GAP-429HOB

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.

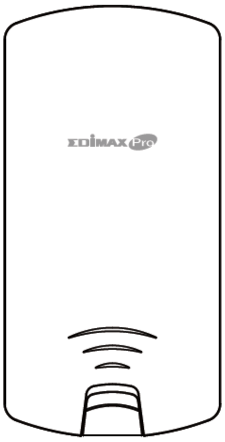
Repeater Mode is a wireless repeater (also called wireless range extender) that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network.

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

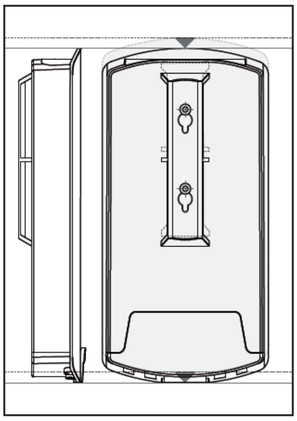
Client Bridge Mode determines the device to be a client bridge. The client bridge receives wireless signal and provides it to devices connected to the bridge via Ethernet cable.

I Product Information

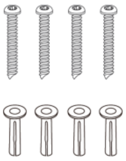
I-1 Package Contents



1



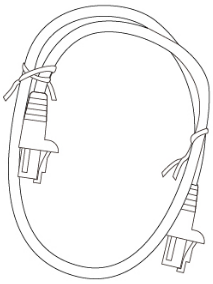
2



3

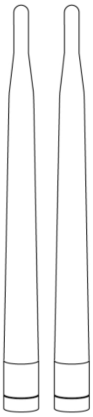
4

5



6

7



8

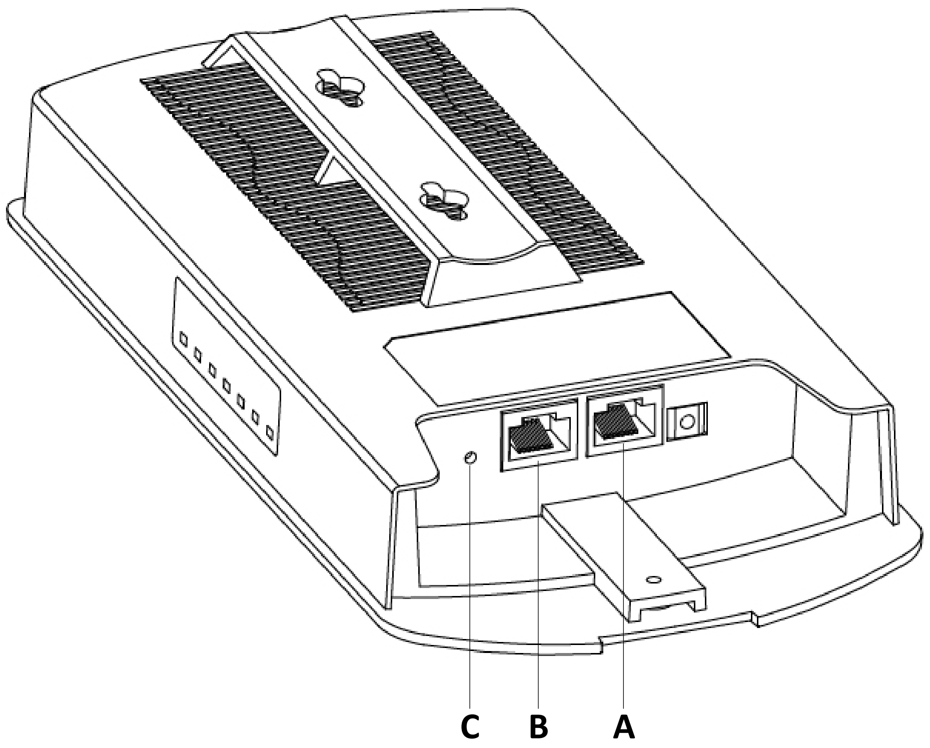
1. GAP-429HOB Access Point
2. Wall Mount Screw Template
3. Wall Mount Screw Set
4. CD
5. Quick Installation Guide
6. Ethernet Cable
7. Pole Mount Strap x2
8. Antenna x2

I-2 System Requirements

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

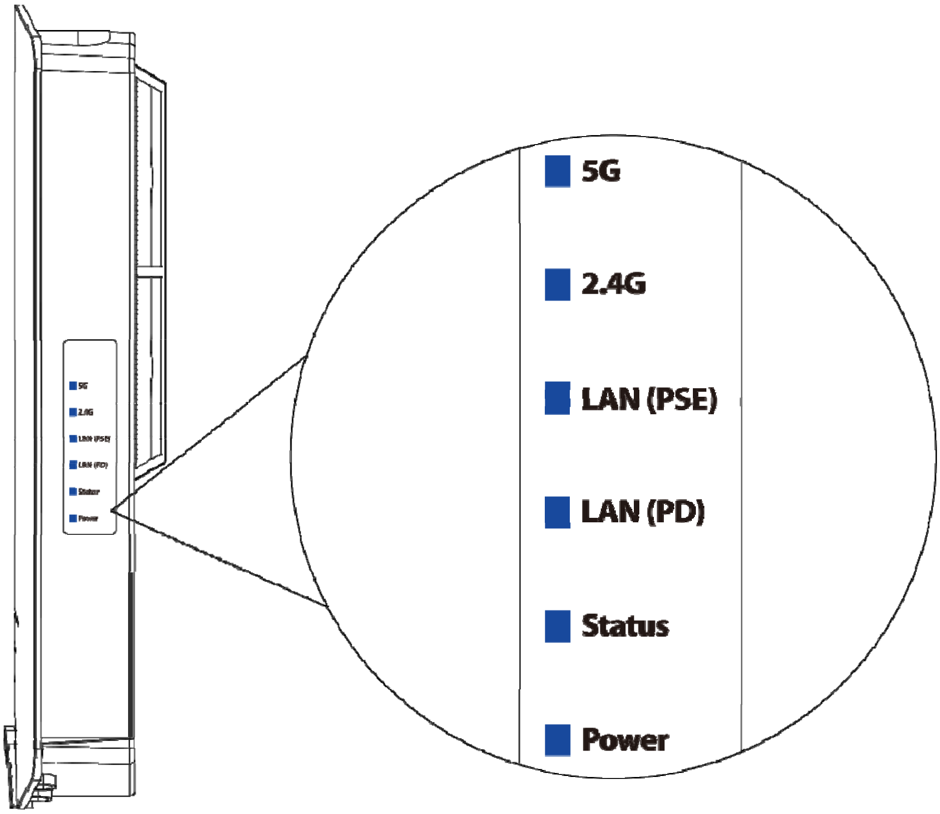
I-3 Hardware Overview

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



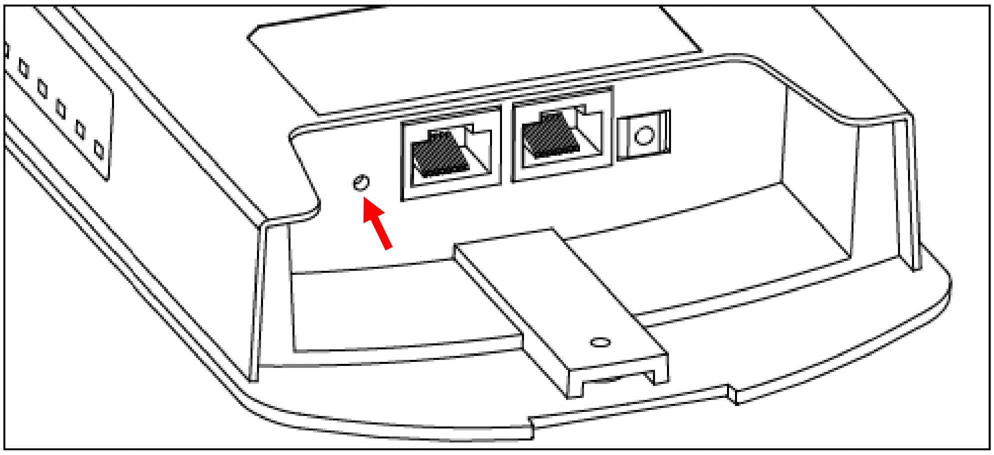
LED	LED Status	Description
5G (WLAN)	On	Wireless enabled.
	Off	Wireless disabled.
2.4G (WLAN)	On	Wireless enabled.
	Off	Wireless disabled.
LAN (PSE)	On	LAN port connected.
	Flashing	Activity (transmitting and receiving).
	Off	LAN port not connected.
LAN (PD)	On	LAN port connected.
	Flashing	Activity (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.

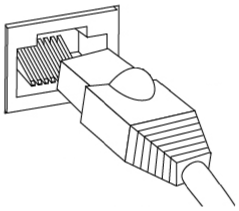
II-1 Default Mode: Access Point Mode

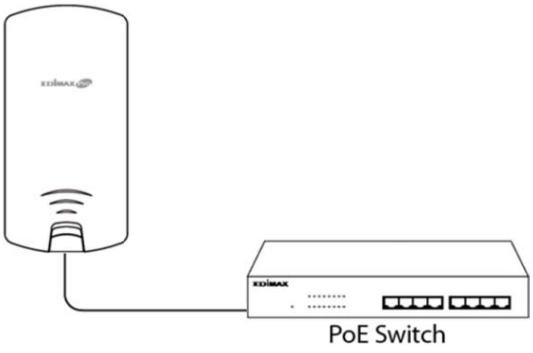
1. Set your computer's IP address to **192.168.2.x** where **x** is a number in the range **3 – 100**. If you are unsure how to do this, please refer to ***V-1 Configuring your IP address*** for more information.

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.

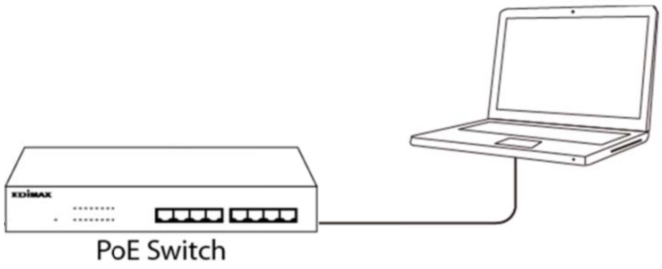
LAN 1 (PoE-In) Port



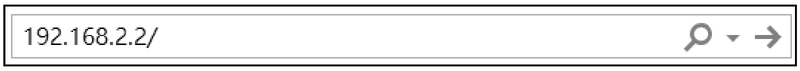


3. Please wait a moment for the device to start up. The device is ready when the Power LED is turned on.

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

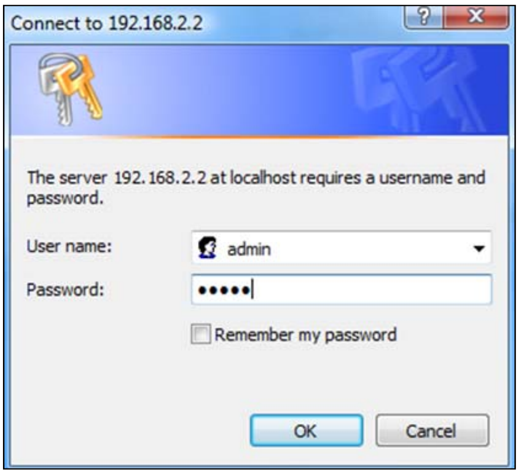


5. Enter the device's default IP address 192.168.2.2 into the URL bar of a web browser.



192.168.2.2/

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



Connect to 192.168.2.2

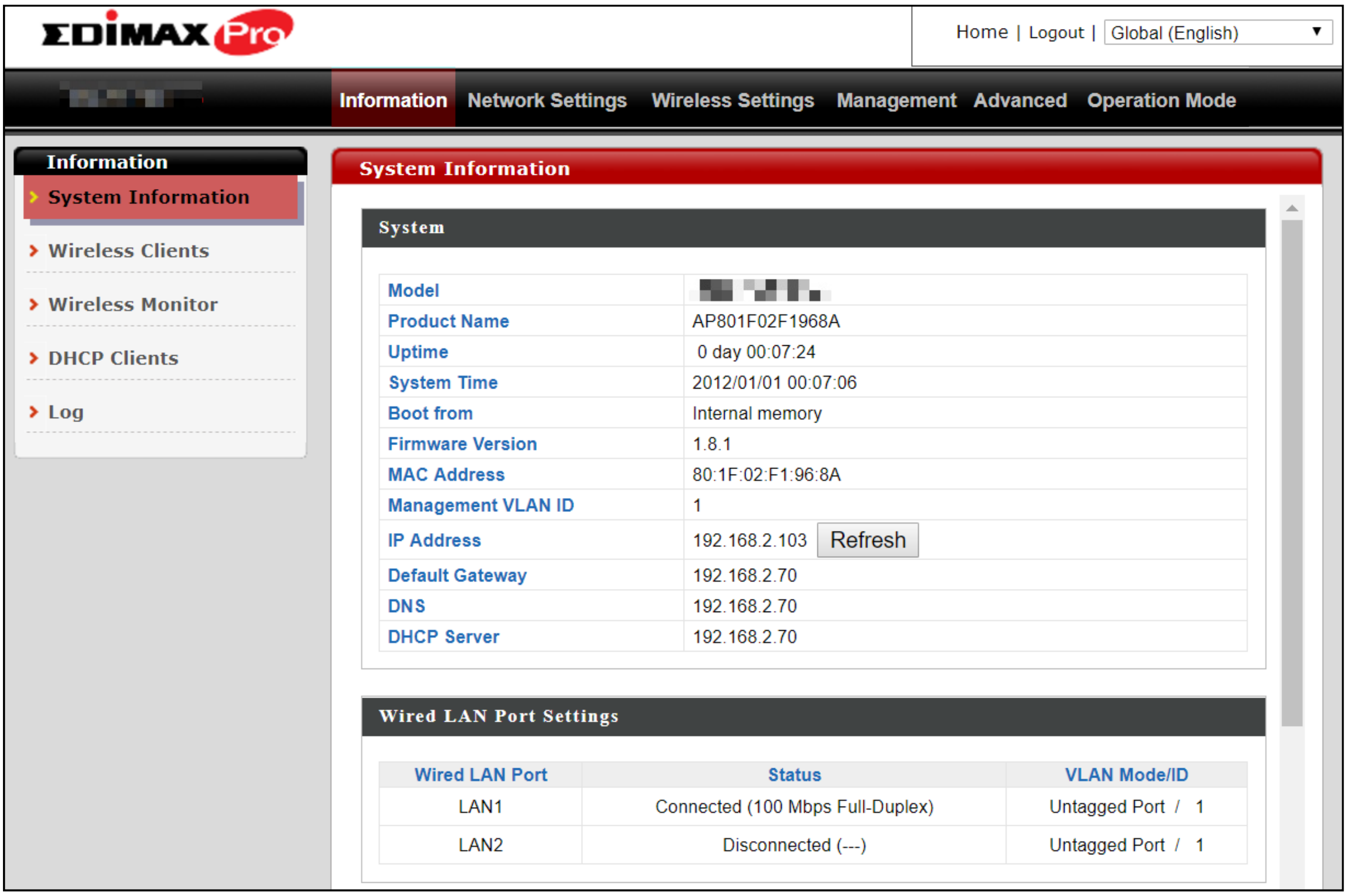
The server 192.168.2.2 at localhost requires a username and password.

User name: admin

Password: •••••

□ Remember my password

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



System Information

System

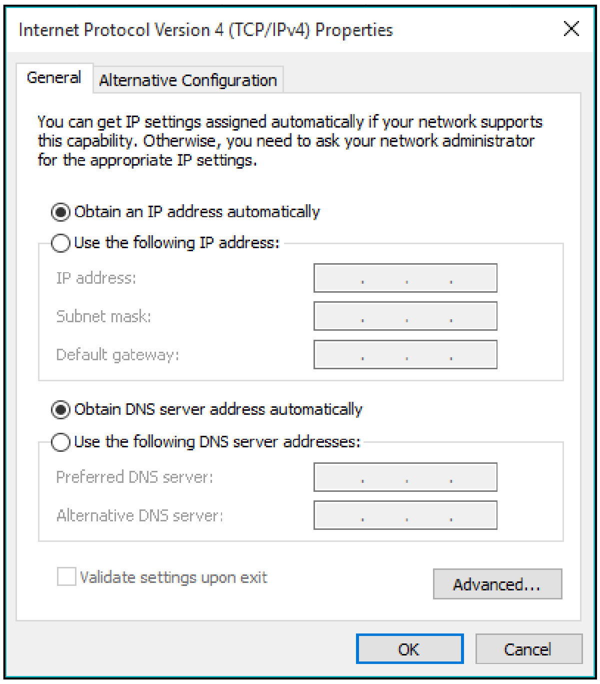
Model	[redacted]
Product Name	AP801F02F1968A
Uptime	0 day 00:07:24
System Time	2012/01/01 00:07:06
Boot from	Internal memory
Firmware Version	1.8.1
MAC Address	80:1F:02:F1:96:8A
Management VLAN ID	1
IP Address	192.168.2.103 Refresh
Default Gateway	192.168.2.70
DNS	192.168.2.70
DHCP Server	192.168.2.70

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

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternative Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

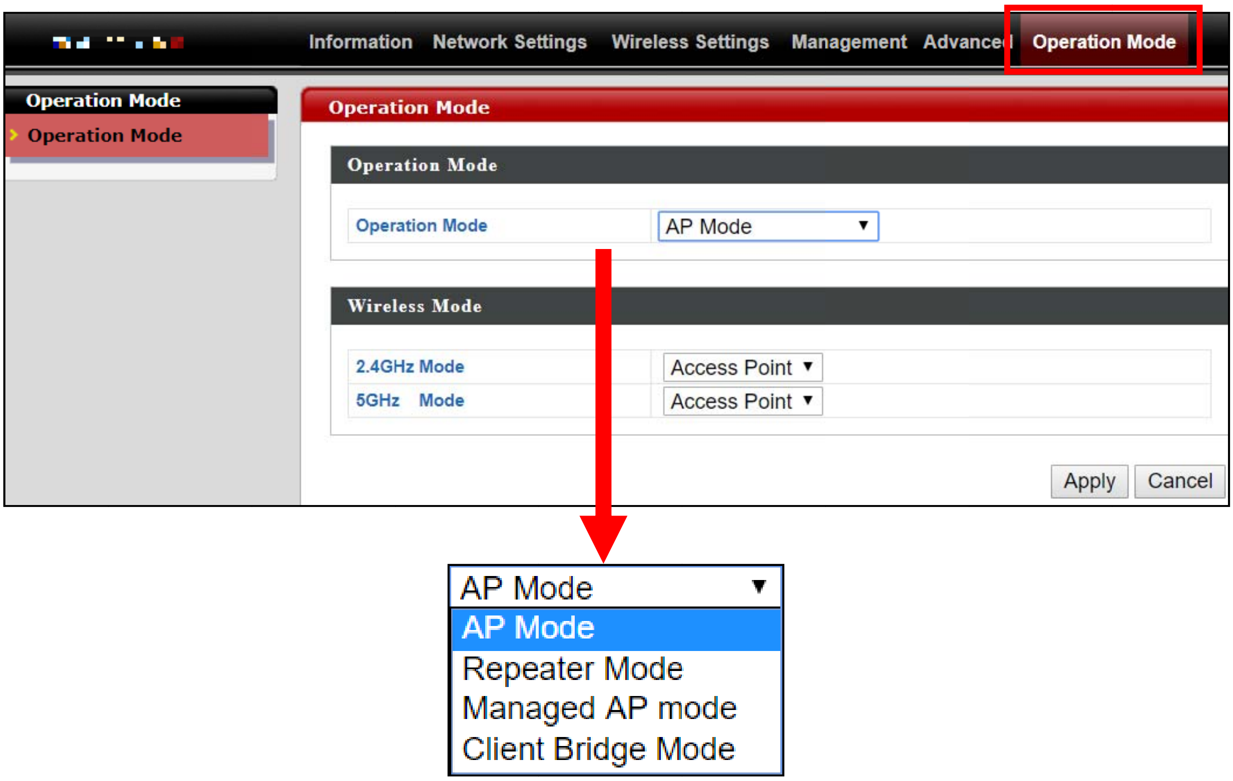
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

□ Validate settings upon exit

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.



