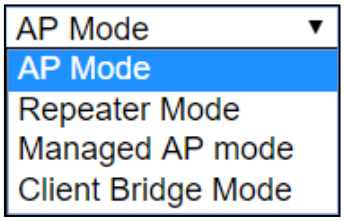
To manually change to “Managed AP Mode”:

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

1. Connect an AP Controller to the switch currently connected to the access point and computer.



2. From the default mode above, select Managed AP Mode from the operation mode drop down menu:



3. Press “Apply” and wait for the device to reboot into Managed AP Mode:

Wait for a few minutes for the settings to sync.

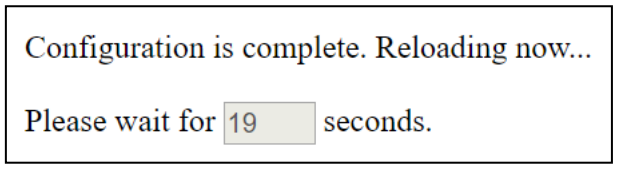
II-5 Basic Settings

Basic settings of the access point are:

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

It is recommended that these settings are configured before using the access point.

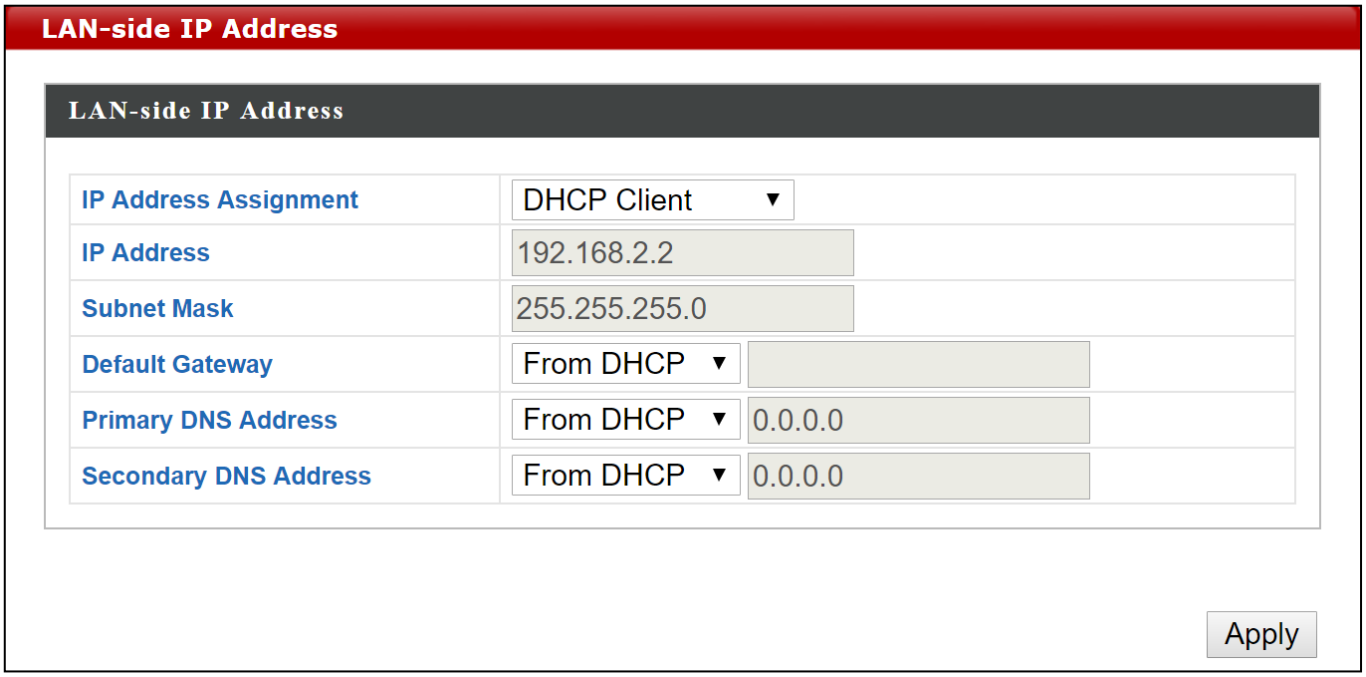
Whenever a new setting is applied to the access point, the webpage will reload, as shown below:



Instructions below will help you configure these settings:

Changing IP Address:

1. Go to **"Network Settings" > "LAN-side IP Address"** for the screen below:



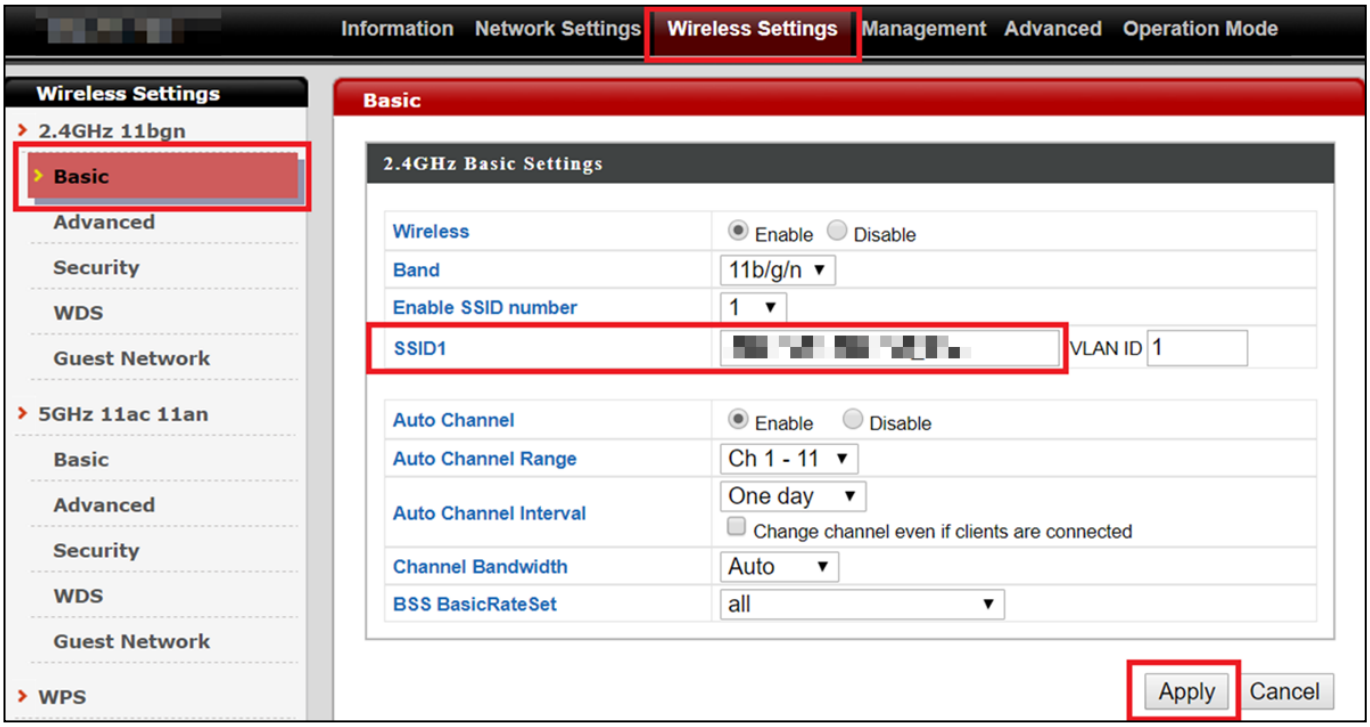
2. Enter the IP address settings you wish to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click "Apply" to save the changes and wait a few moments for the access point to reload.

When you change your access point'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.*

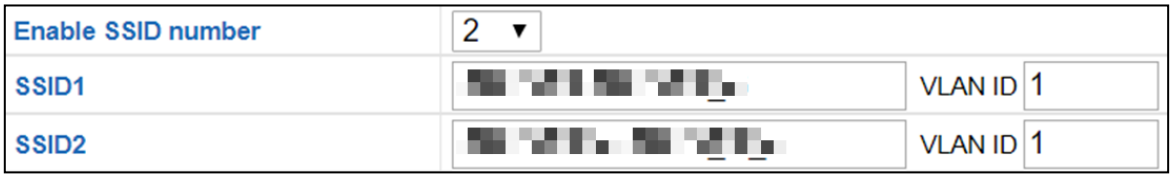
Changing SSID for 2.4GHz wireless network

1. Go to **"Wireless Settings" > "2.4GHz 11bgn" > "Basic"**.

2. Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".

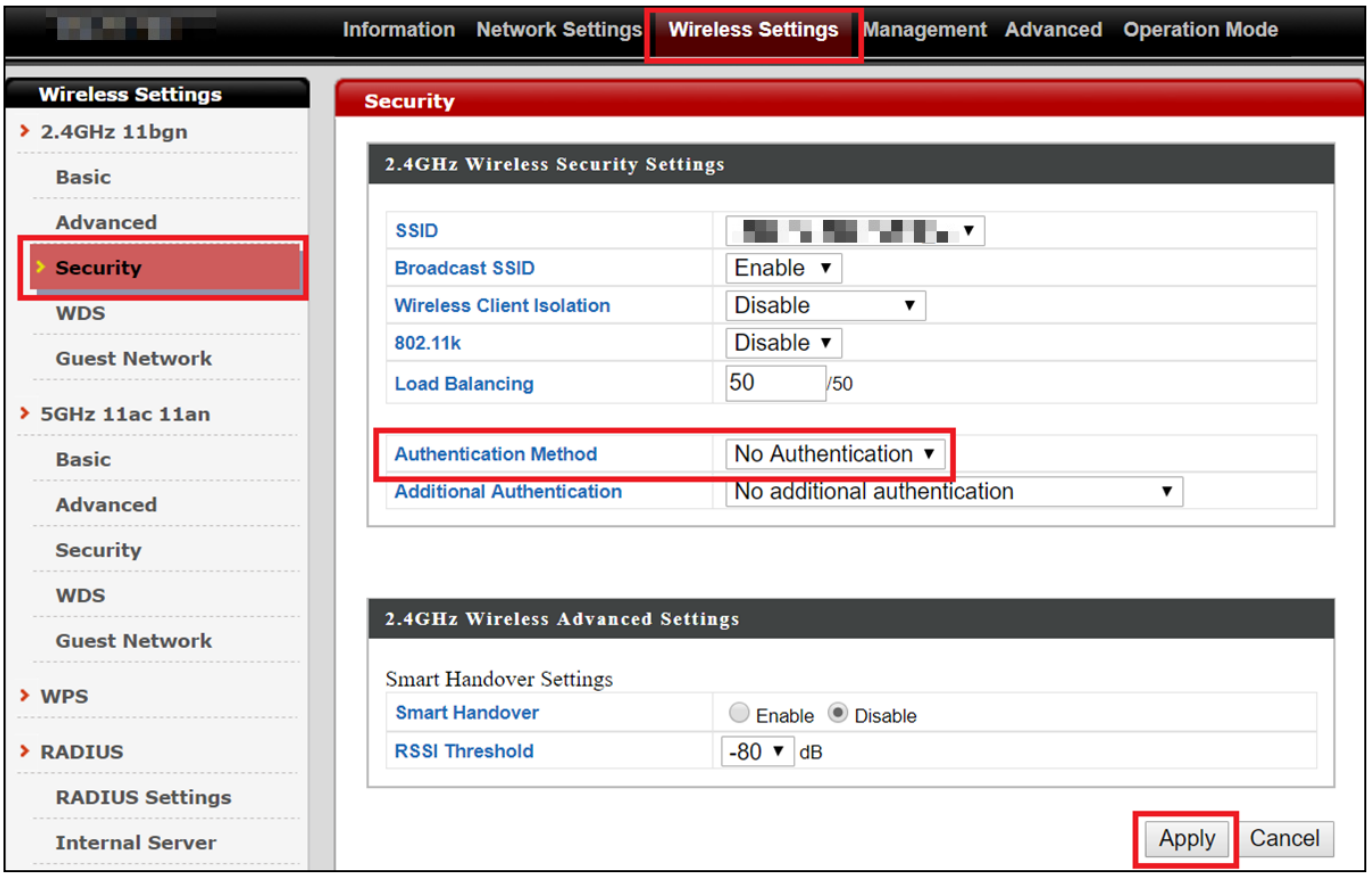


To utilize multiple 2.4GHz SSIDs, open the drop down menu labelled *"Enable SSID number"* ***and select how many SSIDs you require. Then enter a new SSID in the corresponding numbered fields below, before clicking "Apply".***

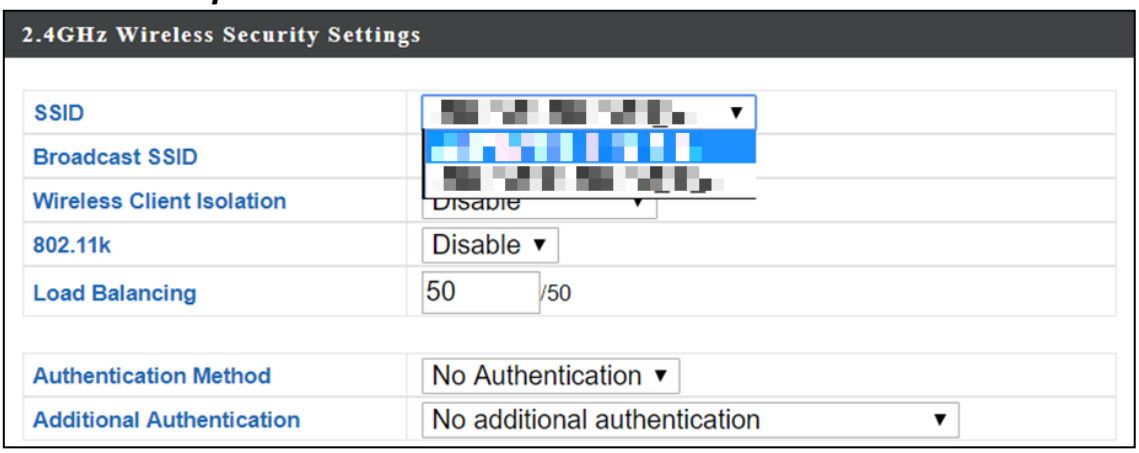


Configuring Security Settings of 2.4GHz wireless network

1. Go to **“Wireless Settings” > “2.4GHz 11bgn” > “Security”**.
2. 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.



Changing SSID and Configuring 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.

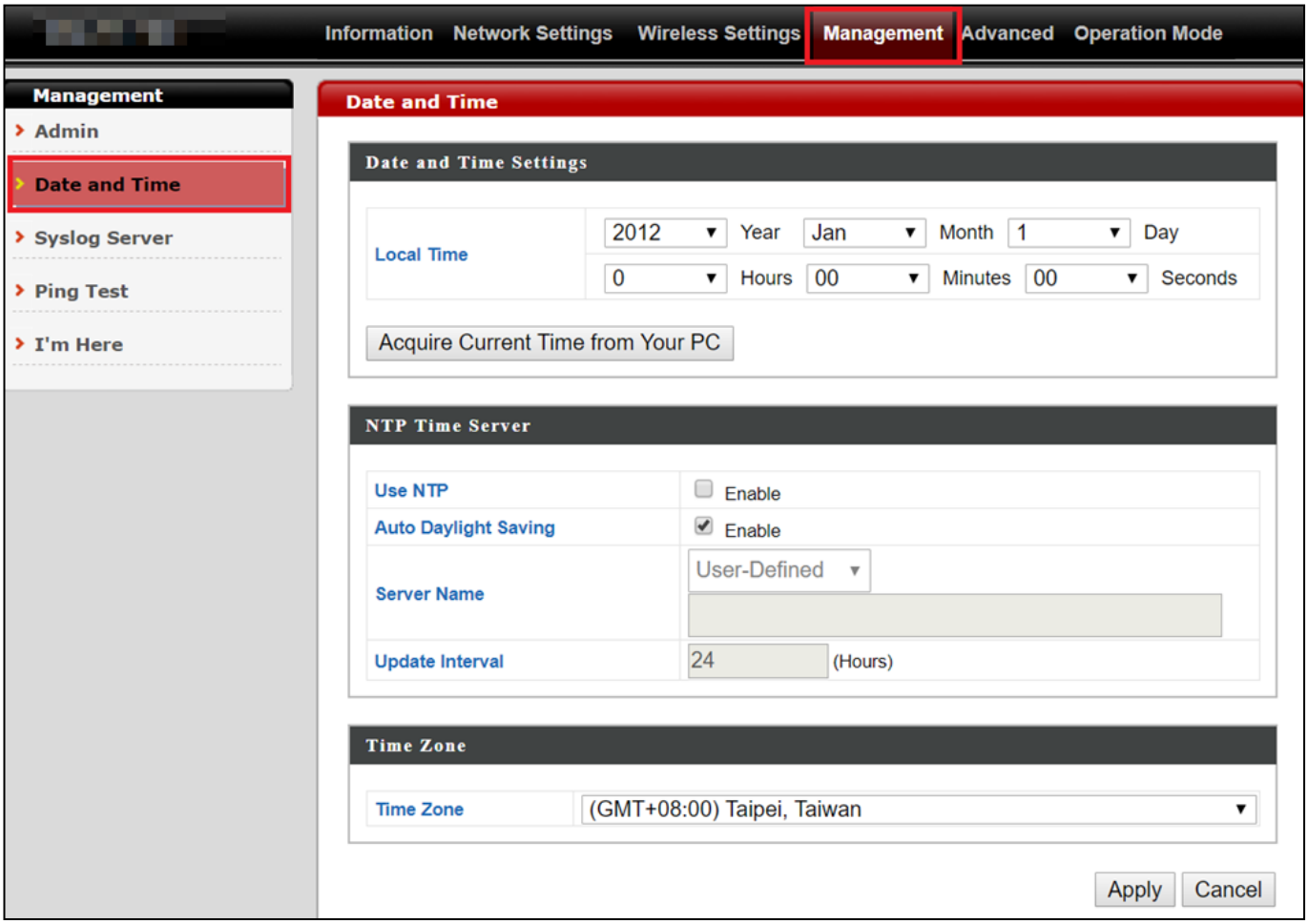
Changing Admin Name and Password

1. Go to **“Management” > “Admin”** as shown below:

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

Changing Date and Time

1. Go to **“Management” > “Date and Time”**.



2. Set the correct time and time zone for your access point using the drop down menus. The access point also supports NTP (Network Time Protocol) so, 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 access point to the same time as your PC.

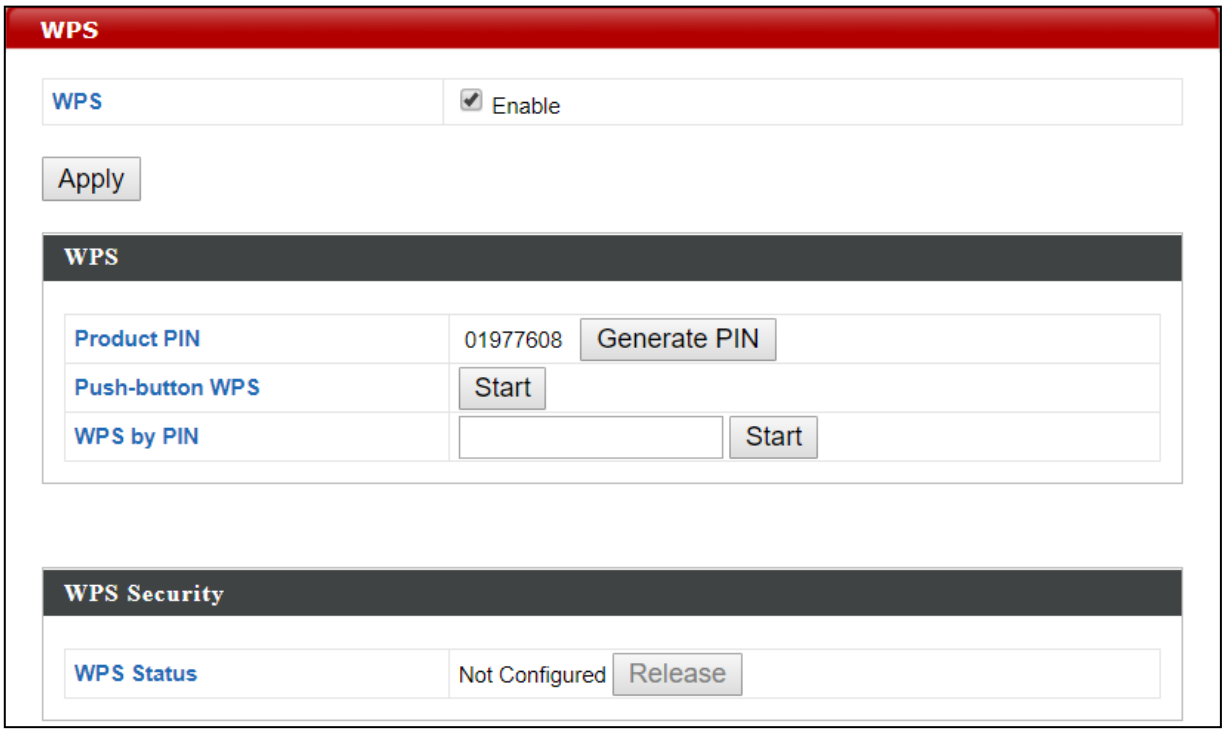
The basic settings of your access point are now configured. Please refer to **III Hardware Installation** for guidance on connecting your access point to a PoE switch.

II-6 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. You can use the WPS button or the configuration webpage activate the access point's WPS function.

1. Go to **"Wireless Settings" > "WPS"** on your configuration webpage.

2. Check the checkbox of "Enable" and click "Apply".



3. On the "Push-button WPS" line, click "Start" to activate WPS on the AP for approximately 2 minutes.
(For more information on "WPS by PIN", please refer to ***IV-3-3 WPS***).

4. Within two minutes, activate WPS on your WPS-compatible wireless device. Please check the documentation of your wireless device for information regarding its WPS function.

5. The devices will establish a connection.

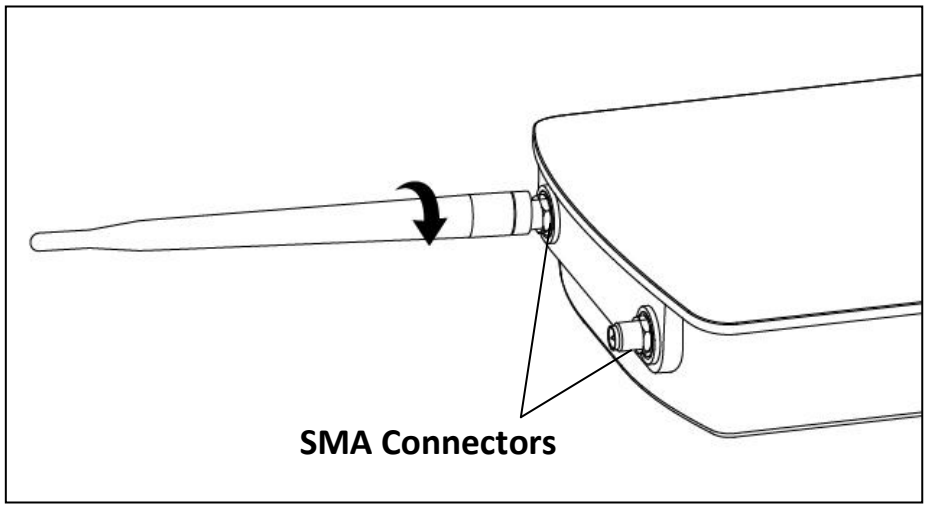
III Hardware Installation

After finishing the above setup processes, you may relocate the access point to the desired location.

III-1 Antenna

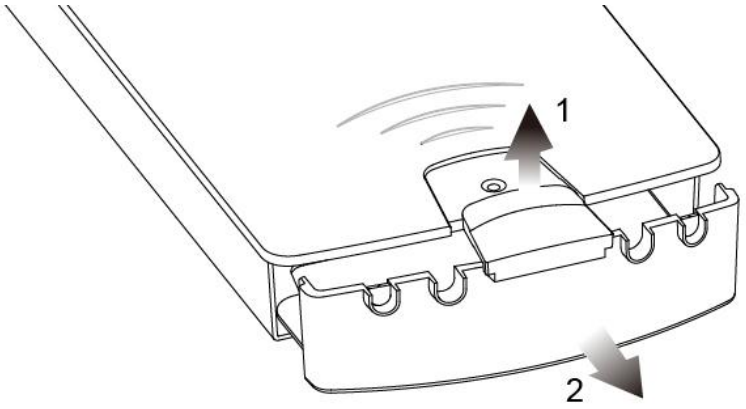
The antennae must be screwed onto the access point.

Please screw both antennae on clock-wise onto the SMA connectors as demonstrated below:

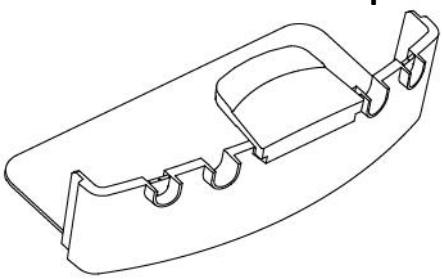


III-2 Powering on the Access Point Outdoor

1. Remove the cap from the underside of the access point by 1) pulling the hook upwards, and 2) pulling the cap downward, as shown below:

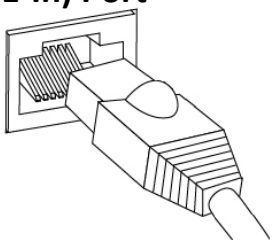


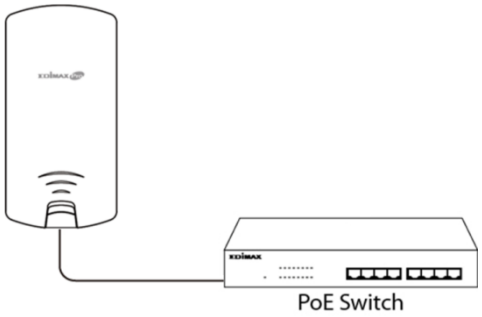
Removed Underside Cap



2. Wire an Ethernet cable to the **LAN 1 (PoE-In)** port of the access point and the PoE switch to power up the access point.

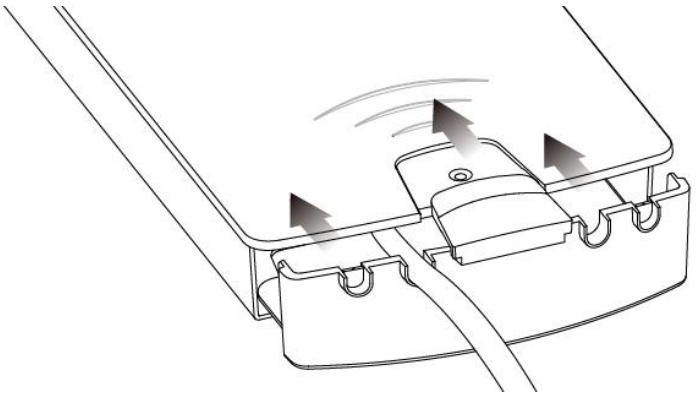
LAN 1 (PoE-In) Port



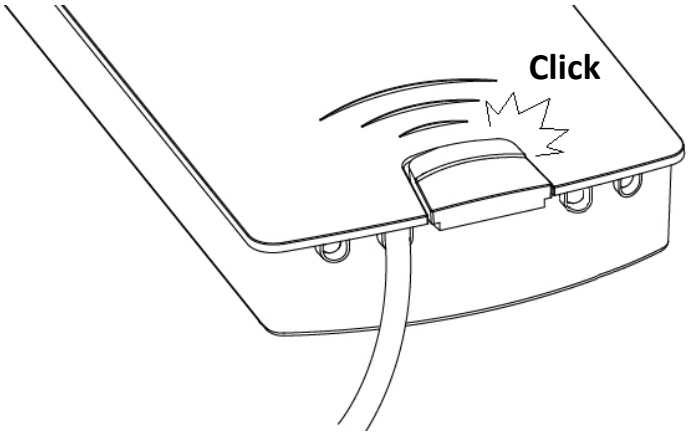


3. The access point will be powered by the PoE switch. Connect another Ethernet cable to **LAN 2** where necessary.

4. Replace the cap and allow the cable(s) to rest in the arch(es) of the cap.



5. Let the hook click with the access point and make sure it does not come off easily. The cap serves as a rain-proof design suitable for use in the open.

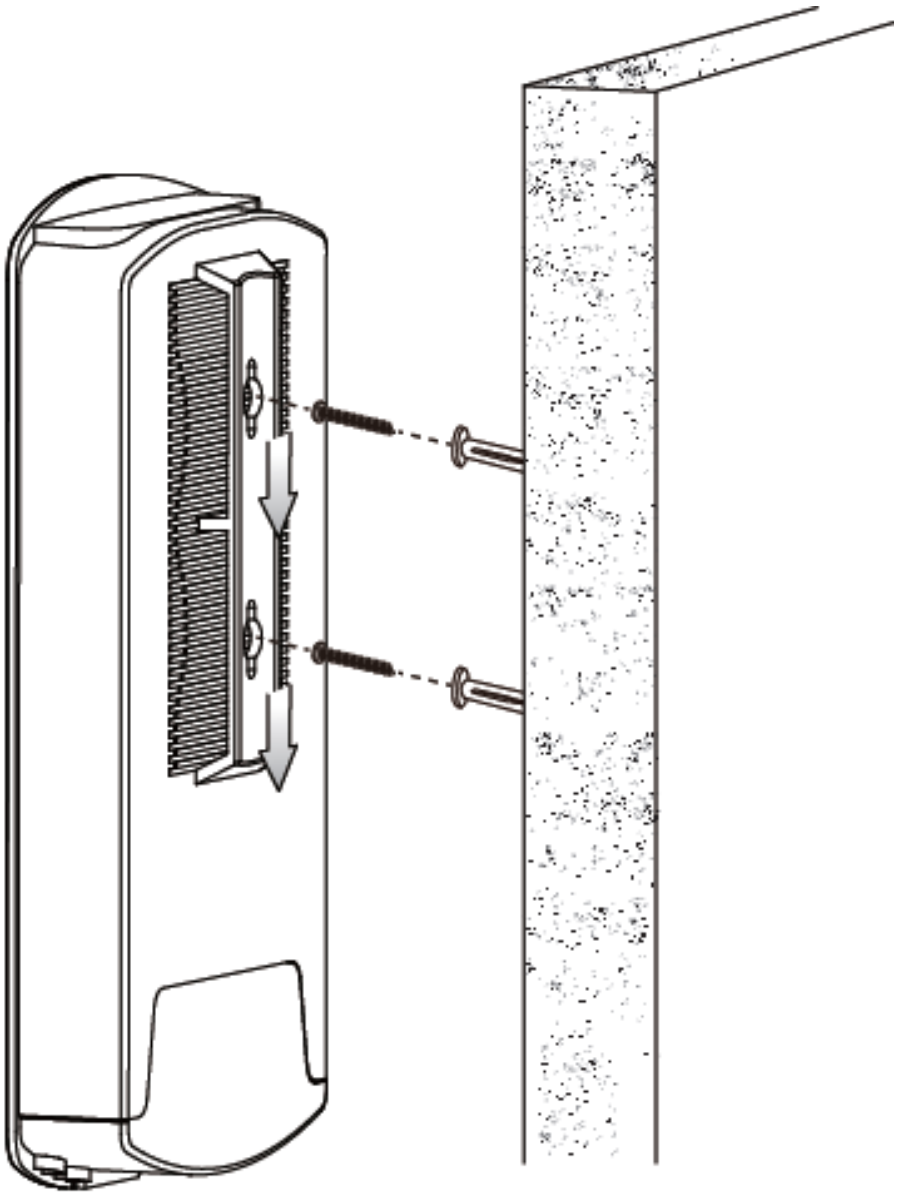


III-3 Mounting

After powering up the access point, mount it according to the desired mounting options: **Wall** or **Pole Mount**

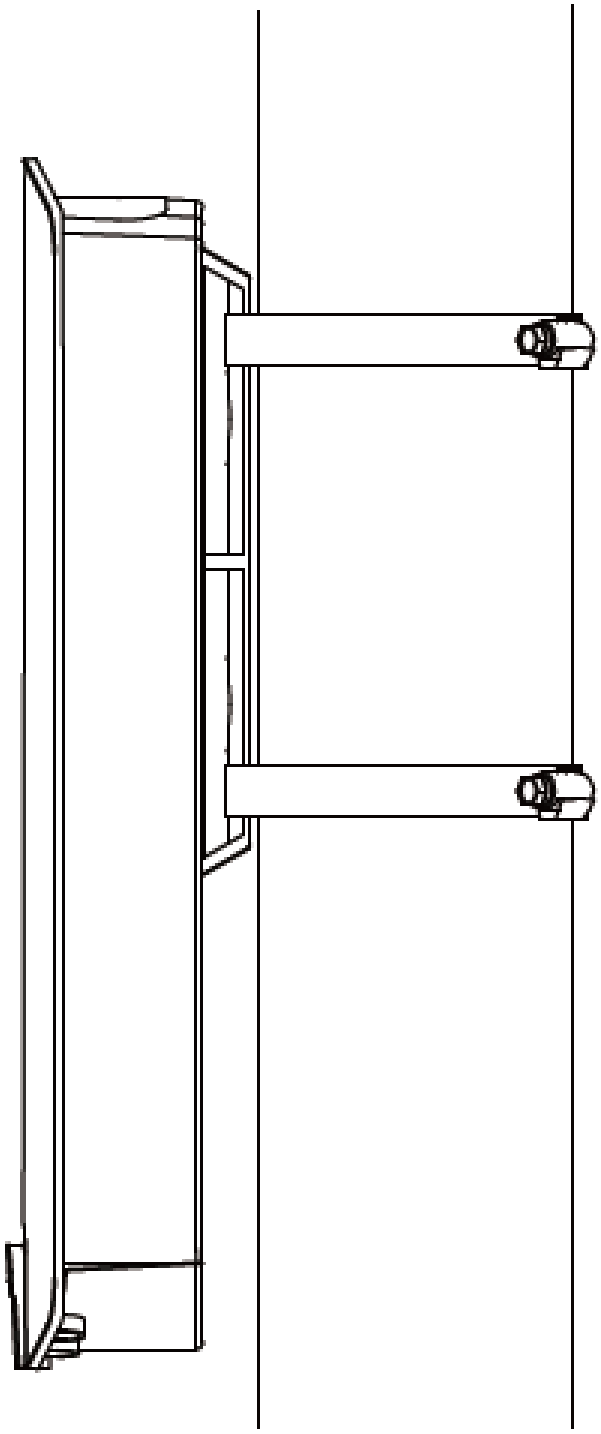
Wall Mount

Attach the mount and access point to a wall using the included wall mount template and wall mount screw sets.