Operation Mode

Operation Mode

Operation Mode: AP Mode

Wireless Mode

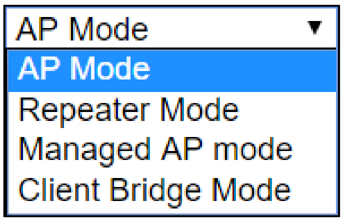
2.4GHz Mode: Access Point

5GHz Mode: Access Point

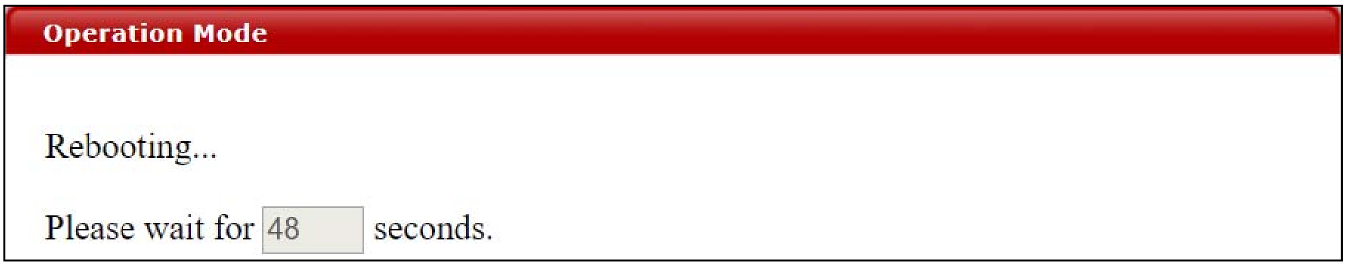
II-2 Repeater Mode

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:

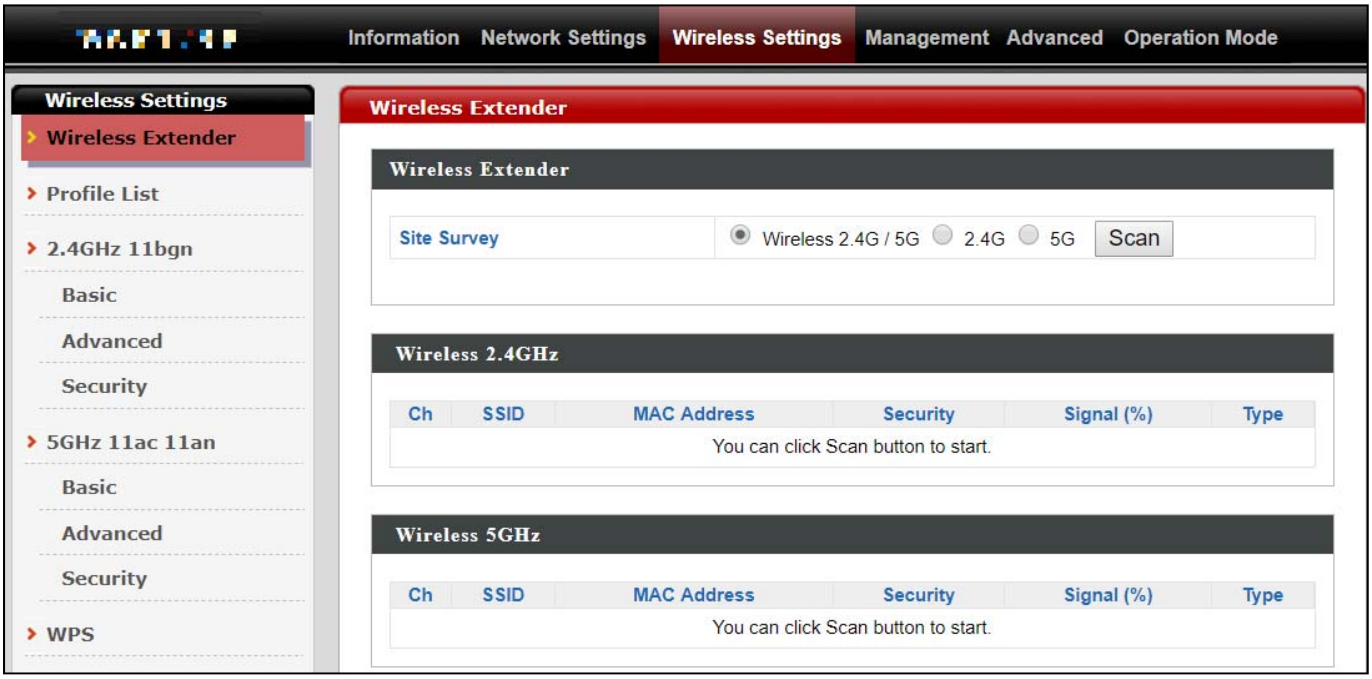


Operation Mode

Rebooting...

Please wait for 48 seconds.

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



Wireless Extender

Site Survey ● Wireless 2.4G / 5G ○ 2.4G ○ 5G Scan

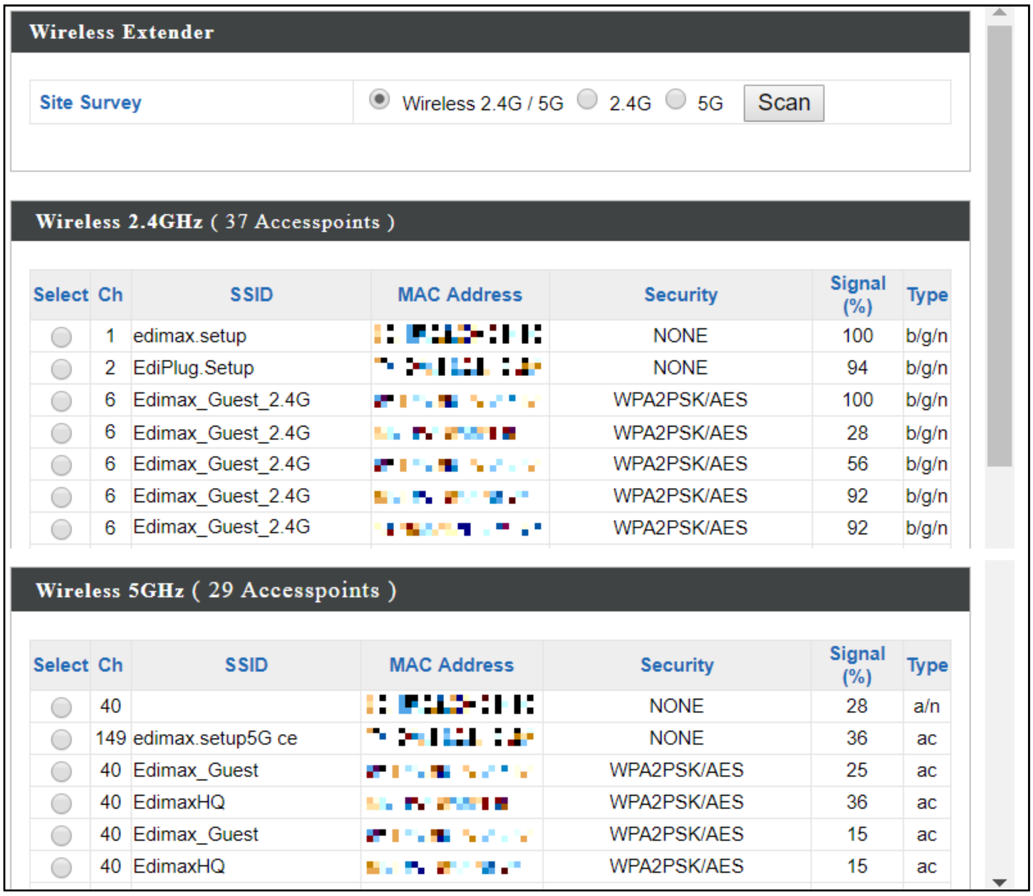
Wireless 2.4GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type
You can click Scan button to start.					

Wireless 5GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type
You can click Scan button to start.					

4. Click Scan to search for and display available SSIDs



Wireless Extender

Site Survey	● Wireless 2.4G / 5G ○ 2.4G ○ 5G Scan

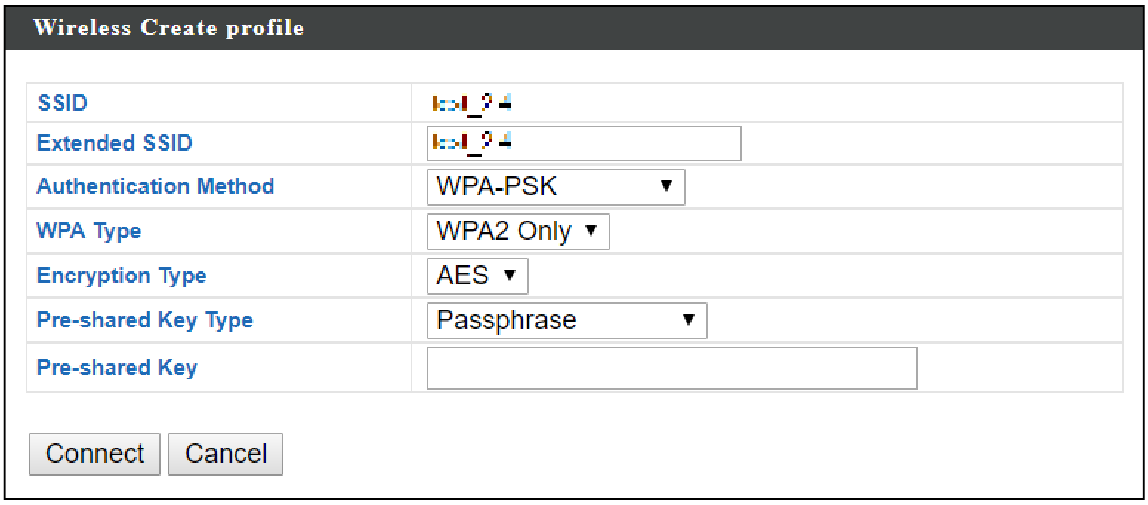
Wireless 2.4GHz (37 Accesspoints)

Select	Ch	SSID	MAC Address	Security	Signal (%)	Type
○	1	edimax.setup	[redacted]	NONE	100	b/g/n
○	2	EdiPlug.Setup	[redacted]	NONE	94	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	100	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	28	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	56	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	92	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	92	b/g/n

Wireless 5GHz (29 Accesspoints)

Select	Ch	SSID	MAC Address	Security	Signal (%)	Type
○	40		[redacted]	NONE	28	a/n
○	149	edimax.setup5G ce	[redacted]	NONE	36	ac
○	40	Edimax_Guest	[redacted]	WPA2PSK/AES	25	ac
○	40	EdimaxHQ	[redacted]	WPA2PSK/AES	36	ac
○	40	Edimax_Guest	[redacted]	WPA2PSK/AES	15	ac
○	40	EdimaxHQ	[redacted]	WPA2PSK/AES	15	ac

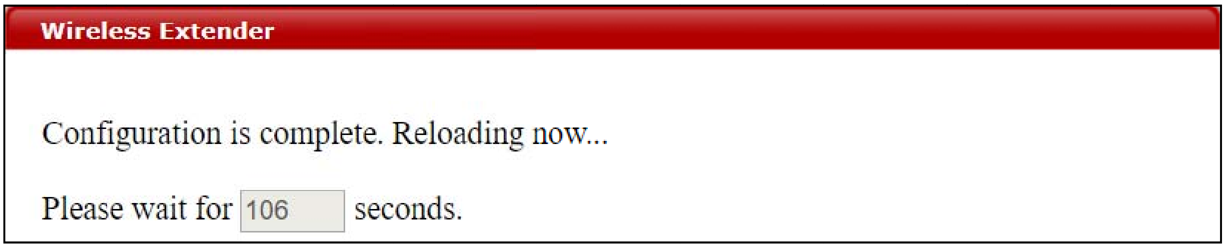
5. Click the circle icon to connect to an available source SSID. SSIDs can be configured independently for each frequency 2.4GHz & 5GHz.



Wireless Create profile

SSID	[redacted]
Extended SSID	[redacted]
Authentication Method	WPA-PSK ▼
WPA Type	WPA2 Only ▼
Encryption Type	AES ▼
Pre-shared Key Type	Passphrase ▼
Pre-shared Key	

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:

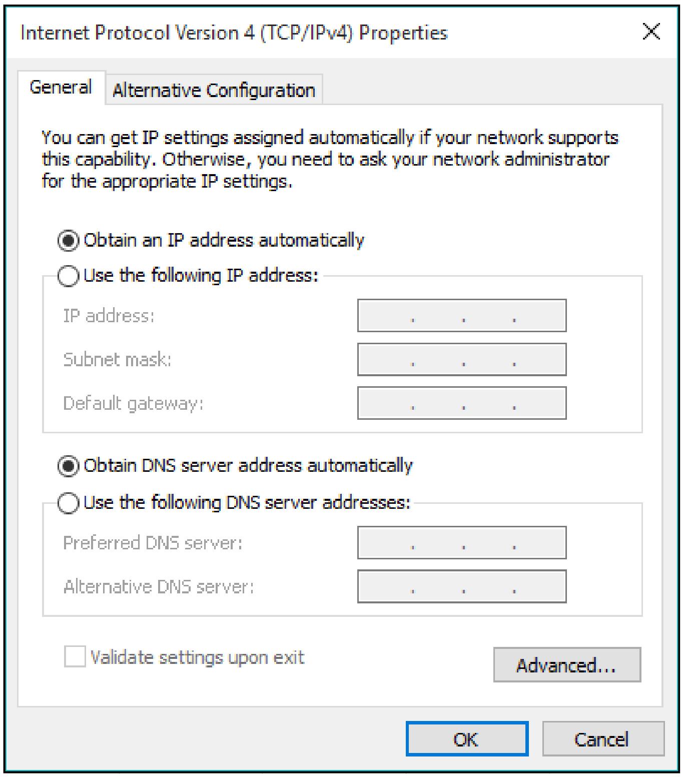


Wireless Extender

Configuration is complete. Reloading now...

Please wait for 106 seconds.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server: . . .
Alternative DNS server: . . .

□ Validate settings upon exit

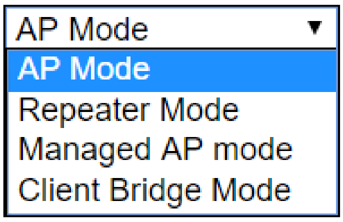
8. To access the web user interface, check your router/root AP's settings to determine the device's new IP address. Enter the new IP address into the browser for the web user interface.

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

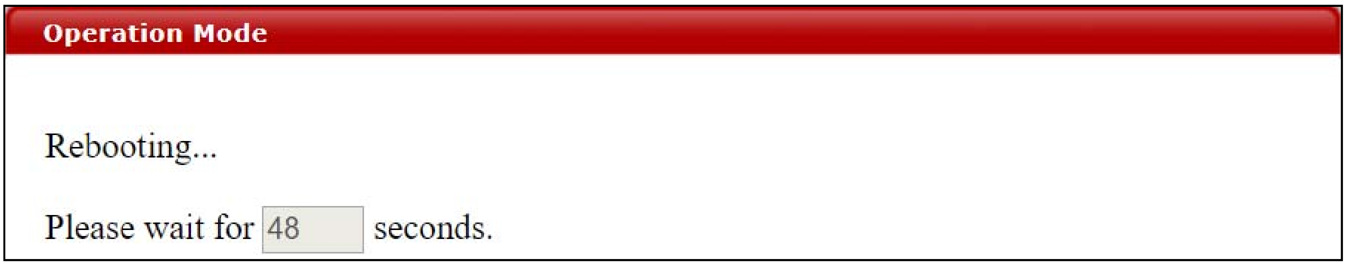
II-3 Client Bridge Mode

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:

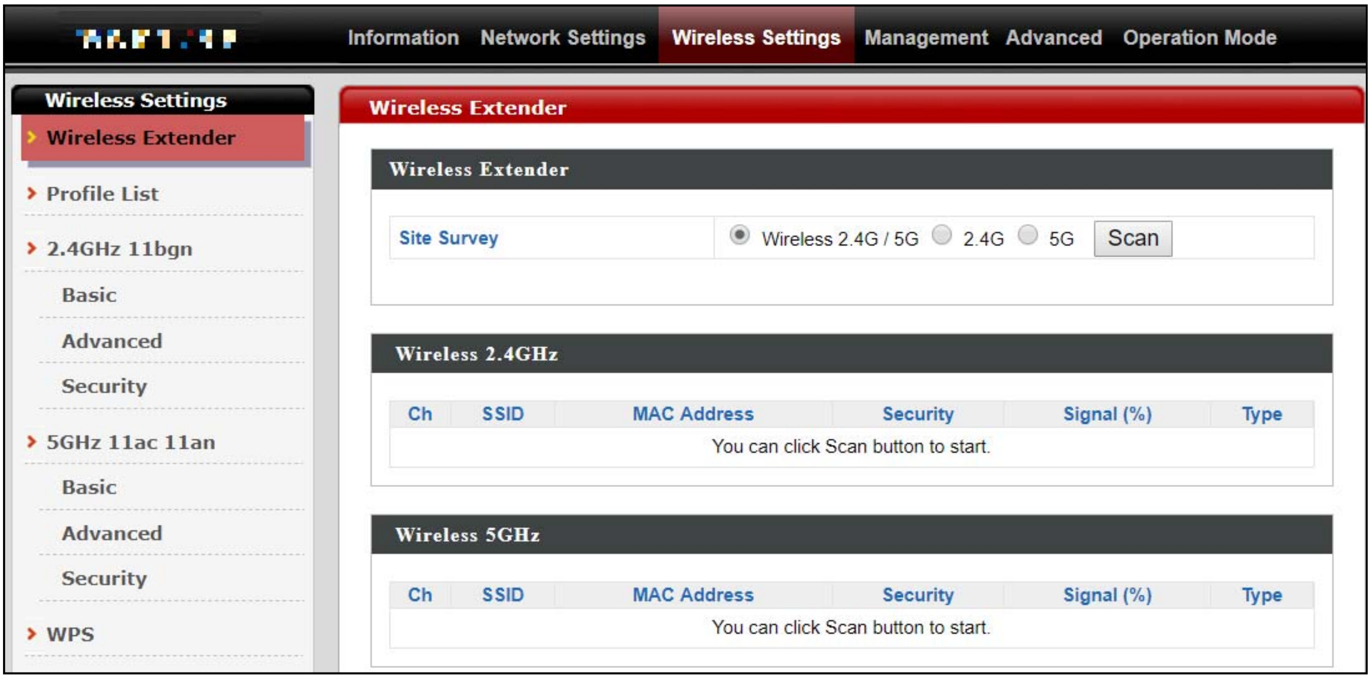


Operation Mode

Rebooting...

Please wait for 48 seconds.

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



Wireless Extender

Wireless Extender

Site Survey ● Wireless 2.4G / 5G ○ 2.4G ○ 5G

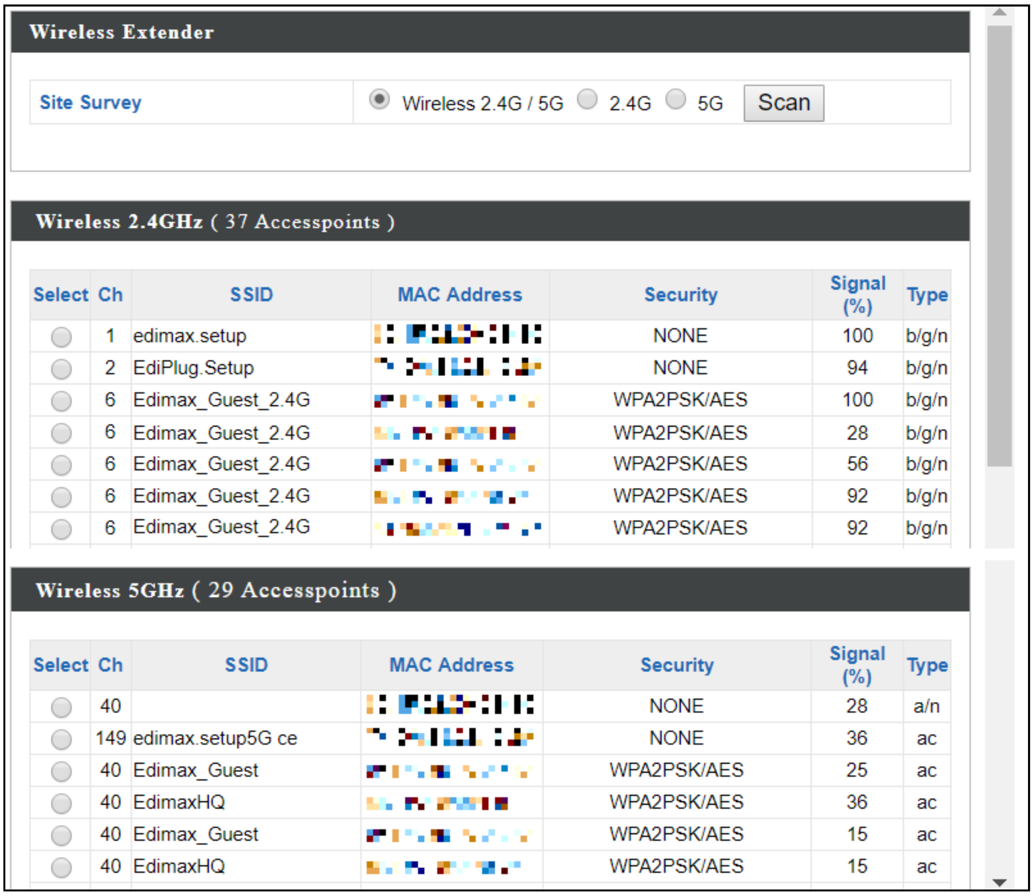
Wireless 2.4GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type
You can click Scan button to start.					

Wireless 5GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type
You can click Scan button to start.					

4. Click Scan to search for and display available SSIDs



Wireless Extender

Site Survey	● Wireless 2.4G / 5G ○ 2.4G ○ 5G Scan

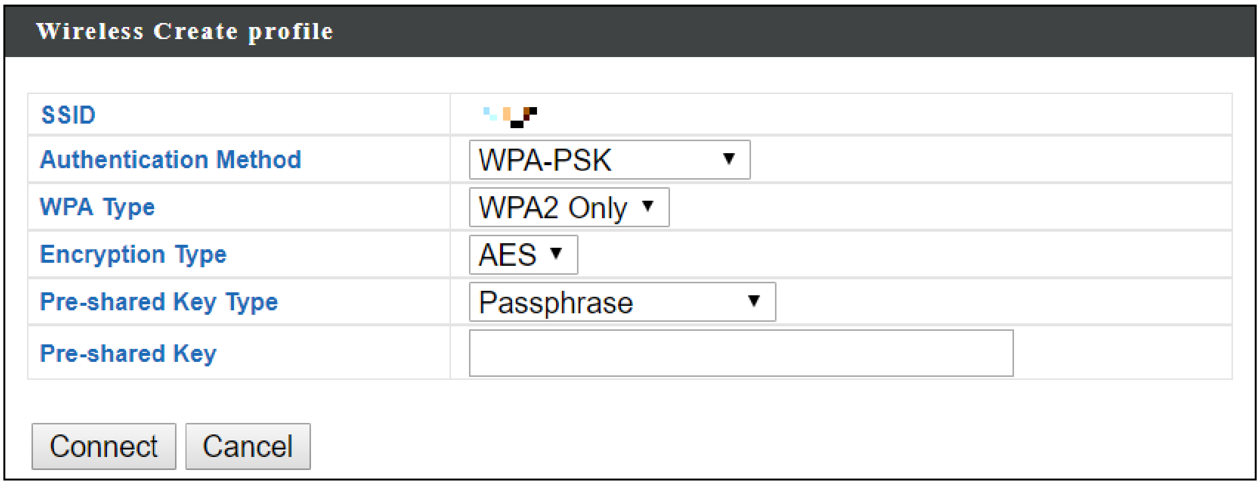
Wireless 2.4GHz (37 Accesspoints)

Select	Ch	SSID	MAC Address	Security	Signal (%)	Type
○	1	edimax.setup	[redacted]	NONE	100	b/g/n
○	2	EdiPlug.Setup	[redacted]	NONE	94	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	100	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	28	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	56	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	92	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	92	b/g/n

Wireless 5GHz (29 Accesspoints)

Select	Ch	SSID	MAC Address	Security	Signal (%)	Type
○	40		[redacted]	NONE	28	a/n
○	149	edimax.setup5G ce	[redacted]	NONE	36	ac
○	40	Edimax_Guest	[redacted]	WPA2PSK/AES	25	ac
○	40	EdimaxHQ	[redacted]	WPA2PSK/AES	36	ac
○	40	Edimax_Guest	[redacted]	WPA2PSK/AES	15	ac
○	40	EdimaxHQ	[redacted]	WPA2PSK/AES	15	ac

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

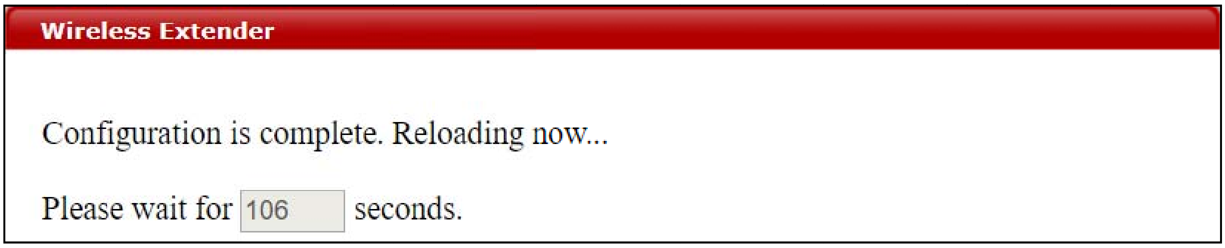


Wireless Create profile

SSID	[redacted]
Authentication Method	WPA-PSK ▼
WPA Type	WPA2 Only ▼
Encryption Type	AES ▼
Pre-shared Key Type	Passphrase ▼
Pre-shared Key	

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:

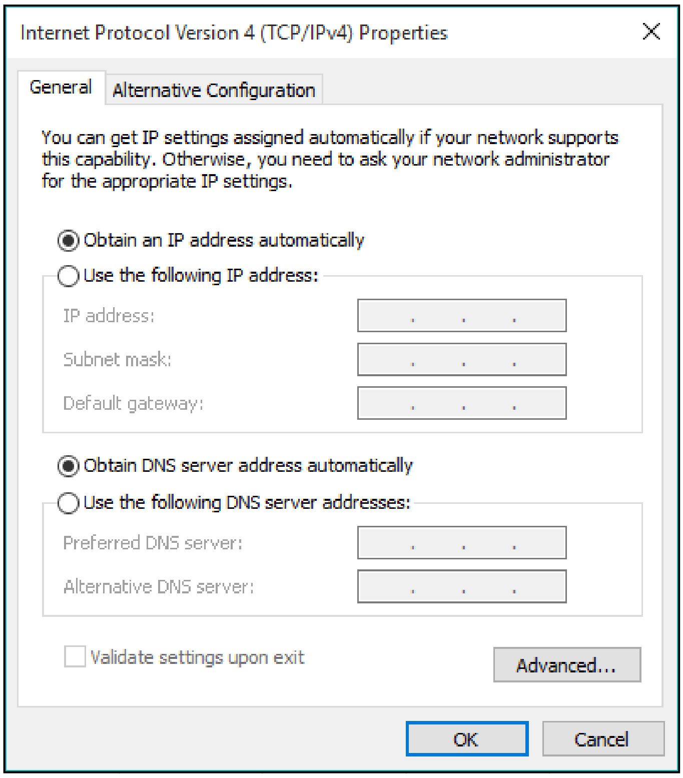


Wireless Extender

Configuration is complete. Reloading now...

Please wait for 106 seconds.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternative Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

□ Validate settings upon exit

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).

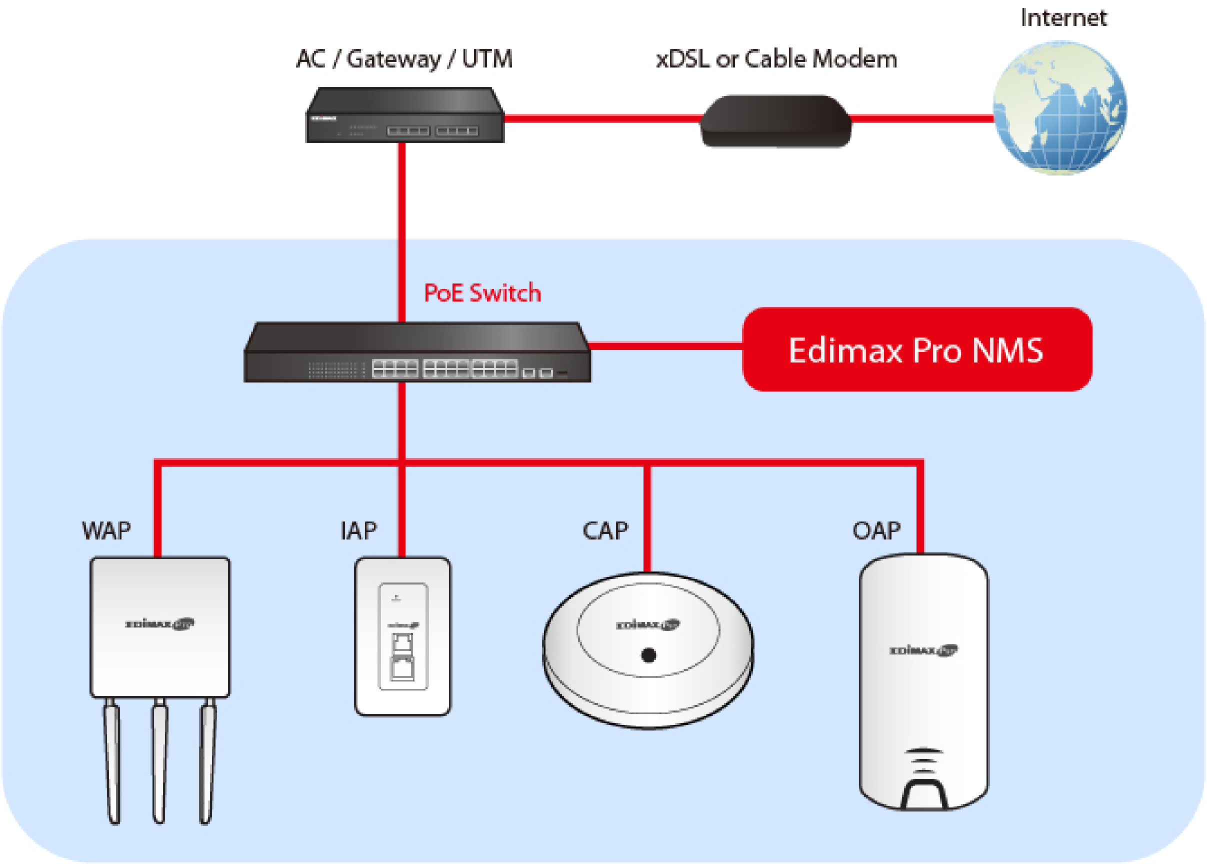
II-4 Managed AP Mode

<u>Scenario: The Unit being managed by an AP Controller</u>

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:

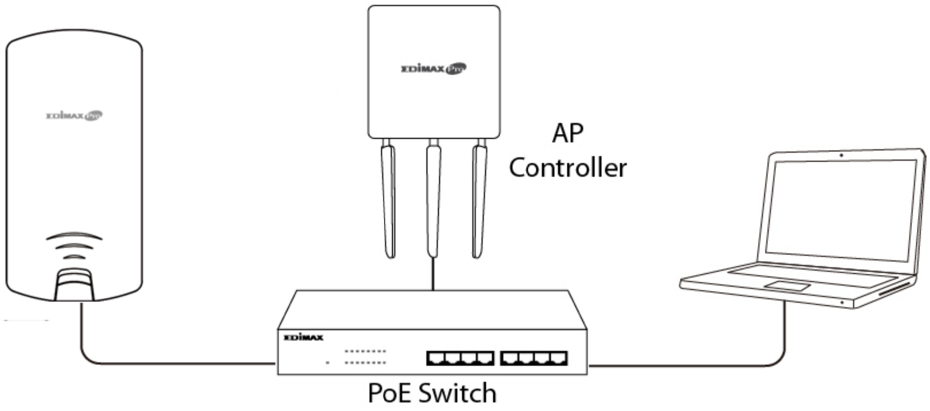


⚠ ***By default, the access point will automatically switch mode if an AP Controller is present in the network.***

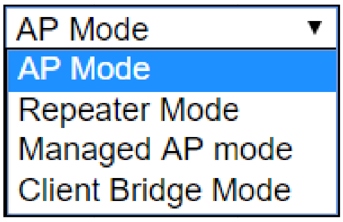
To manually change to “Managed AP Mode”:

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

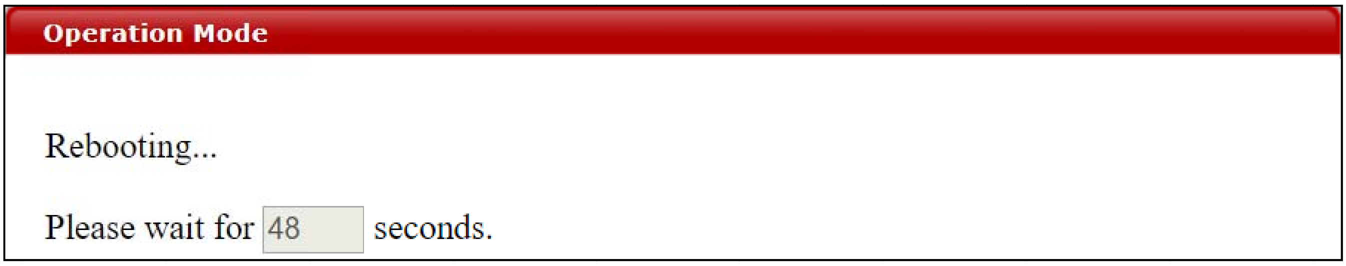
1. Connect an AP Controller to the switch currently connected to the access point and computer.



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:



Operation Mode

Rebooting...

Please wait for 48 seconds.

Wait for a few minutes for the settings to sync.