Pole Mount

Fix the mount and access point to a pole using the included pole mount straps.



IV Browser Based Configuration Interface

Some functions of the browser based configuration interface are disabled for different mode settings, please refer to the sections applicable for your desired mode.

The browser-based configuration interface enables you to configure the device's advanced features. The OAP1300 features a range of advanced functions such as MAC filtering, MAC RADIUS authentication, VLAN configurations, up to 32 SSIDs and many more. To access the browser based configuration interface:

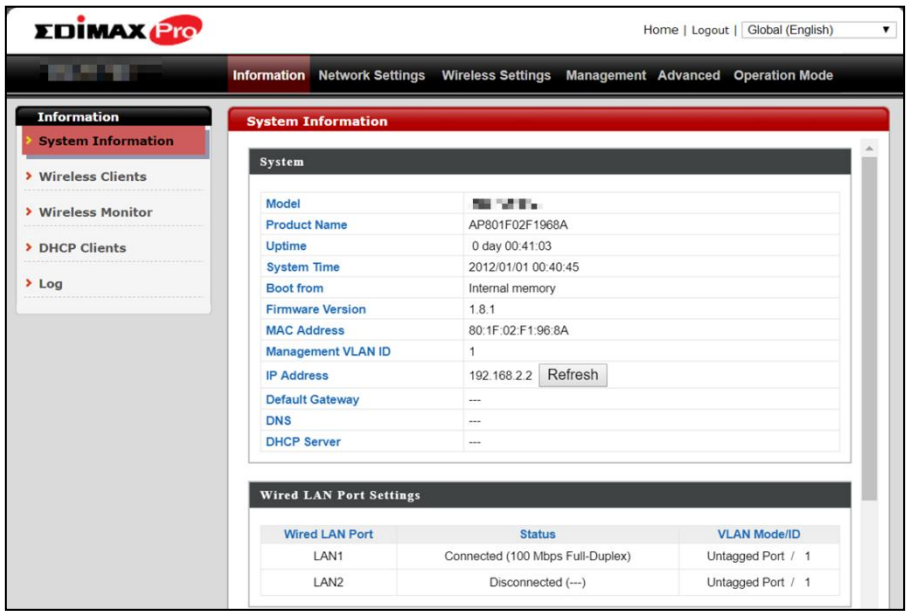
1. Connect a computer to your access point using an Ethernet cable.

2. Enter your access point's IP address in the URL bar of a web browser. The access point's default IP address is **192.168.2.2.**

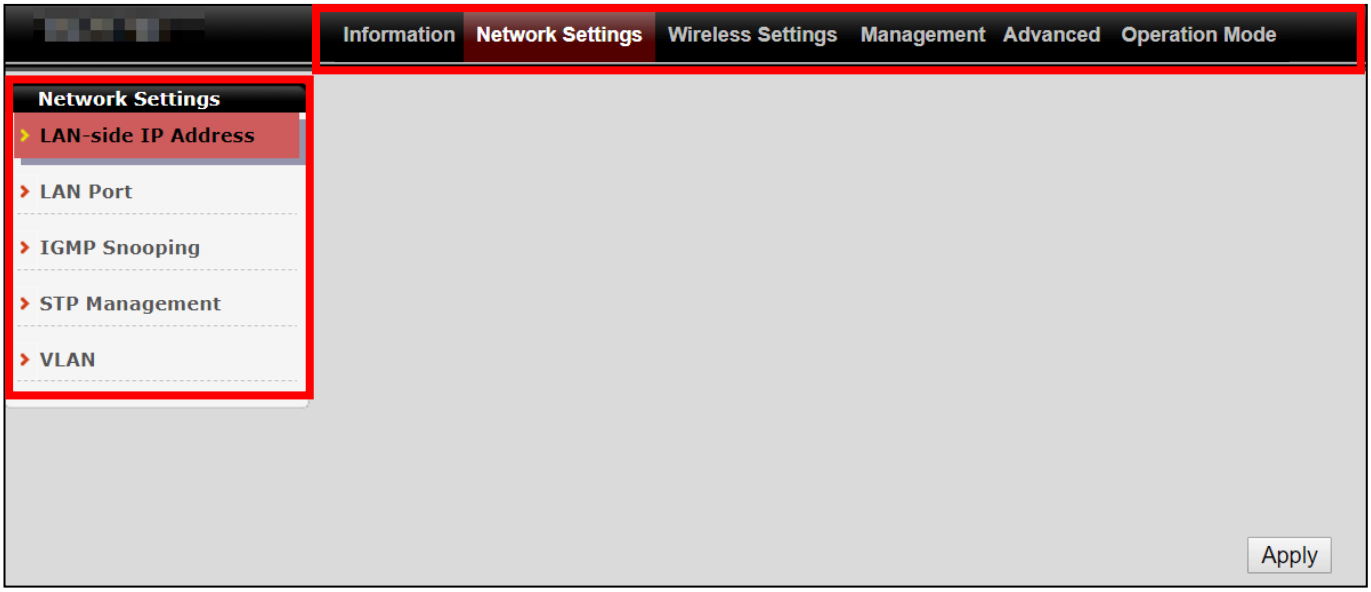
3. You will be prompted for a username and password. The default username is "admin" and the default password is "1234", though it was recommended that you change the password during setup (see ***II-5 Basic Settings***).

If you cannot remember your password, reset the access point back to its factory default settings. Refer to *0* **Reset.**

4. You will arrive at the “System Information” screen shown below.

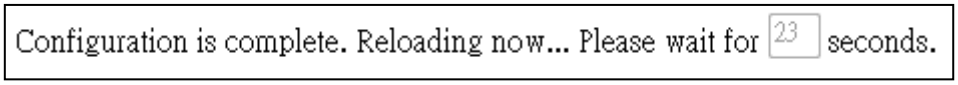


5. Use the menu across the top and down the left side to navigate.



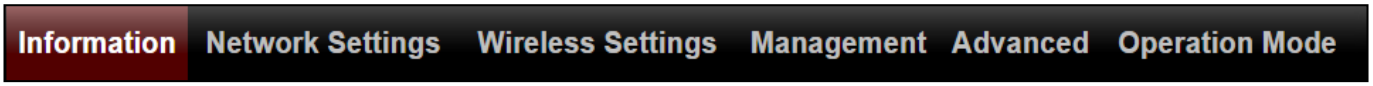
6. Where applicable, click “Apply” to save changes and reload the access point, or “Cancel” to cancel changes.

Please wait a few seconds for the access point to reload after you “Apply” changes. A countdown will be shown as exemplified below.



7. Please refer to the following chapters for full descriptions of the browser based configuration interface.

IV-1 Information



IV-1-1 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 access point.
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 access point’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. See **IV-2-5 VLAN**.

Wireless 2.4GHz (5GHz)	
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or disabled).
MAC Address	Displays the access point’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.

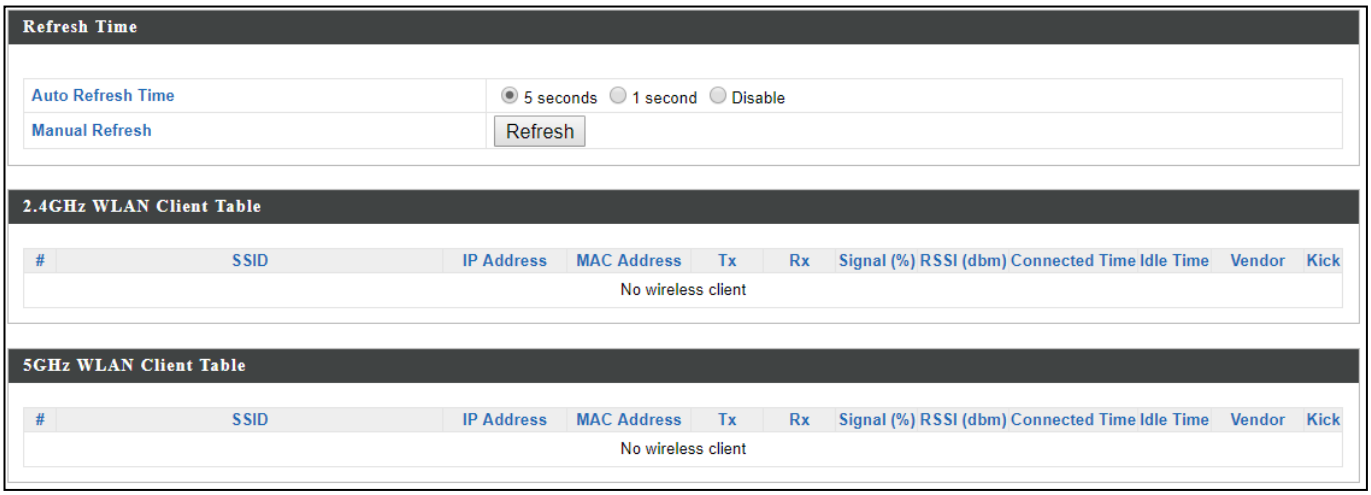
Wireless 2.4GHZ (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID. See **IV-3 Wireless Settings**.
Encryption Type	Displays the encryption type for the specified SSID. See **IV-3 Wireless Settings**.
VLAN ID	Displays the VLAN ID for the specified SSID. See **IV-2-5 VLAN**.
Additional Authentication	Displays the additional authentication type for the specified SSID. See **IV-3 Wireless Settings**.
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID. See **IV-2-5 VLAN**.

Wireless 2.4GHZ (5GHz) / WDS Status	
MAC Address	Displays the peer access point's MAC address.
Encryption Type	Displays the encryption type for the specified WDS. See **IV-3-1-4 WDS**.
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See **IV-3-1-4 WDS**.

Select "Refresh" to refresh all information.

IV-1-2 Wireless Clients

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

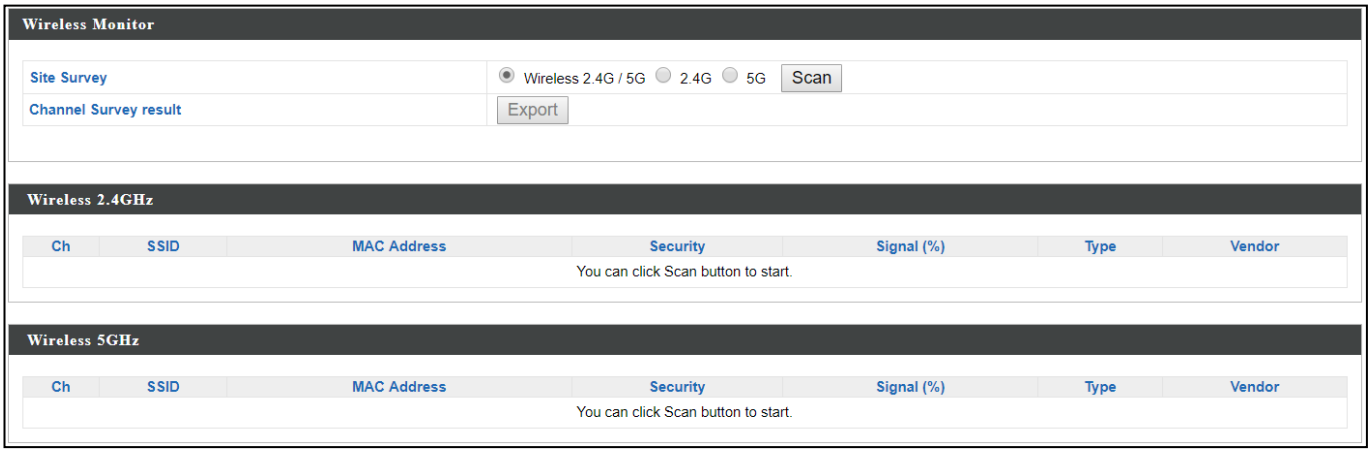


Refresh time	
Auto Refresh Time	Select a time interval for the client table list to automatically refresh.
Manual Refresh	Click refresh to manually refresh the client table.

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 access point.
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.

IV-1-3 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.

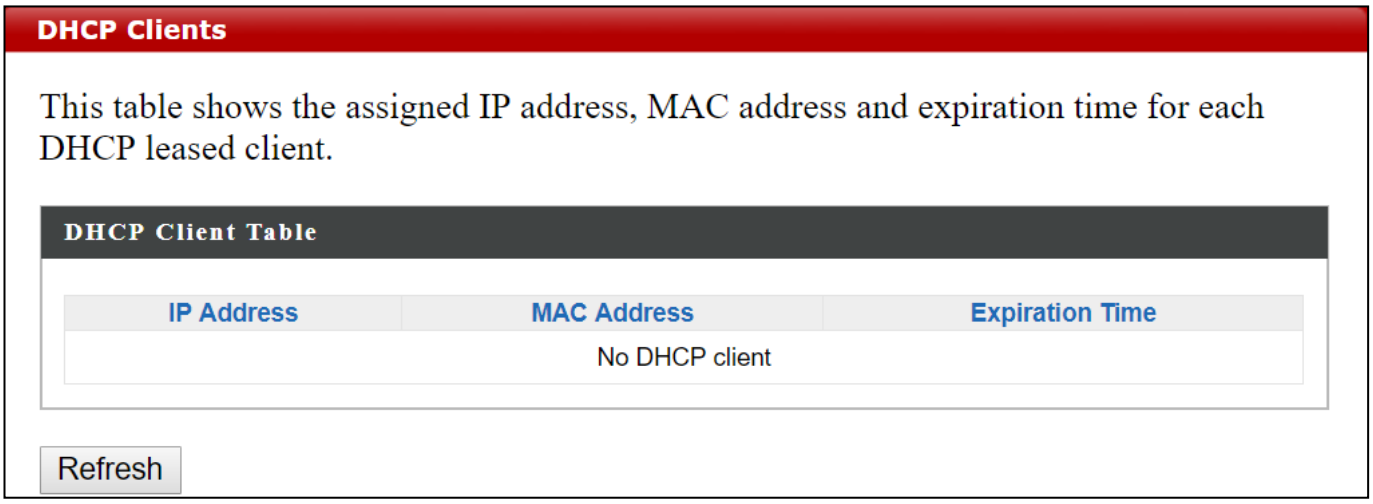


Wireless Monitor	
Site Survey	Select which frequency (or both) to scan, and click “Scan” to begin.
Channel Survey Result	After a scan is complete, click “Export” to save the results to local storage.

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/access point 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/access point for the specified SSID.

IV-1-4 DHCP Clients

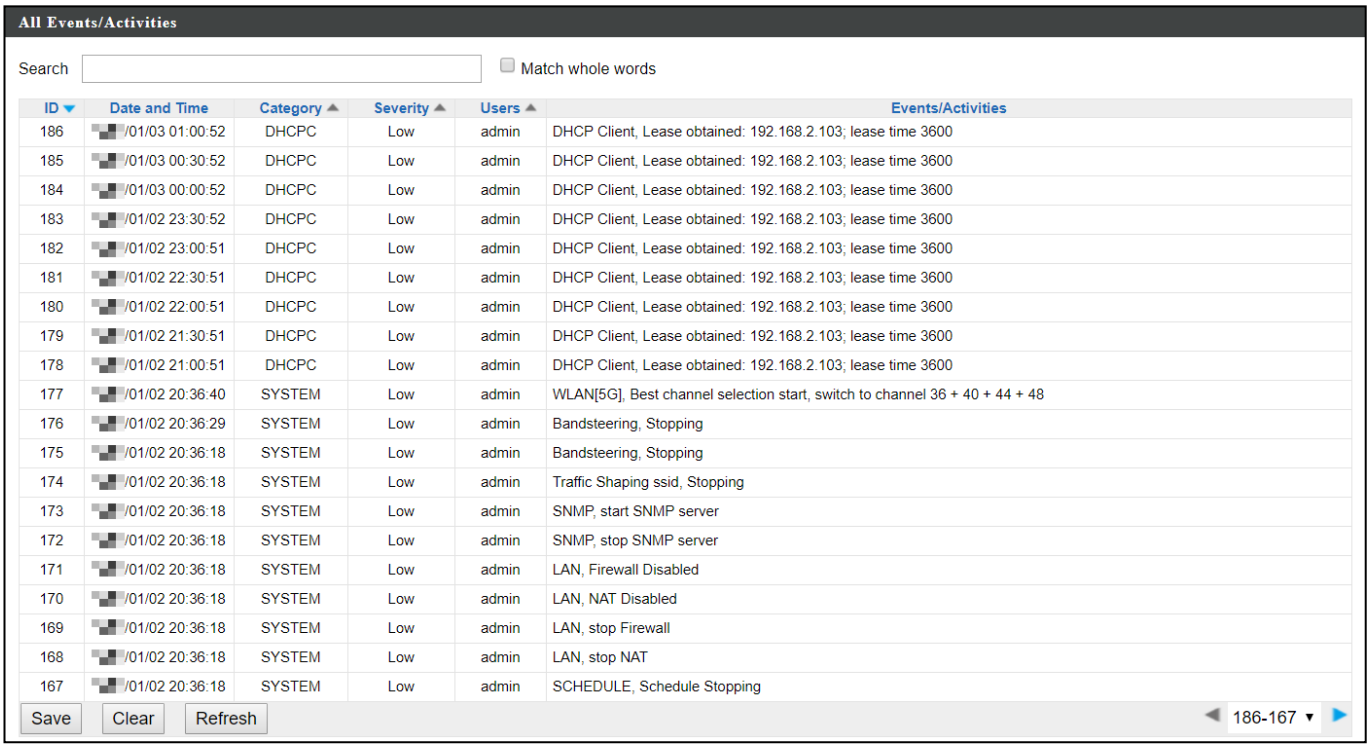
“DHCP Clients” shows information of DHCP leased clients.



IV-1-5 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



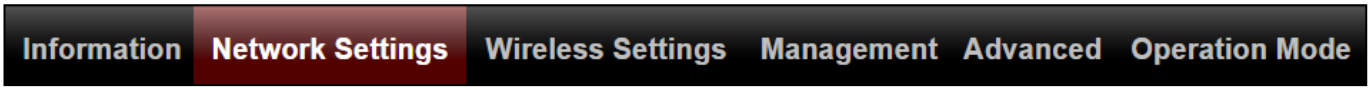
Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

The following information/events are recorded by the log:

- **USB**
  Mount & unmount
- **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**
- **System Boot**
  Displays current model name
- **NTP Client**
- **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)**
  WLAN (2.4G] channel status and country/region status
- **WLAN (5G)**
  WLAN (5G) channel status and country/region status

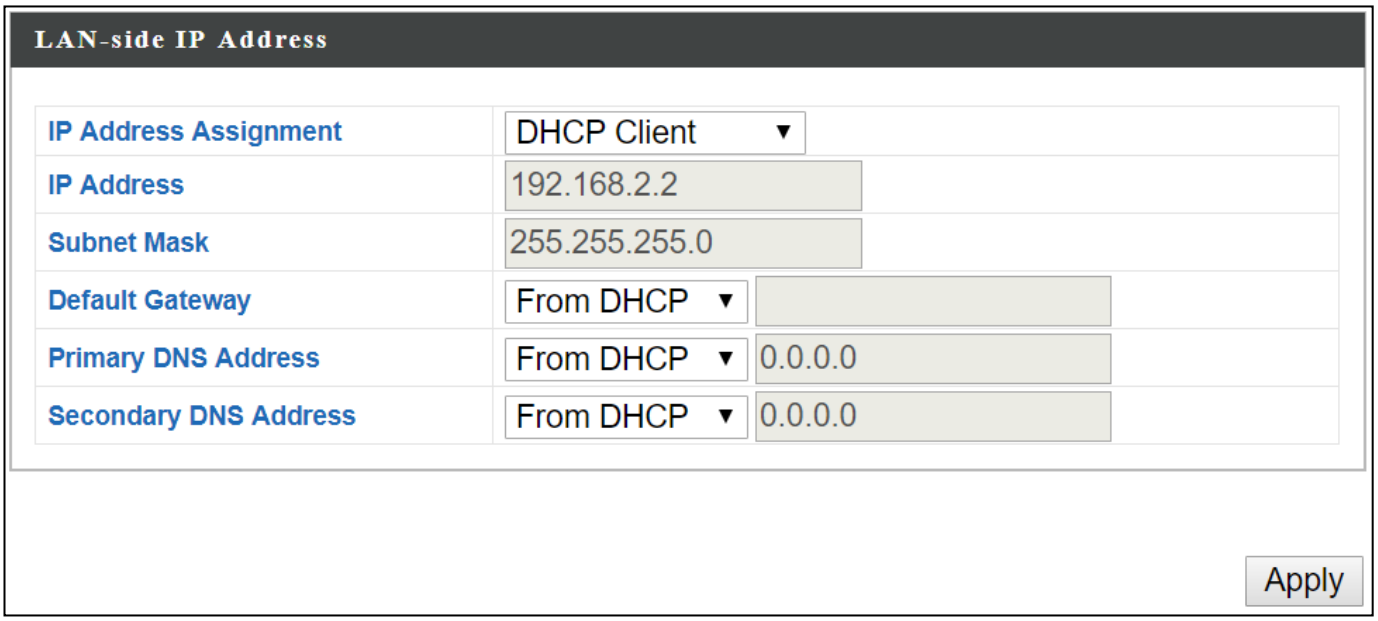
IV-2 Network Settings



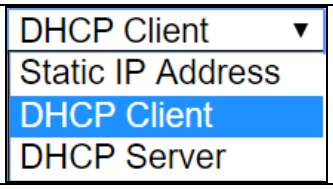
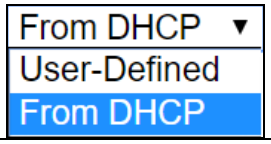
IV-2-1 LAN-Side IP Address

"LAN-side IP address" page allows you to configure your access point on your Local Area Network (LAN). You can enable the access point to dynamically receive an IP address from your router's DHCP server or you can specify a static IP address for your access point, as well as configure DNS servers.

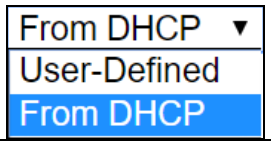
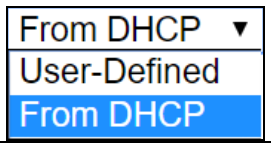
The access point's default IP address is 192.168.2.2.



LAN-side IP Address	
IP Address Assignment	Select "DHCP Client" for your access point 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 access point (below). Select "DHCP Server" for your access point 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 access point 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. 

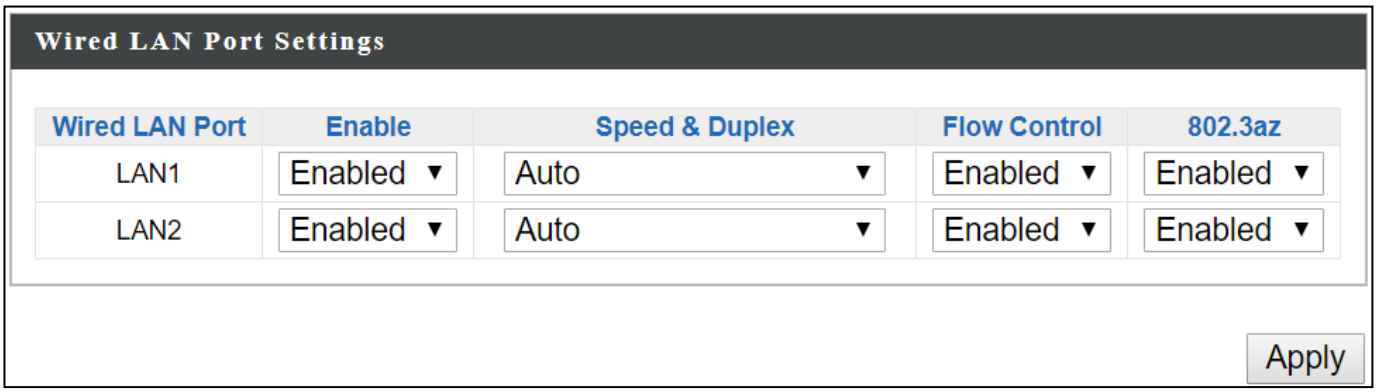
DHCP users can select to get DNS servers’ IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

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”. 

Press “Apply” to confirm the settings.

IV-2-2 LAN Port

“LAN Port” page allows you to configure the settings for your access point’s two wired LAN (Ethernet) ports.



Wired LAN Port	Identifies LAN port 1 or 2.
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 is an Energy Efficient Ethernet feature which disables unused interfaces to reduce power usage.

Press “Apply” to confirm the settings.

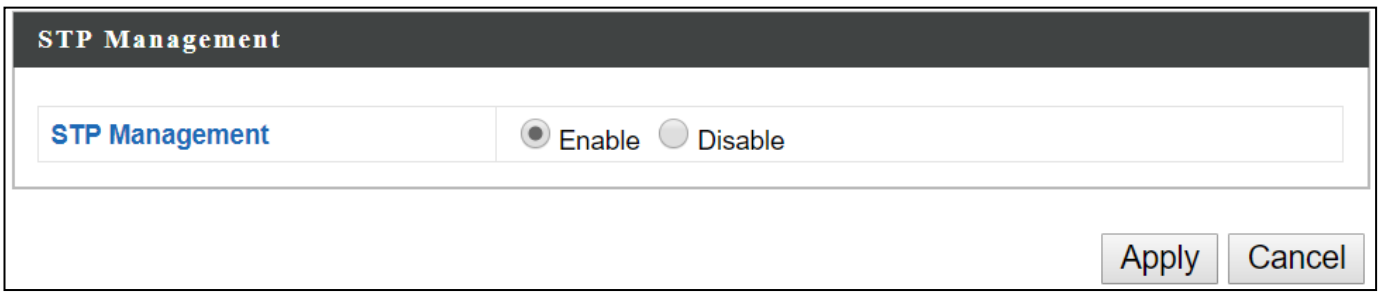
IV-2-3 IGMP Snooping

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 IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.
This page allows you to enable/disable this feature.

Press “Apply” to confirm the settings.

IV-2-4 STP Management

When enabled, STP ensures that you do not create loops when you have redundant paths in your network (as loops are deadly to a network).
This page allows you to enable / disable STP management.

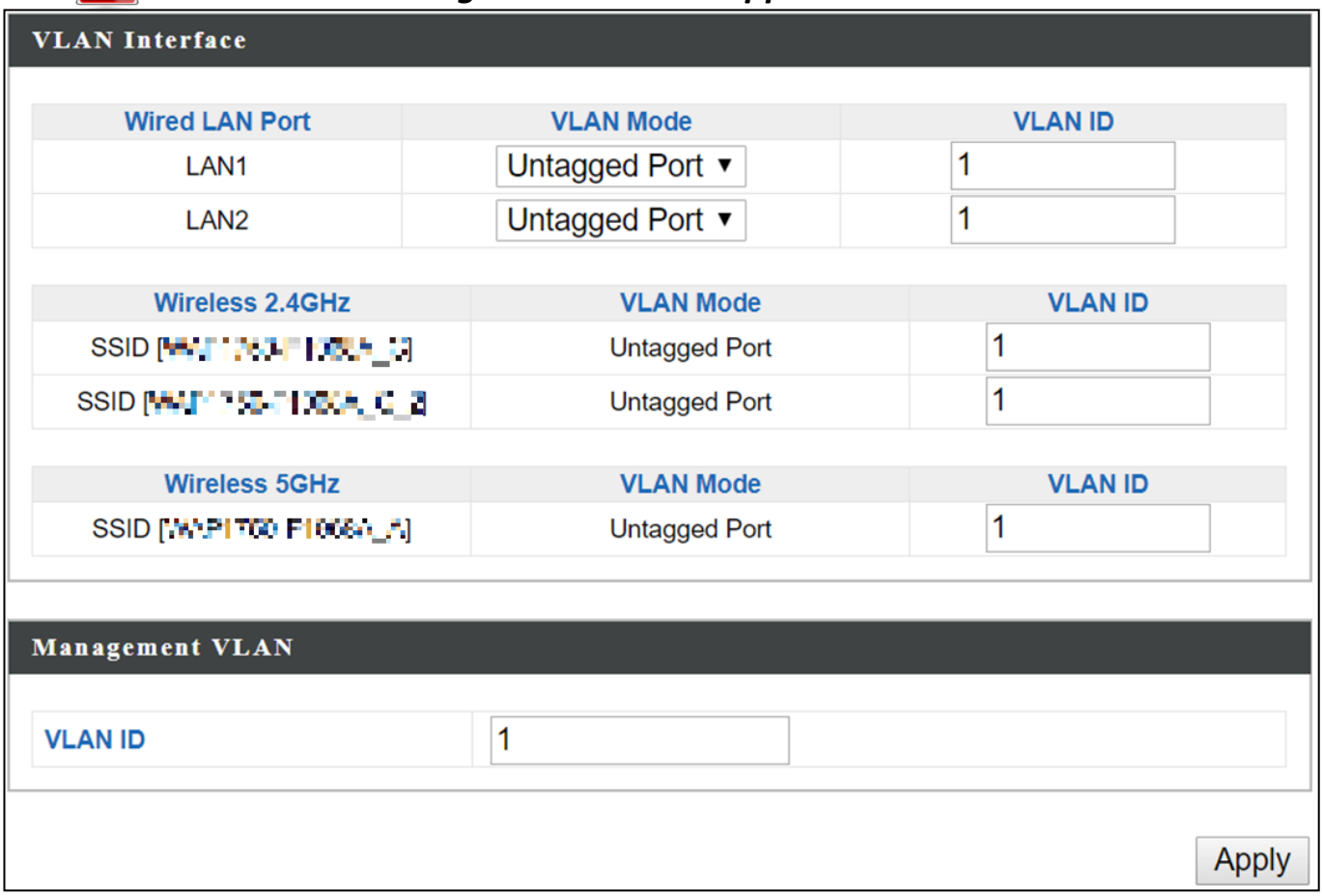


Press “Apply” to confirm the settings.

IV-2-5 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 or 2 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.

Press "Apply" to confirm the settings.

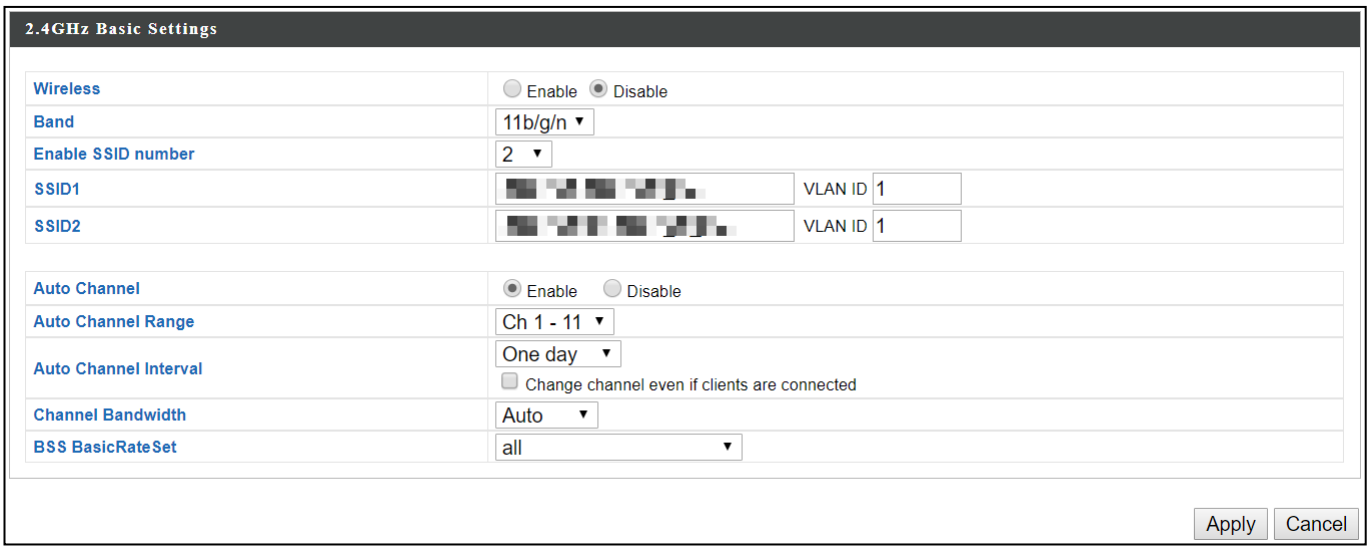
IV-3 Wireless Settings

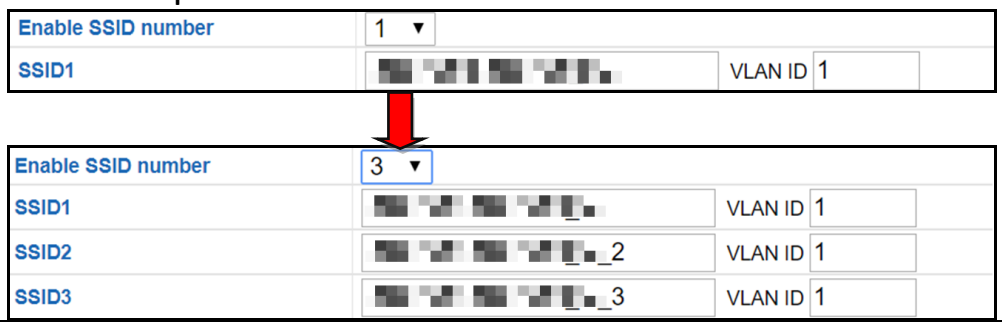
IV-3-1 2.4GHz 11bgn

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

IV-3-1-1 Basic

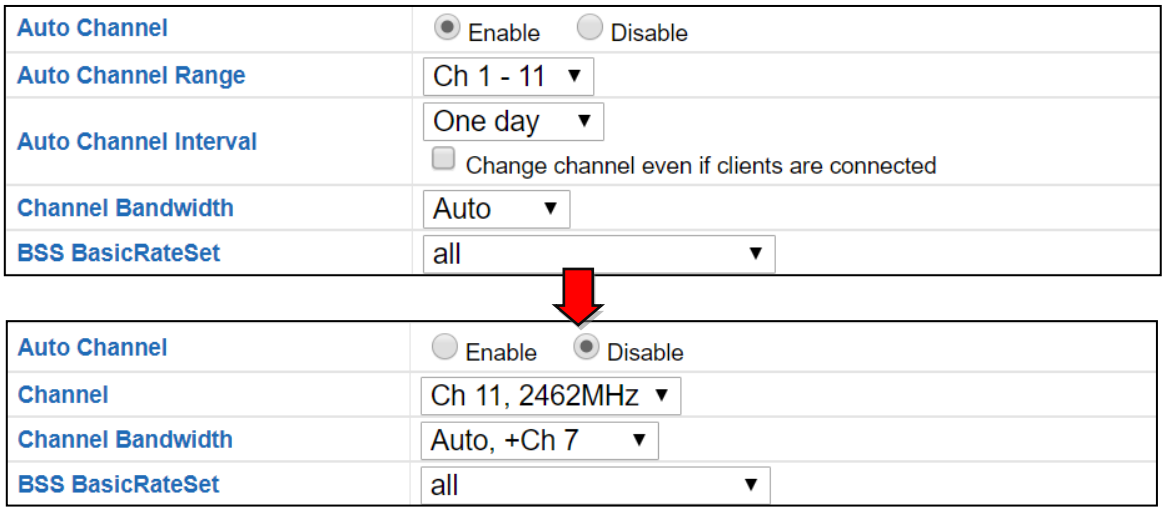
The “Basic” screen displays basic settings for your access point’s 2.4GHz Wi-Fi network (s).