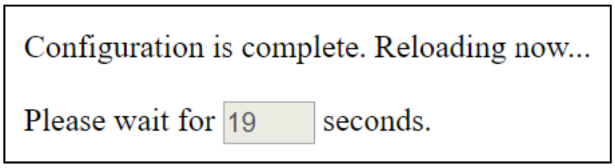
II-5 Basic Settings

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:



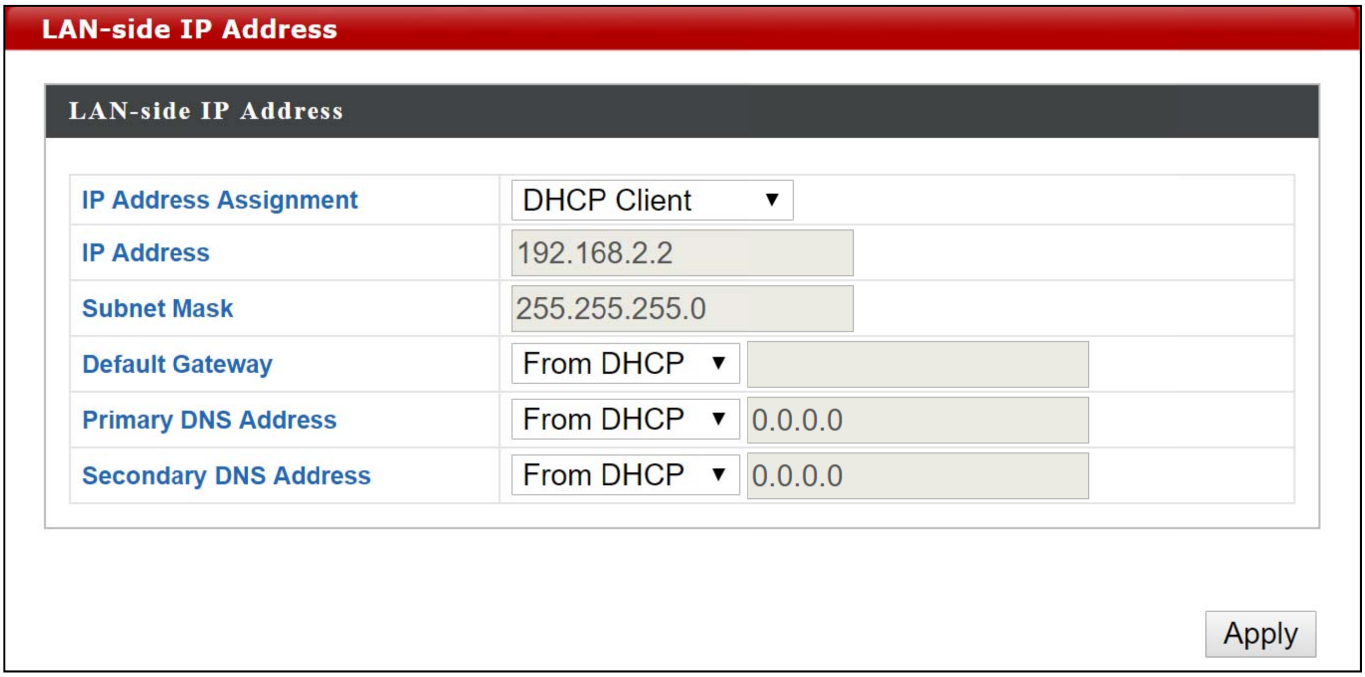
Configuration is complete. Reloading now...

Please wait for 19 seconds.

Instructions below will help you configure these settings:

Changing IP Address:

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



LAN-side IP Address

LAN-side IP Address

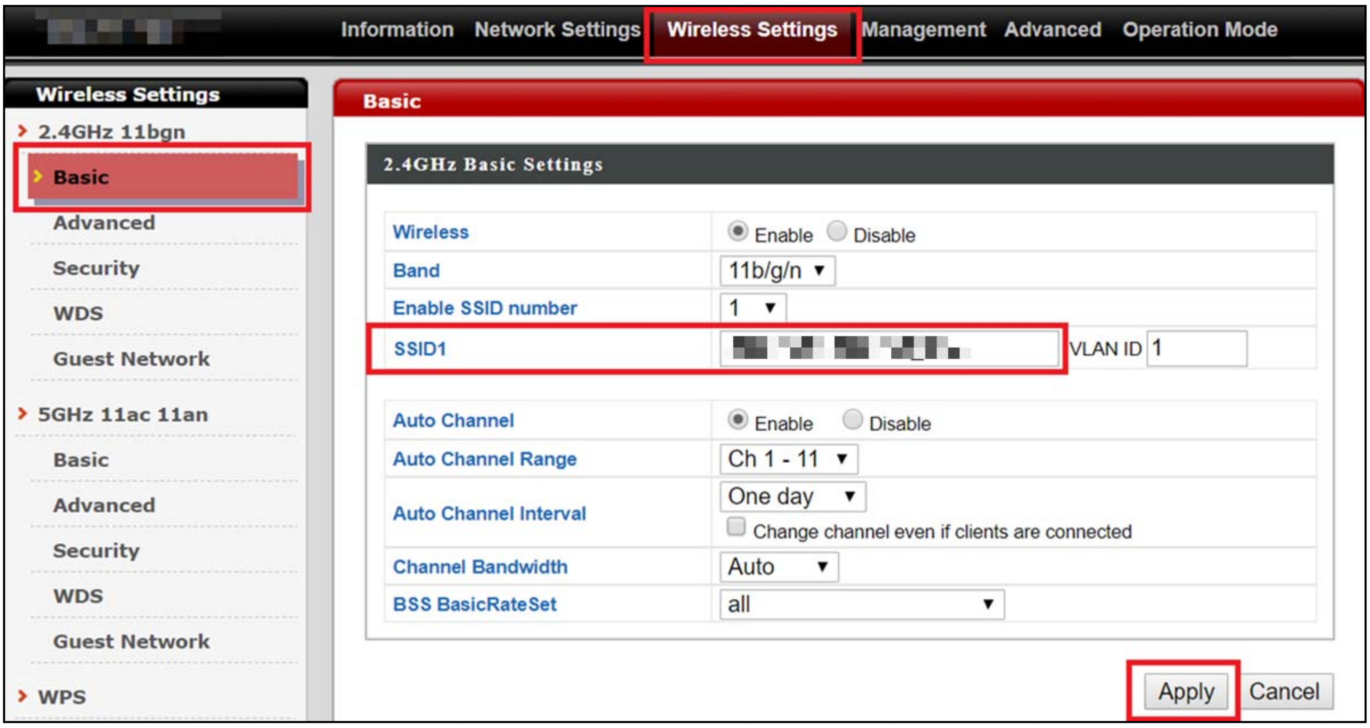
IP Address Assignment	DHCP Client ▼
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	From DHCP ▼
Primary DNS Address	From DHCP ▼ 0.0.0.0
Secondary DNS Address	From DHCP ▼ 0.0.0.0

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.*

<u>Changing SSID for 2.4GHz wireless network</u>

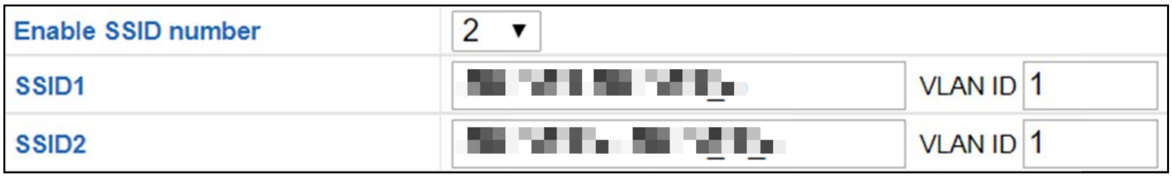
1. Go to **“Wireless Settings” > “2.4GHz 11bgn” > “Basic”**.
2. Enter the new SSID for your 2.4GHz wireless network in the “SSID1” field and click “Apply”.



2.4GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n ▾
Enable SSID number	1 ▾
SSID1	[redacted] VLAN ID 1
Auto Channel	● Enable ○ Disable
Auto Channel Range	Ch 1 - 11 ▾
Auto Channel Interval	One day ▾ □ Change channel even if clients are connected
Channel Bandwidth	Auto ▾
BSS BasicRateSet	all ▾

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”.***

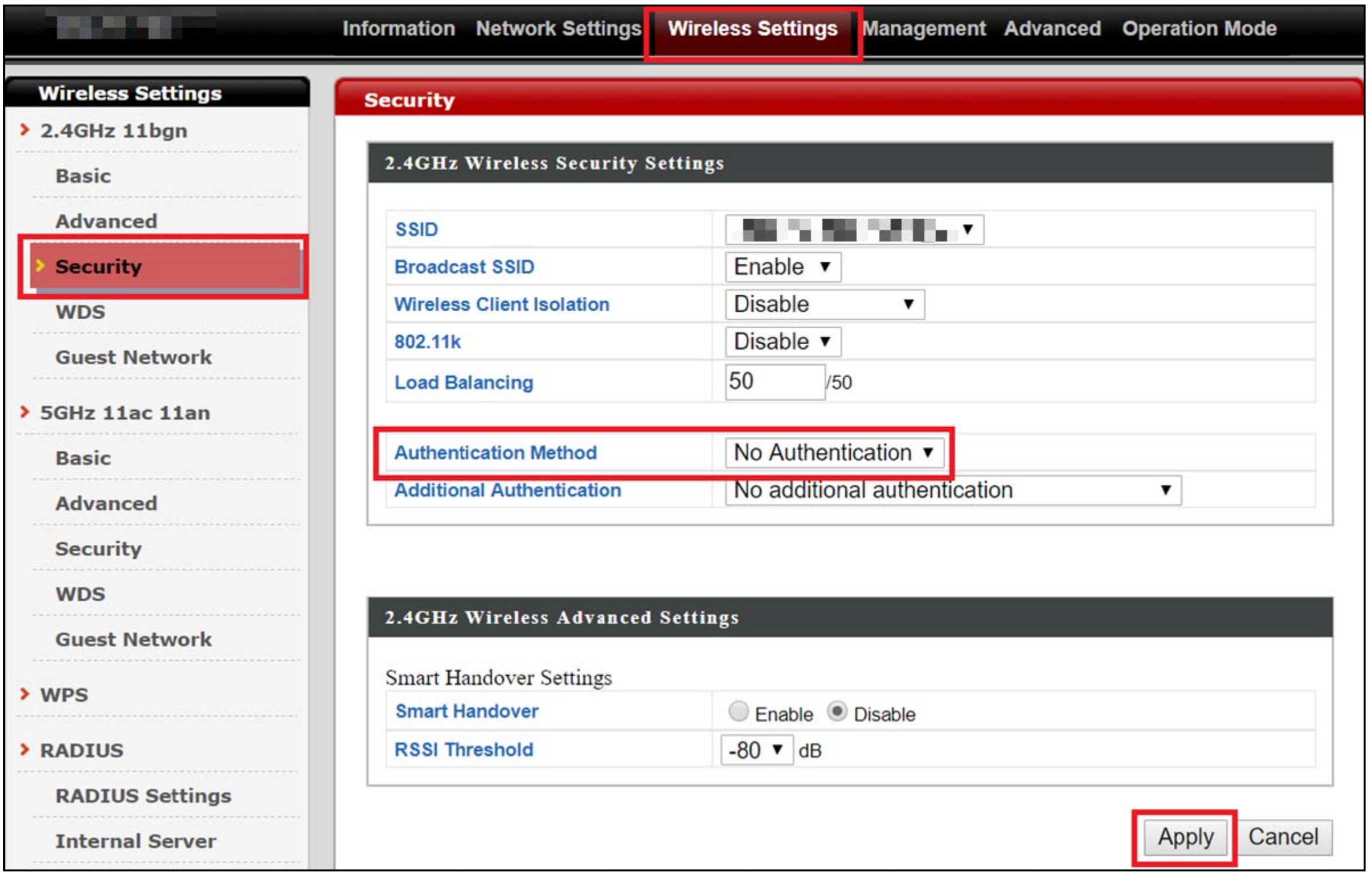


Enable SSID number	2 ▾	
SSID1	[redacted]	VLAN ID 1
SSID2	[redacted]	VLAN ID 1

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".



2.4GHz Wireless Security Settings

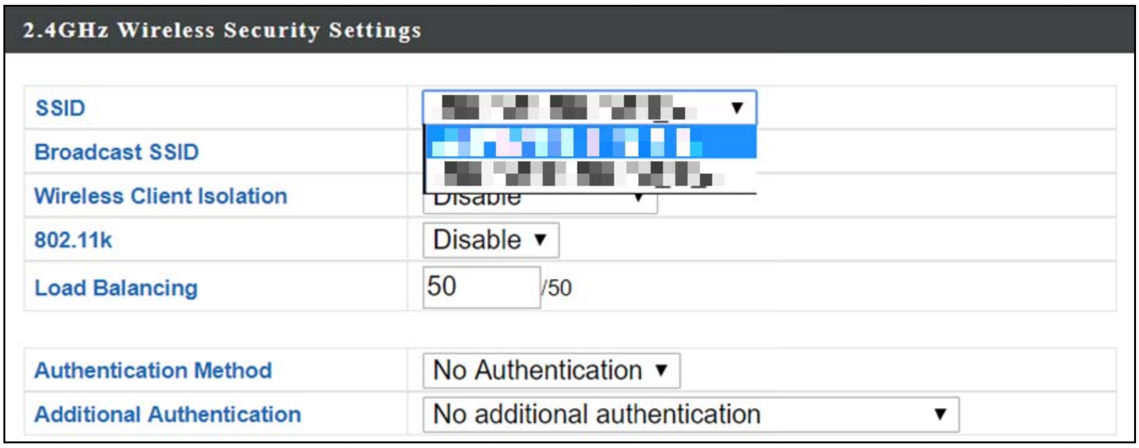
SSID	[redacted] ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
802.11k	Disable ▾
Load Balancing	50 /50
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

2.4GHz Wireless Advanced Settings

Smart Handover Settings

Smart Handover	○ Enable ● Disable
RSSI Threshold	-80 ▾ dB

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



2.4GHz Wireless Security Settings

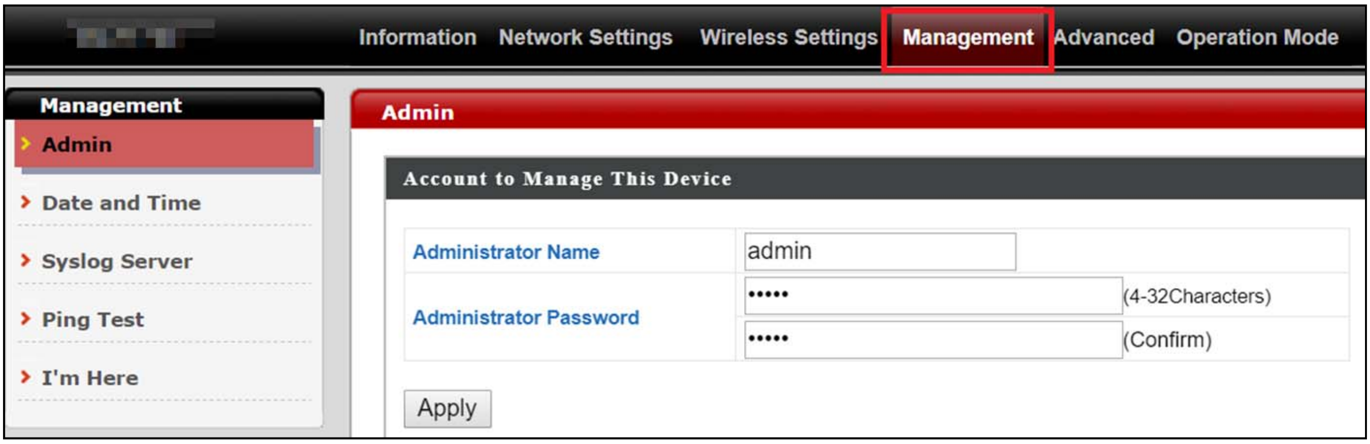
SSID	[redacted] ▾ [redacted] [redacted]
Broadcast SSID	
Wireless Client Isolation	Disable ▾
802.11k	Disable ▾
Load Balancing	50 /50
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

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:

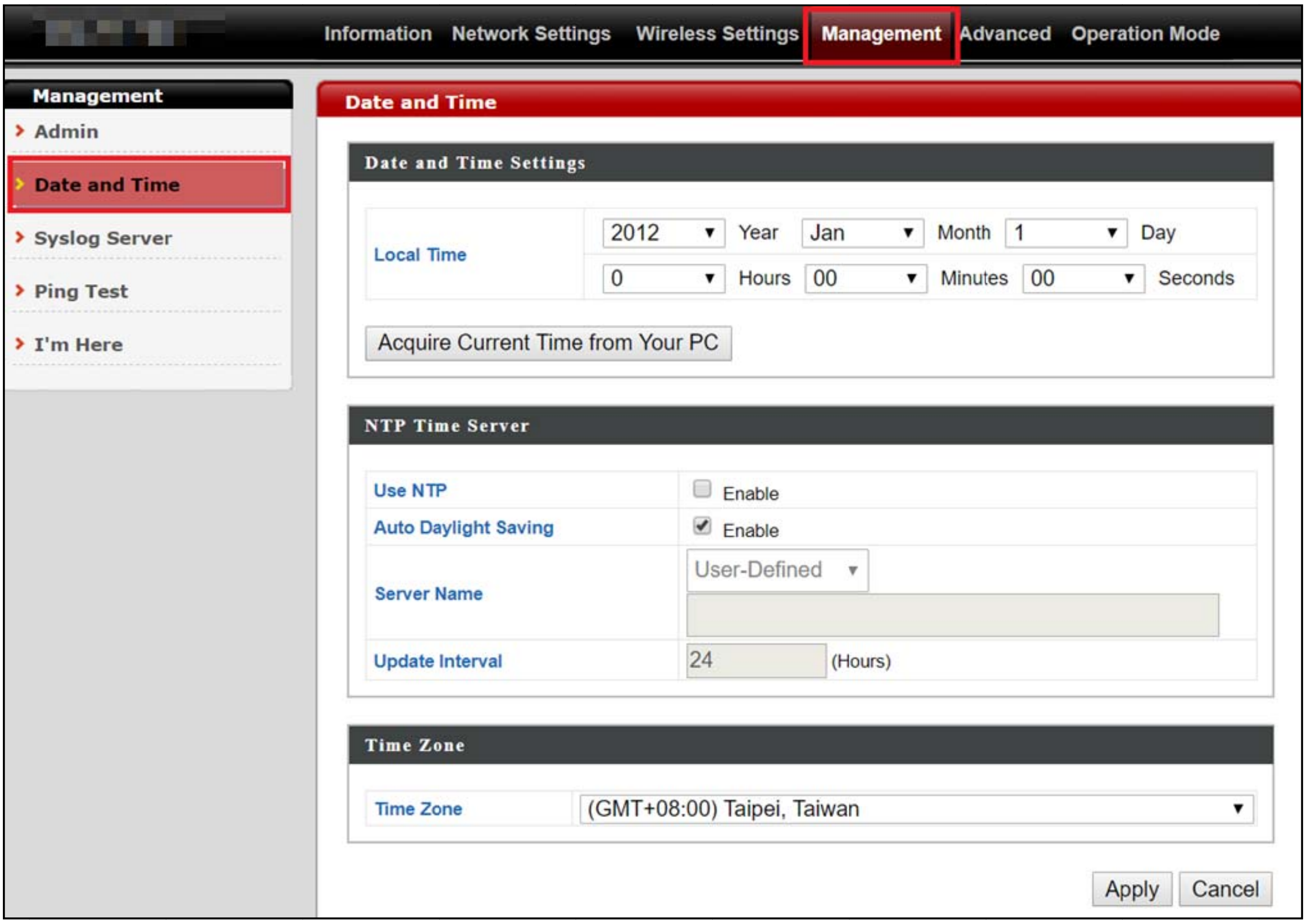


Administrator Name	admin
Administrator Password	••••• (4-32Characters) ••••• (Confirm)

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

Changing Date and Time

1. Go to **"Management" > "Date and Time"**.



Date and Time Settings

Local Time	2012 ▾ Year Jan ▾ Month 1 ▾ Day 0 ▾ Hours 00 ▾ Minutes 00 ▾ Seconds

Acquire Current Time from Your PC

NTP Time Server

Use NTP	□ Enable
Auto Daylight Saving	☑ Enable
Server Name	User-Defined ▾
Update Interval	24 (Hours)

Time Zone

Time Zone	(GMT+08:00) Taipei, Taiwan ▾

Apply Cancel

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.***

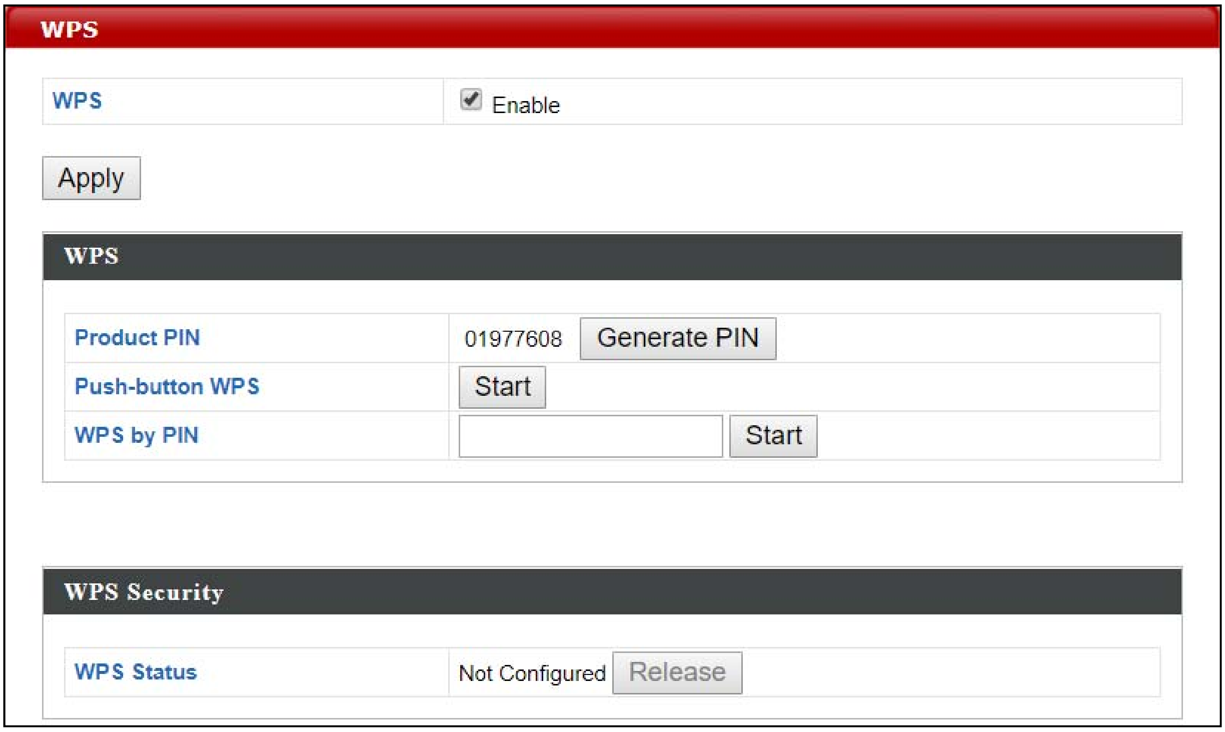
The basic settings of your access point are now configured. Please refer to **III Hardware Installation** for guidance on connecting your access point to a PoE switch.

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".



WPS

WPS	☑ Enable

WPS

Product PIN	01977608 Generate PIN
Push-button WPS	Start
WPS by PIN	Start

WPS Security

WPS Status	Not Configured Release

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.

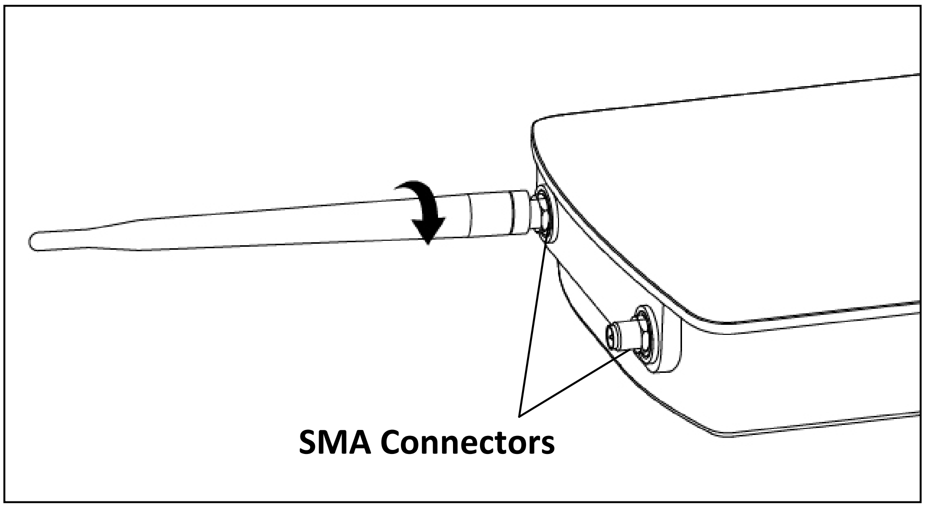
III Hardware Installation

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

III-1 Antenna

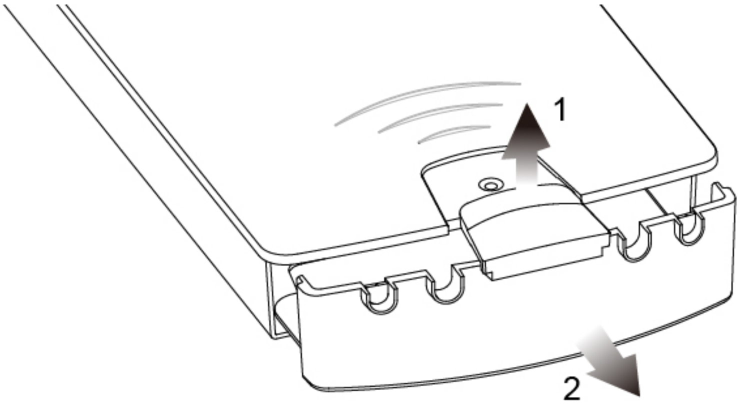
The antennae must be screwed onto the access point.

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

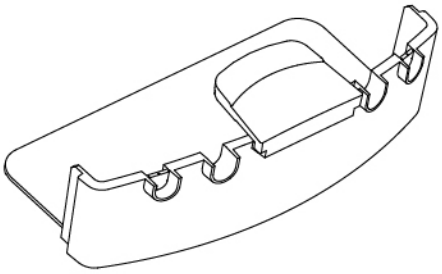


III-2 Powering on the Access Point Outdoor

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:

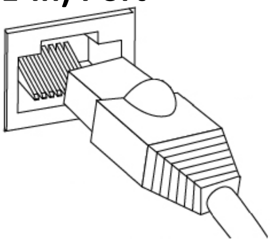


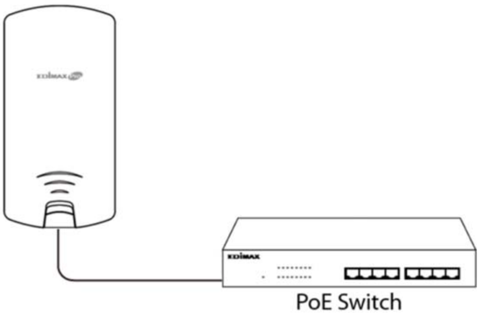
Removed Underside Cap



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.

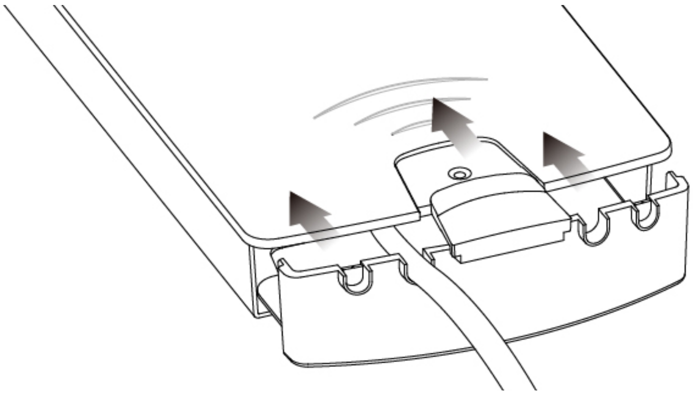
LAN 1 (PoE-In) Port



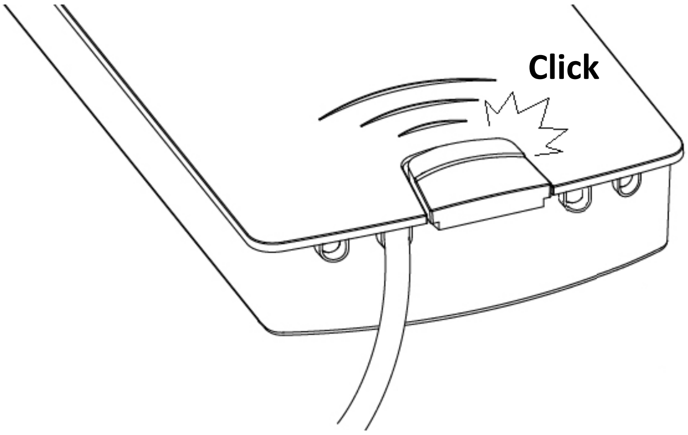


3. The access point will be powered by the PoE switch. Connect another Ethernet cable to **LAN 2** where necessary.

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.

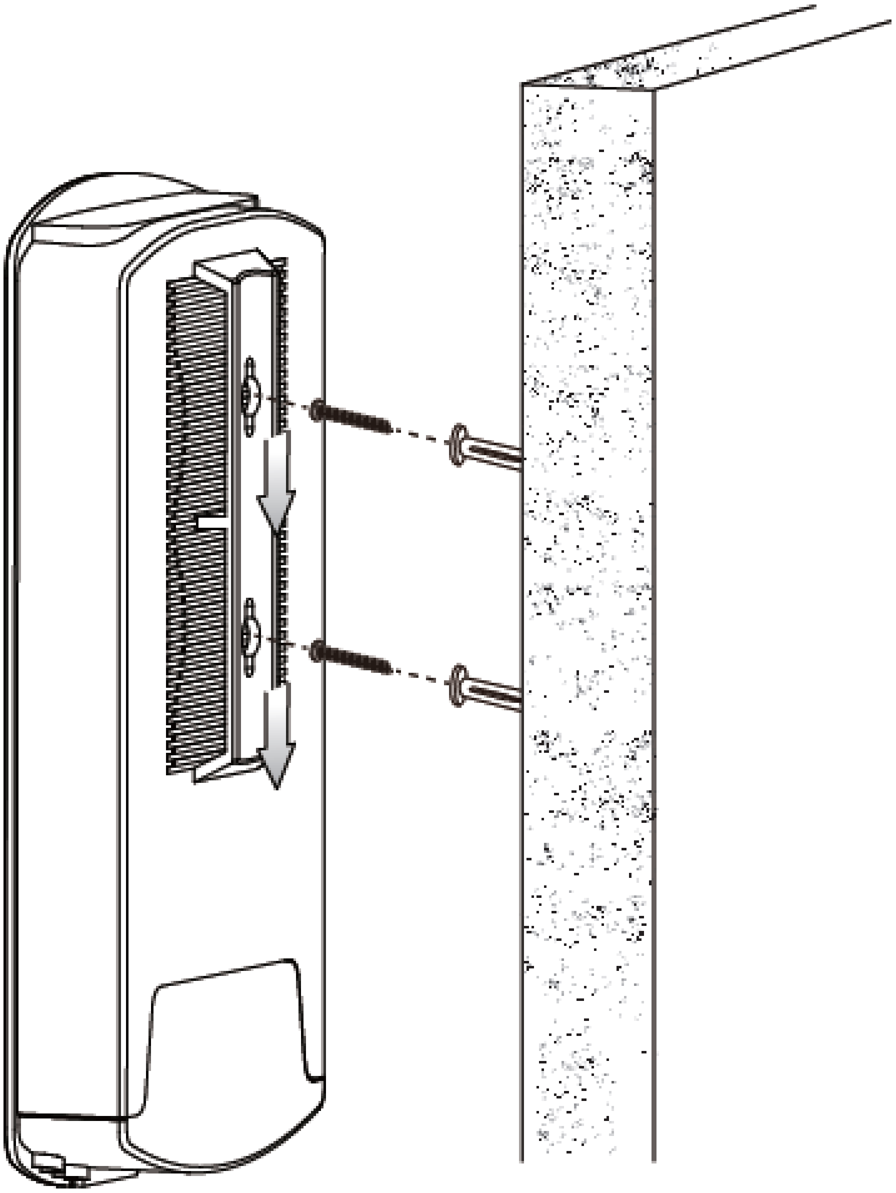


III-3 Mounting

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

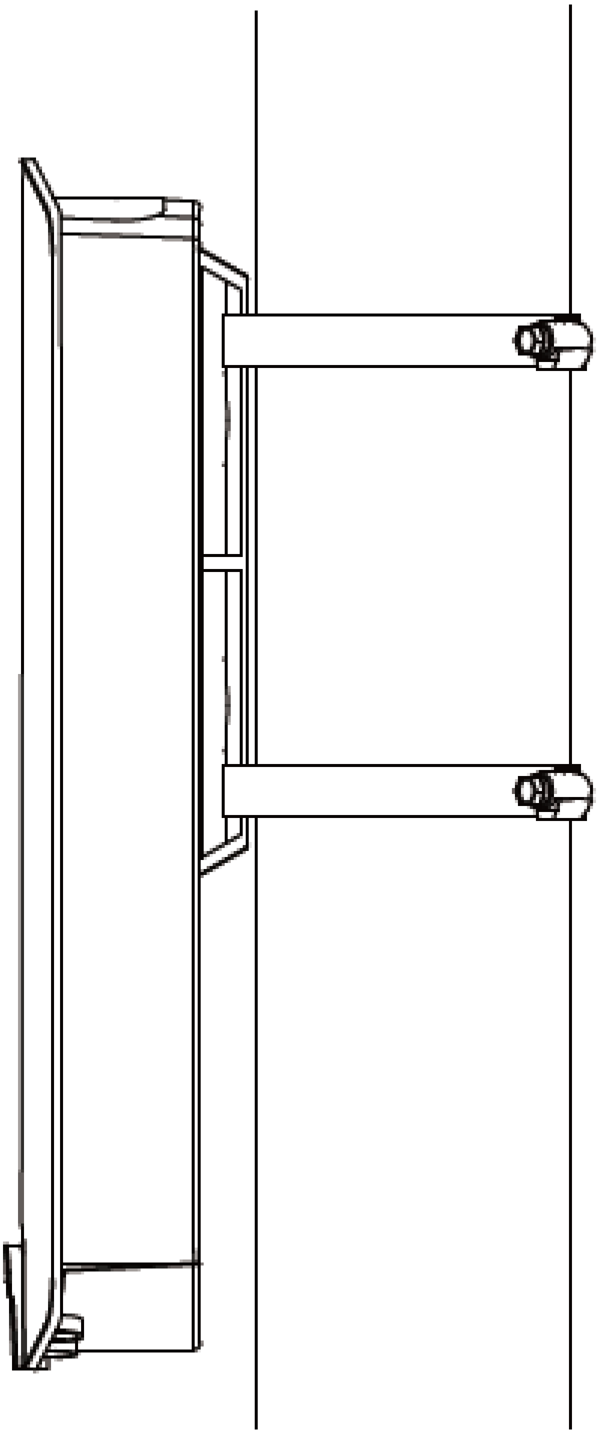
Wall Mount

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 GAP-429HOB 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:

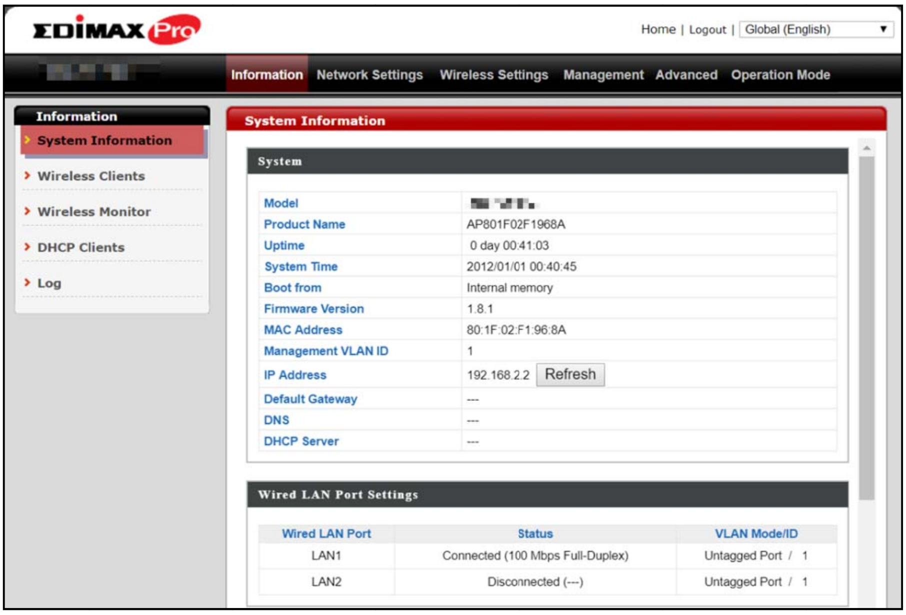
1. Connect a computer to your access point using an Ethernet cable.