Wireless	Enable or disable the access point’s 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active.
Band	Wireless standard used for the access point. 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 access point’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:



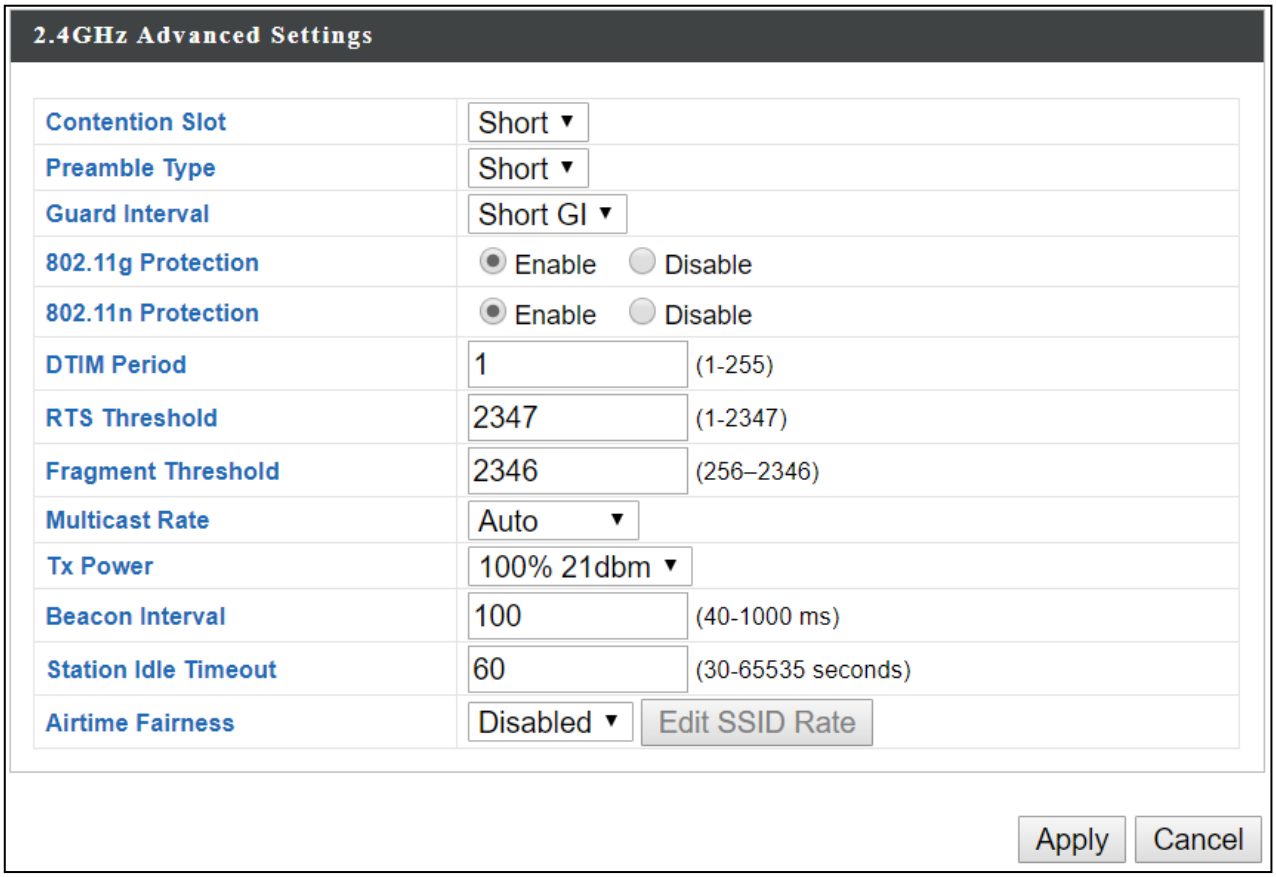
Channel	Select a wireless channel from 1 – 11.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference); or 40MHz (higher performance but potentially higher interference); or Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service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

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

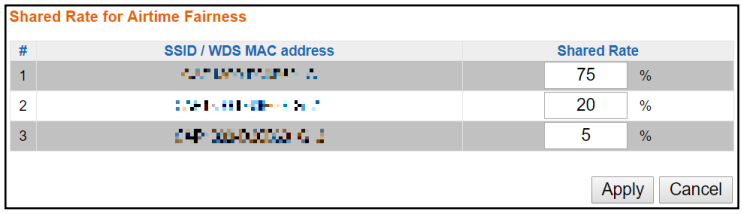
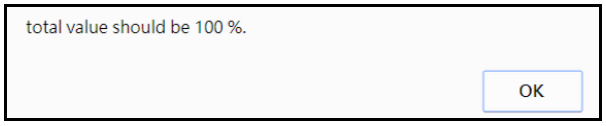
IV-3-1-2 Advanced

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 access point.



Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM (see ***IV-3-6 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 access point 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 access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client).

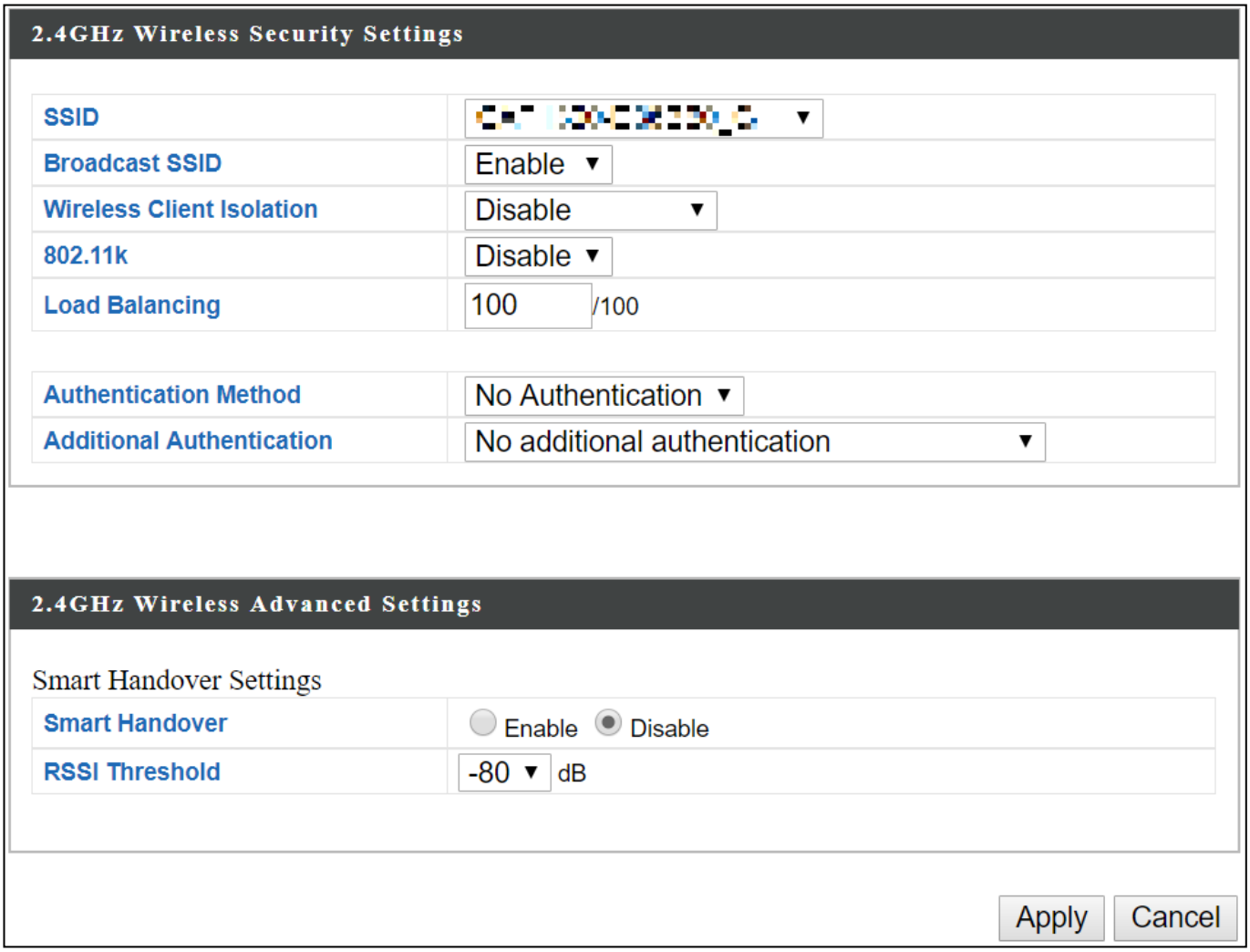
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client).
DTIM Period	Set the DTIM (delivery traffic indication 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 access point 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”. **Auto**: Share rate is automatically managed. **Static**: Press “Edit SSID Rate” to manually enter a % for each SSID’s share rate as shown below:  The % field must add up to 100% or a message will be displayed:  Airtime fairness is disabled if “Disable” is selected.

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

IV-3-1-3 Security

The access point 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 access point 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-3-1-3-1 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 access point. 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. See** IV-3-3 WPS **for WPS settings.

MAC Address Filter

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

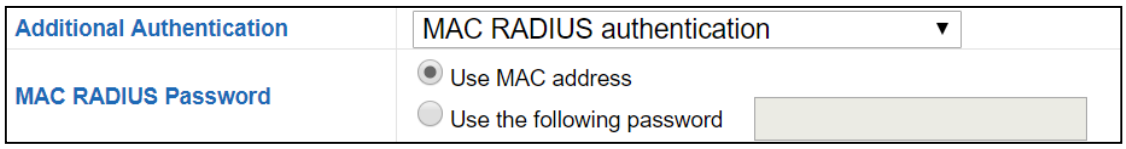
See** IV-3-5 MAC Filter **to configure MAC filtering.

MAC-RADIUS Authentication

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

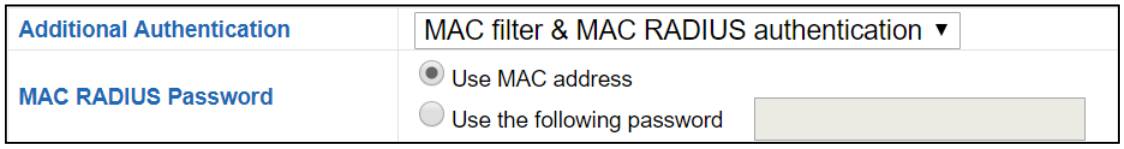
See** IV-3-4 RADIUS **to configure RADIUS servers.

WPS must be disabled to use MAC-RADIUS authentication. See** IV-3-3 WPS **for WPS settings.



MAC Filter & MAC-RADIUS Authentication

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

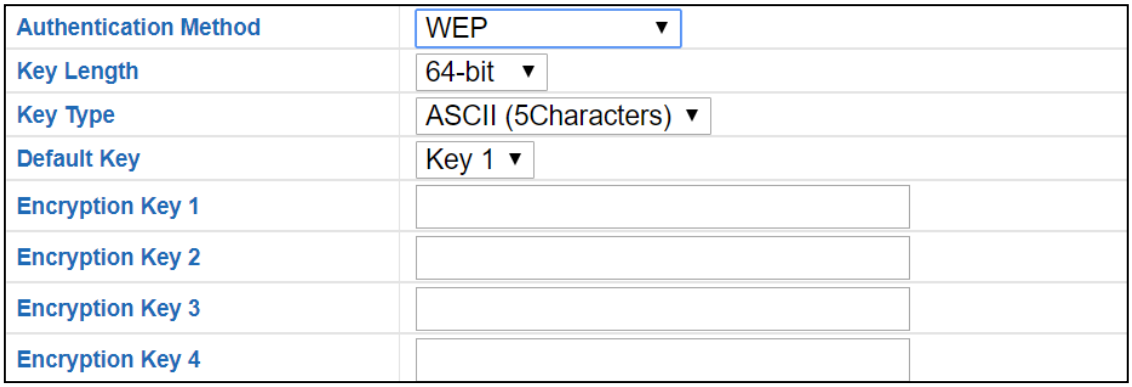


MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select “Use the following password”, enter the password in the field below. The password should match the “Shared Secret” used in **IV-3-4 RADIUS**.

IV-3-1-3-2 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:

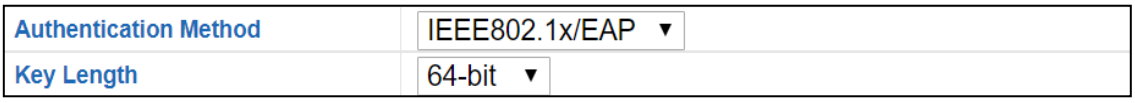


Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
Key Type	Choose from “ASCII” (any alphanumerical character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key (1 – 4 below) is the default key. For security 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.

IV-3-1-3-3 IEEE802.1x/EAP

Below is a figure showing the configurable fields:

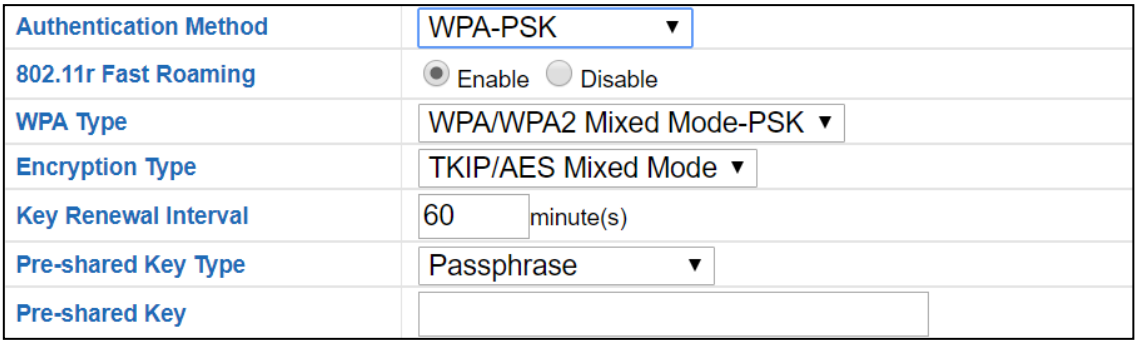


Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.

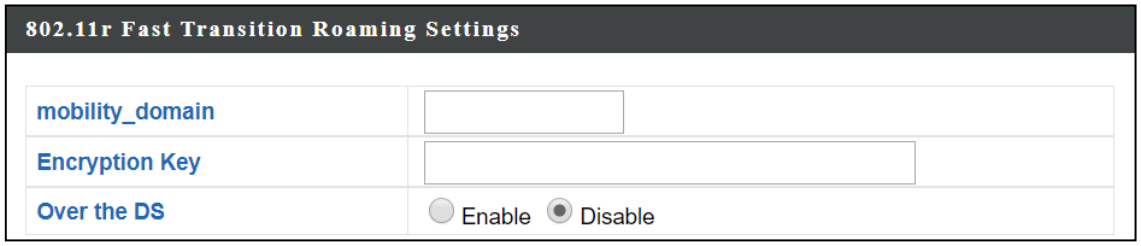
IV-3-1-3-4 WPA-PSK

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:



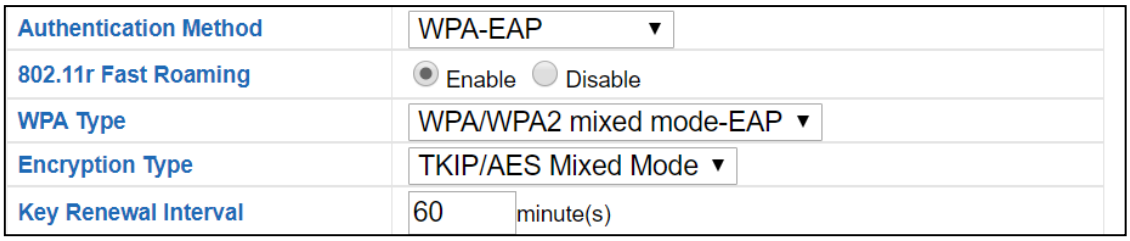
Fast Roaming Settings will also be shown:



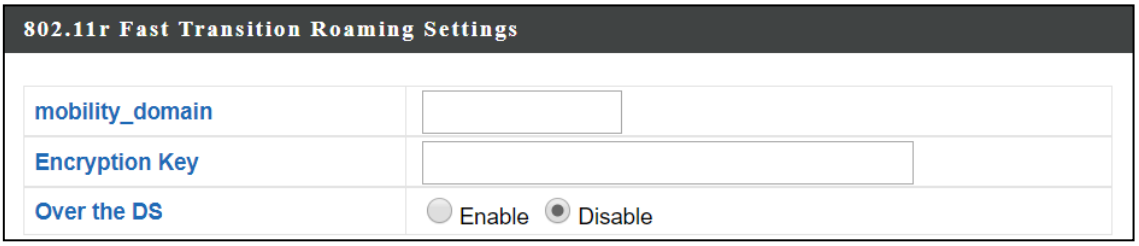
802.11r Fast Roaming	When your device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both preshared key (PSK) and 802.1X authentication methods.
WPA Type	Select from WPA/WPA2 Mixed Mode-PSK, 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.

IV-3-1-3-5 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.

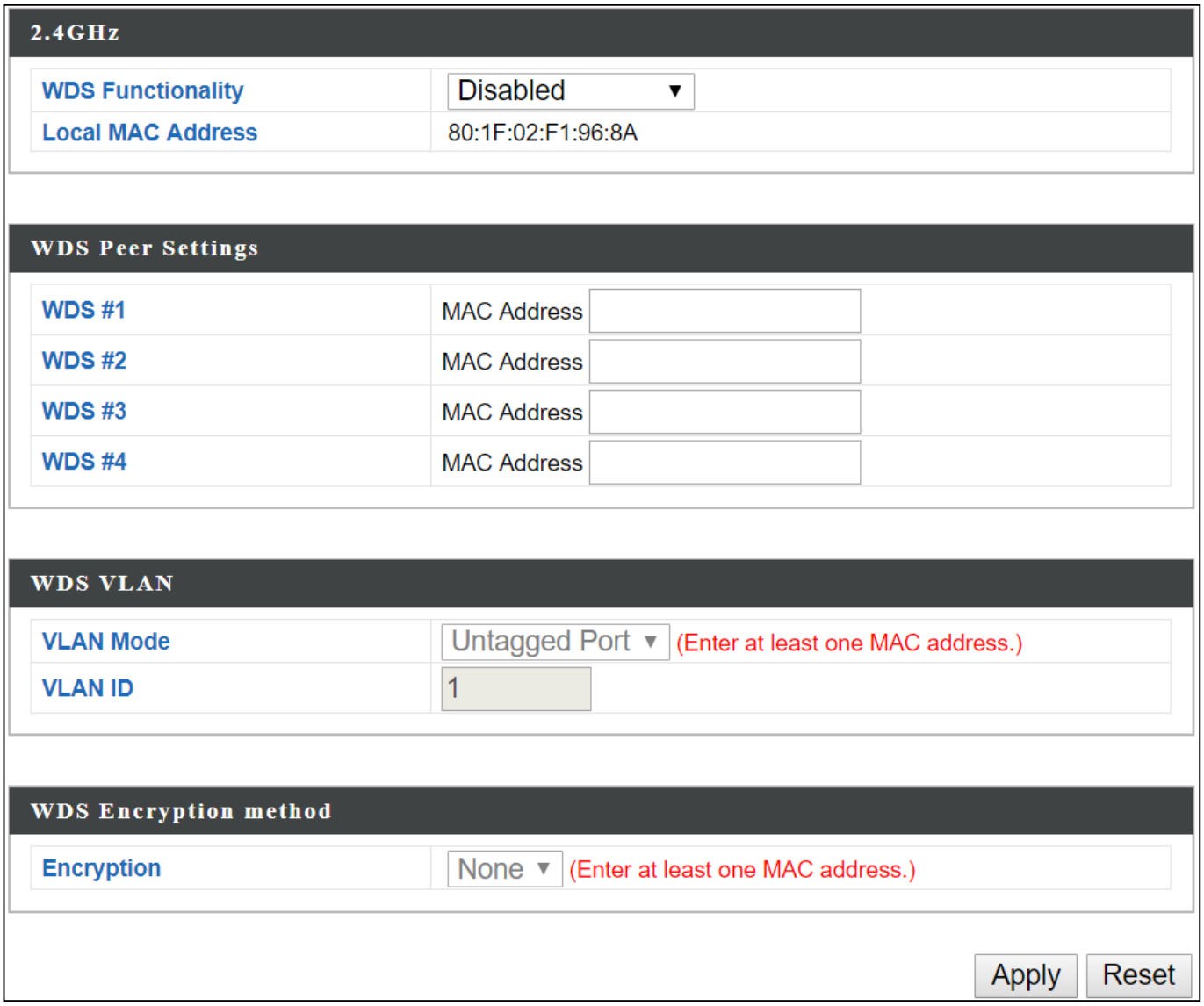
Press “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

IV-3-1-4 WDS

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

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

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



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

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.

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

IV-3-1-5 Guest Network

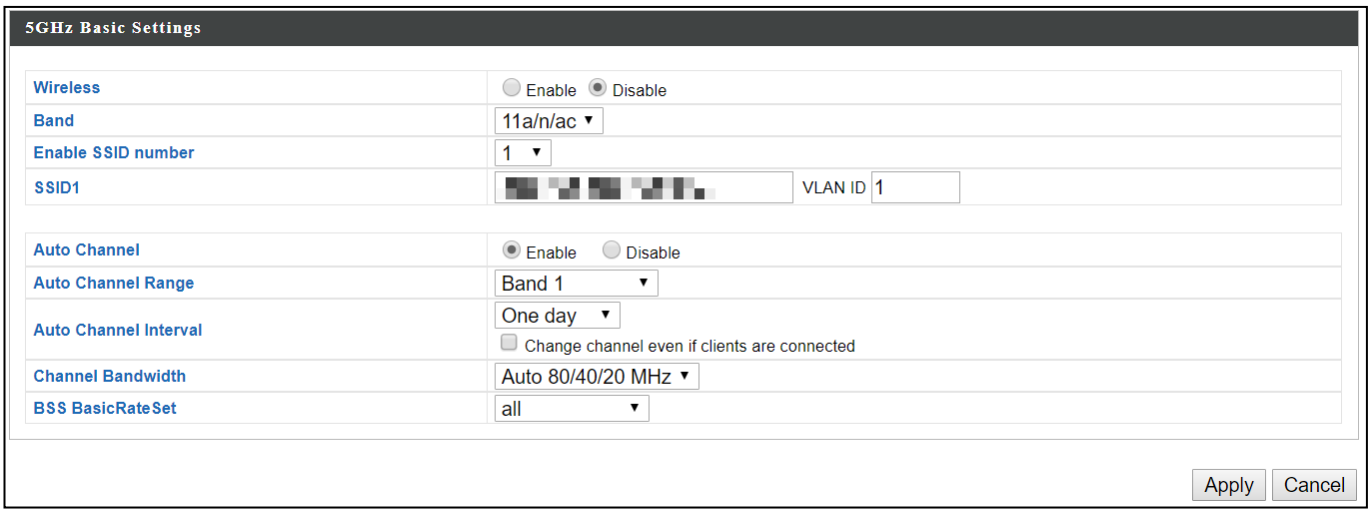
Enable / disable guest network to allow clients to connect as guests.

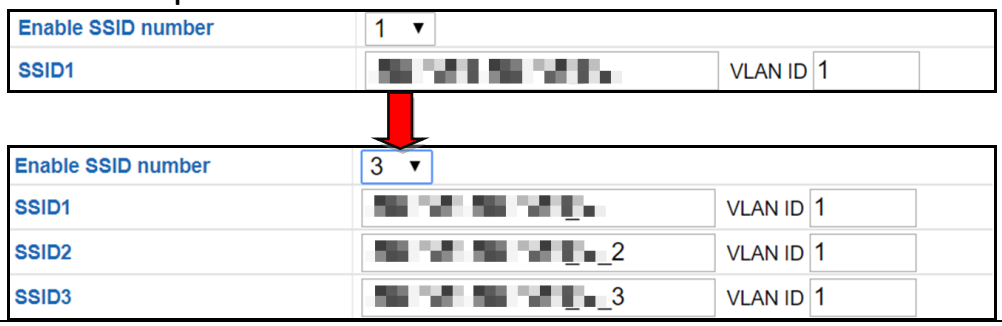
IV-3-2 5GHz 11ac 11an

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

IV-3-2-1 Basic

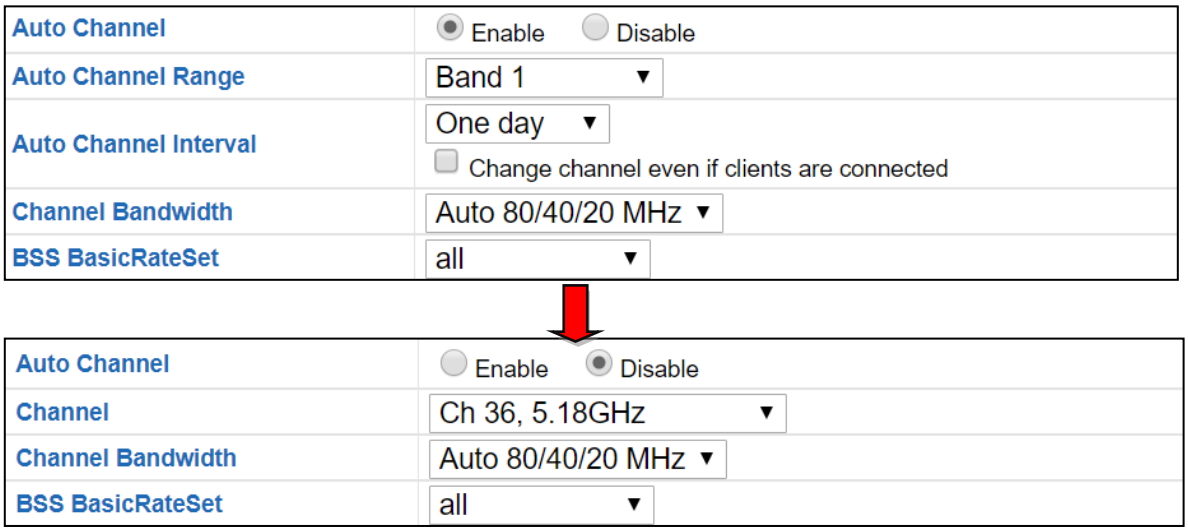
The “Basic” screen displays basic settings for your access point’s 5GHz Wi-Fi network (s).



Wireless	Enable or disable the access point’s 5GHz wireless radio. When disabled, no 5GHz SSIDs will be active.
Band	Wireless standard used for the access point. 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 access point’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:



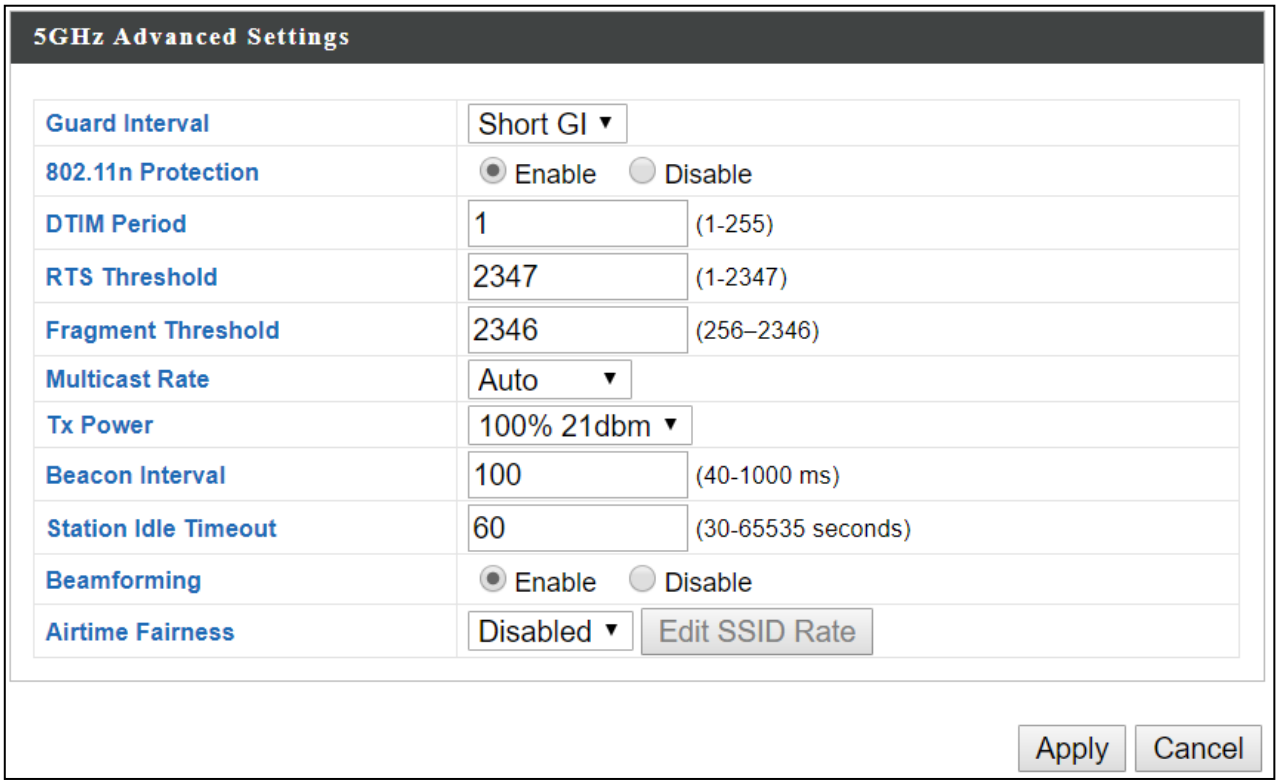
Channel	Select a wireless channel.
Channel Bandwidth	Select the channel bandwidth: 20MHz (lower performance but less interference); or Auto 40/20 MHz; or Auto 80/40/20 MHz (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates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

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

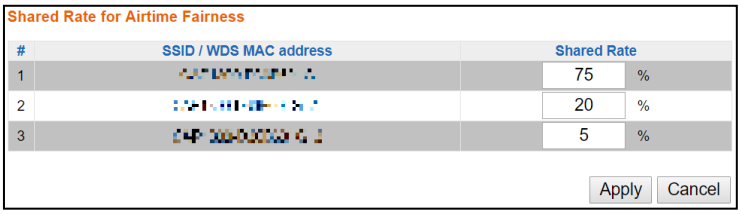
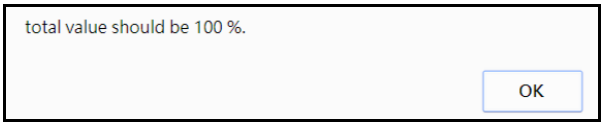
IV-3-2-2 Advanced

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 access point.



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 access point, and access point 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.

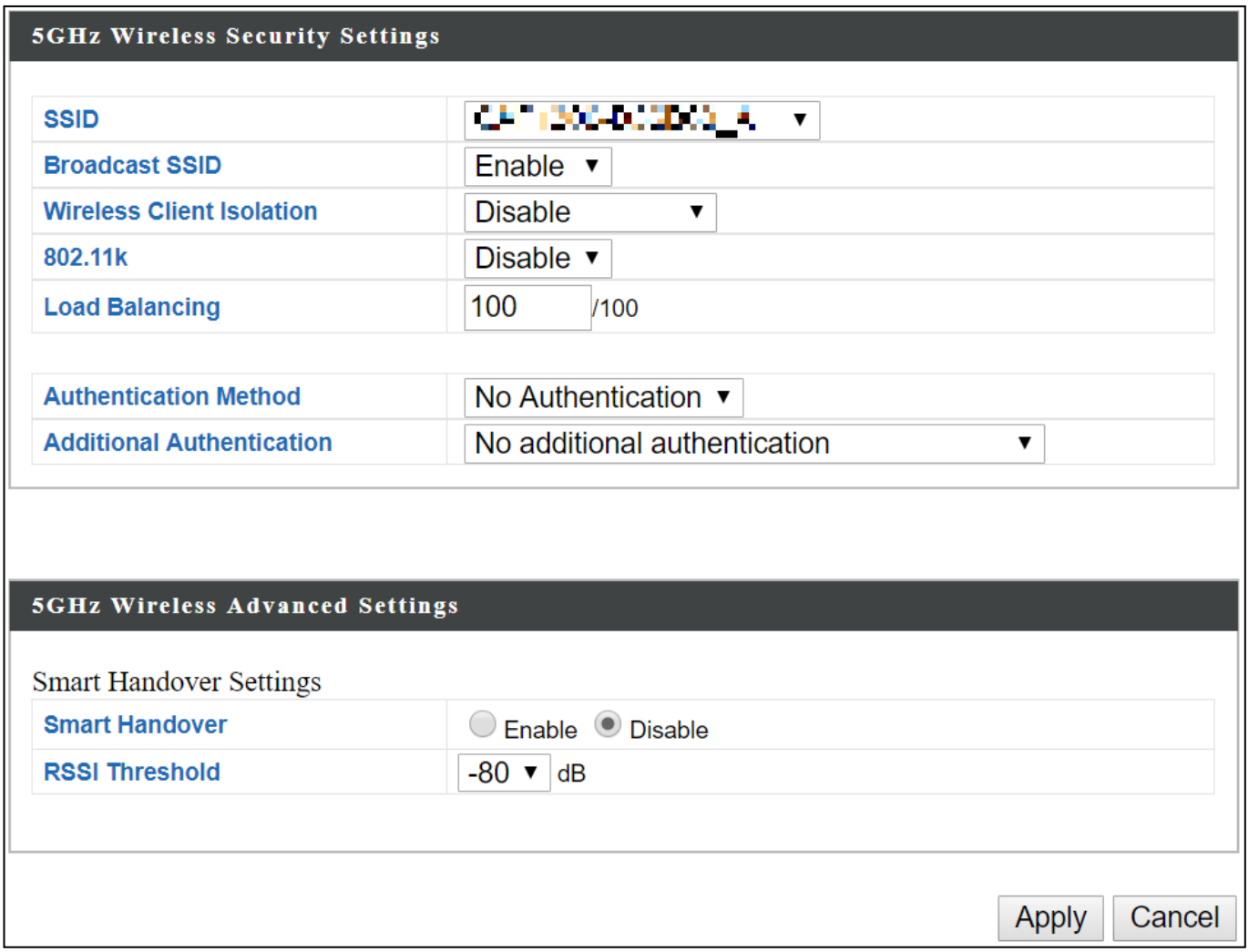
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the access point 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”. Auto: Share rate is automatically managed. Static: Press “Edit SSID Rate” to manually enter a % for each SSID’s share rate as shown below:  The % field must add up to 100% or a message will be displayed:  Airtime fairness is disabled if “Disable” is selected.

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

IV-3-2-3 Security

The access point 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 access point 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 in **IV-3-1-3 Security** for your method.

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

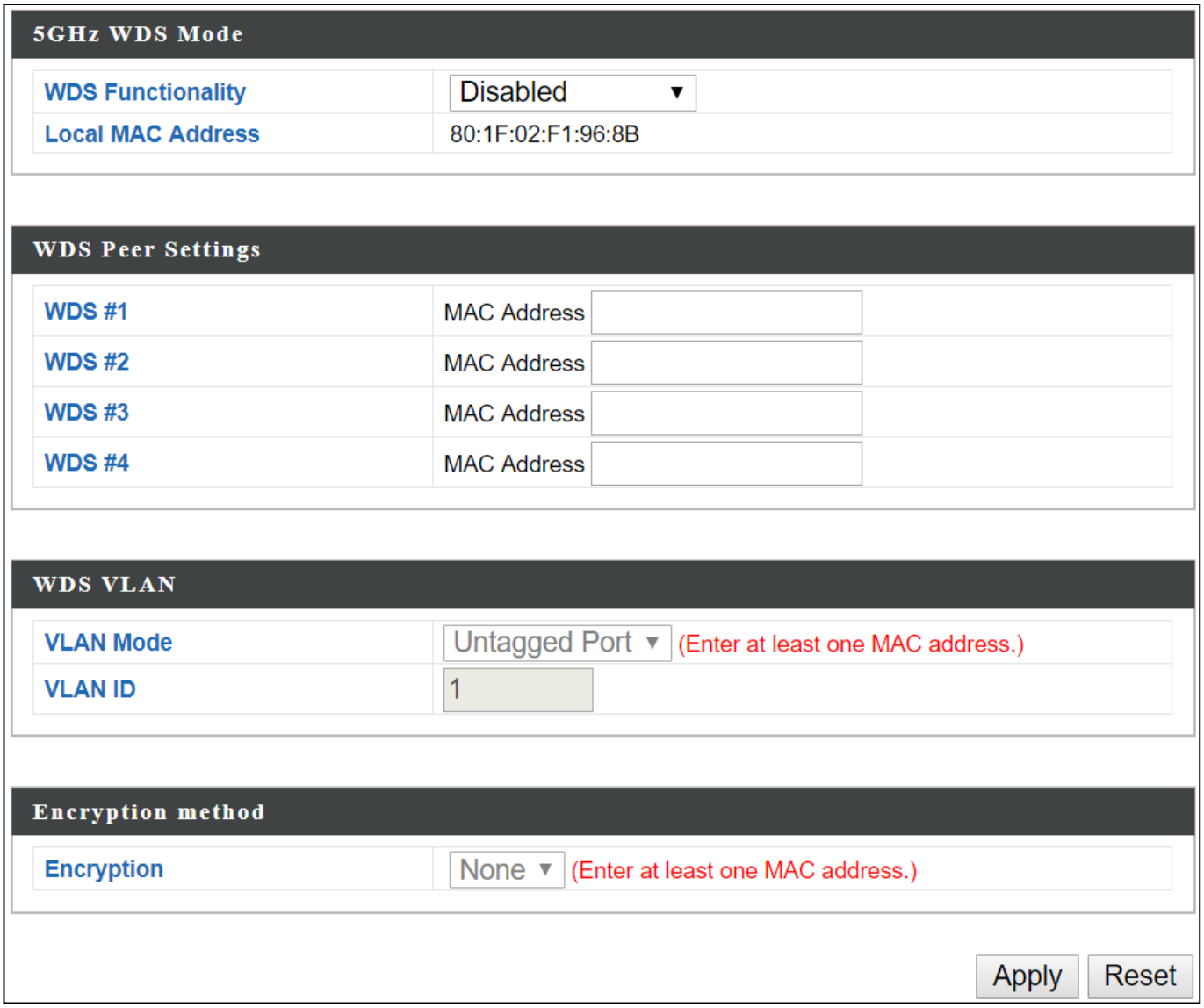
Please refer back to **IV-3-1-3 Security** for more information on authentication and additional authentication types.

IV-3-2-4 WDS

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

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

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



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

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.

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

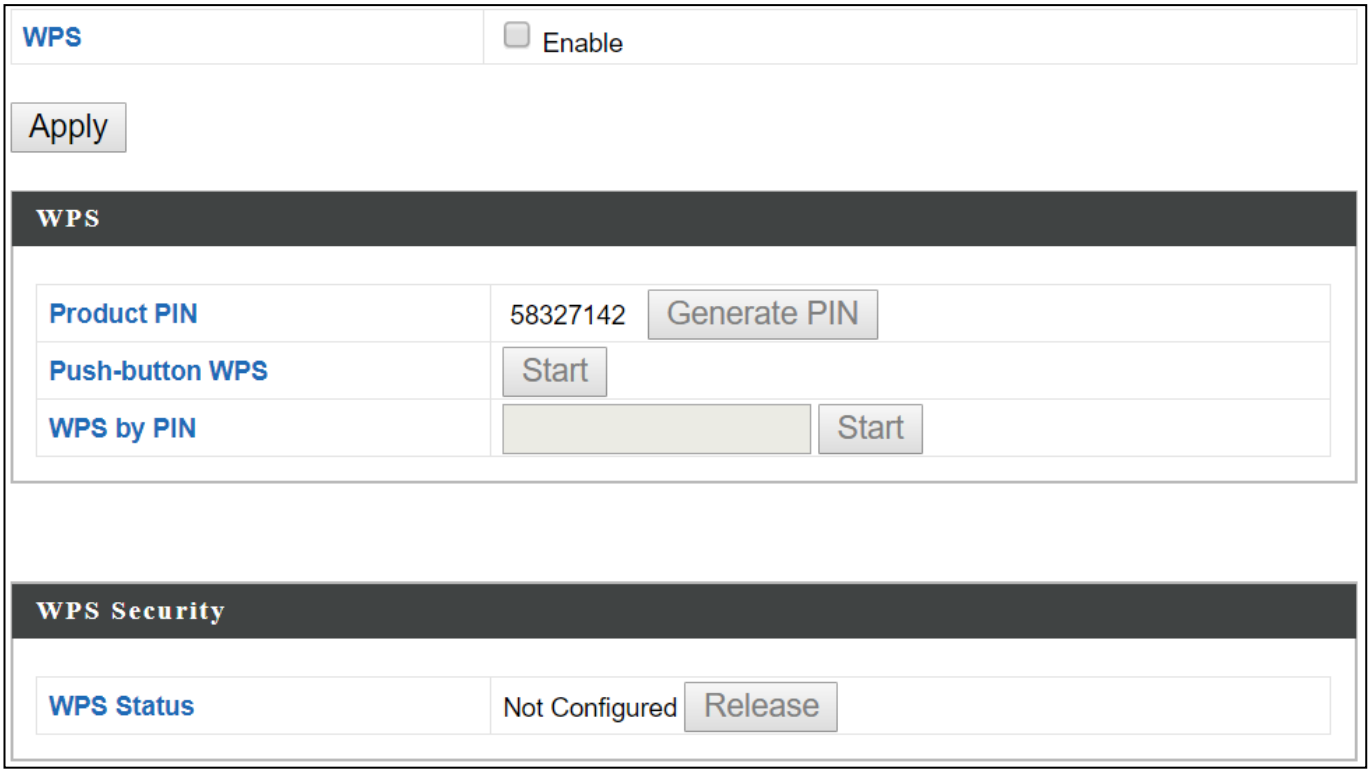
IV-3-2-5 Guest Network

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

IV-3-3 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 manufacturer's instructions for your other WPS device.



WPS	Check/uncheck this box to enable/disable WPS functionality. Press "Apply" to apply the settings. WPS must be disabled when using MAC-RADIUS authentication (see ***IV-3-4 RADIUS***).

Press "Apply" to apply the configuration.

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 device 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.

IV-3-4 RADIUS

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

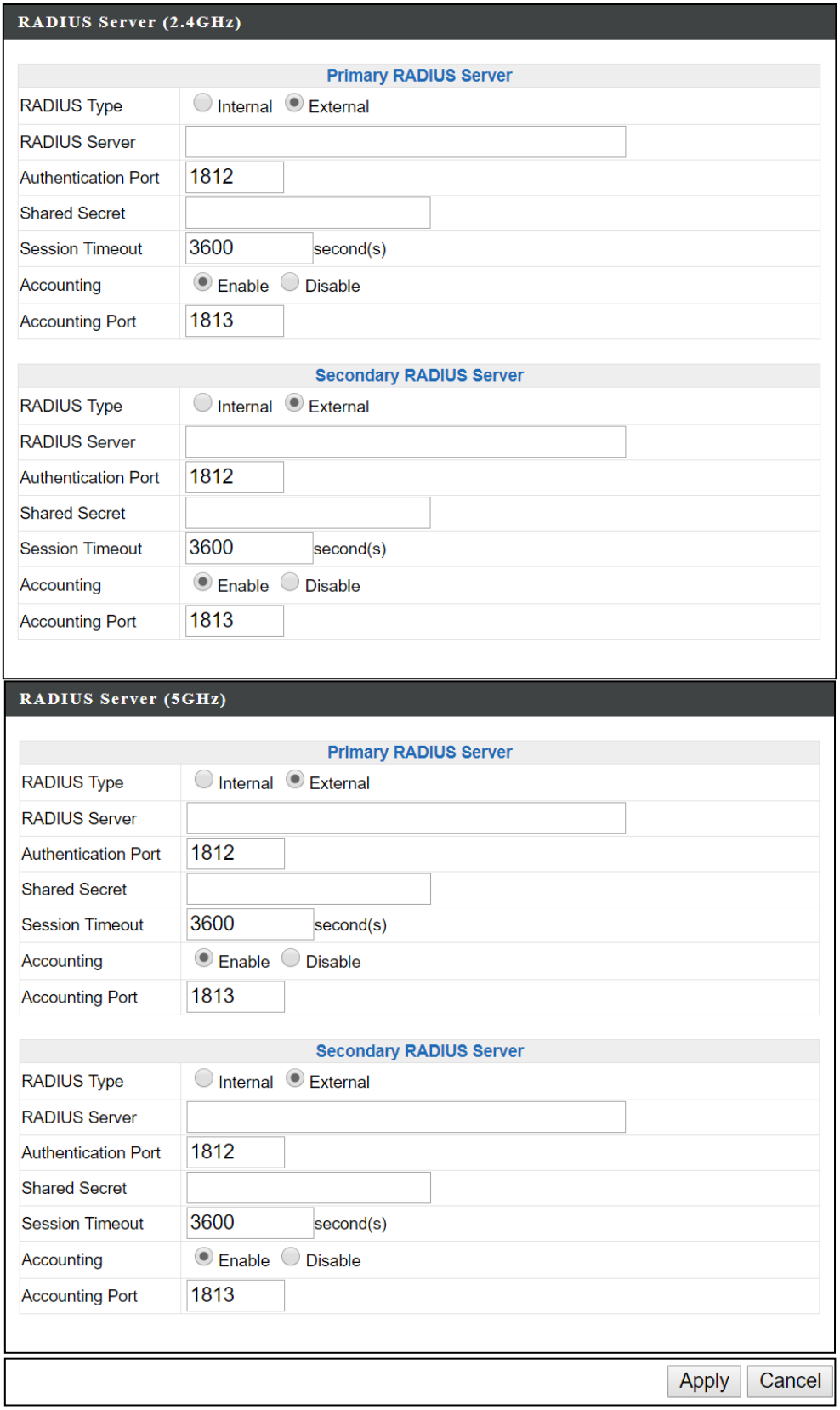
A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

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

To use RADIUS servers, go to *"Wireless Settings"* → *"Security"* ***and select*** *"MAC RADIUS Authentication"* → *"Additional Authentication"* ***and select*** *"MAC RADIUS Authentication"* ***(see*** *IV-3-1-3* ***or*** *IV-3-2-3****).***

IV-3-4-1 RADIUS Settings

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



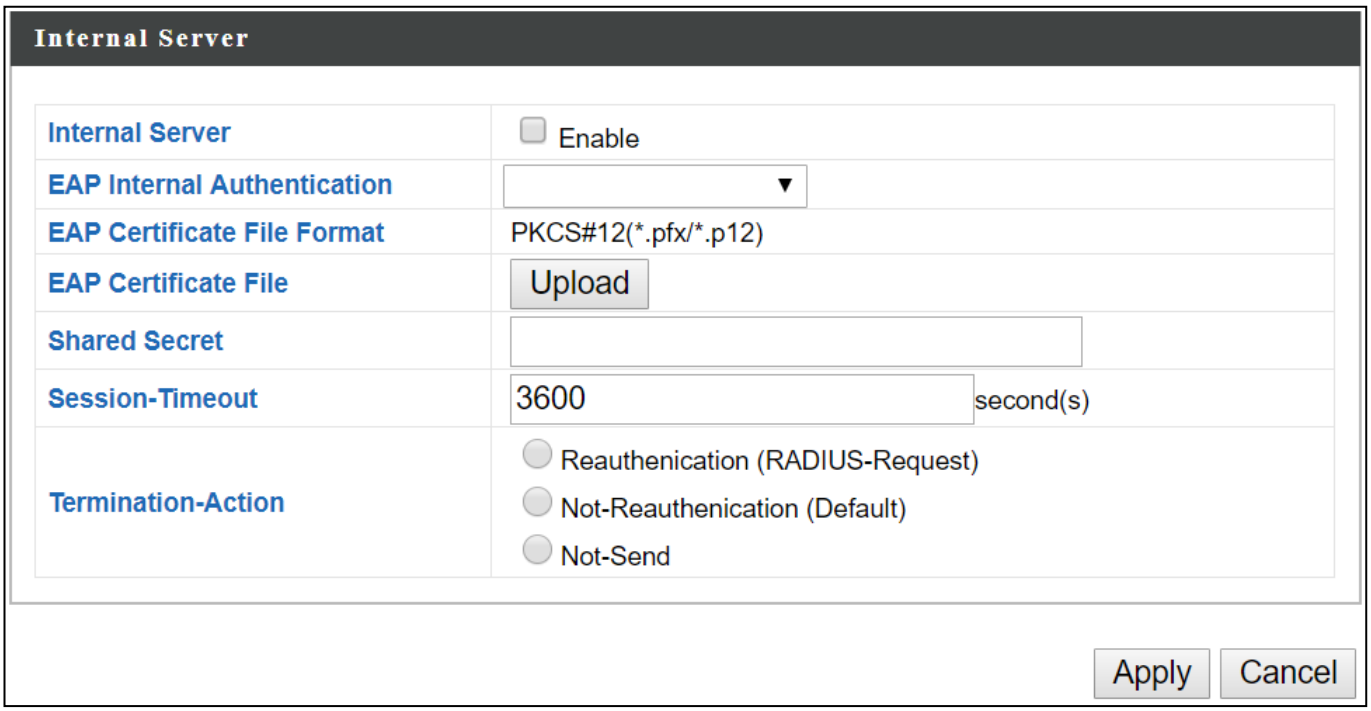
RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in ***IV-3-1-3*** or ***IV-3-2-3***.
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.

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

IV-3-4-2 Internal Server

The access point features a built-in RADIUS server which can be configured as shown below used when "Internal" is selected for "RADIUS Type" in the "Wireless Settings" → "RADIUS" → "RADIUS Settings" menu.

To use RADIUS servers, go to** "Wireless Settings" → "Security" **and select** "MAC RADIUS Authentication" → "Additional Authentication" **and select** "MAC RADIUS Authentication" **(see** IV-3-1-3 **&** IV-3-2-3**).



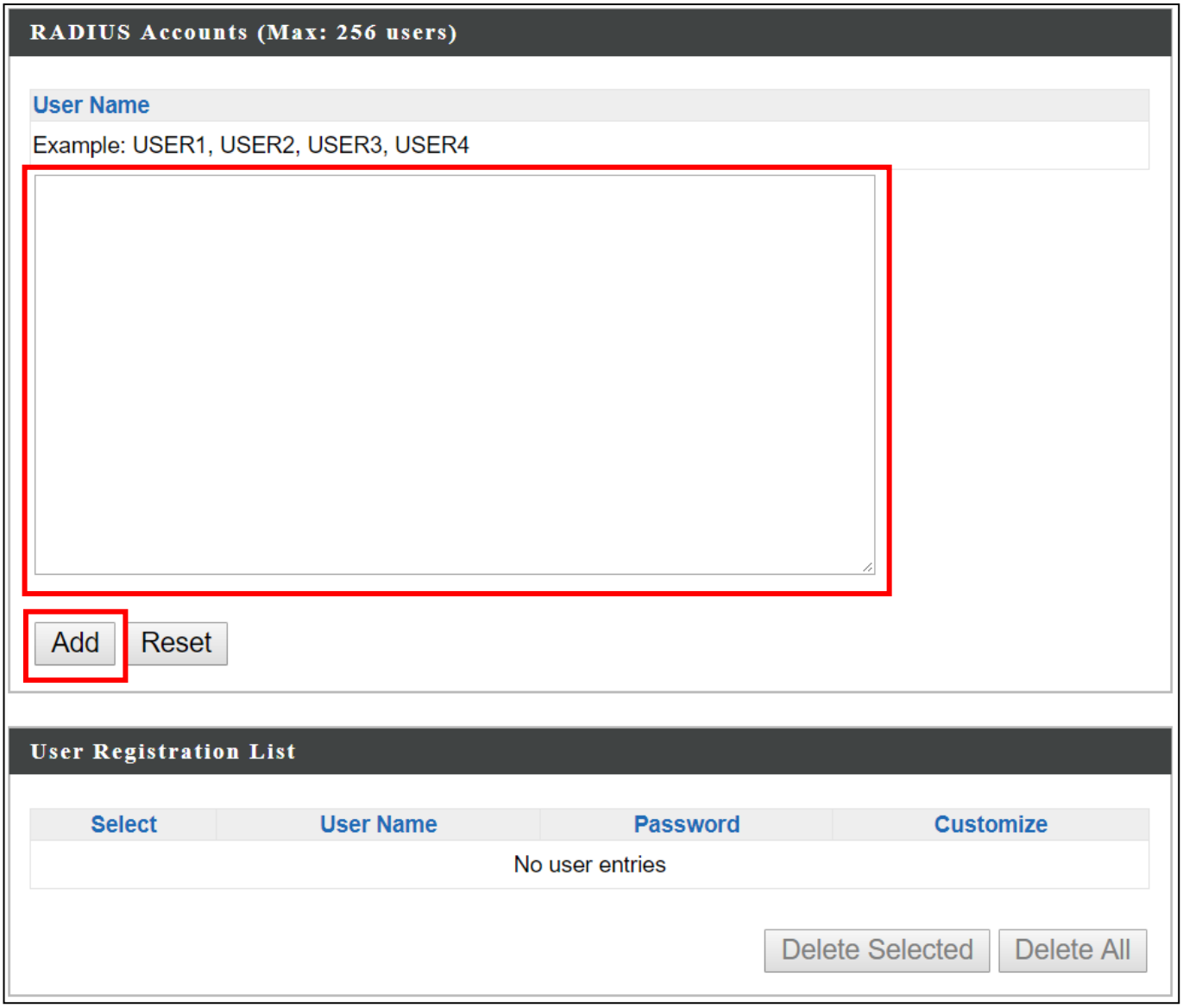
Internal Server	Check/uncheck to enable/disable the access point's internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click "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. This should match the "MAC-RADIUS" password used in ***IV-3-1-3*** or ***IV-3-2-3***.

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 access point; or, Not-Reauthentication: sends a default termination-action attribute to the access point; or Not-Send: no termination-action attribute is sent to the access point.

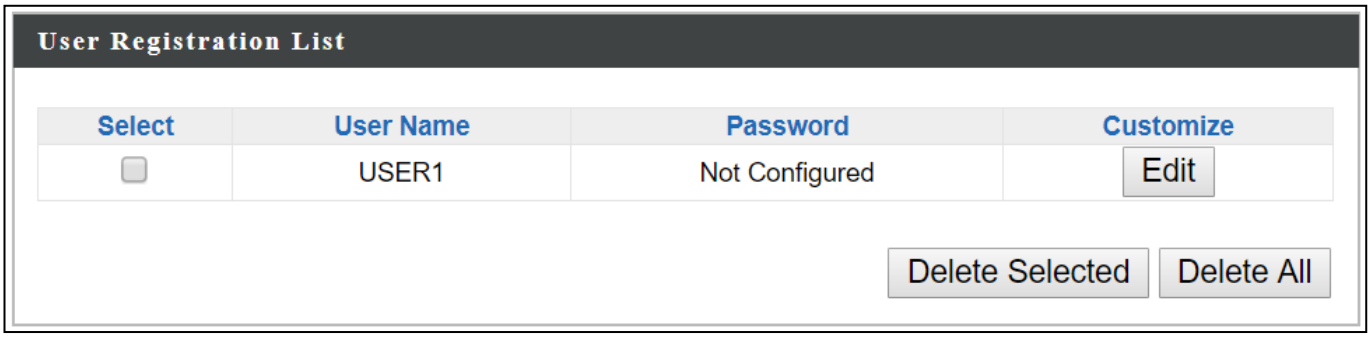
Press “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

IV-3-4-3 RADIUS Accounts

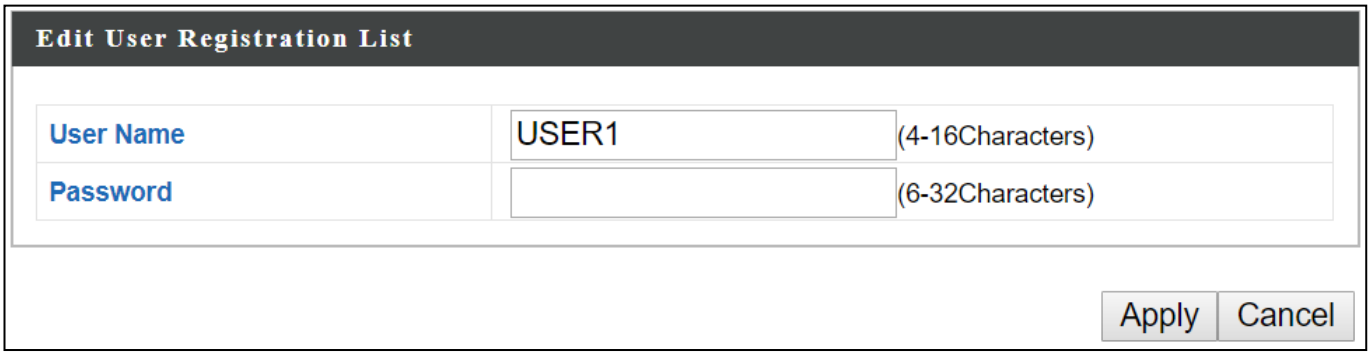
The internal RADIUS server can authenticate up to 256 user accounts. The "RADIUS Accounts" page allows you to configure and manage users.



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



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



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

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.

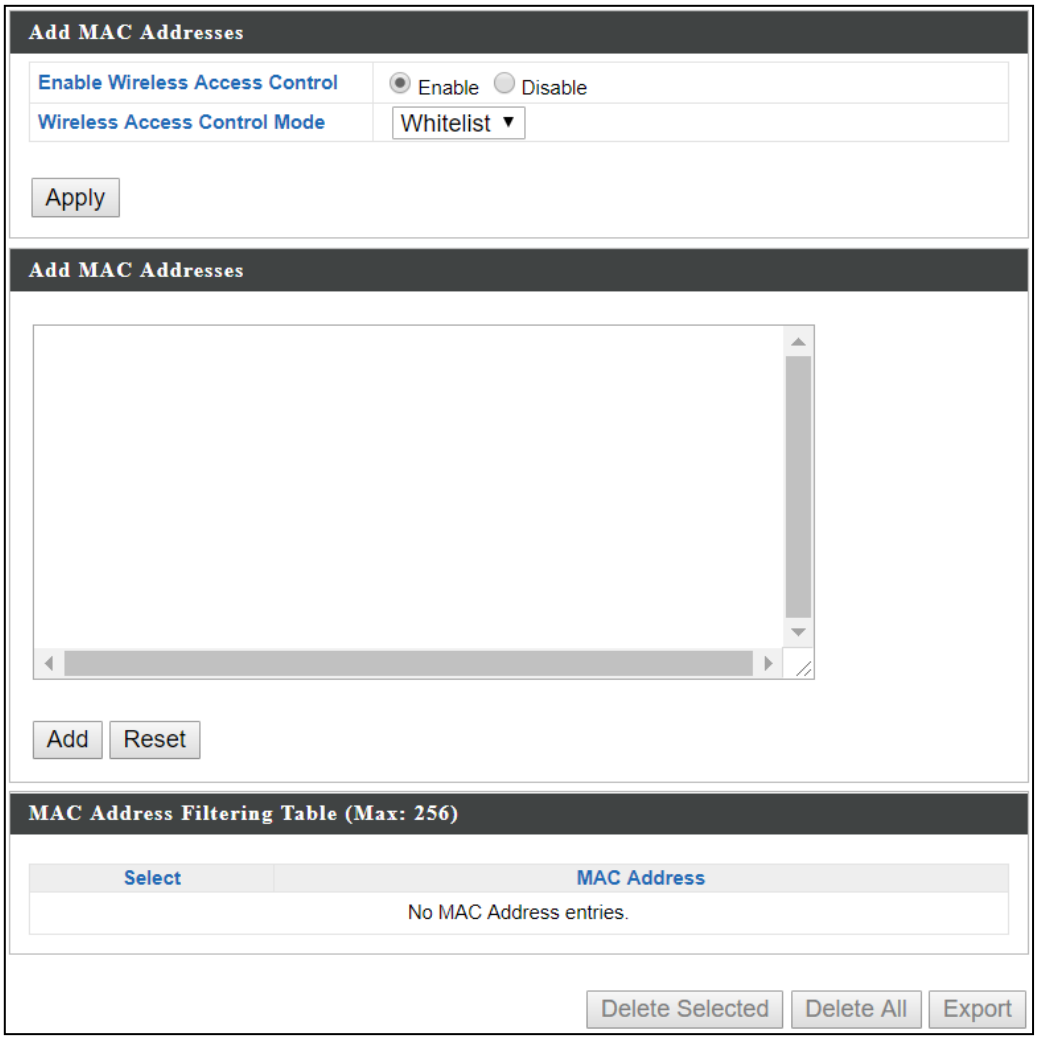
IV-3-5 MAC Filter

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

This function allows you to define a list of network devices permitted to connect to the access point. 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 access point, it will be denied.

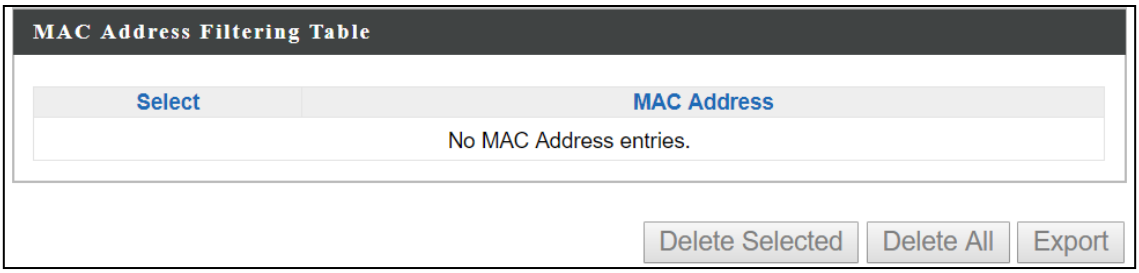
> ***To enable MAC filtering, go to*** *"Wireless Settings"* → *"2.4G Hz 11bgn"* → *"Security"* → *"Additional Authentication"* ***and select*** *"MAC Filter"* ***(see*** *IV-3-1-3* ***or*** *IV-3-2-3****).***

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.

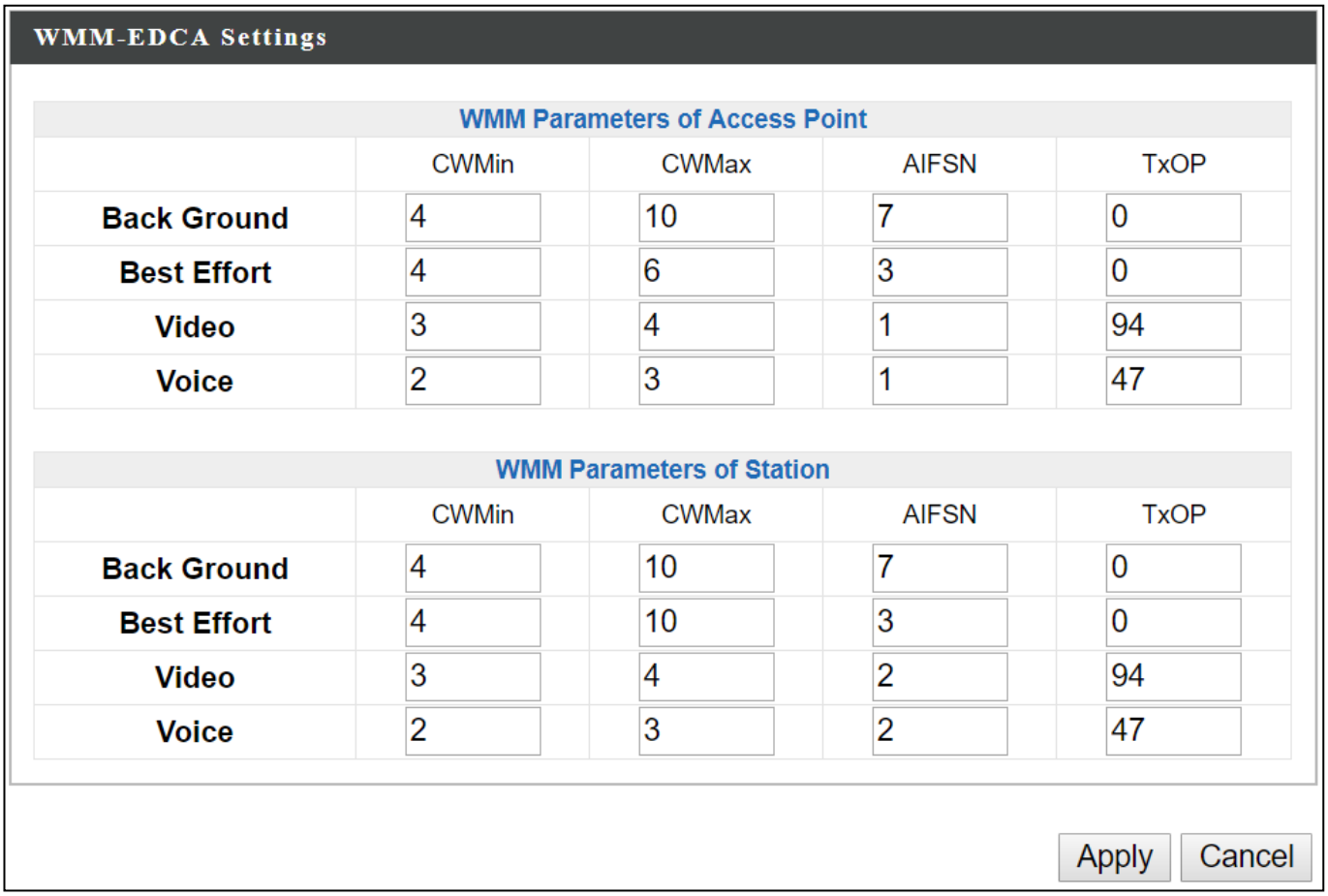
MAC address entries will be listed in the "MAC Address Filtering Table". Select an entry using the "Select" checkbox.



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.

IV-3-6 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.