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.



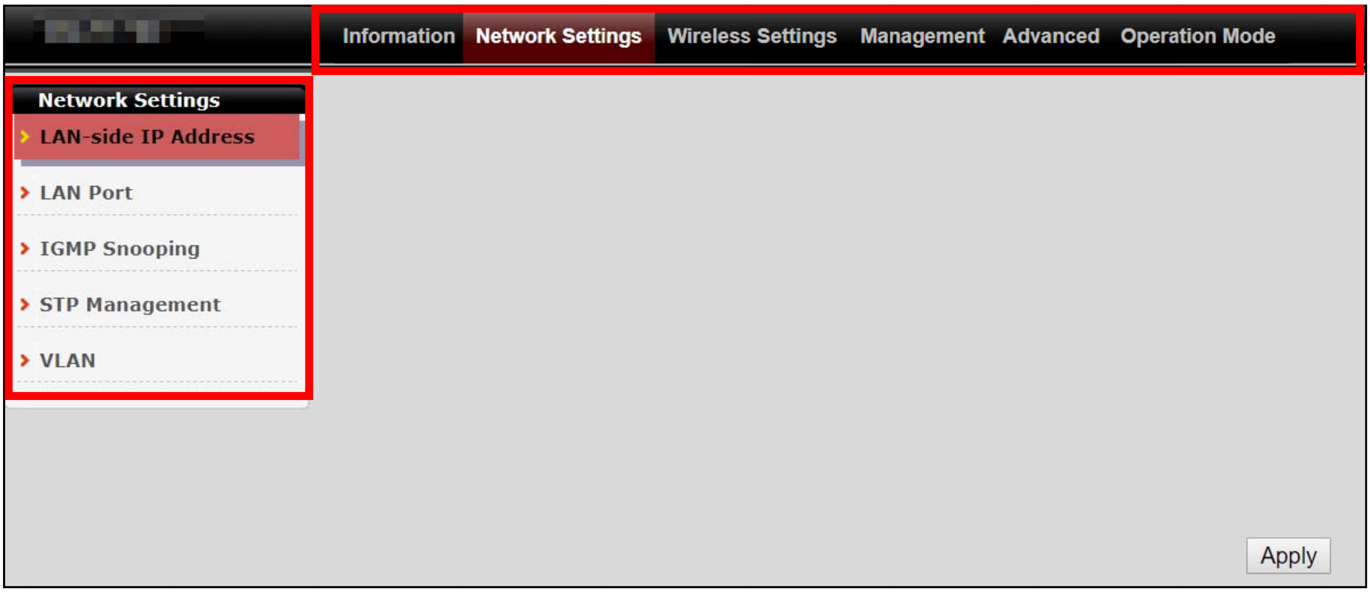
System

Model	[redacted]
Product Name	AP801F02F1968A
Uptime	0 day 00:41:03
System Time	2012/01/01 00:40:45
Boot from	Internal memory
Firmware Version	1.8.1
MAC Address	80:1F:02:F1:96:8A
Management VLAN ID	1
IP Address	192.168.2.2 Refresh
Default Gateway	---
DNS	---
DHCP Server	---

Wired LAN Port Settings

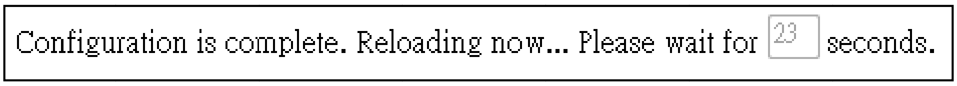
Wired LAN Port	Status	VLAN Mode/ID
LAN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1

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.



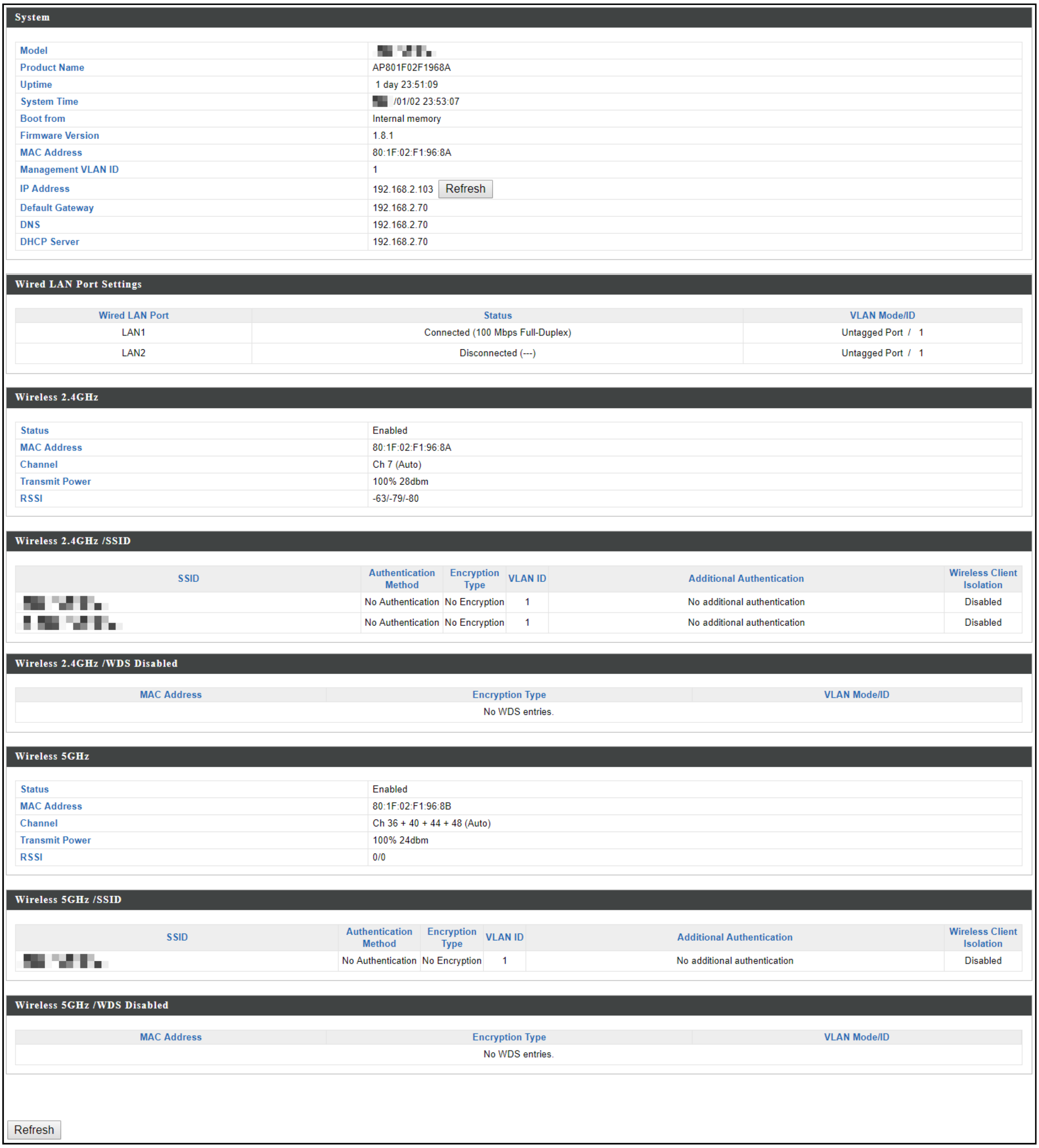
Configuration is complete. Reloading now... Please wait for 23 seconds.

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.

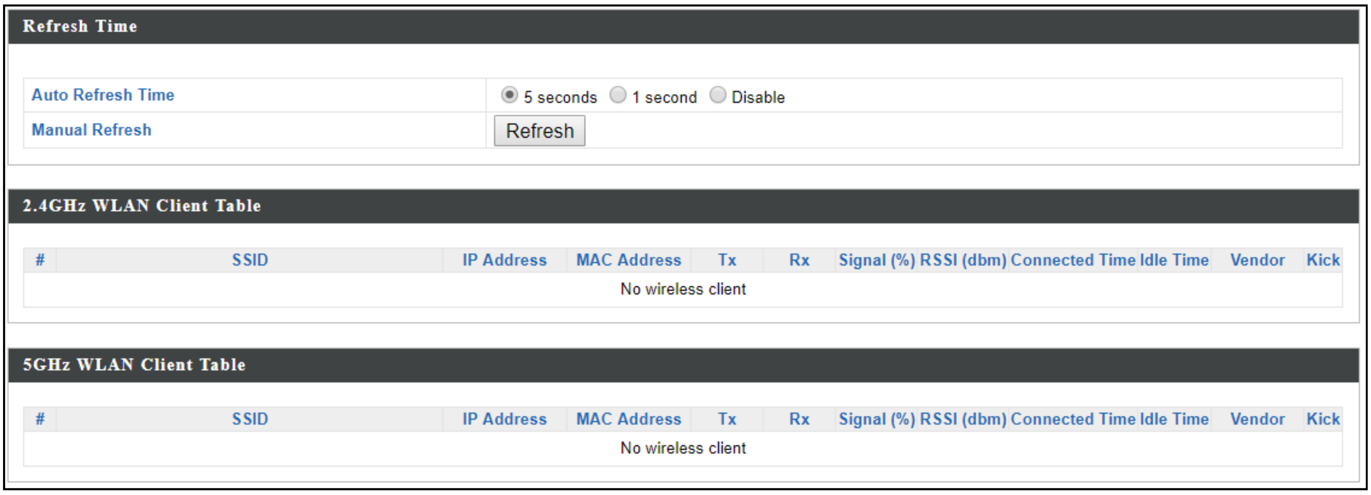
Wireless 2.4GHZ (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID. See **IV-3 Wireless Settings**.
Encryption Type	Displays the encryption type for the specified SSID. See **IV-3 Wireless Settings**.
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	● 5 seconds ○ 1 second ○ Disable
Manual Refresh	Refresh

2.4GHz WLAN Client Table

#	SSID	IP Address	MAC Address	Tx	Rx	Signal (%)	RSSI (dbm)	Connected Time	Idle Time	Vendor	Kick
No wireless client											

5GHz WLAN Client Table

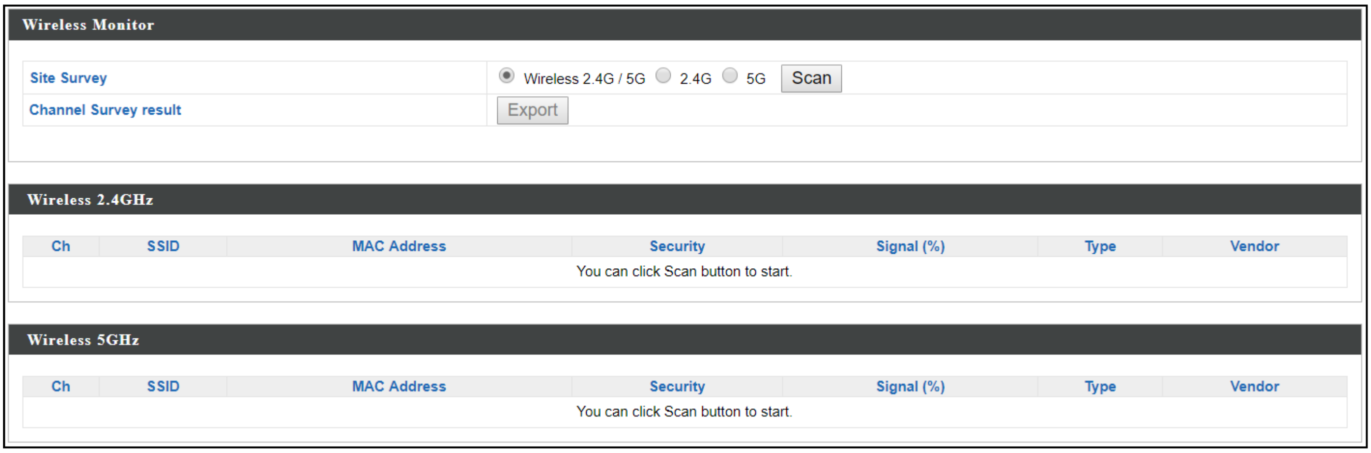
#	SSID	IP Address	MAC Address	Tx	Rx	Signal (%)	RSSI (dbm)	Connected Time	Idle Time	Vendor	Kick
No wireless client											

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	● Wireless 2.4G / 5G ○ 2.4G ○ 5G Scan
Channel Survey result	Export

Wireless 2.4GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

Wireless 5GHz

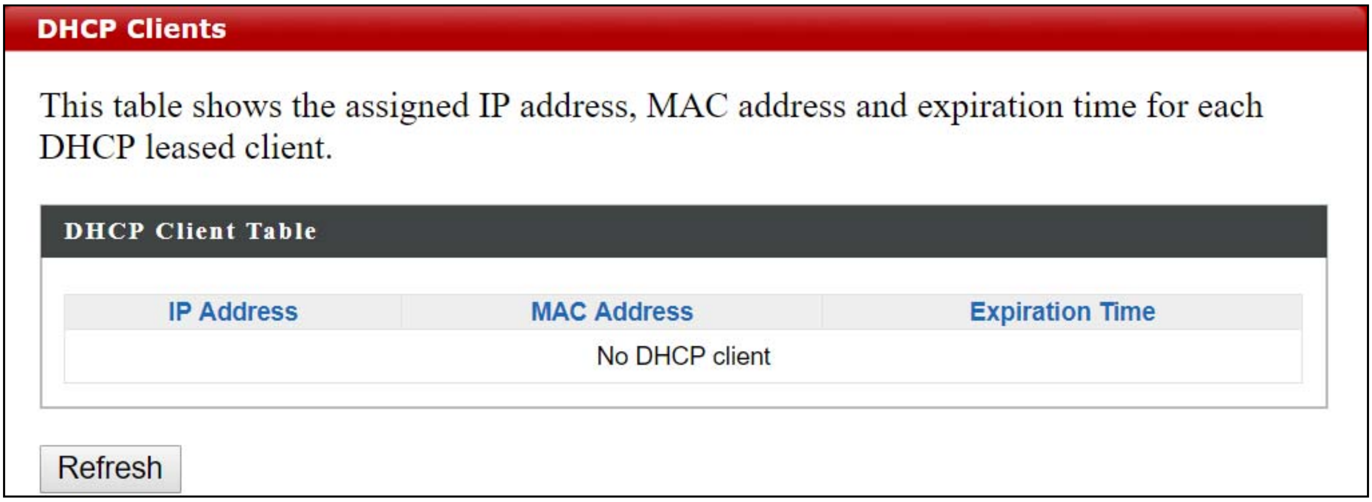
Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

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.



DHCP Clients

This table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

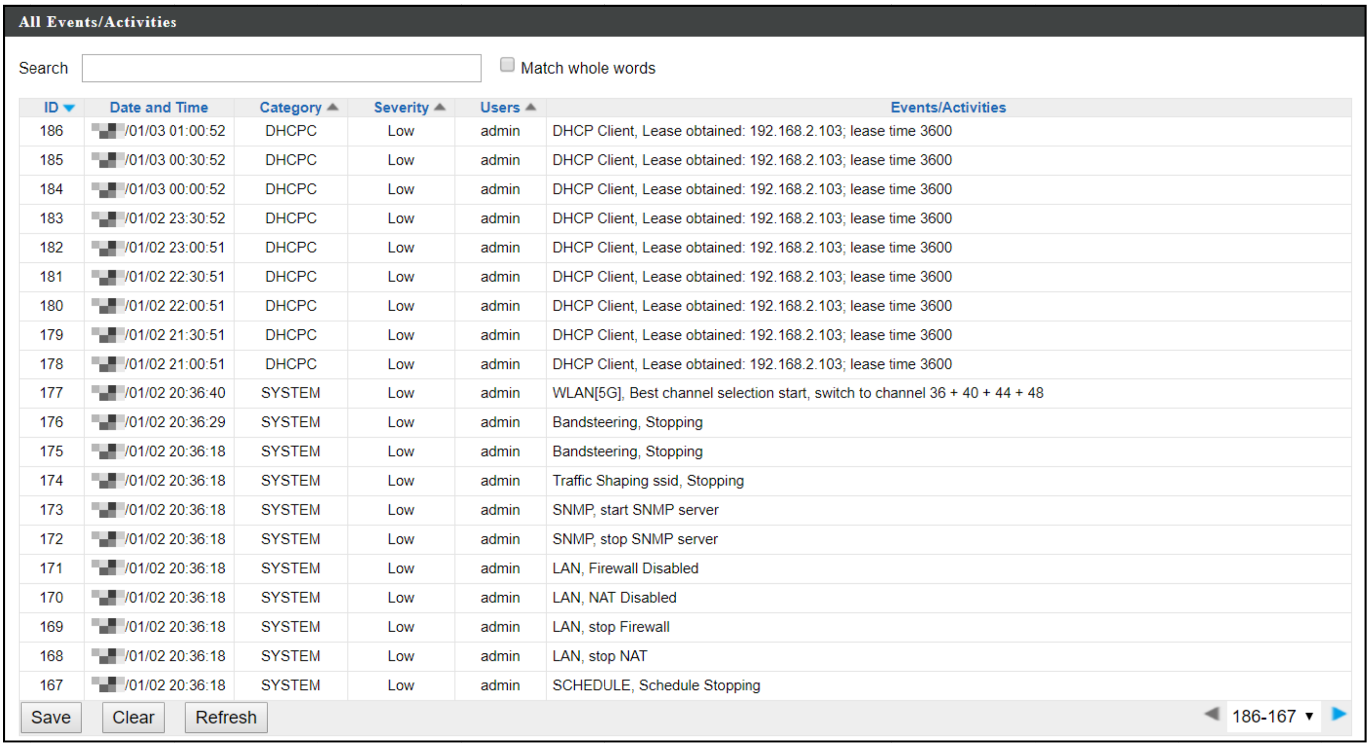
DHCP Client Table

IP Address	MAC Address	Expiration Time
No DHCP client		

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



All Events/Activities

Search ________ □ Match whole words

ID ▼	Date and Time	Category ▲	Severity ▲	Users ▲	Events/Activities
186	[redacted]/01/03 01:00:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
185	[redacted]/01/03 00:30:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
184	[redacted]/01/03 00:00:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
183	[redacted]/01/02 23:30:52	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
182	[redacted]/01/02 23:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
181	[redacted]/01/02 22:30:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
180	[redacted]/01/02 22:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
179	[redacted]/01/02 21:30:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
178	[redacted]/01/02 21:00:51	DHCPC	Low	admin	DHCP Client, Lease obtained: 192.168.2.103; lease time 3600
177	[redacted]/01/02 20:36:40	SYSTEM	Low	admin	WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
176	[redacted]/01/02 20:36:29	SYSTEM	Low	admin	Bandsteering, Stopping
175	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	Bandsteering, Stopping
174	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	Traffic Shaping ssid, Stopping
173	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	SNMP, start SNMP server
172	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	SNMP, stop SNMP server
171	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	LAN, Firewall Disabled
170	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	LAN, NAT Disabled
169	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	LAN, stop Firewall
168	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	LAN, stop NAT
167	[redacted]/01/02 20:36:18	SYSTEM	Low	admin	SCHEDULE, Schedule Stopping