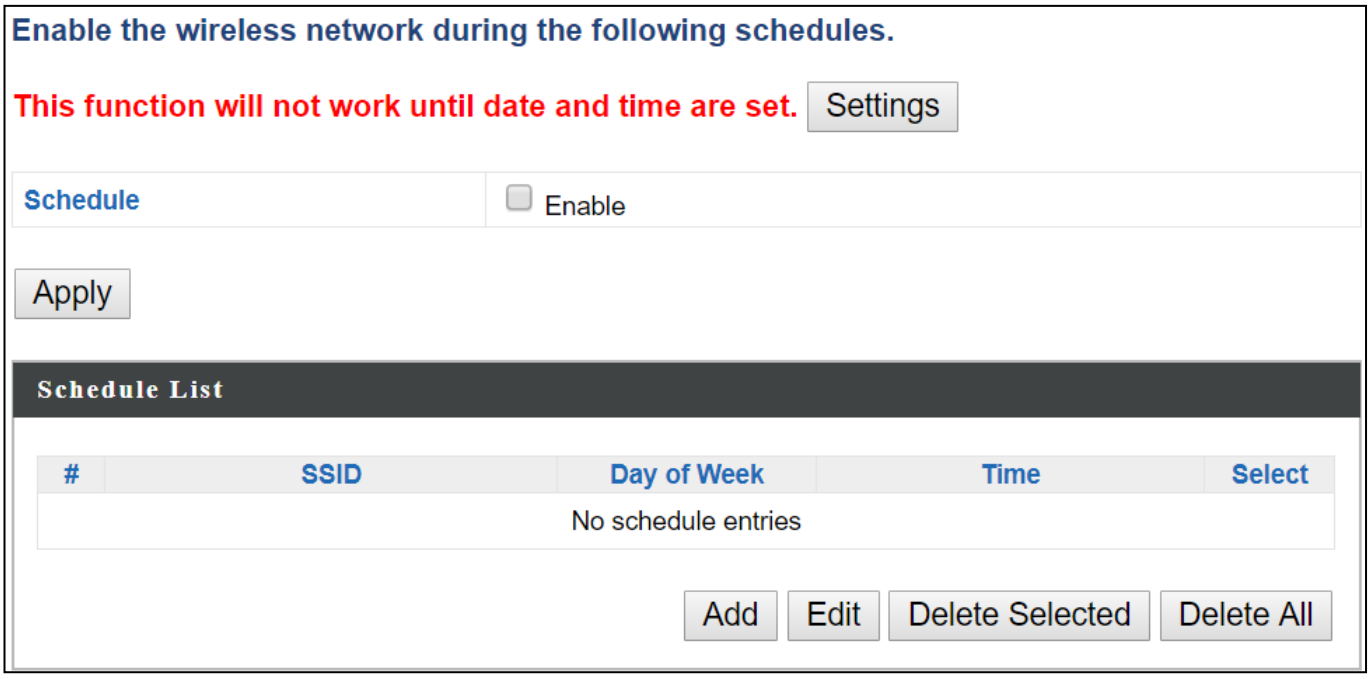
Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can be adjusted further manually:

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.

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

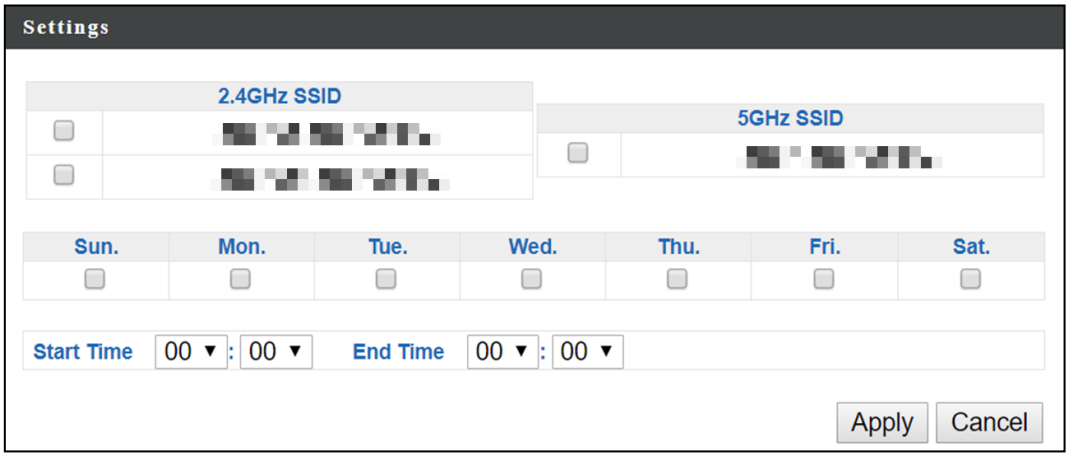
IV-3-7 Schedule

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.
Check/uncheck the box “Enable” and select “Apply” to enable/disable the wireless scheduling function.

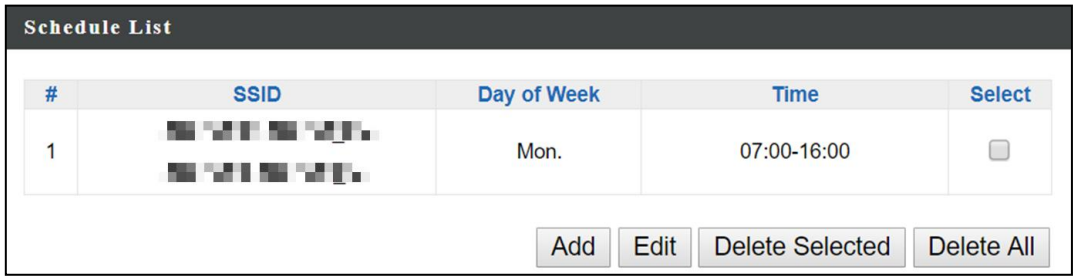


1. Select “Add” to add a schedule.

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:



3. Select “Add” to add more schedules; or
Check the box of currently available schedule, select “Edit” to edit, or select “Delete Selected” to delete; or
Select “Delete All” to delete all schedules.

IV-3-8 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.
Check the checkbox to enable traffic shaping, specify the down link and up link values, and click “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

Traffic Shaping for ssid(2.4GHz)

☐ Enable

Unlimited : 0 Mbps

Down Link/Up Link Maximum : 1024 Mbps

SSID	Down Link	Up Link
[redacted]-F1968A_G	0 Mbps	0 Mbps
[redacted]F1968A_G_2	0 Mbps	0 Mbps
[redacted]F1968A_G_3	0 Mbps	0 Mbps
[redacted]F1968A_G_4	0 Mbps	0 Mbps
[redacted]F1968A_G_5	0 Mbps	0 Mbps
[redacted]F1968A_G_6	0 Mbps	0 Mbps
[redacted]F1968A_G_7	0 Mbps	0 Mbps
[redacted]F1968A_G_8	0 Mbps	0 Mbps
[redacted]F1968A_G_9	0 Mbps	0 Mbps
[redacted]F1968A_G_10	0 Mbps	0 Mbps
[redacted]F1968A_G_11	0 Mbps	0 Mbps
[redacted]F1968A_G_12	0 Mbps	0 Mbps
[redacted]F1968A_G_13	0 Mbps	0 Mbps
[redacted]F1968A_G_14	0 Mbps	0 Mbps
[redacted]F1968A_G_15	0 Mbps	0 Mbps
[redacted]F1968A_G_16	0 Mbps	0 Mbps

Traffic Shaping for ssid(5GHz)

Enable

Unlimited : 0 Mbps

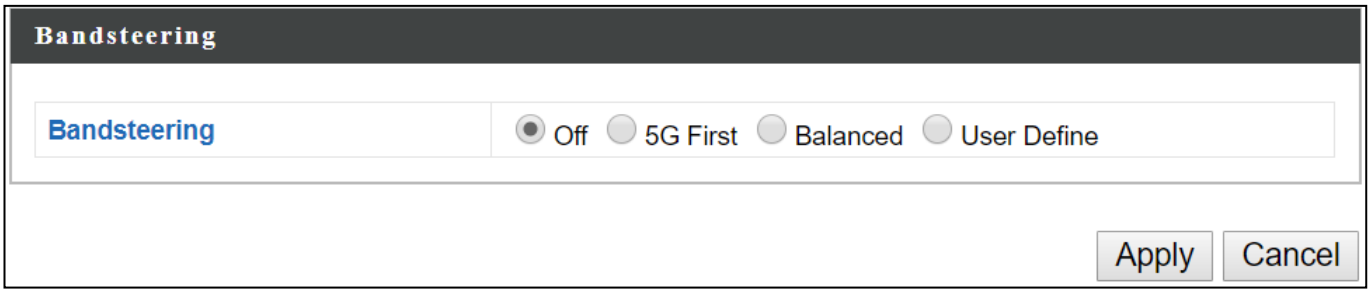
Down Link/Up Link Maximum : 1024 Mbps

SSID	Down Link	Up Link
F1968A_A	0 Mbps	0 Mbps
F1968A_A_2	0 Mbps	0 Mbps
F1968A_A_3	0 Mbps	0 Mbps
F1968A_A_4	0 Mbps	0 Mbps
F1968A_A_5	0 Mbps	0 Mbps
F1968A_A_6	0 Mbps	0 Mbps
F1968A_A_7	0 Mbps	0 Mbps
F1968A_A_8	0 Mbps	0 Mbps
F1968A_A_9	0 Mbps	0 Mbps
F1968A_A_10	0 Mbps	0 Mbps
F1968A_A_11	0 Mbps	0 Mbps
F1968A_A_12	0 Mbps	0 Mbps
F1968A_A_13	0 Mbps	0 Mbps
F1968A_A_14	0 Mbps	0 Mbps
F1968A_A_15	0 Mbps	0 Mbps
F1968A_A_16	0 Mbps	0 Mbps

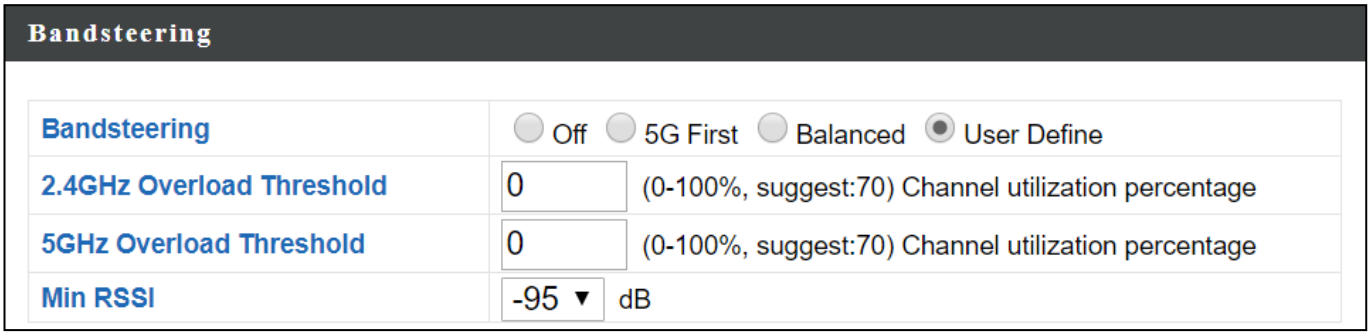
Apply Cancel

IV-3-9 Bandsteering

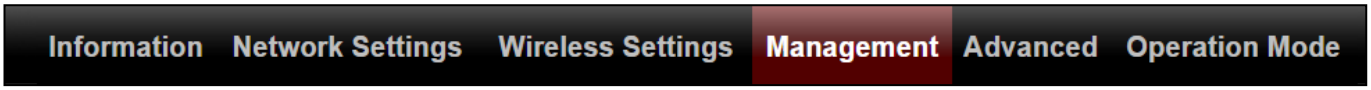
Band steering detects clients capable of 5GHz operation and steers them there to make the more crowded 2.4 GHz band available for clients only capable of connecting to 2.4GHz band. This helps improve end user experience by reducing channel utilization, especially in high density environments.



If “User Define” is selected, specify the numbers in the fields below:



IV-4 Management

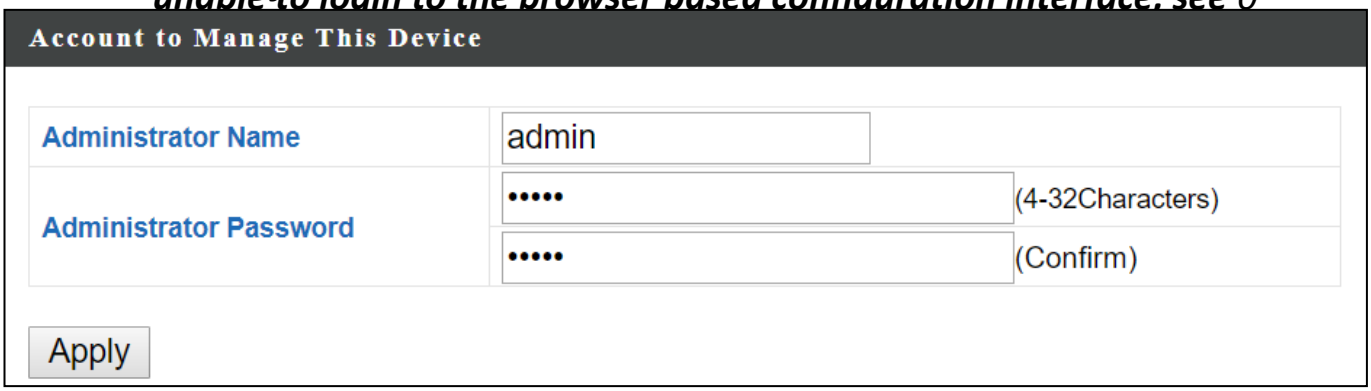


(Configurable for AP Mode only)

IV-4-1 Admin

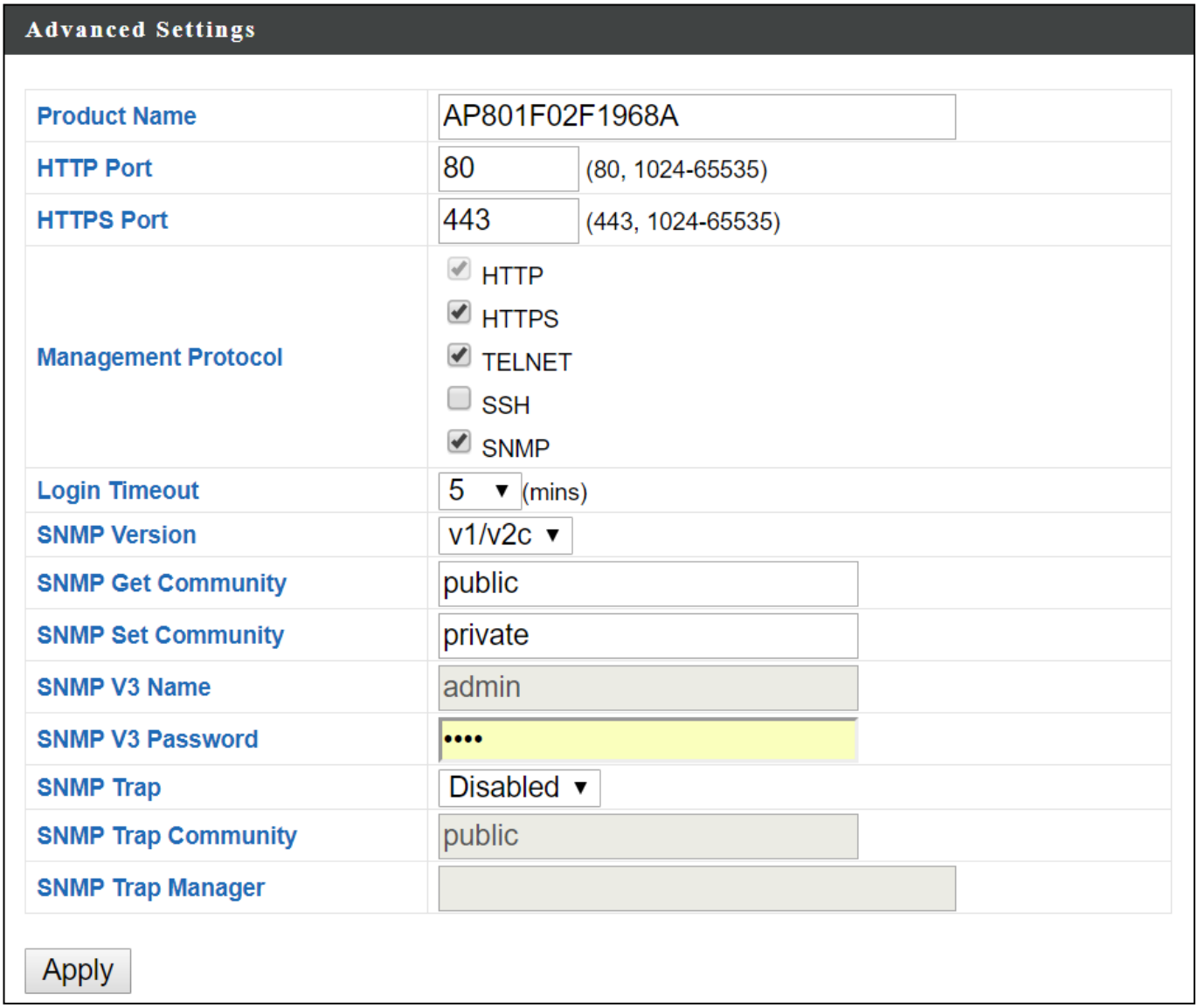
You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

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, see 0 Reset for how to reset the access point.



Account to Manage This Device	
Administrator Name	Set the access point'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 access point'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).

Press "Apply" to apply the configuration.



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	Enter an SNMP Trap Community name for verification with

Community	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.

HTTP

Internet browser HTTP protocol management interface

TELNET

Client terminal with telnet protocol management interface

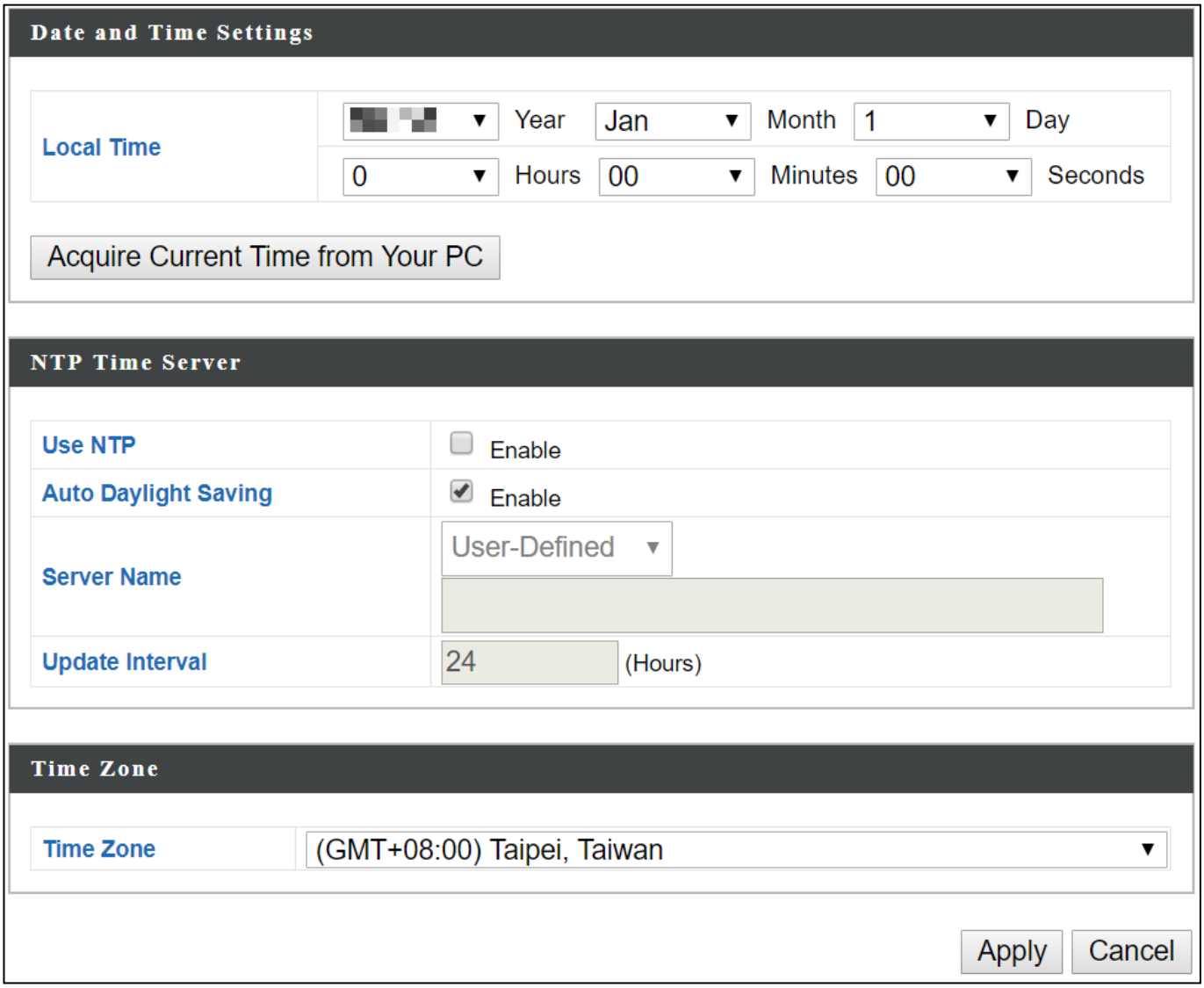
SNMP

Simple Network Management Protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (USM) architecture.

Press “Apply” to apply the configuration.

IV-4-2 Date and Time

Configure the date and time settings of the access point 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 access point'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.

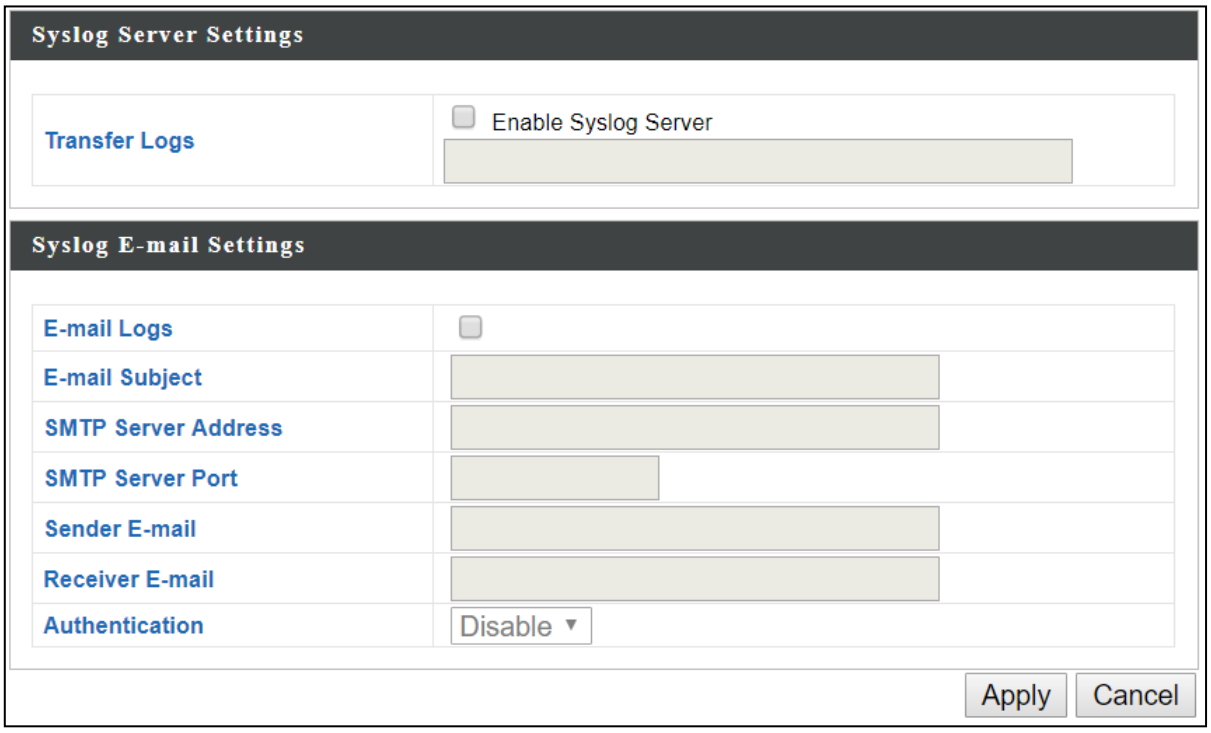
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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.

IV-4-3 Syslog Server

The system log can be sent to a server.



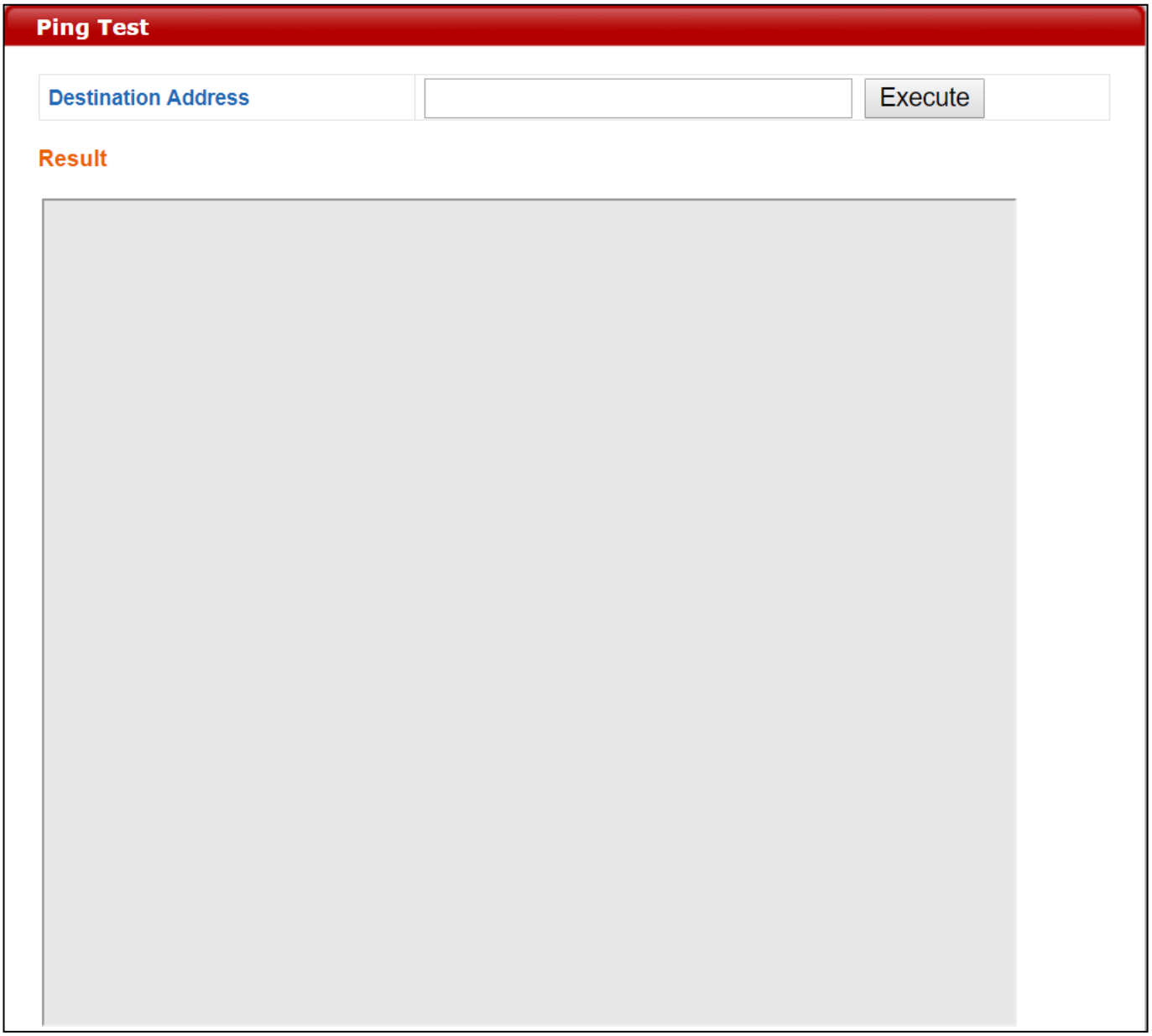
Syslog Server Settings	
Transfer Logs	Check the box to enable the use of a syslog server. Enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.

Syslog E-mail Settings	
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.

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

IV-4-4 Ping Test

The access point includes a built-in ping test function. 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.

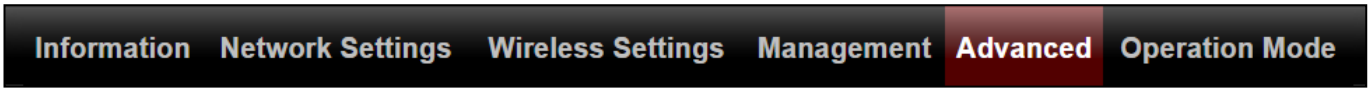
IV-4-5 I’m Here

The access point features a built-in buzzer which can sound on command using the “I’m Here” page. This is useful for network administrators and engineers working in complex network environments to locate the access point.

The buzzer is loud!

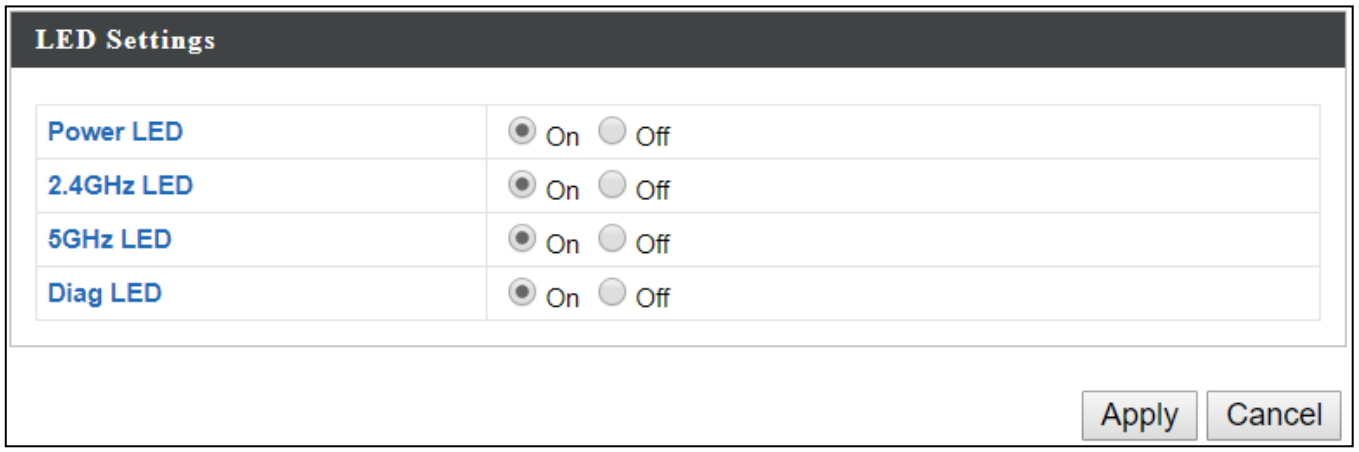
Duration of Sound	Set the duration for which the buzzer will sound when the “Sound Buzzer” button is clicked.
Sound Buzzer	Activate the buzzer sound for a duration specified above.

IV-5 Advanced



IV-5-1 LED Settings

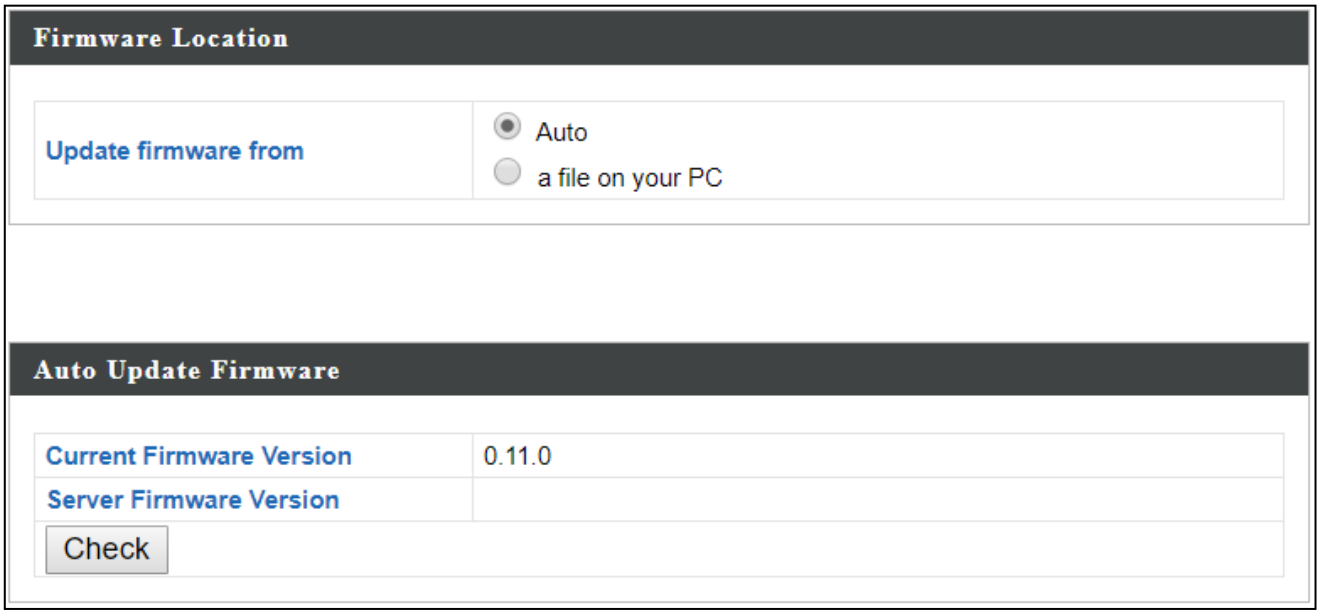
The access point's LEDs can be manually enabled or disabled according to your preference.



Power LED	Select on or off.
2.4GHz LED	Select on or off.
5GHz LED	Select on or off.
Diag LED	Select on or off.

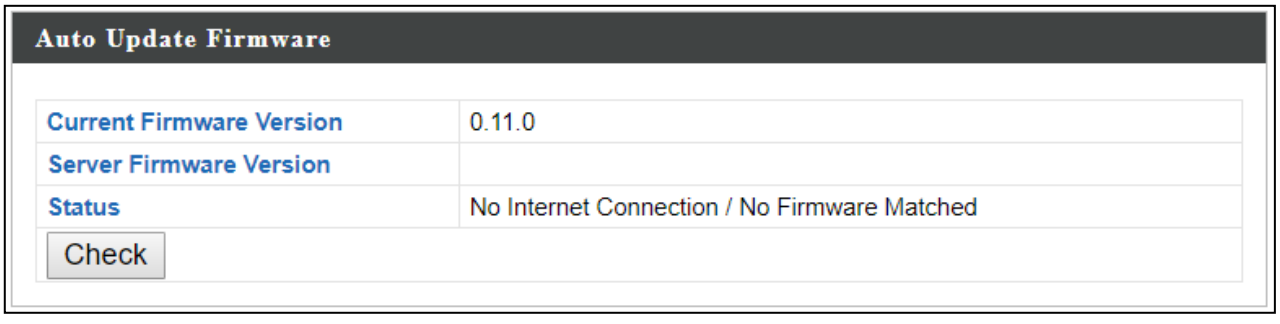
IV-5-2 Update Firmware

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.

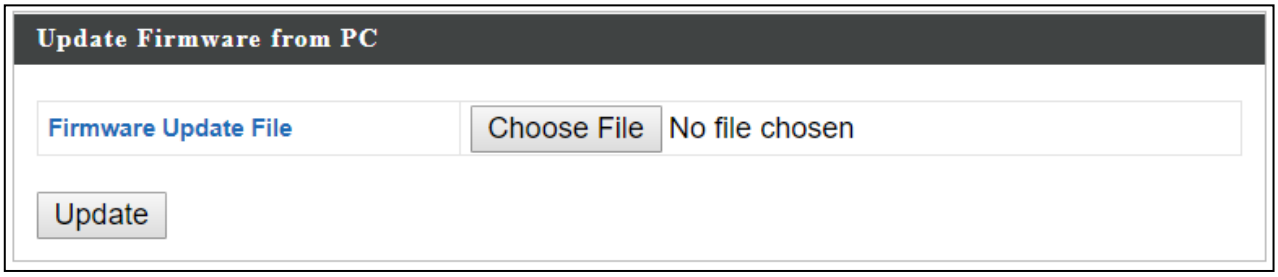


Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.

Firmware Location: Auto	
Current Firmware Version	Displays current firmware version.
Server Firmware Version	Displays available firmware version on the server.
Status	Displays availability of firmware.
Check	Click to check available firmware version.

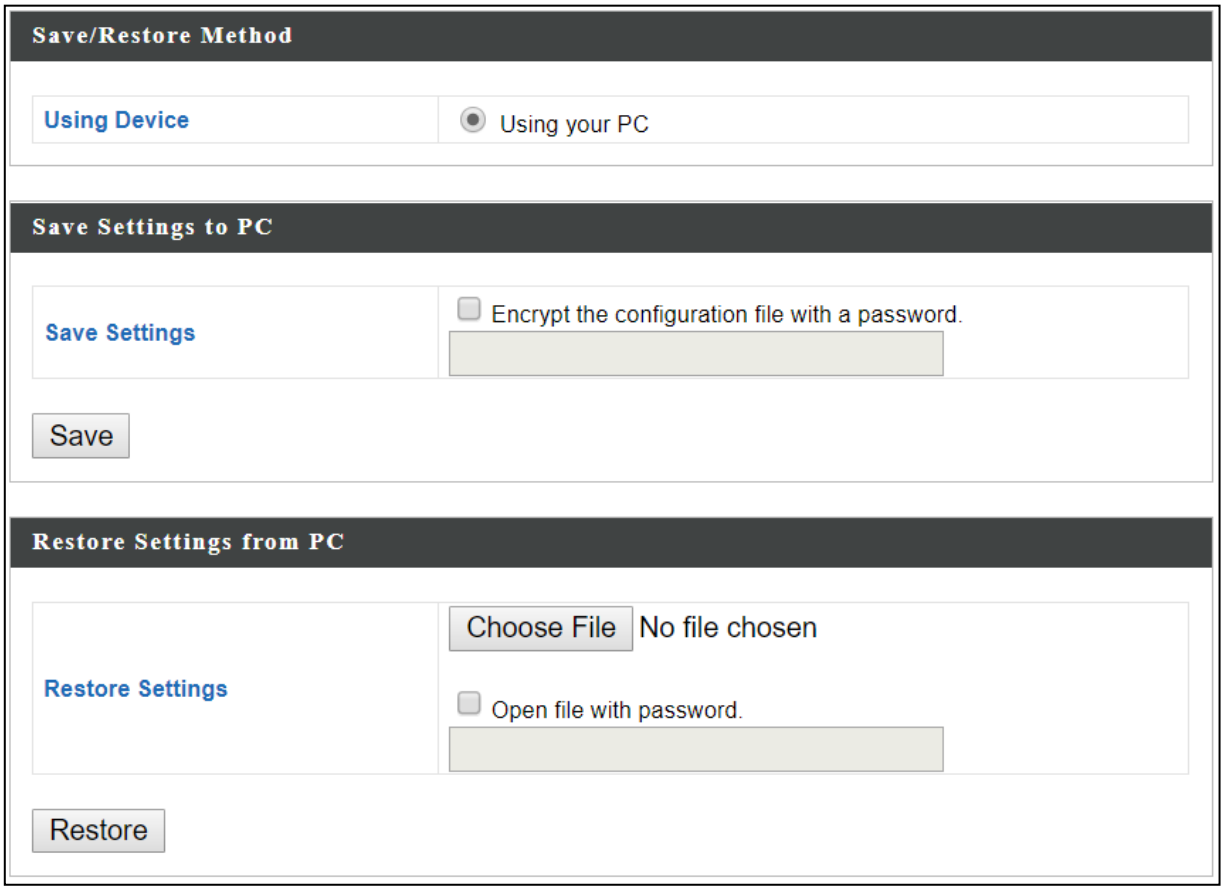


Firmware Location: a file on your PC	
Firmware Update File	Click “Choose File” to select firmware from your PC.
Update	Click to update the firmware.



IV-5-3 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 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-5-4 Factory Default

If the access point malfunctions or is not responding, rebooting the device (**IV-5-5 Reboot**) maybe an option to consider. If rebooting does not work, try resetting the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the reset button is not readily accessible.

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

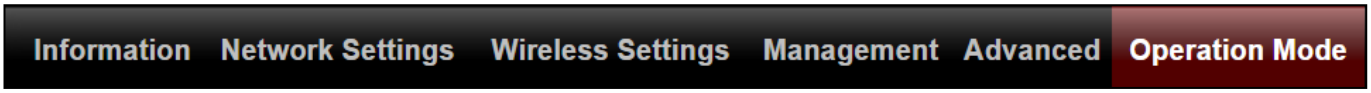
After resetting to factory defaults, please wait for the access point to reset and restart.

IV-5-5 Reboot

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

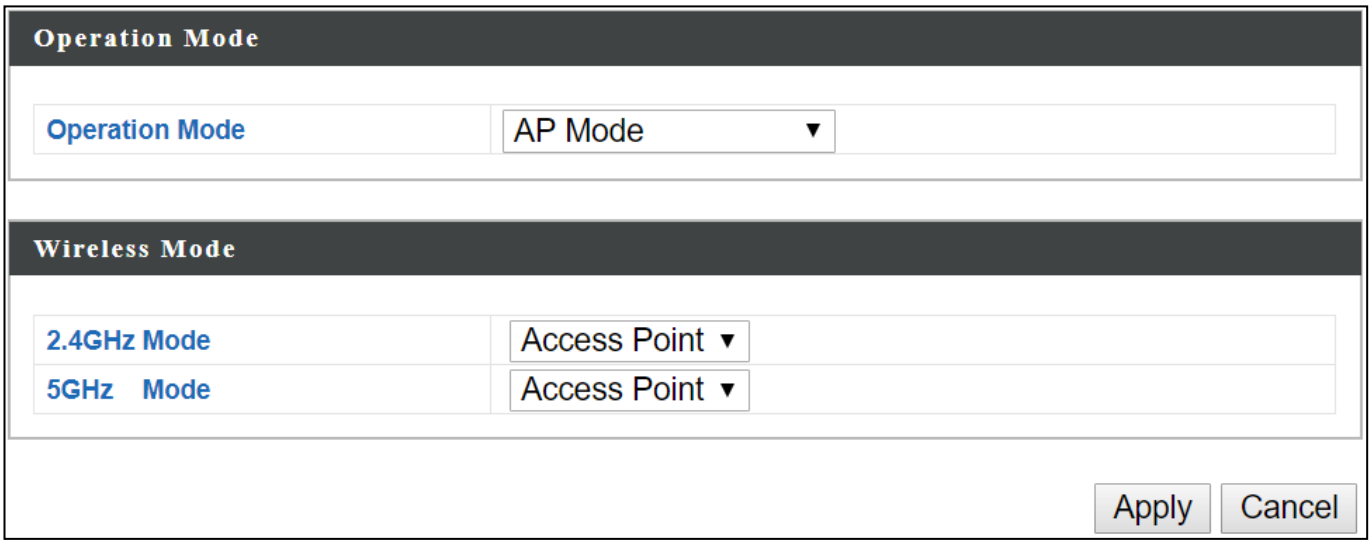
Reboot	Click “Reboot” to reboot the device. A countdown will indicate the progress of the reboot.

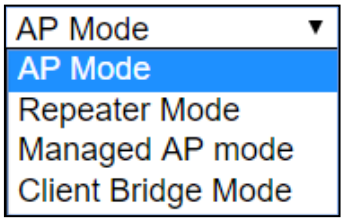
IV-6 Operation Mode



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

1. AP Mode: The device acts as a standalone access point
2. Repeater Mode: The device acts as a wireless repeater (also called wireless range extender) that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network.
3. Managed AP Mode: The device acts as a slave AP within an AP array.
4. Client Bridge Mode: The device is now a client bridge. The client bridge receives wireless signal and provides it to devices connected to the bridge (via Ethernet cable).





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

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

V Appendix

V-1 Configuring your IP address

The access point uses the default IP address **192.168.2.2**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254).**

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system.

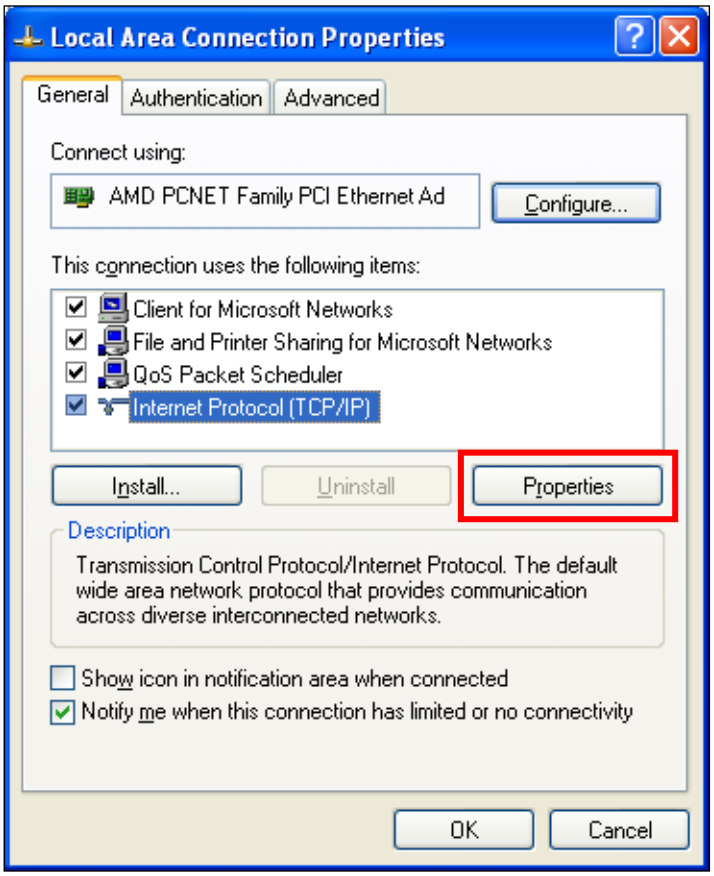
In the following examples we use the IP address **192.168.2.10** though you can use any IP address in the range **192.168.2.x (x = 3 – 254).**

If you've changed the AP Controller's IP address, or if your gateway/router uses a DHCP server, make sure you enter the correct IP address. Refer to your gateway/router's settings. Your computer's IP address must be in the same subnet as the AP Controller.

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

V-1-1 Windows XP

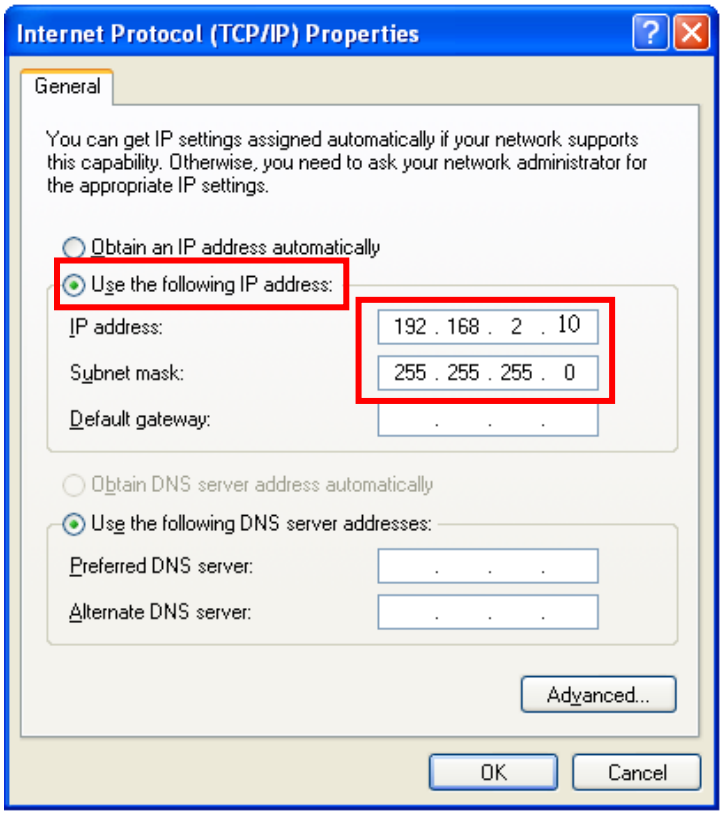
1. Click the “Start” button (it should be located in the lower-left corner of your computer) → “Control Panel” → “Network and Internet Connections” → “Network Connections” → “Local Area Connection”. The “Local Area Connection Properties” window will appear, select “Internet Protocol (TCP / IP)”, and click “Properties”.



2. Select “Use the following IP address”, then input the following values:

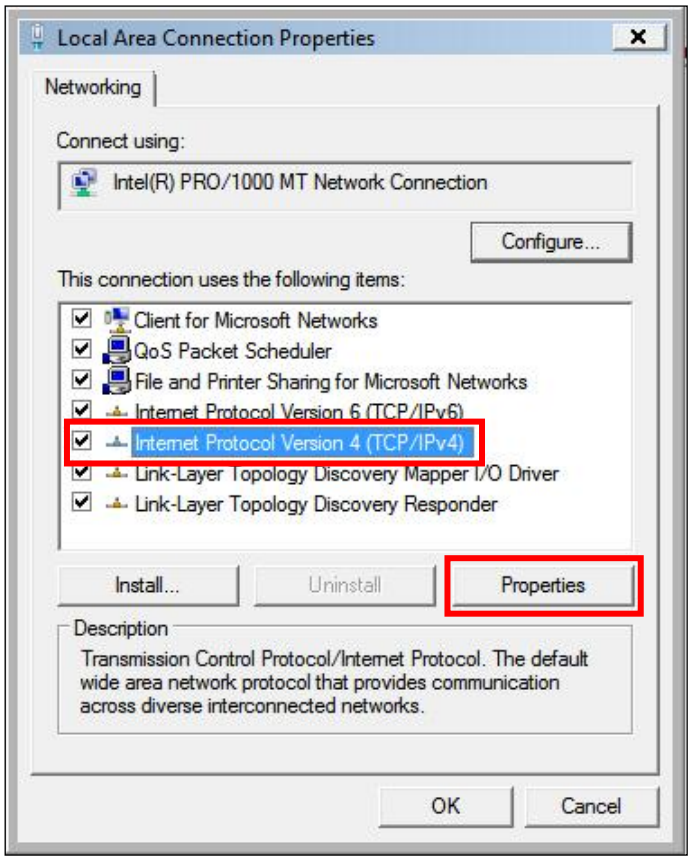
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



V-1-2 Windows Vista

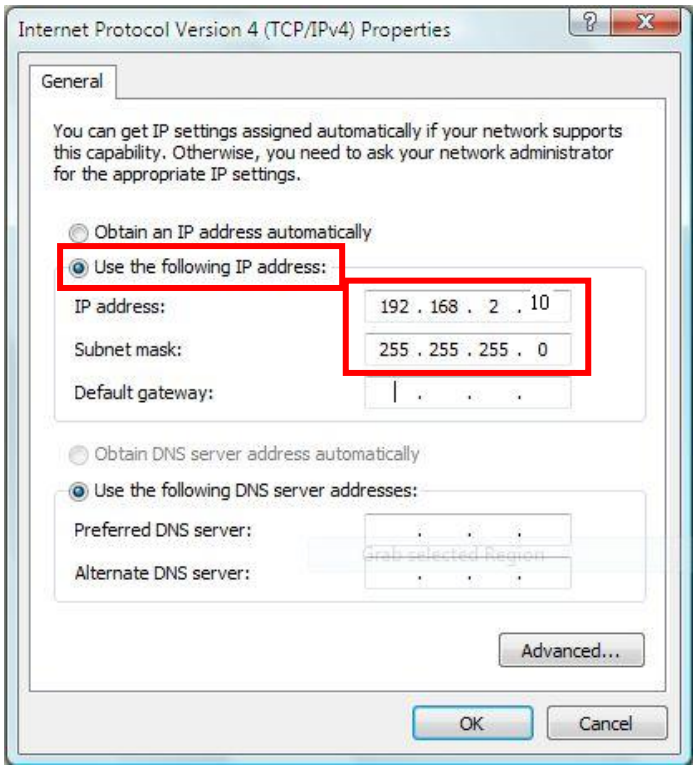
1. Click the “Start” button (it should be located in the lower-left corner of your computer) → “Control Panel” → “View Network Status and Tasks” → “Manage Network Connections” → “Local Area Network” → “Properties”. The “Local Area Connection Properties” window will appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”.



2. Select “Use the following IP address”, then input the following values:

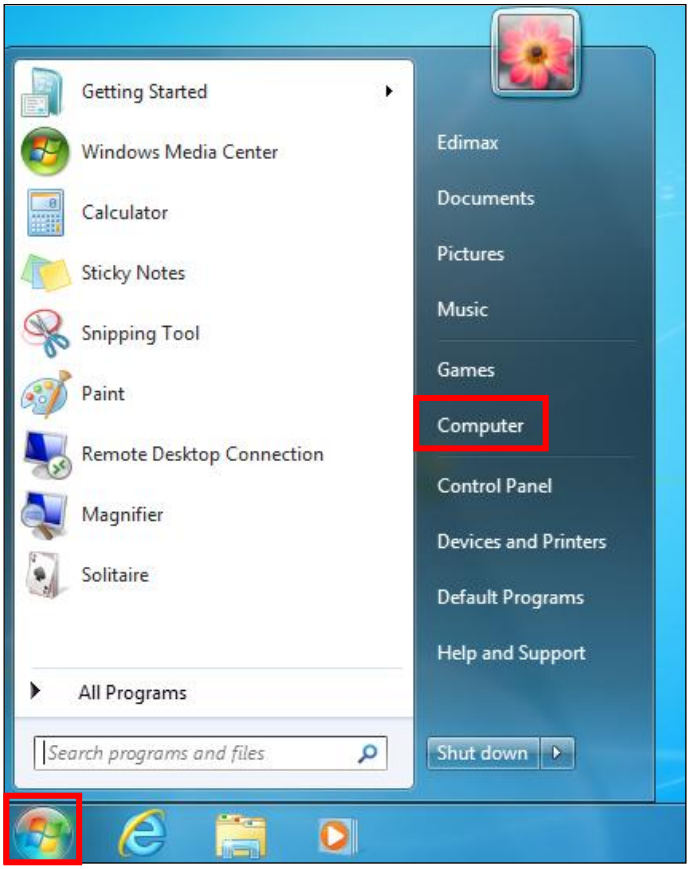
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

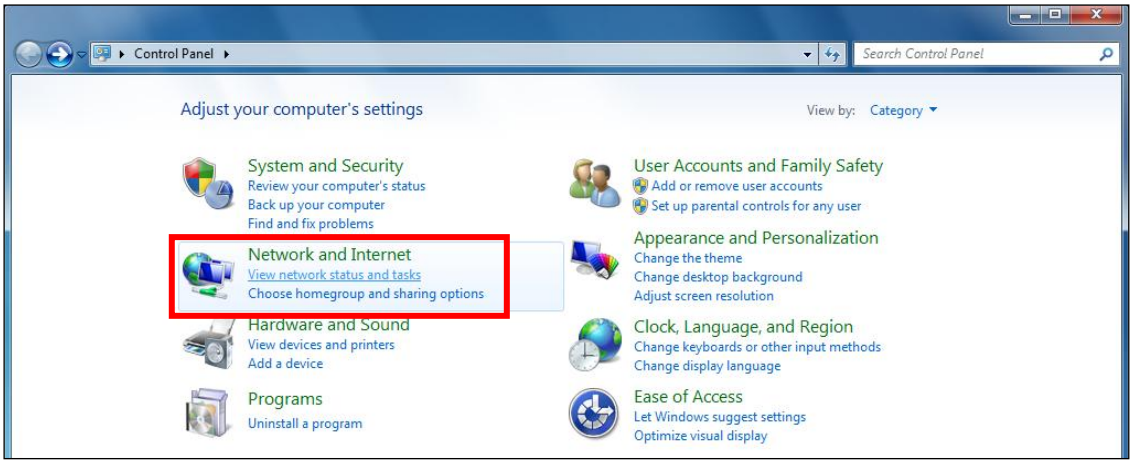


V-1-3 Windows 7

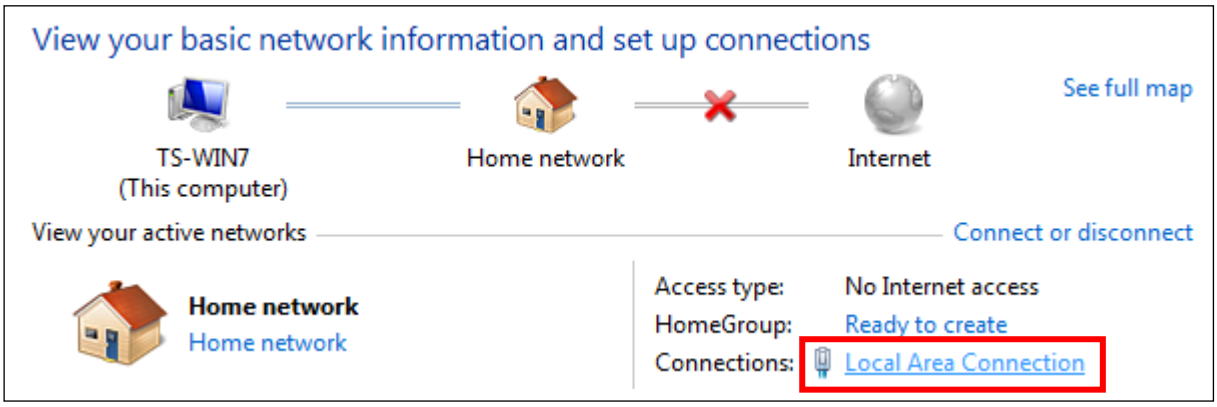
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



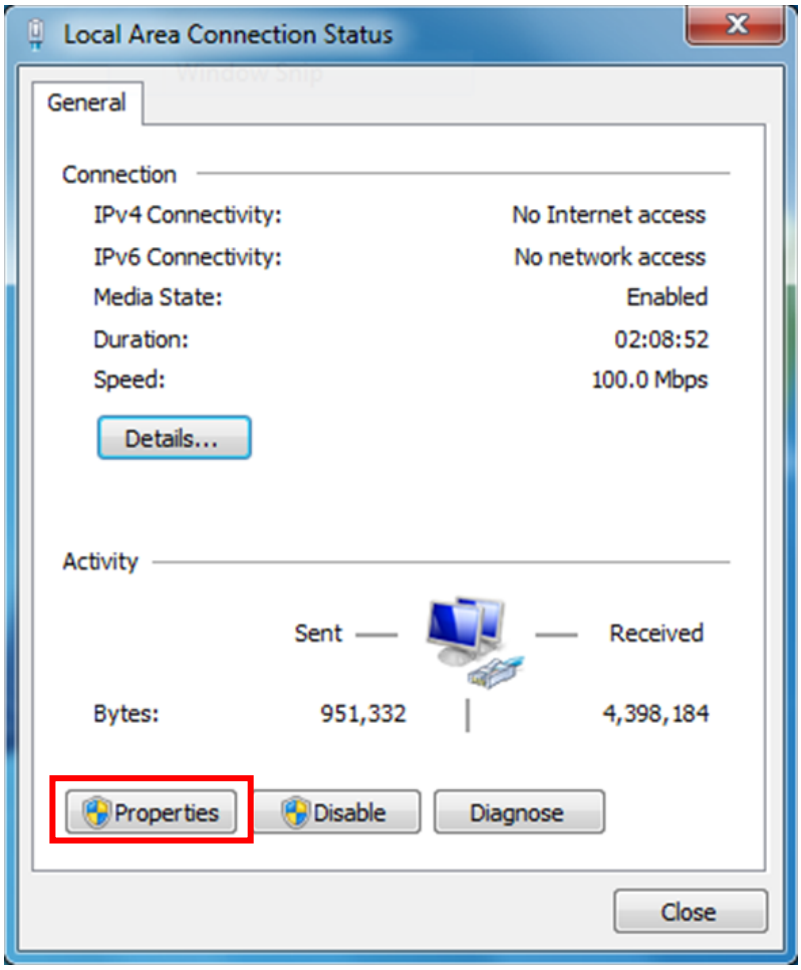
2. Under “Network and Internet” click “View network status and tasks”.



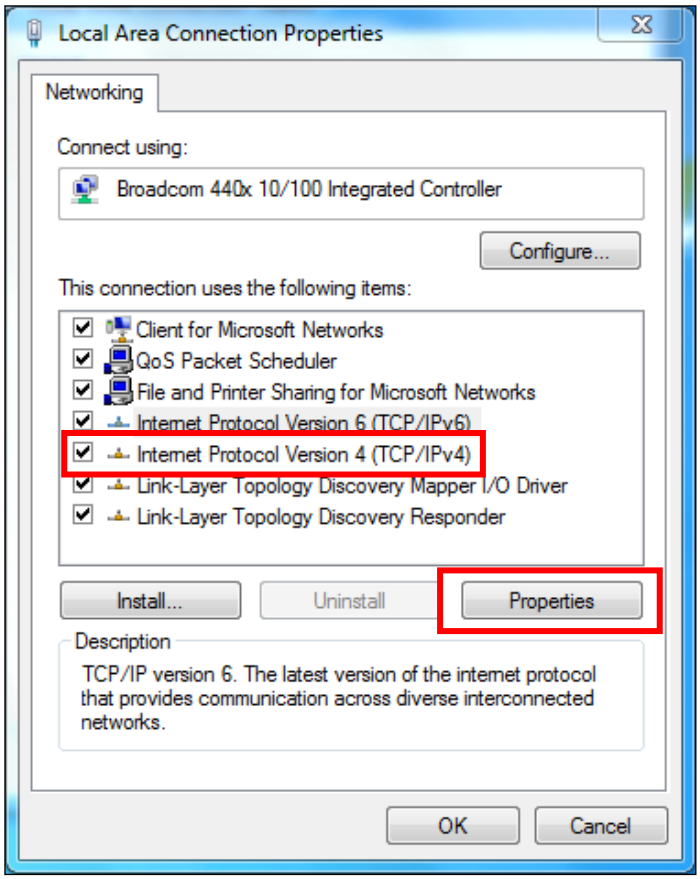
3. Click “Local Area Connection”.



4. Click “Properties”.



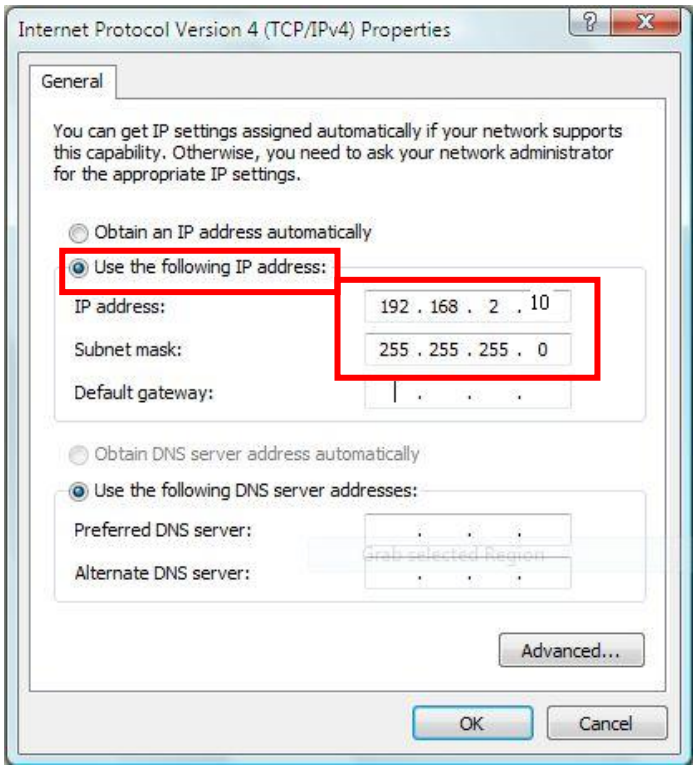
5. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



6. Select “Use the following IP address”, then input the following values:

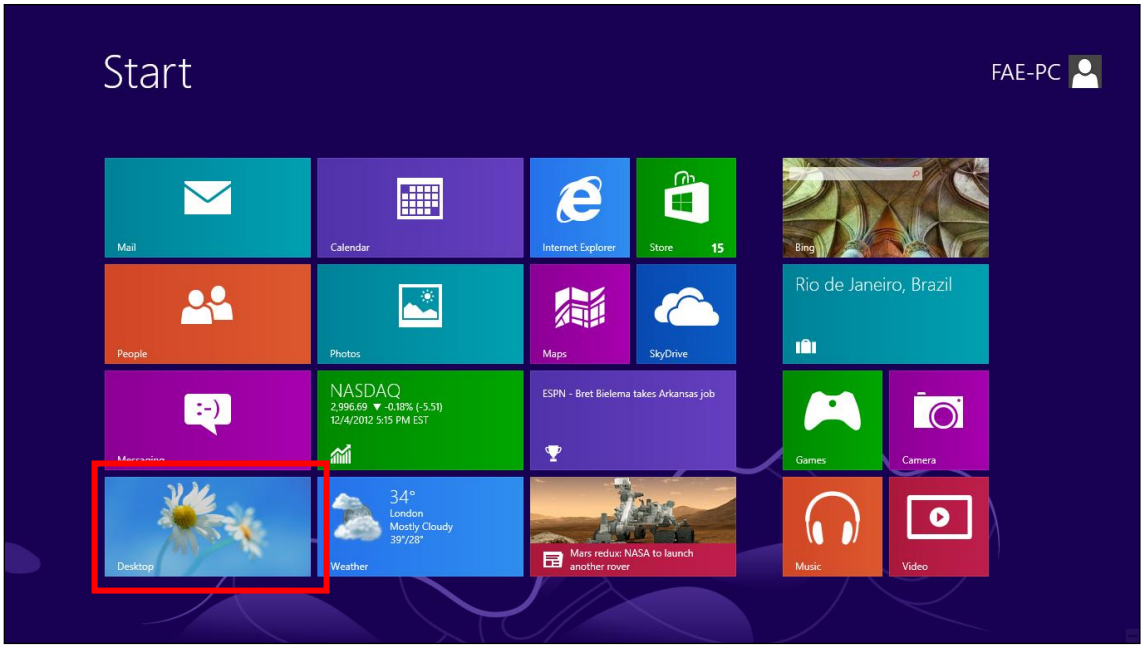
IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

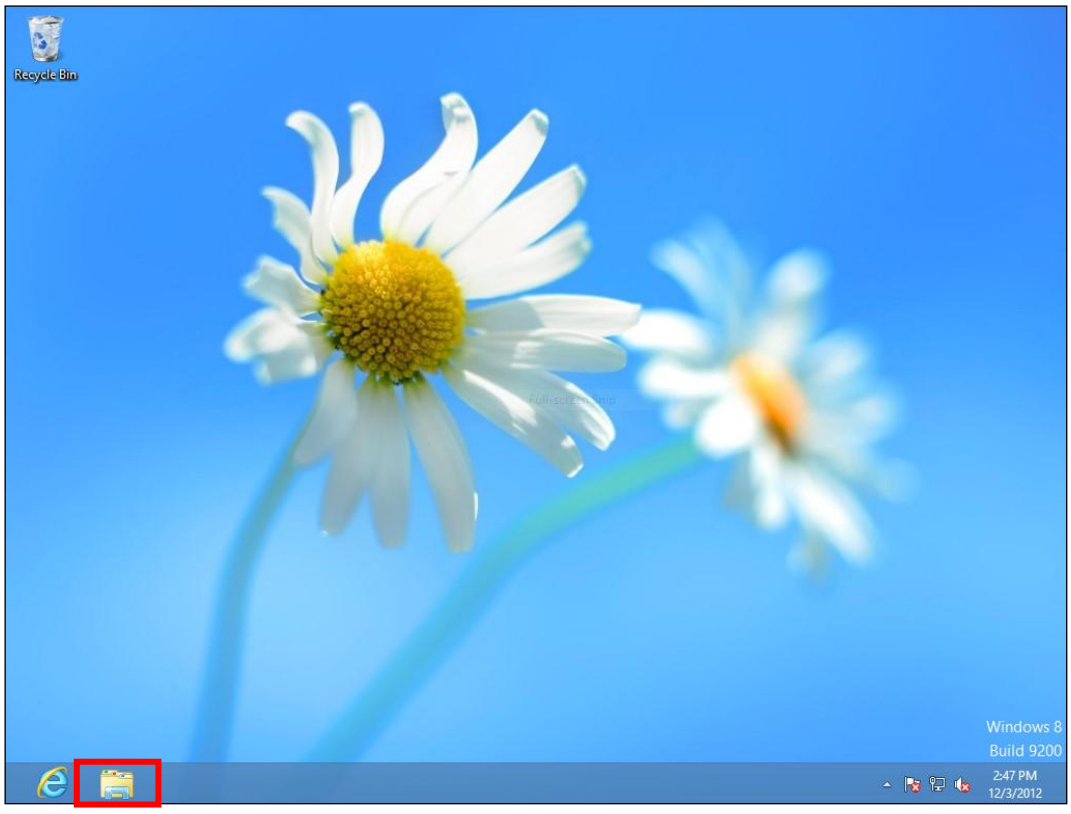


V-1-4 Windows 8

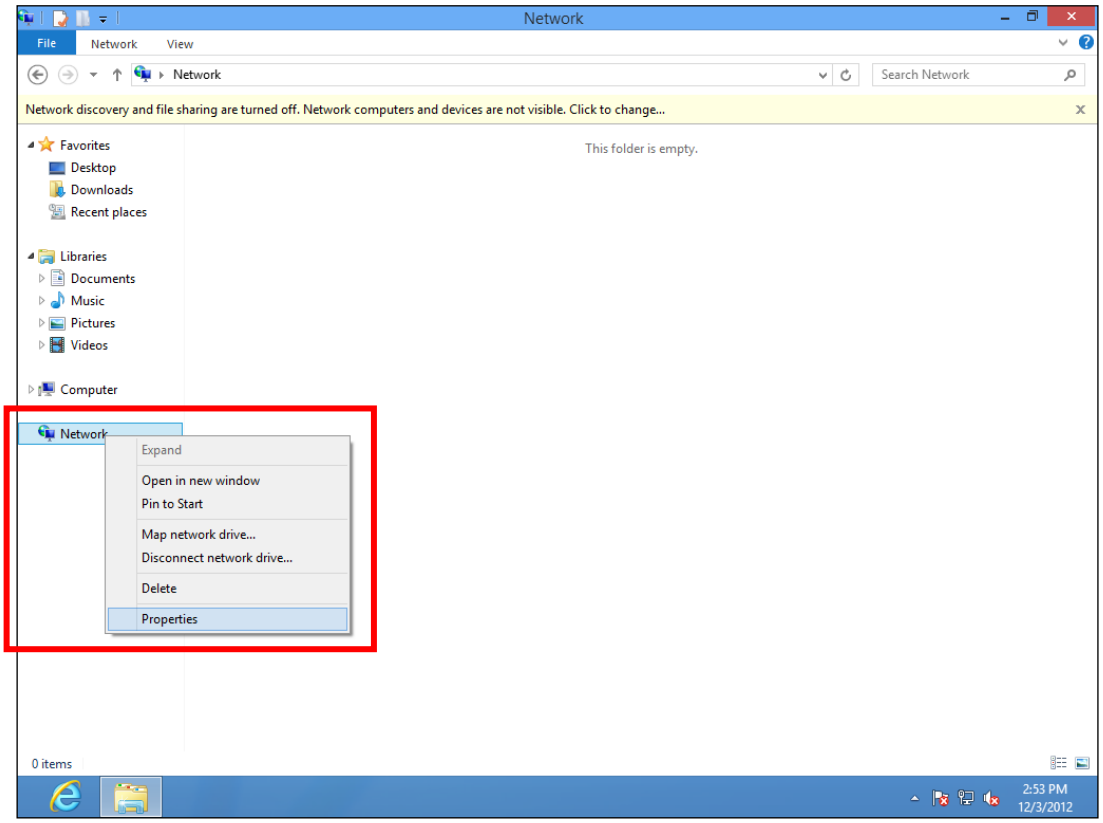
1. From the Windows 8 Start screen, switch to desktop mode by clicking the “Desktop” box.