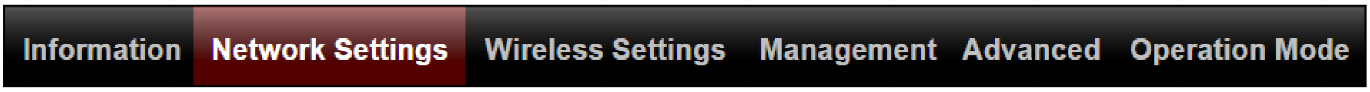
Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

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

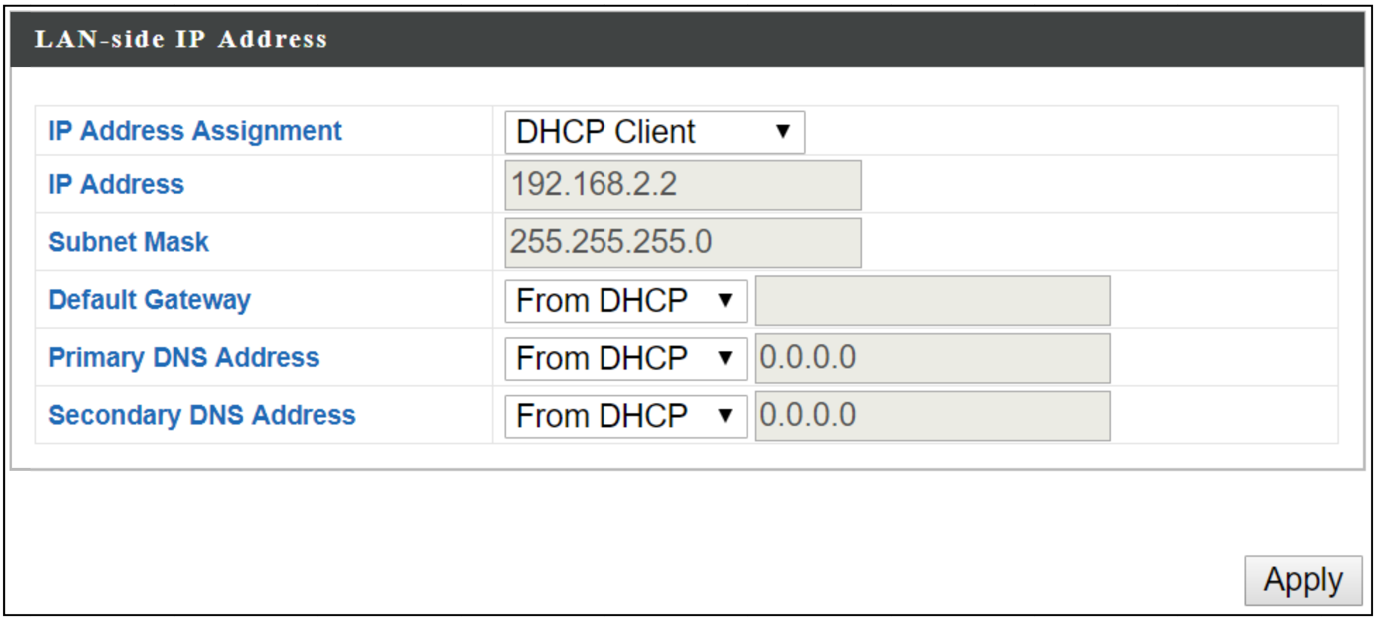
IV-2 Network Settings



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.

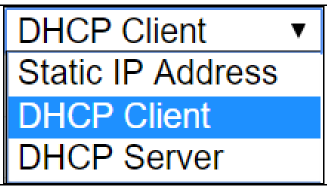
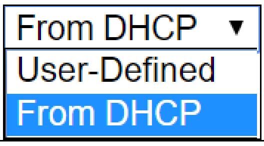
The access point's default IP address is 192.168.2.2.



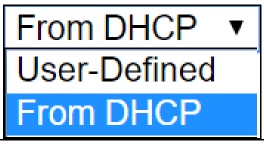
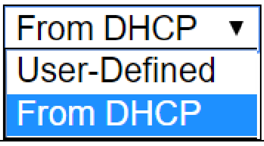
LAN-side IP Address

IP Address Assignment	DHCP Client ▼	
IP Address	192.168.2.2	
Subnet Mask	255.255.255.0	
Default Gateway	From DHCP ▼	
Primary DNS Address	From DHCP ▼	0.0.0.0
Secondary DNS Address	From DHCP ▼	0.0.0.0

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.

	 DHCP Client ▼ Static IP Address DHCP Client DHCP Server
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. 

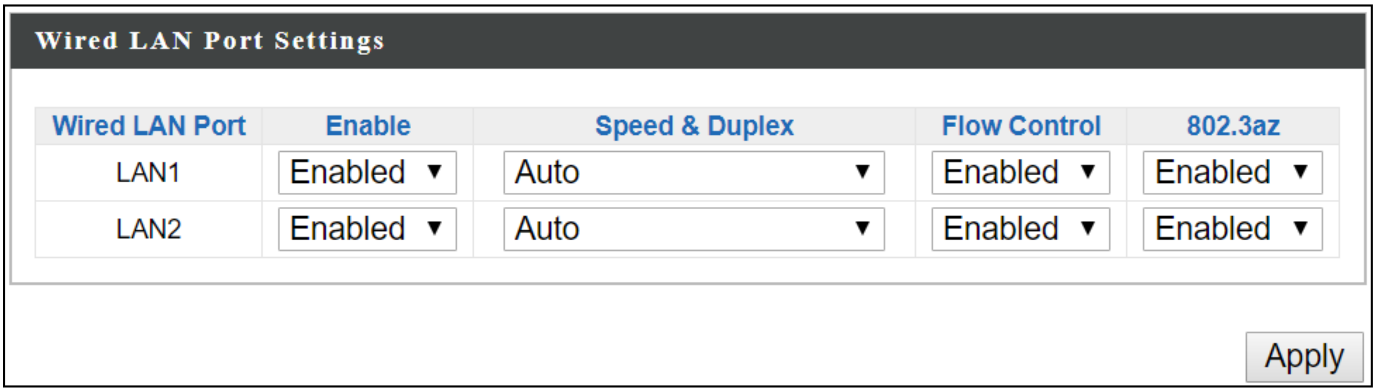
DHCP users can select to get DNS servers' IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

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.

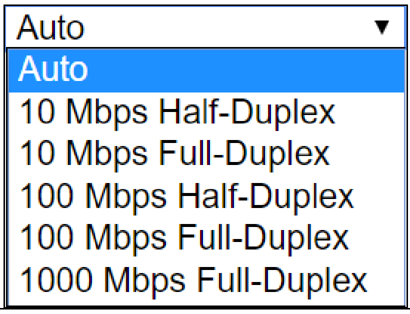
IV-2-2 LAN Port

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



Wired LAN Port Settings

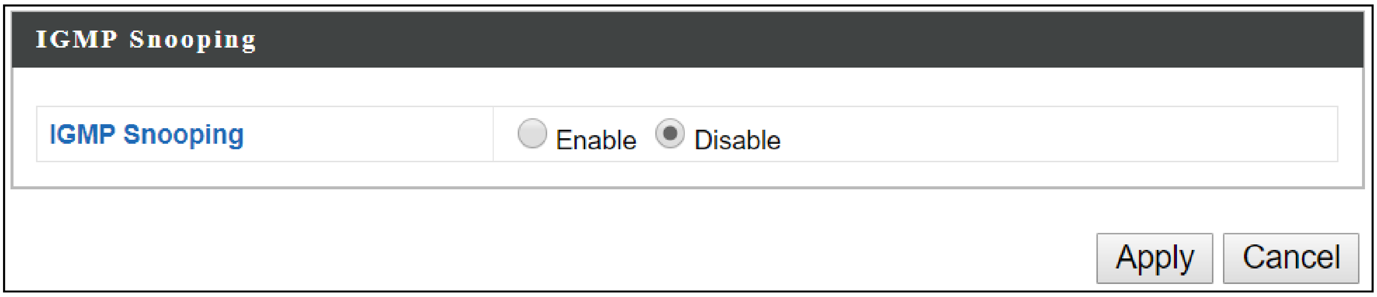
Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
LAN1	Enabled	Auto	Enabled	Enabled
LAN2	Enabled	Auto	Enabled	Enabled

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.



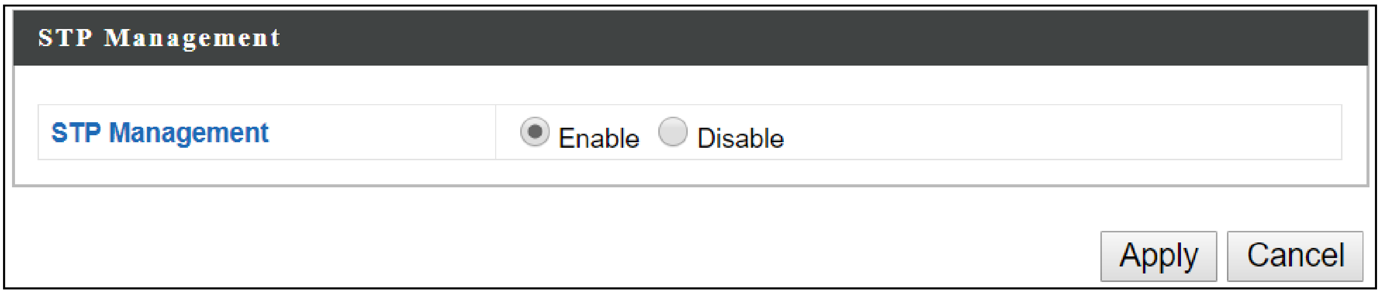
IGMP Snooping

IGMP Snooping ○ Enable ● Disable

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.



STP Management

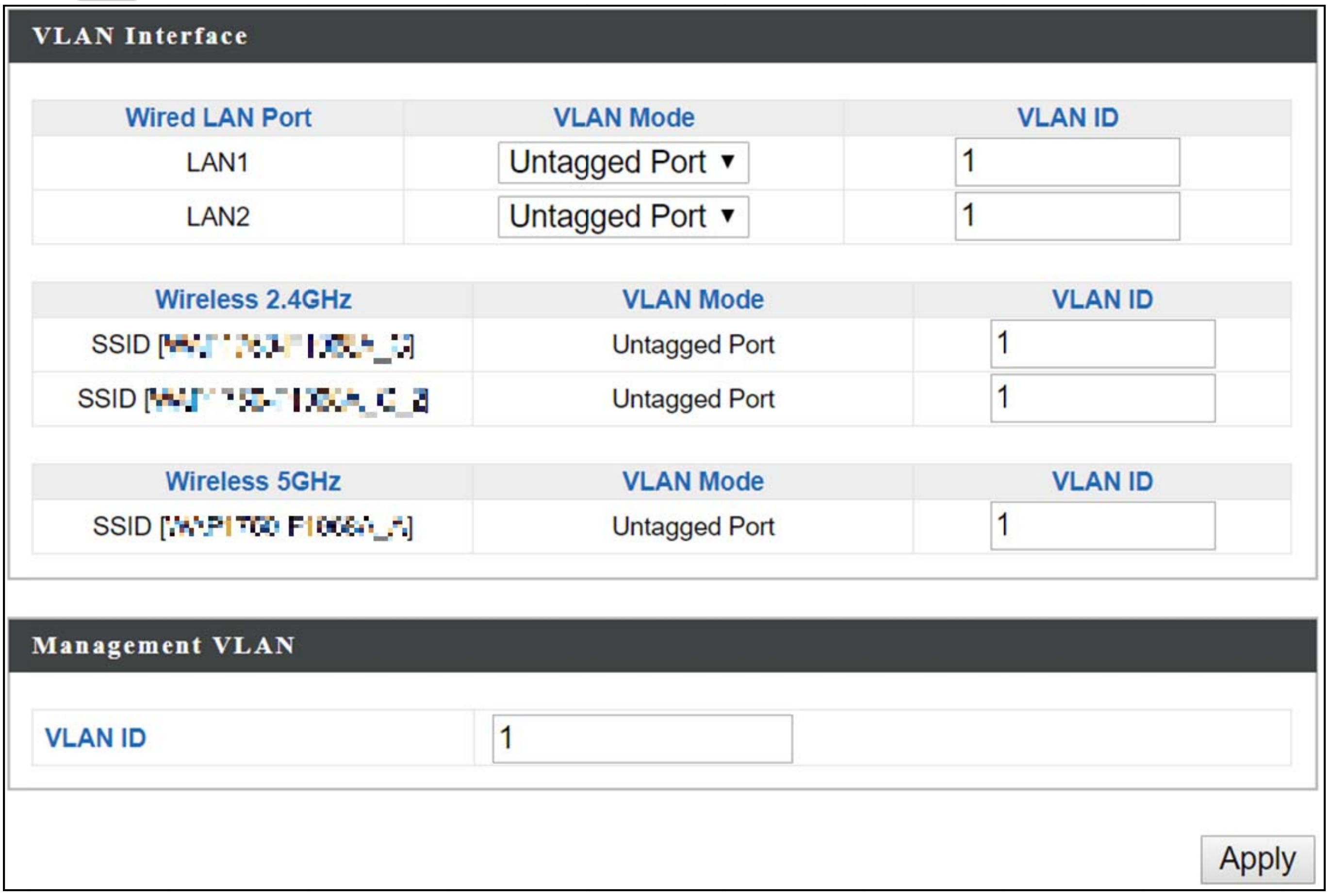
STP Management ● Enable ○ Disable

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	VLAN Mode	VLAN ID
LAN1	Untagged Port ▾	1
LAN2	Untagged Port ▾	1

Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [redacted]	Untagged Port	1
SSID [redacted]	Untagged Port	1

Wireless 5GHz	VLAN Mode	VLAN ID
SSID [redacted]	Untagged Port	1

Management VLAN

VLAN ID	1

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

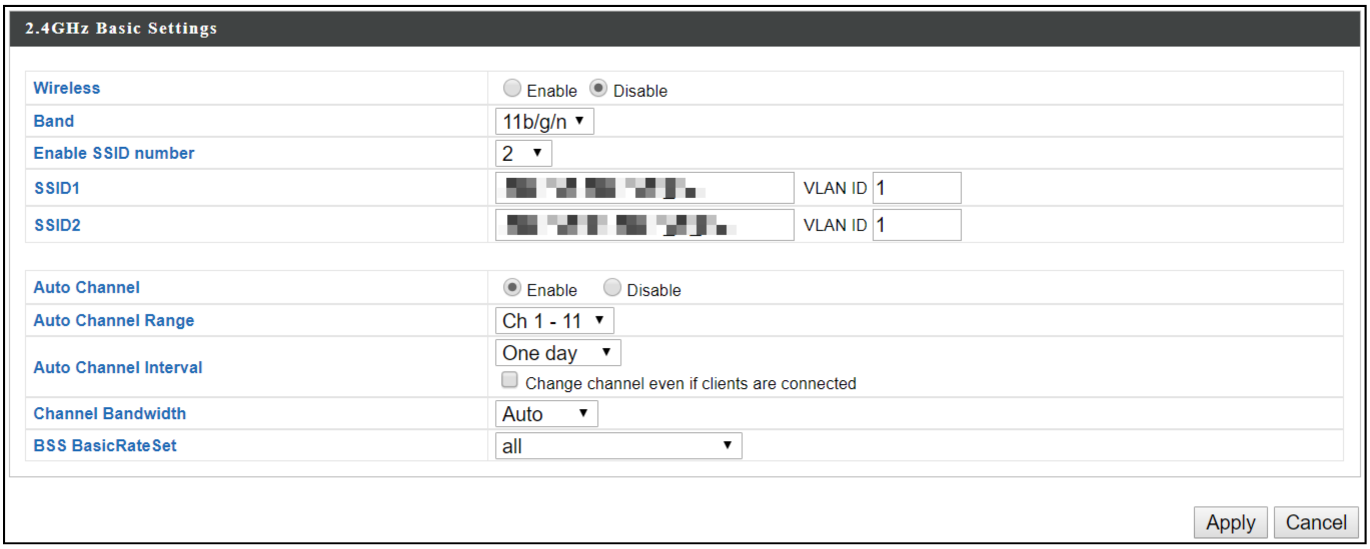
Information Network Settings Wireless Settings Management Advanced Operation Mode

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.