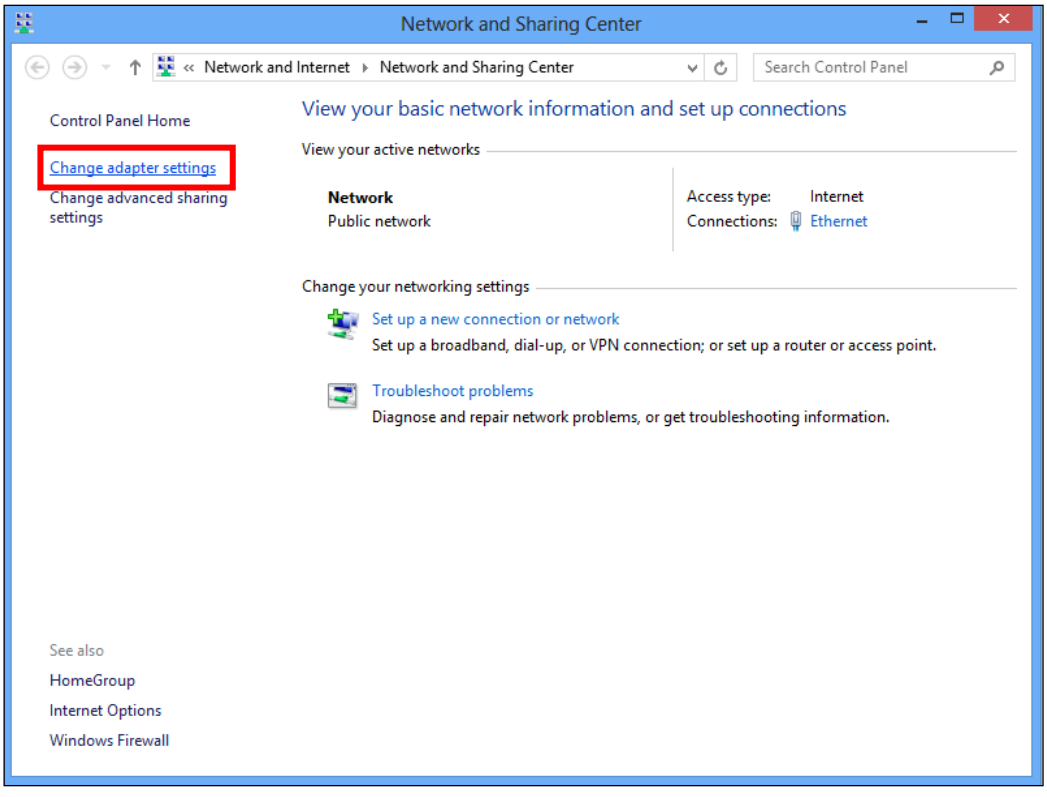
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



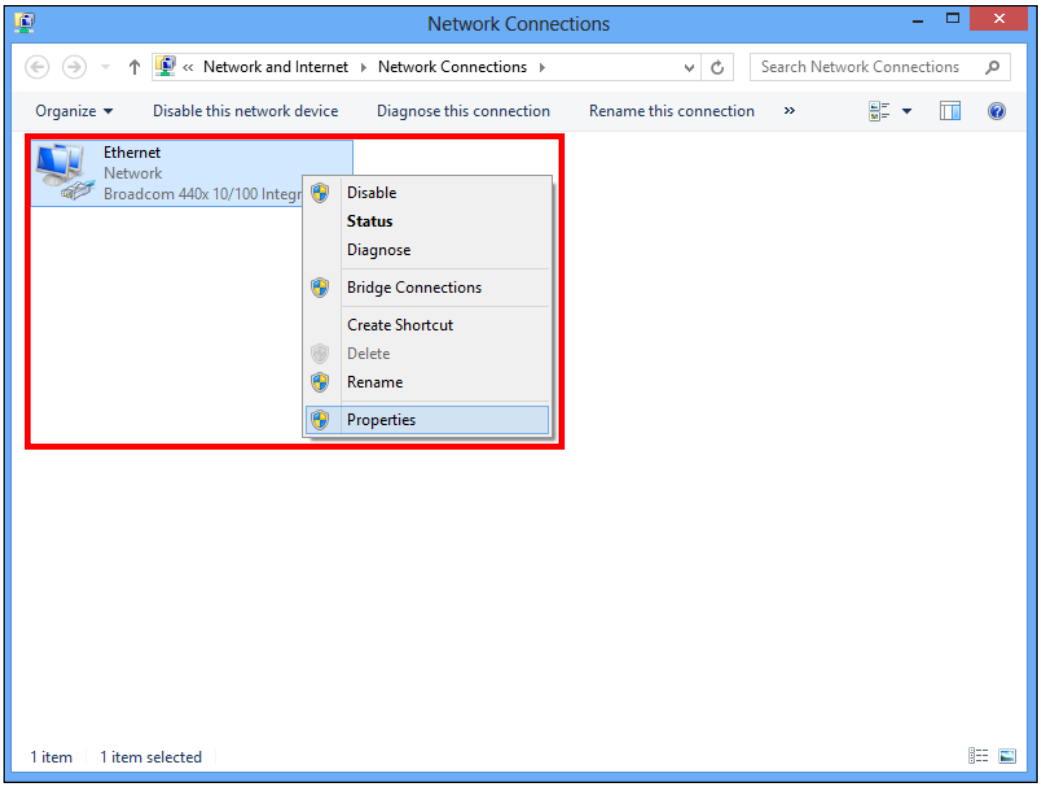
3. Right click “Network” and select “Properties”.



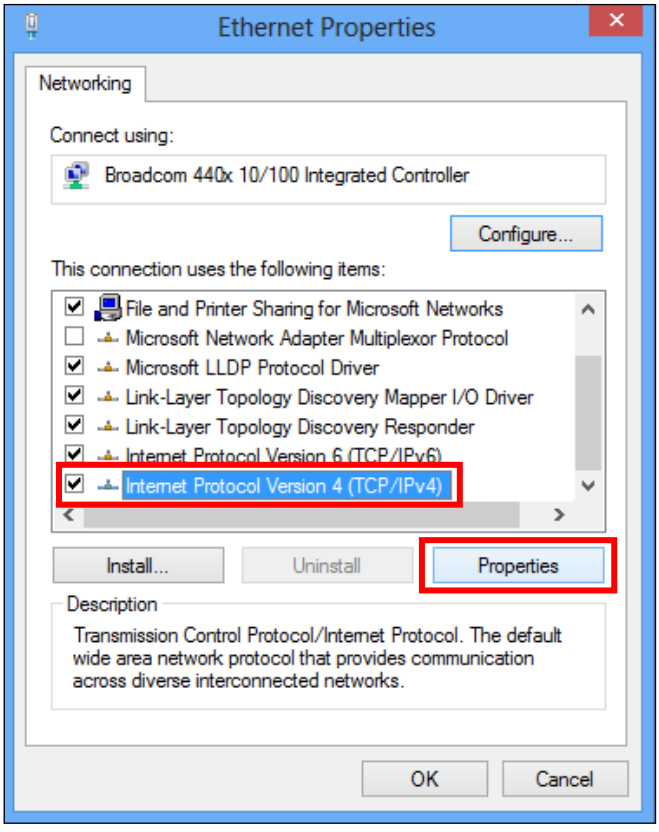
4. In the window that opens, select “Change adapter settings” from the left side.



5. Right click the connection and select “Properties”.



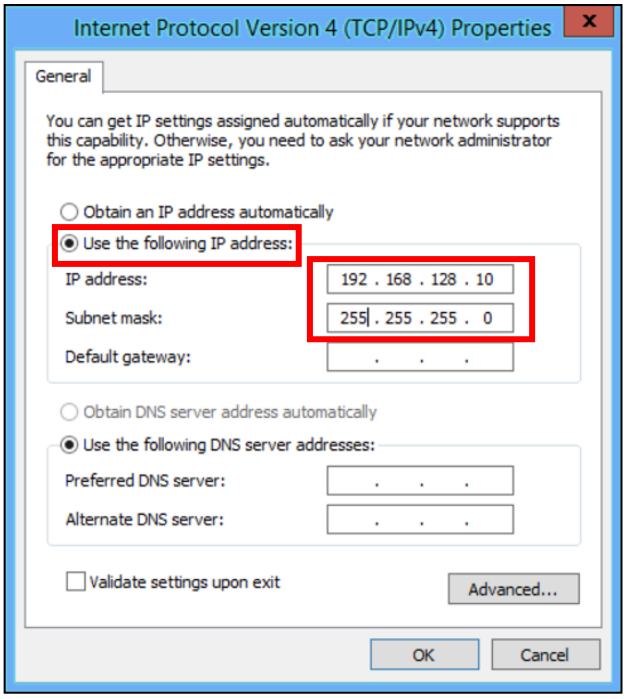
6. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



7. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

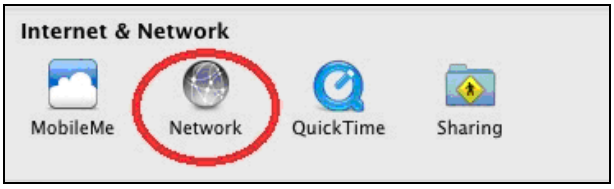
Click ‘OK’ when finished.



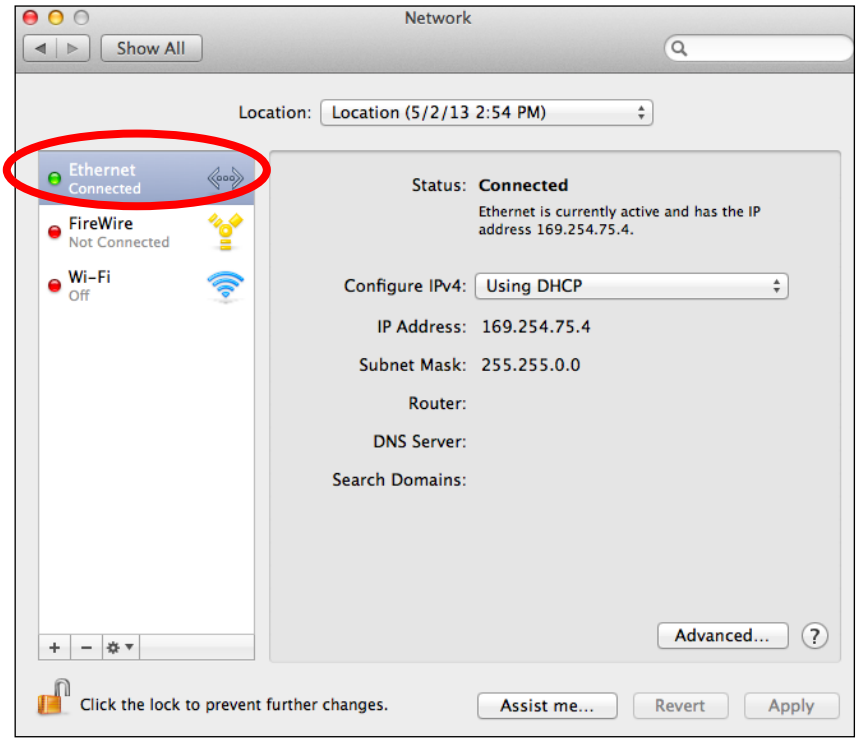
V-1-5 Mac

1. Have your Macintosh computer operate as usual, and click on “System Preferences”

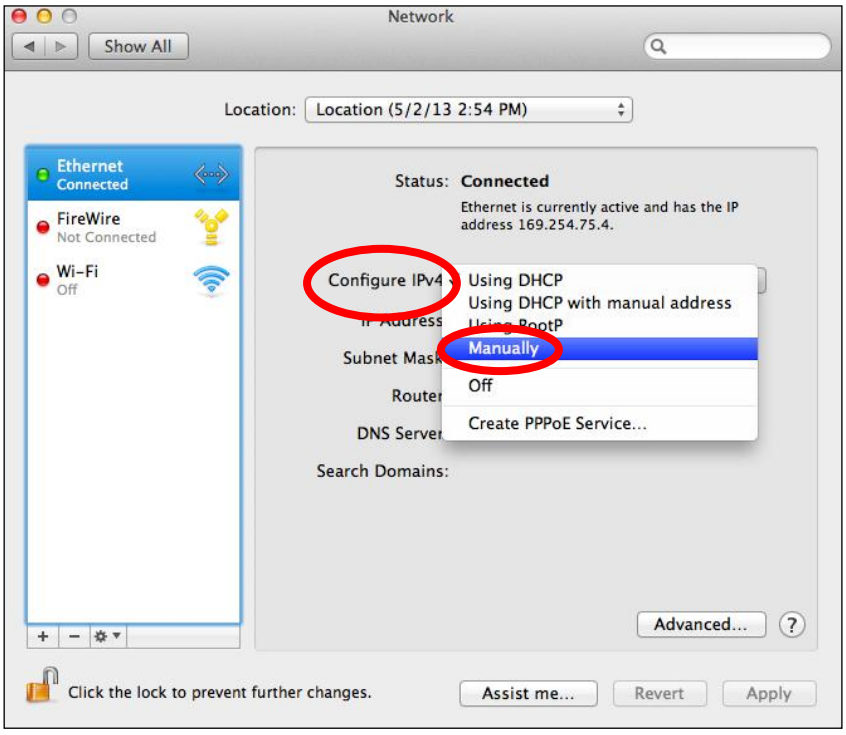
2. In System Preferences, click on “Network”.



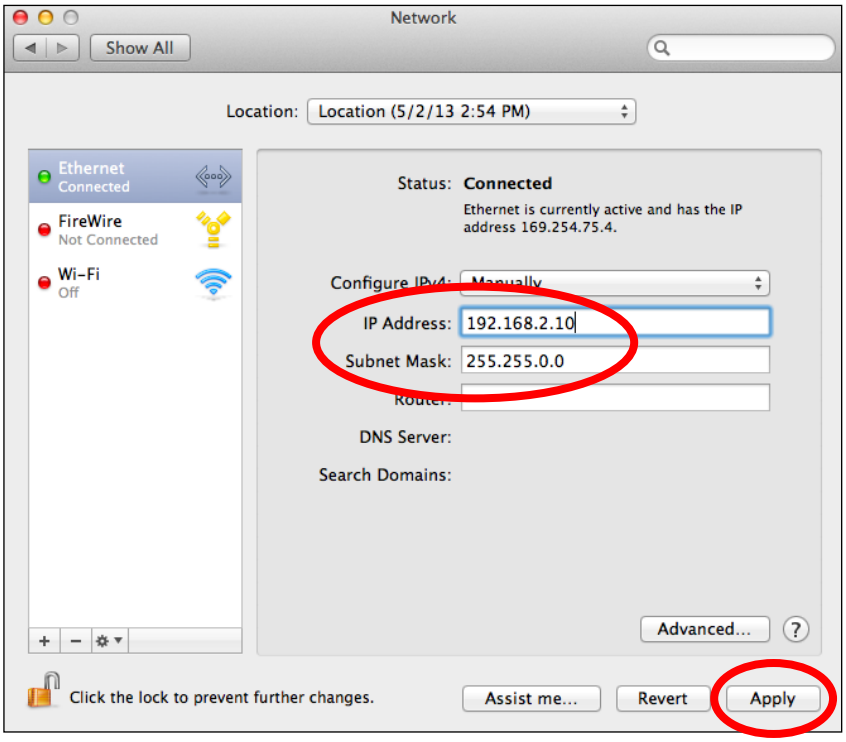
3. Click on “Ethernet” in the left panel.



4. Open the drop-down menu labeled “Configure IPv4” and select “Manually”.



5. Enter the IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on “Apply” to save the changes.

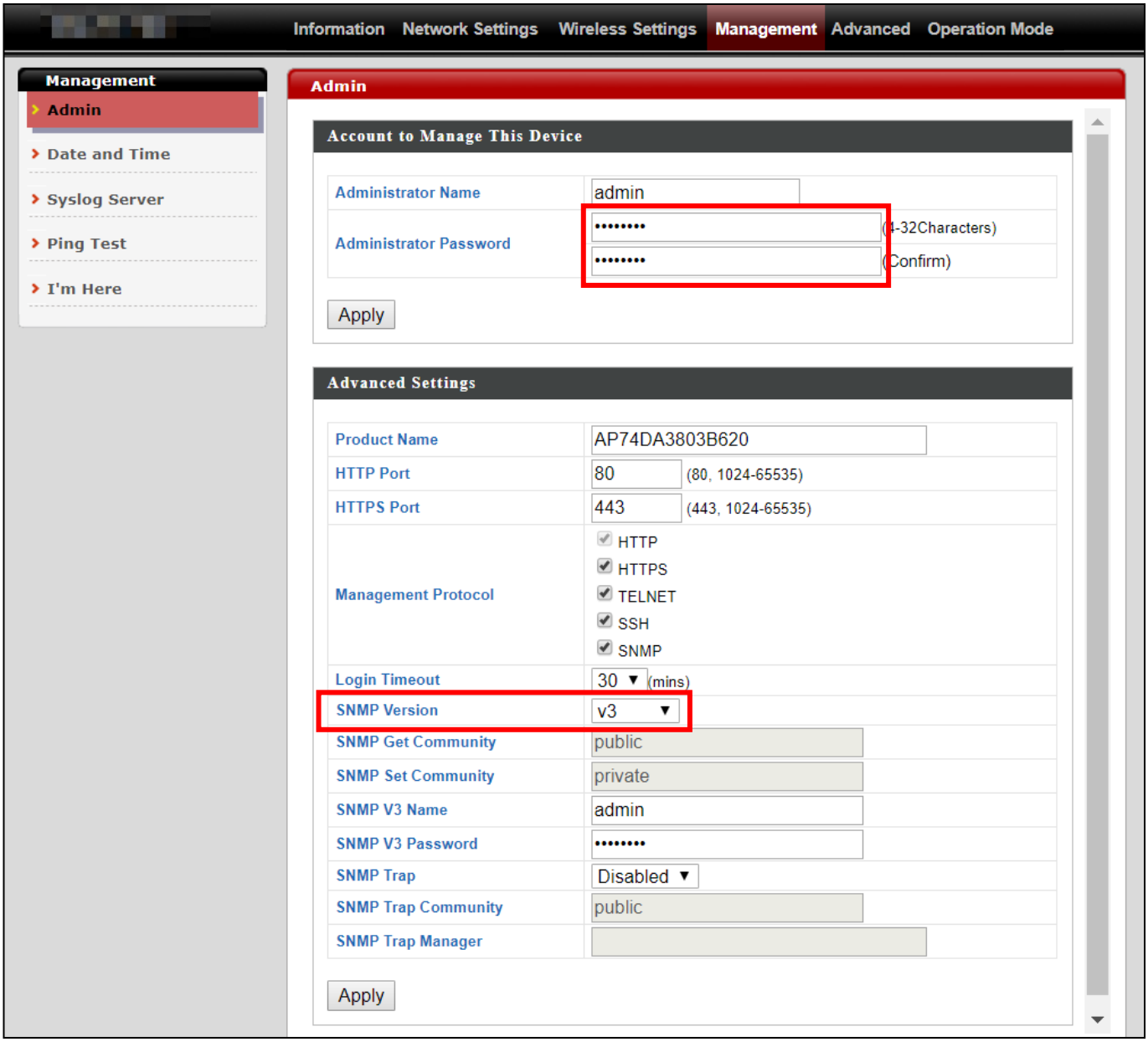


V-2 Setting AP via ManageEngine MibBrowser with SNMPv3 - Example

V-2-1 Setting in Web

1. The length of the password needs to be equal or greater than 8.

2. SNMP Version: V3



V-2-2 Setting Rule

If you want to set Basic Wireless Setting via SNMP, the related variables need to be set together. Please refer to the file *Edimax-7476HPC_private_MIB_20150715_v1.1*, for setting Radio or SSID.

Example: Basic Wireless Settings	Settings
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.3.3 i 2	Auto Channel Disable
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.2.3 i 3	11b/g/n: band
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.4.3 i 7	7: channel
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.6.3 i 1	20M: Bandwidth
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.7.3 i 5	all: basic rate

STRING: -v3 -l noAuthNoPriv -u admin -a MD5 -x DES

Reference: Radio Related page of *Edimax-7476HPC_private_MIB_20150715_v1.1*

V-2-3 Setting in ManageEngine MibBrowser

1. Set the version of SNMP

Figure 1 Step 1:Edit → Settings

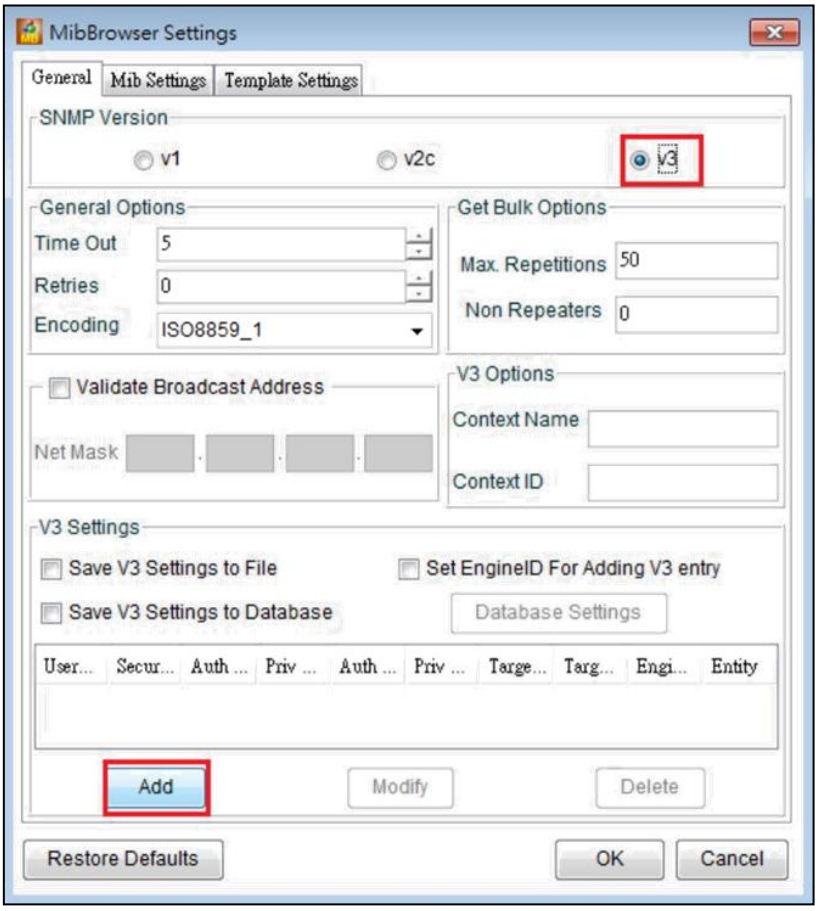


Figure 2 Step 2: Check v3 and click Add

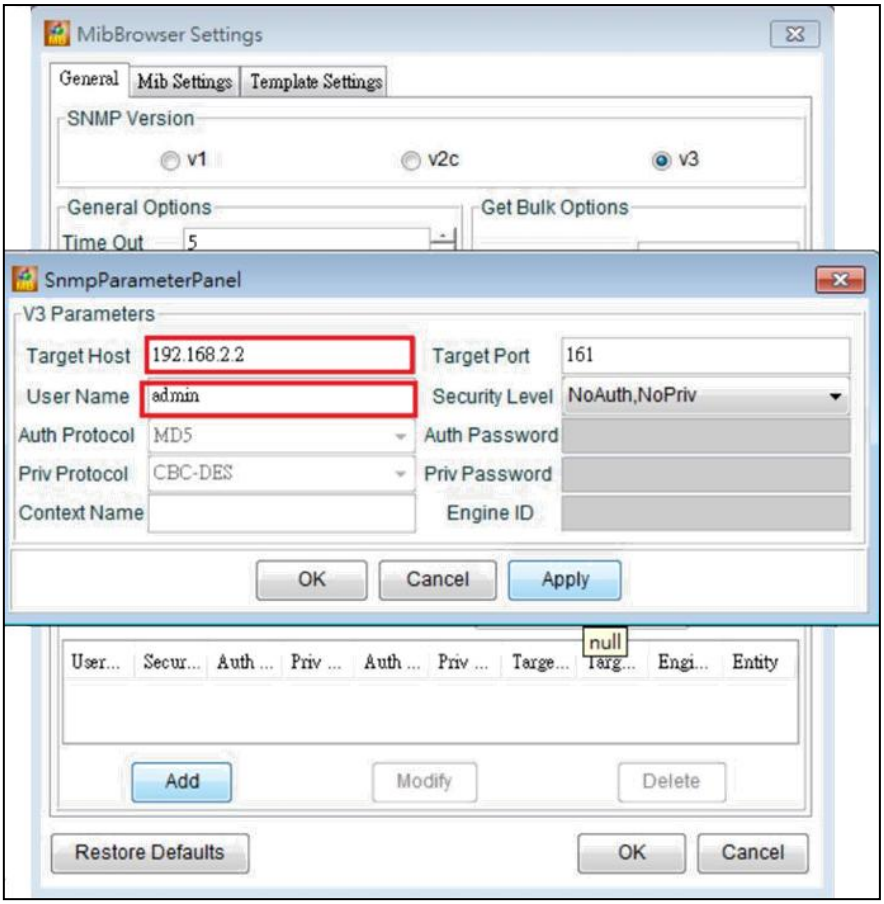


Figure 3 Step 3: Enter AP's IP and Administrator Name (User Name)

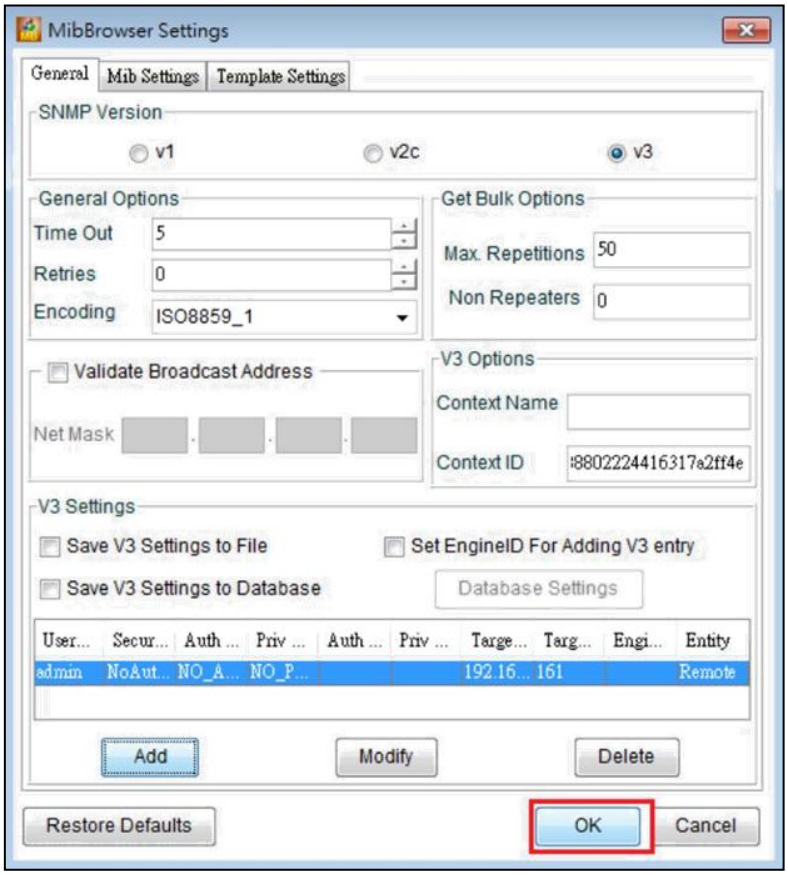


Figure 4 Step 4: Click OK

2. Load MIB Module

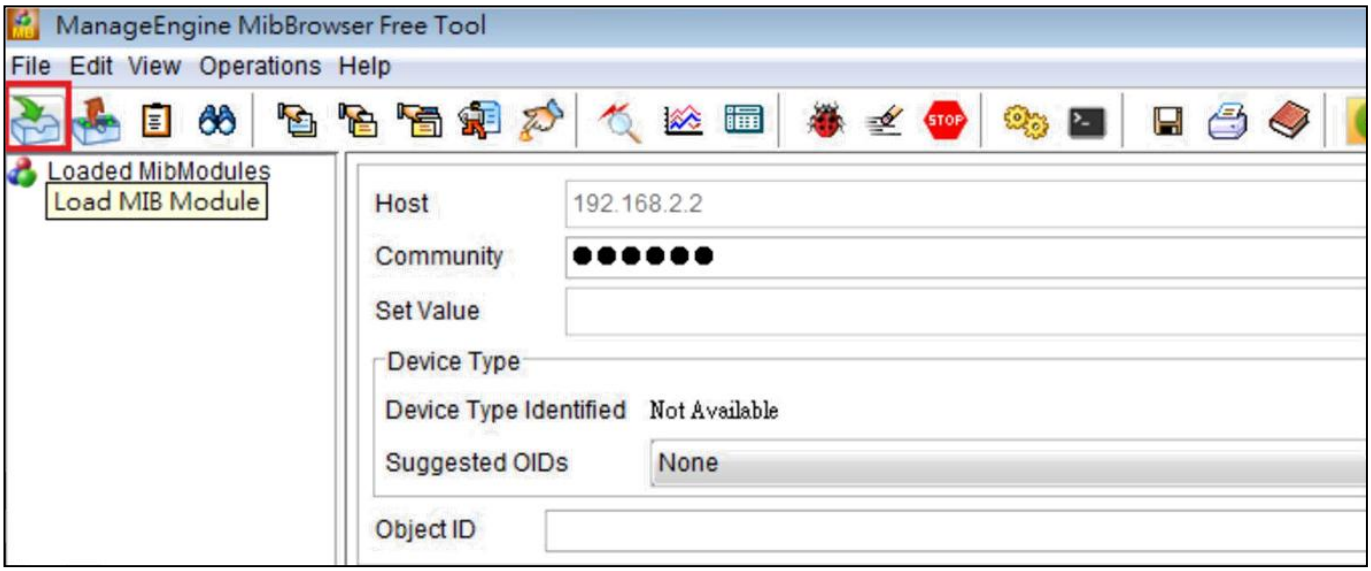


Figure 5 Click Load MIB Module and choose the file, *edimax_20150728.txt* (MIB file)

3. Add variables

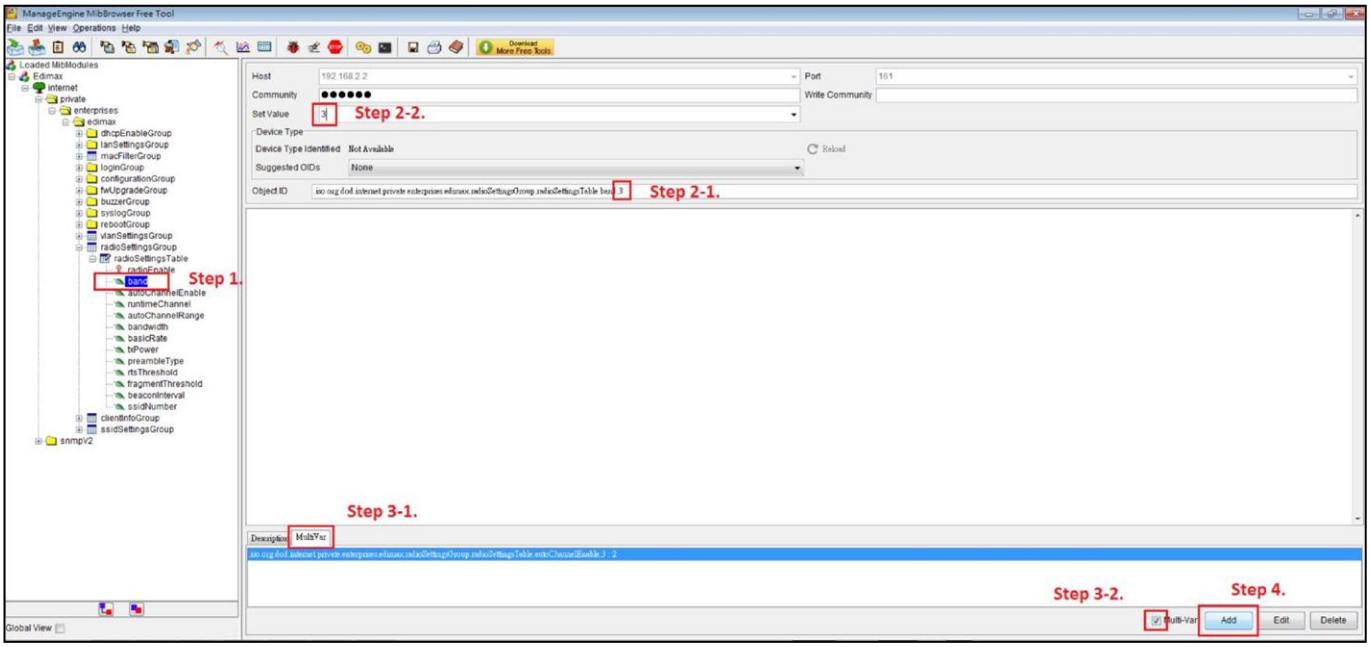


Figure 6 Example of setting the variable

Step 1.: Select the OID.
Step 2-1.: Enter the index of Radio (2.4G).
Step 2-2.: Enter the Set Value.
Step 3-1.: Click MultiVar.
Step 3-2.: Check Multi-Var.
Step 4.: Add this Variable

4. Set SNMP variables

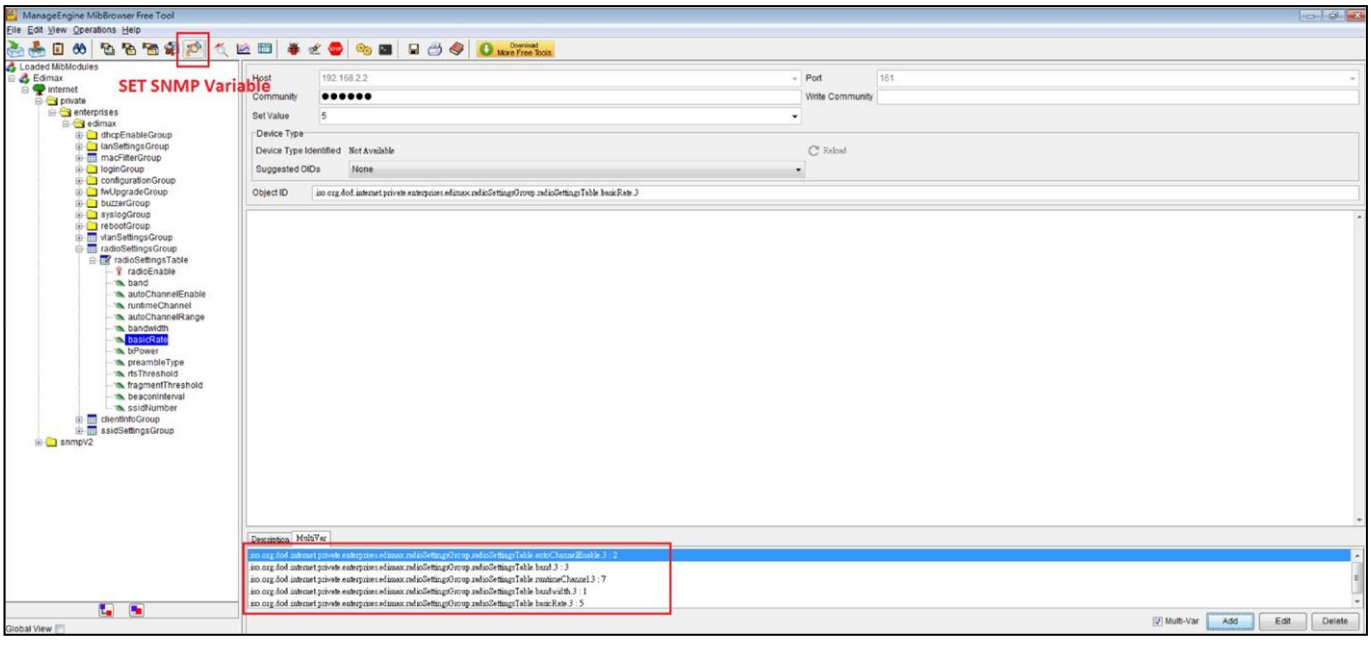


Figure 7 All the variables have been added. Click SET SNMP Variables

VI Best Practice

VI-1 How to Create and Link WLAN & Access Point Groups

NMS can be used to create individual SSIDs and group multiple SSIDs together into WLAN groups. You can then assign individual access points to use those WLAN group settings and/or group multiple access points together into access point groups, which you can also assign to use WLAN group settings.

Follow the example below to:

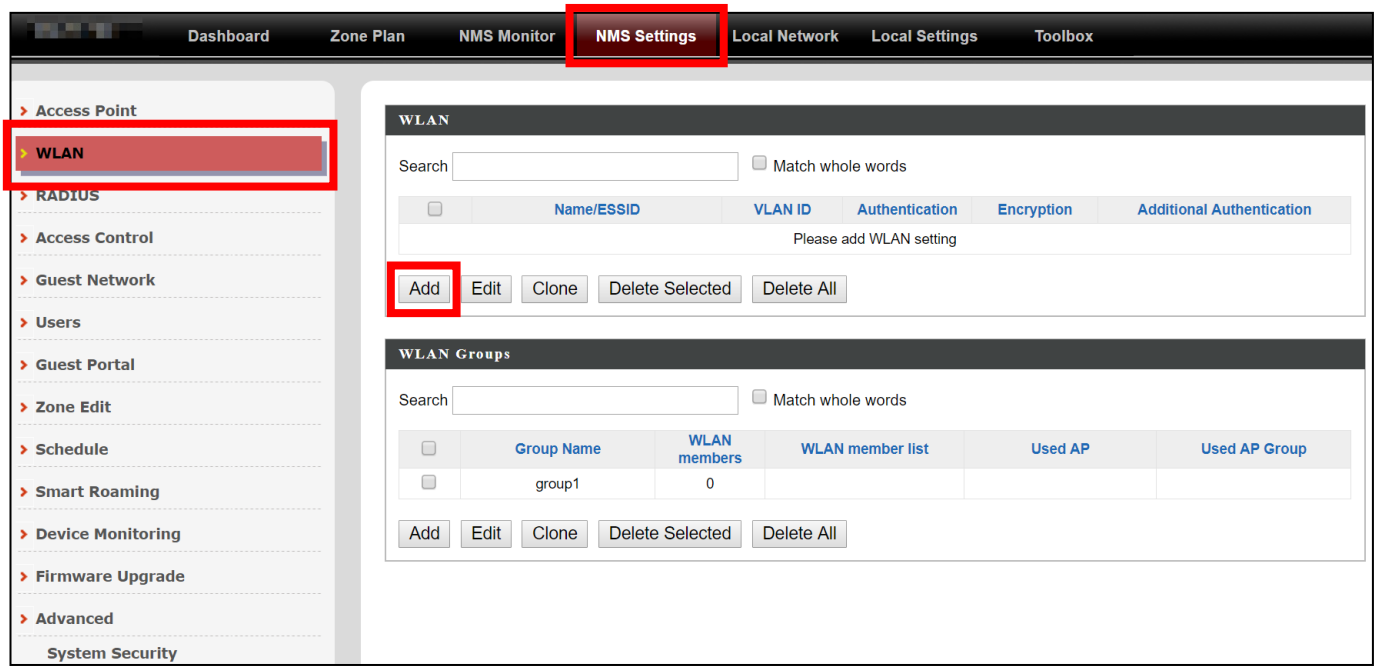
A. Create a WLAN group.

B. Create an access point group.

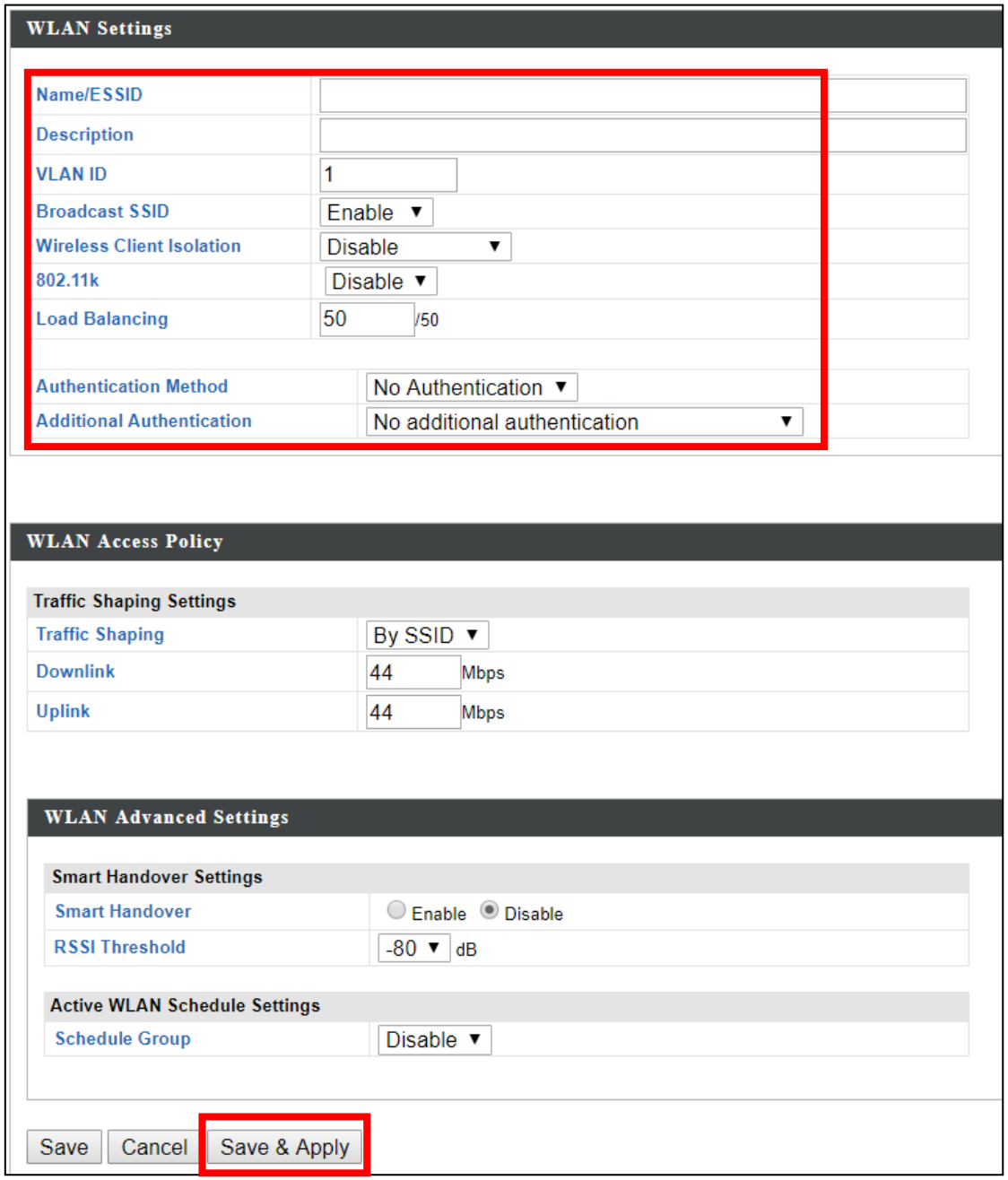
C. Assign the access point group to use the SSID group settings.

VI-1-1 Create WLAN Group

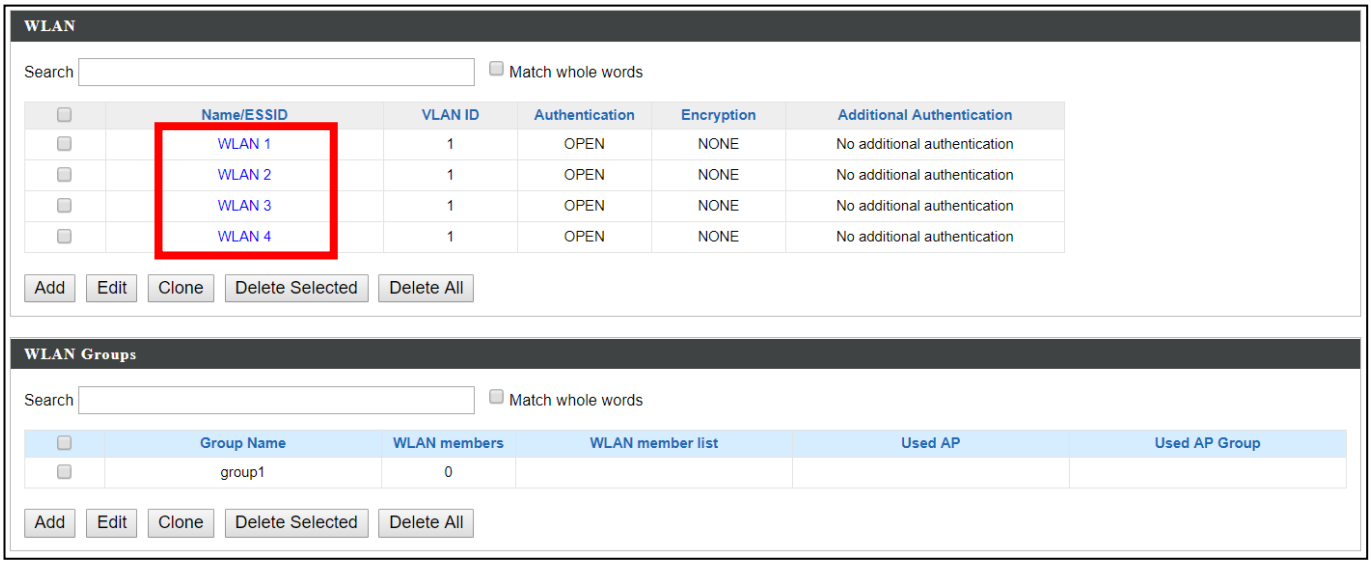
1. Go to **NMS Settings → WLAN** and click **"Add"** in the **WLAN** panel:



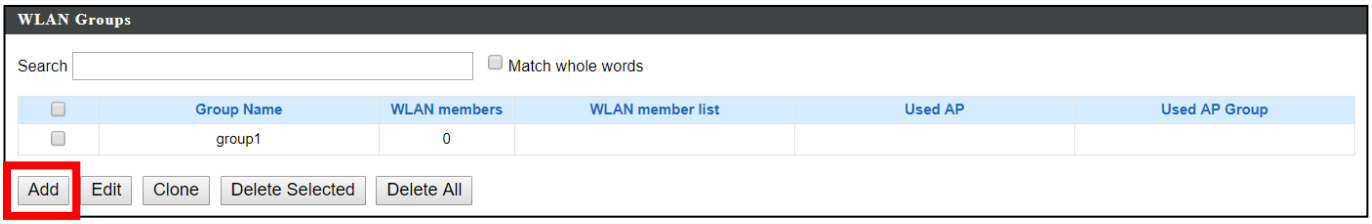
2. Enter an SSID **name** and set **authentication/encryption** and click **"Save & Apply"**:



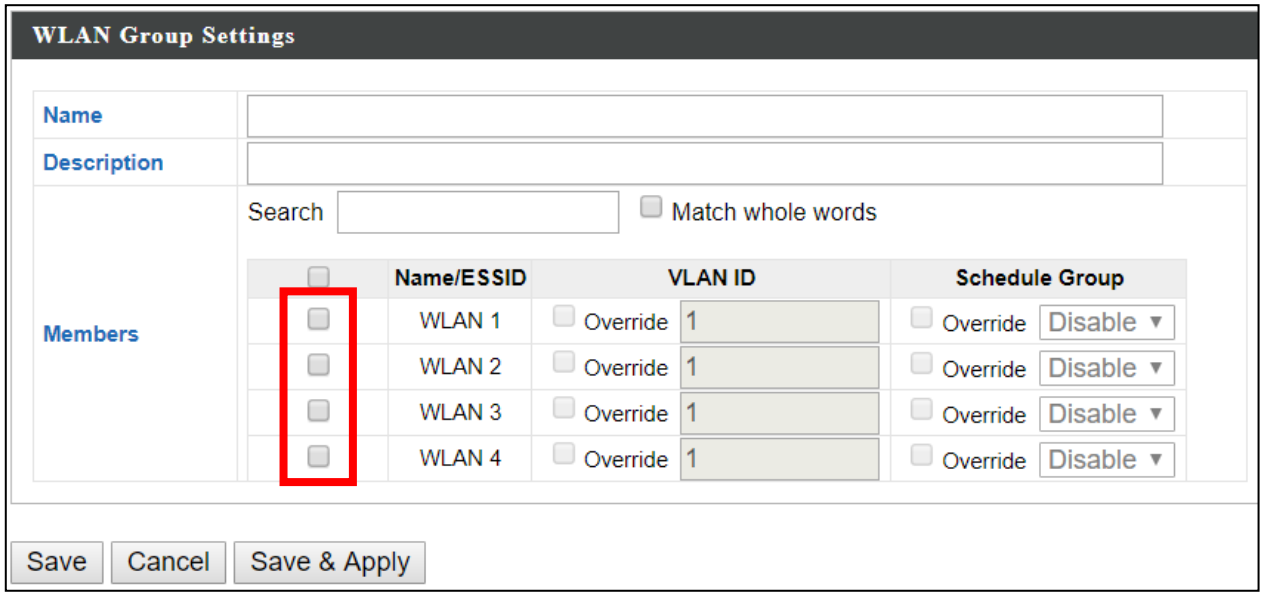
3. The new SSID will be displayed in the **WLAN** panel. **Repeat** to add additional SSIDs according to your preference.



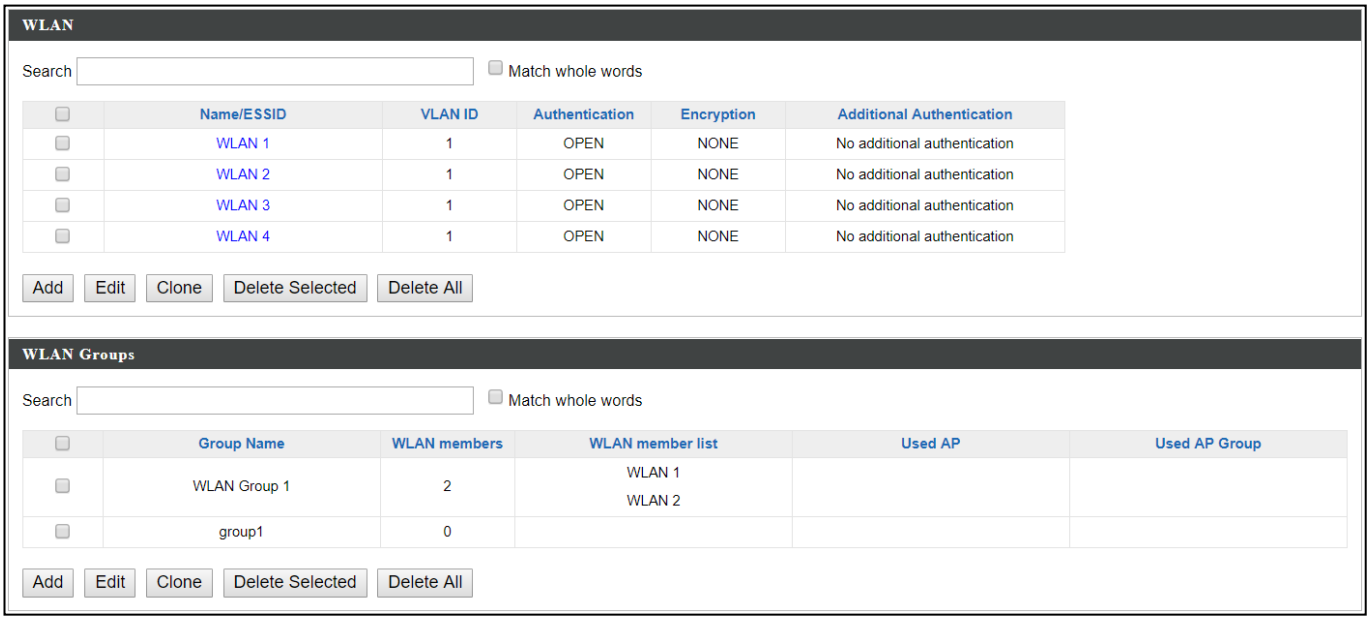
4. Click **"Add"** in the **WLAN Groups** panel:



5. Enter a **name** for the **SSID group** and **check the boxes** to select which SSIDs to include in the group. Click "**Save and Apply**" when done.

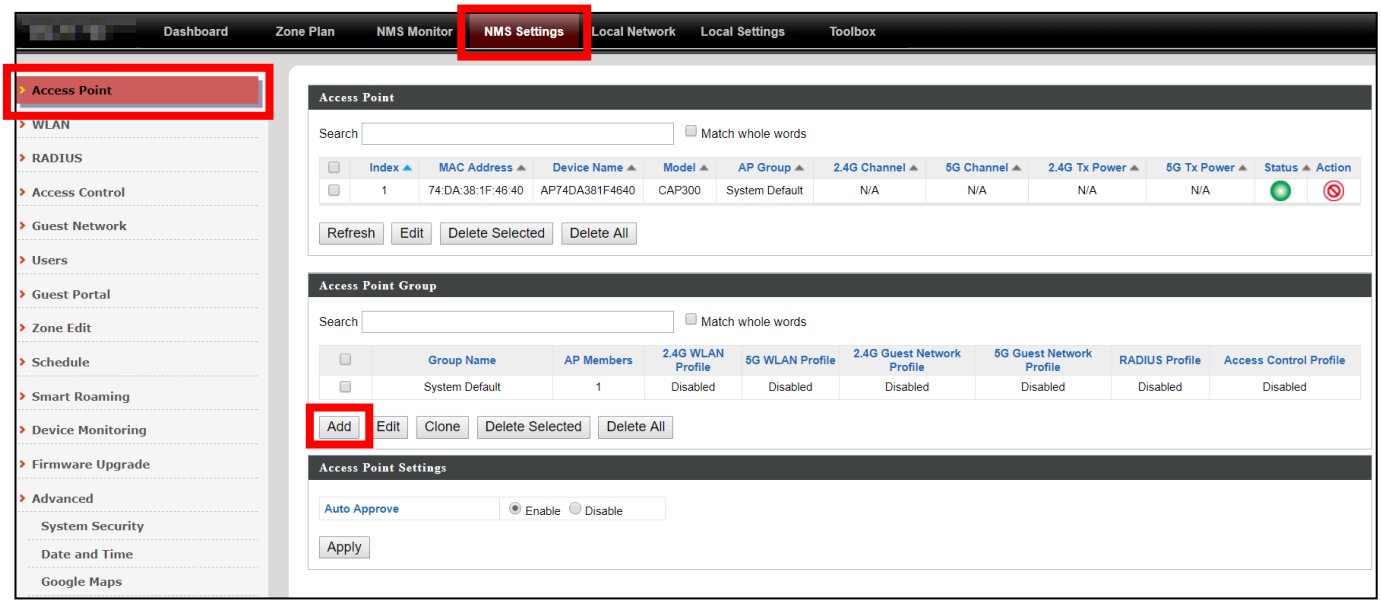


6. The new **WLAN group** will be displayed in the **WLAN Group** panel. **Repeat** to add additional WLAN groups according to your preference:

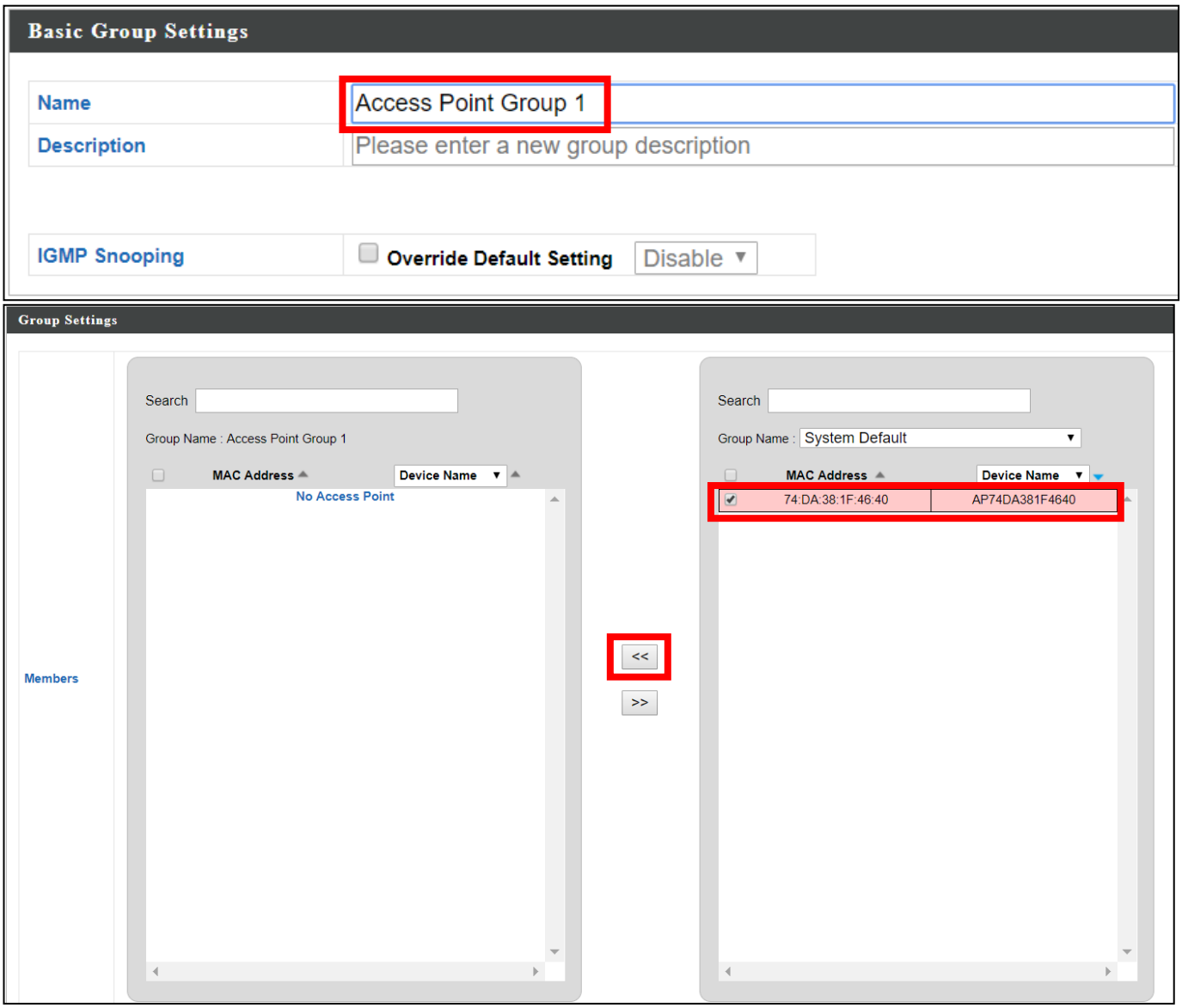


VI-1-2 Create Access Point Group

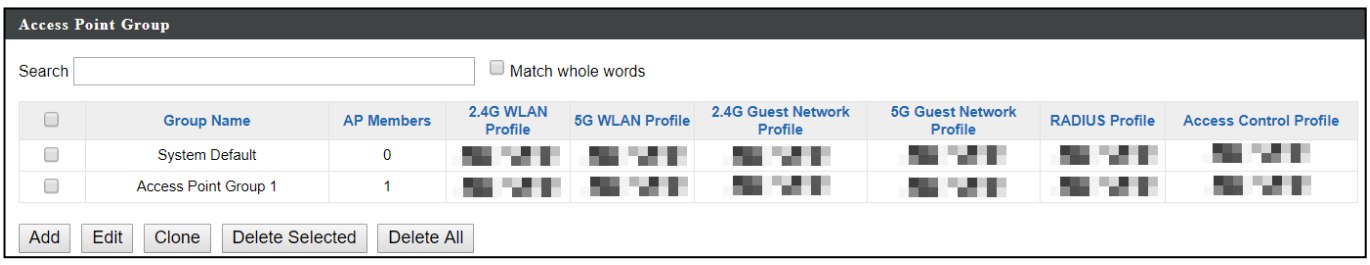
1. Go to **NMS Settings → Access Point** and click “Add” in the Access Point Group panel:



2. Enter a **Name** and then scroll down to the **Group Settings** panel and use the **<<** button to **add** selected access points into your group from the box on the right side. Click **"Save & Apply"** when done.

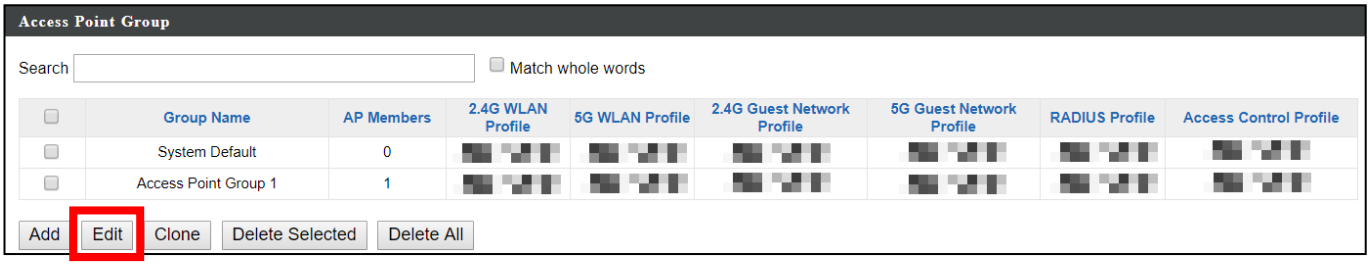


3. The new group will be displayed in the **Access Point Group** panel. **Repeat** to add additional access point groups according to your preference:

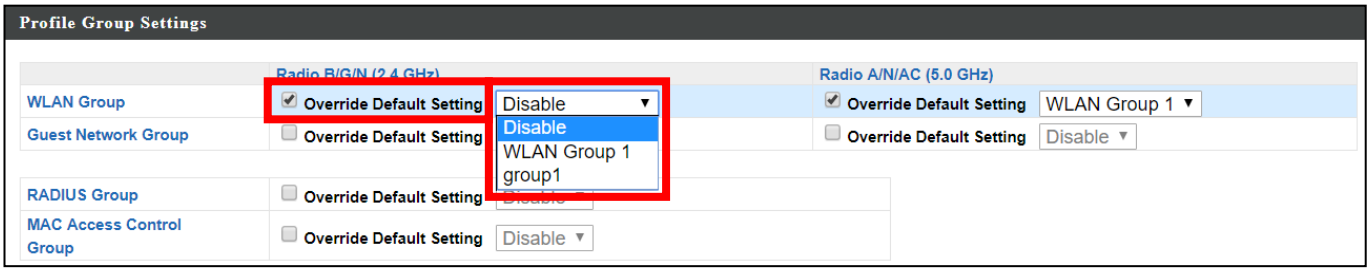


VI-1-3 Assign Access Point Group to use the SSID group settings

1. Go to **NMS Settings → Access Point** and select an access point group using the checkboxes in the **Access Point Group** panel. Click "**Edit**":



2. Scroll down to the **Profile Group Settings** panel and check the "**Override Group Settings**" box for **WLAN Group (2.4GHz and/or 5GHz).** Select your **WLAN group** from the drop-down menu and click "**Apply**":



3. Repeat for other access point groups according to your preference.

Professional installation warning:

This device is point-to-multi-point device. The general user should not attempt to install or change settings, it needs to be installed by a qualified personal who has RF exposure and related rule knowledge or technology.

The installation position and output power does not exceed the limit set forth in US Rule CFR 47 part 15 section 15.247 & 15.407. If violate the rule, could lead to serious federal penalty.

It is complies with §15.407 (a)(1)(i) requirement that the maximum e.i.r.p. at any elevation angle above 30 degrees as measured from the horizon must not exceed 125 mW (21 dBm).

About TDWR 5600-5650 MHz, installation and operation should with a minimum distance of 20 centimeters between the radiator and your body or nearby persons.

Use two type antenna specifications. One type antenna model name is 98623PRSX000, antenna type is dipole antenna with peak gain 4.58dBi for 2.4GHz; 6.18dBi for 5150-5250MHz; 6.22dBi for 5250-5350MHz; 6.12dBi for 5470-5725MHz; 6.05dBi for 5725-5850MHz. Other type antenna model name is C095-510399-A, antenna type is dipole antenna with peak gain 3dBi for 2.4GHz; 4dBi for 5150-5850MHz. Only use manufacturer approved antenna type of antenna.

COPYRIGHT

Copyright © Edimax Technology Co., Ltd. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission from Edimax Technology Co., Ltd.

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.

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

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.

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

FCC Radiation Exposure Statement:

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.

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)
2412-2472	19.66 dBm
5500-5700	27.73 dBm

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

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type **AC1300 Outdoor 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/

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 DE GR HU IE IT LV LT LU MT NL PL PT SK SI ES SE GB IS LI NO CH BG RO RU TR UA

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 directives.

Equipment: **AC1300 Outdoor AP**
Model No.: **OAP1300**

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 V2.1.1 (2017-02)
		EN 301 489-17 V3.2.0 (2017-03)
		EN 55032: 2012 / AC:2013
		EN 55024: 2010
EMF	:	EN 62311:2008

Directives 2014/35/EU

Safety (LVD)	:	IEC 60950-1:2005 (2nd Edition)+Am 1:2009+Am 2:2013
		EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

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: Vivian Ma
Title: Director
Edimax Technology Europe B.V.

Date of Signature: March, 2018
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

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

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.