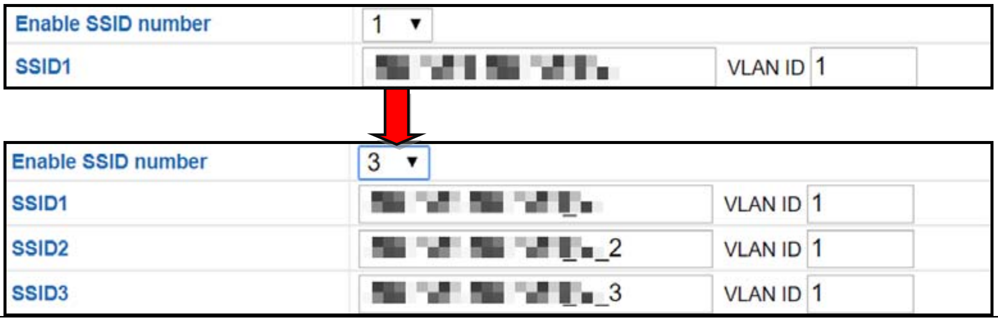
IV-3-1-1 Basic

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



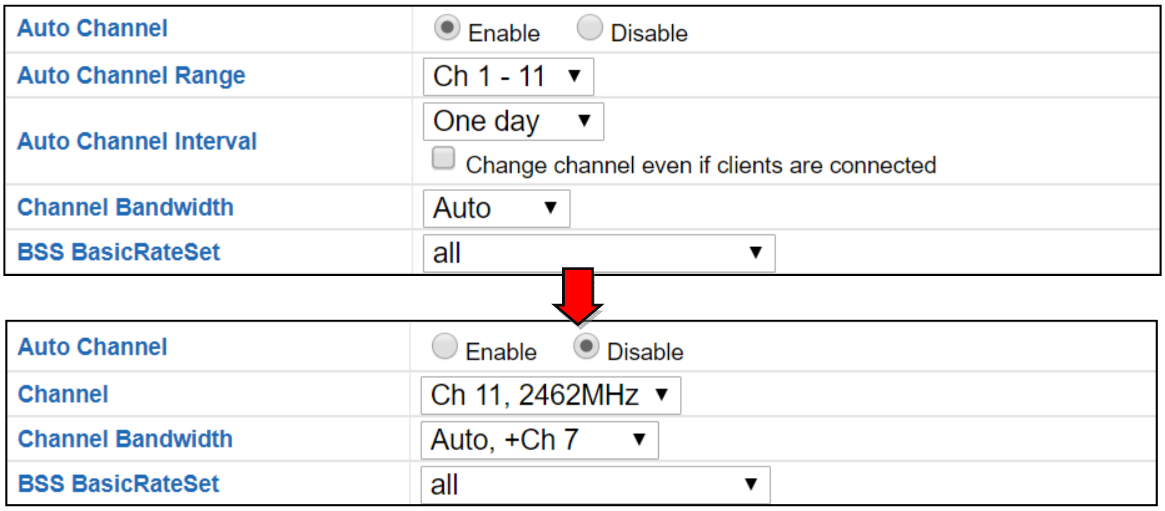
2.4GHz Basic Settings

Wireless	○ Enable ● Disable
Band	11b/g/n ▾
Enable SSID number	2 ▾
SSID1	[redacted] VLAN ID 1
SSID2	[redacted] VLAN ID 1
Auto Channel	● Enable ○ Disable
Auto Channel Range	Ch 1 - 11 ▾
Auto Channel Interval	One day ▾ □ Change channel even if clients are connected
Channel Bandwidth	Auto ▾
BSS BasicRateSet	all ▾

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.  Enable SSID number: 1 ▾ SSID1: [redacted] VLAN ID 1 Enable SSID number: 3 ▾ SSID1: [redacted] VLAN ID 1 SSID2: [redacted]_2 VLAN ID 1 SSID3: [redacted]_3 VLAN ID 1
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:



Auto Channel	● Enable ○ Disable
Auto Channel Range	Ch 1 - 11 ▼
Auto Channel Interval	One day ▼ □ Change channel even if clients are connected
Channel Bandwidth	Auto ▼
BSS BasicRateSet	all ▼

Auto Channel	○ Enable ● Disable
Channel	Ch 11, 2462MHz ▼
Channel Bandwidth	Auto, +Ch 7 ▼
BSS BasicRateSet	all ▼

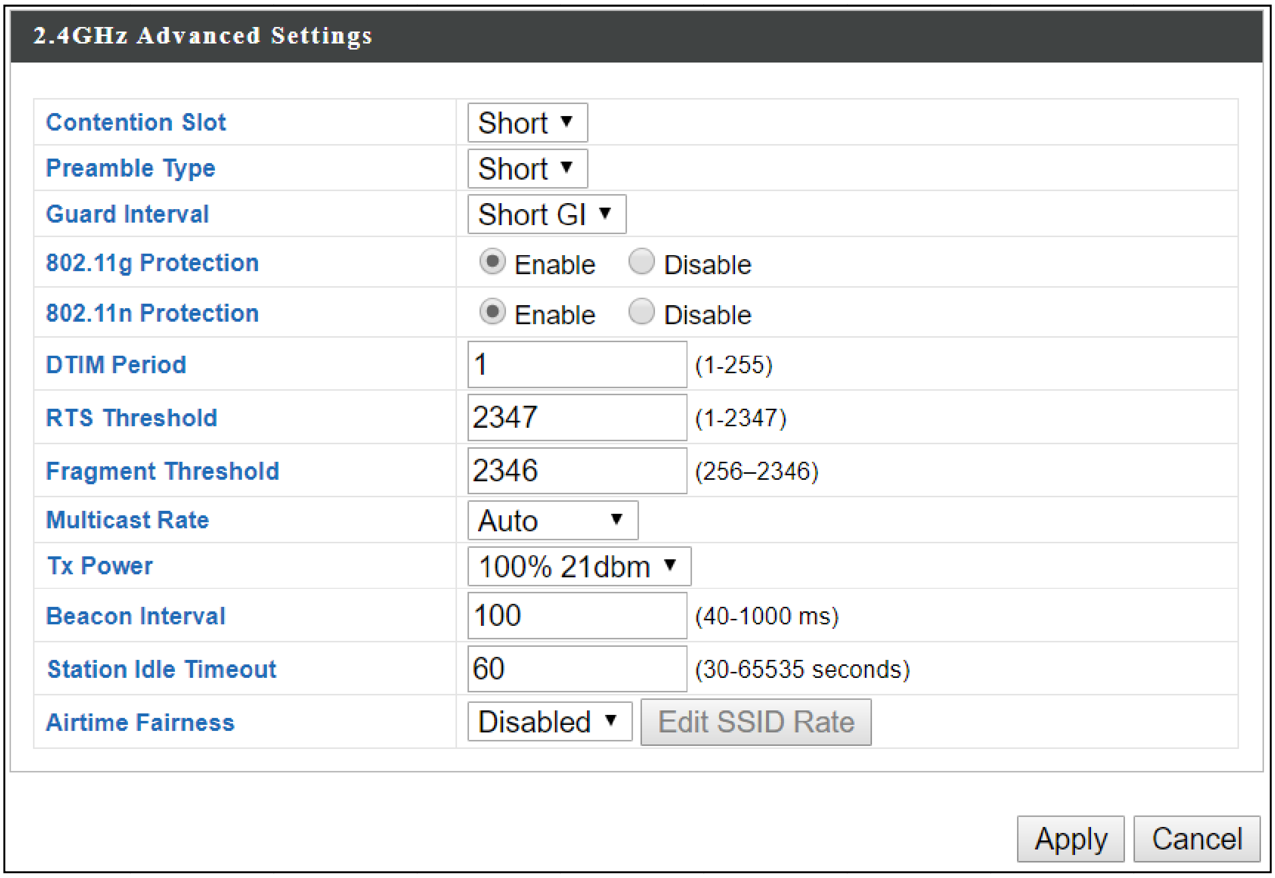
Channel	Select a wireless channel from 1 – 11.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference); or 40MHz (higher performance but potentially higher interference); or Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service 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.

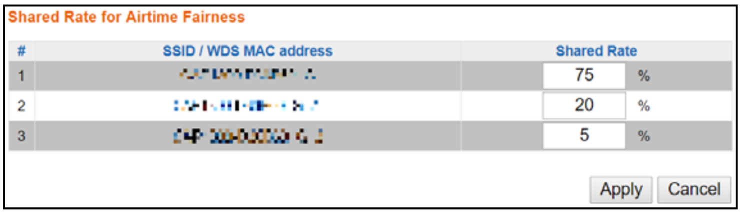
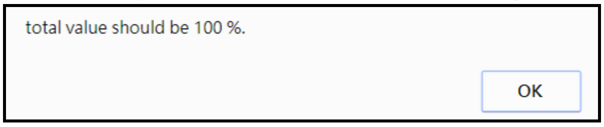
Changing these settings can adversely affect the performance of your access point.



2.4GHz Advanced Settings

Contention Slot	Short ▼
Preamble Type	Short ▼
Guard Interval	Short GI ▼
802.11g Protection	● Enable ○ Disable
802.11n Protection	● Enable ○ Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256–2346)
Multicast Rate	Auto ▼
Tx Power	100% 21dbm ▼
Beacon Interval	100 (40-1000 ms)
Station Idle Timeout	60 (30-65535 seconds)
Airtime Fairness	Disabled ▼ Edit SSID Rate

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).

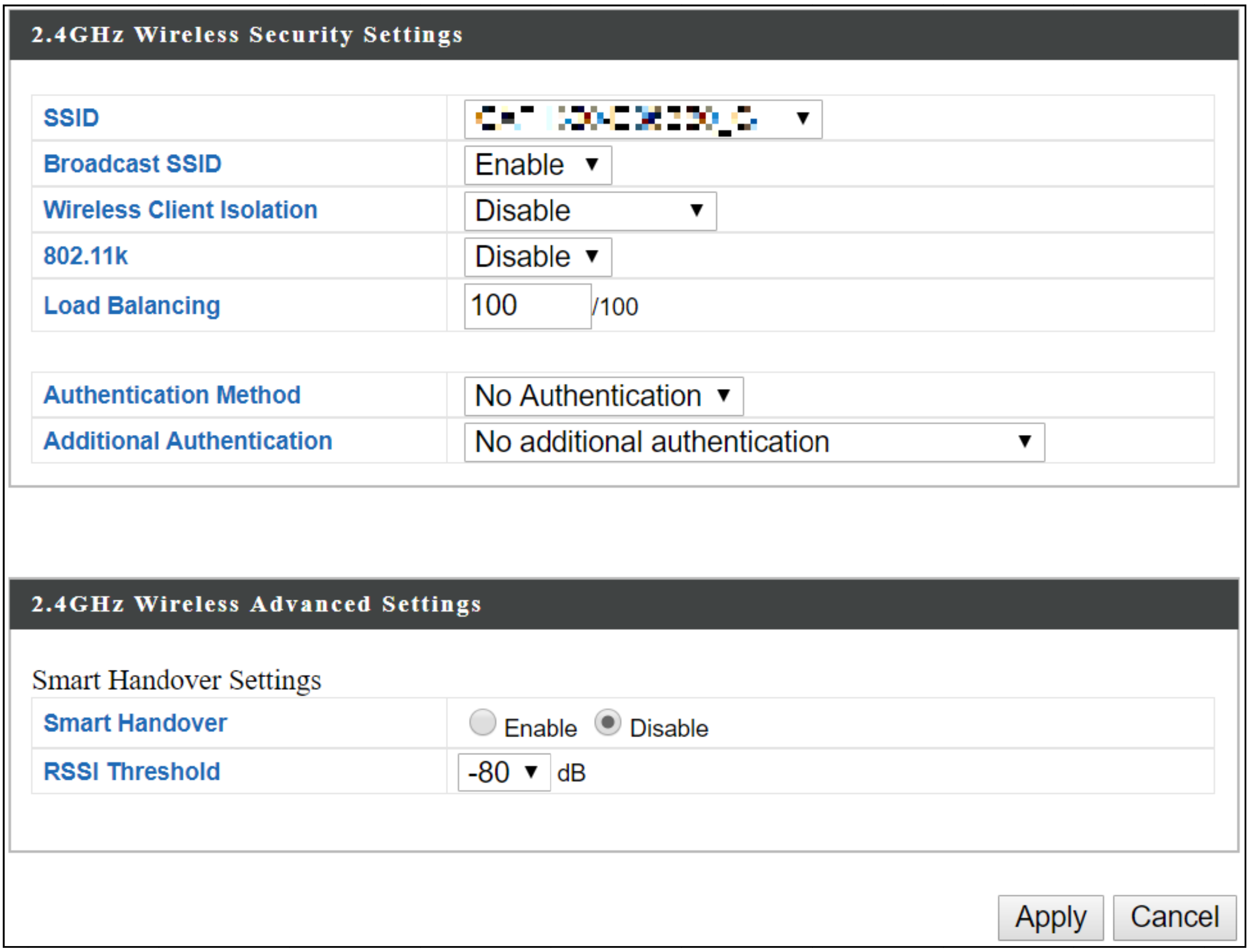
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client).
DTIM Period	Set the DTIM (delivery traffic indication 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:  Shared Rate for Airtime Fairness # | SSID / WDS MAC address | Shared Rate 1 | [redacted] | 75 % 2 | [redacted] | 20 % 3 | [redacted] | 5 % The % field must add up to 100% or a message will be displayed:  total value should be 100 %. 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.



2.4GHz Wireless Security Settings

SSID	[redacted] ▼
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
802.11k	Disable ▼
Load Balancing	100 /100
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

2.4GHz Wireless Advanced Settings

Smart Handover Settings

Smart Handover	○ Enable ● Disable
RSSI Threshold	-80 ▼ dB

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.

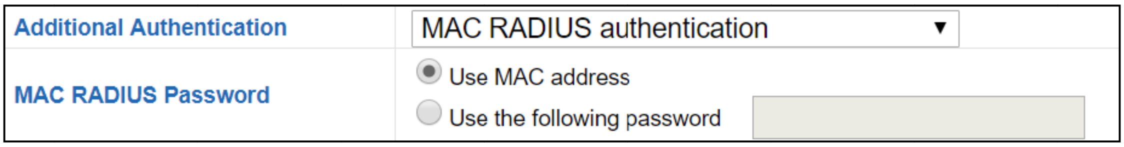
See** IV-3-5 MAC Filter **to configure MAC filtering.

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.

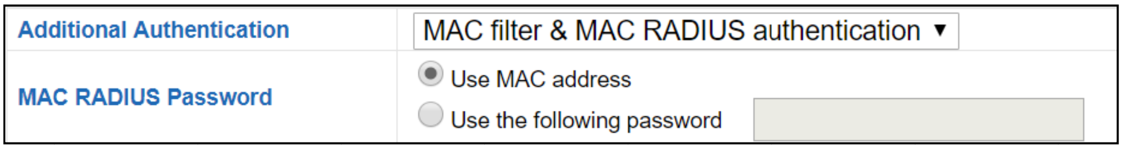
WPS must be disabled to use MAC-RADIUS authentication. See** IV-3-3 WPS **for WPS settings.



Additional Authentication	MAC RADIUS authentication ▼
MAC RADIUS Password	● Use MAC address ○ Use the following password

MAC Filter & MAC-RADIUS Authentication

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

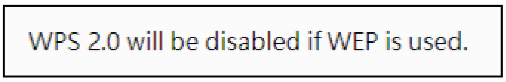


Additional Authentication	MAC filter & MAC RADIUS authentication ▼
MAC RADIUS Password	● Use MAC address ○ Use the following password

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**.

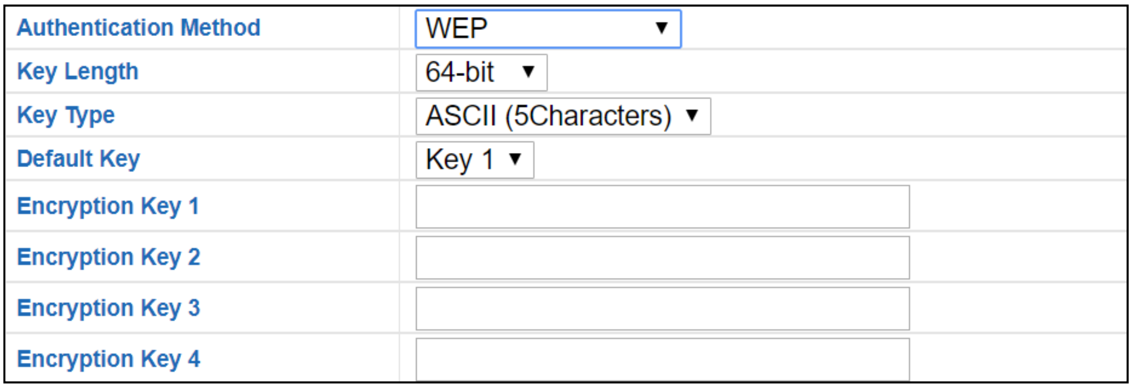
IV-3-1-3-2 WEP

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



WPS 2.0 will be disabled if WEP is used.

Below is a figure showing the configurable fields:



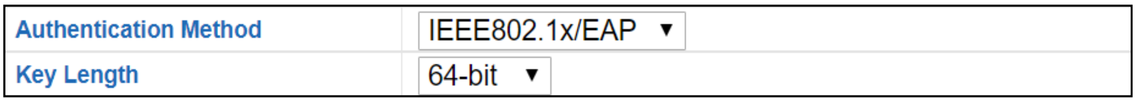
Authentication Method	WEP ▼
Key Length	64-bit ▼
Key Type	ASCII (5Characters) ▼
Default Key	Key 1 ▼
Encryption Key 1	
Encryption Key 2	
Encryption Key 3	
Encryption Key 4	

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:



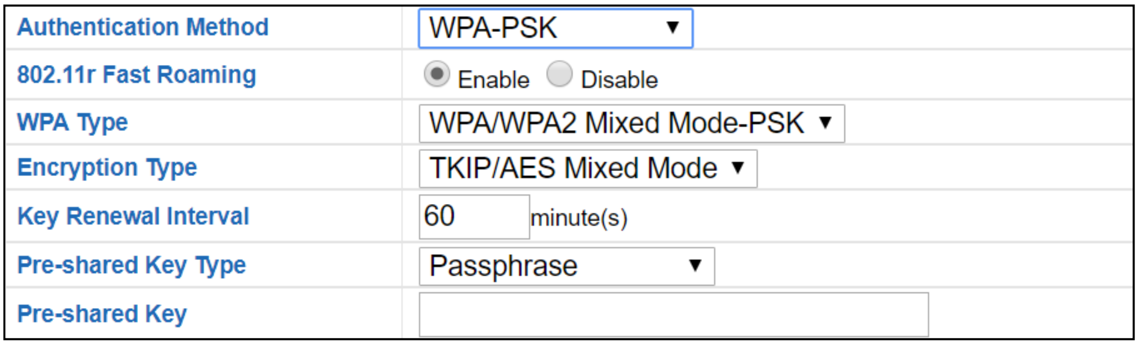
Authentication Method	IEEE802.1x/EAP ▼
Key Length	64-bit ▼

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

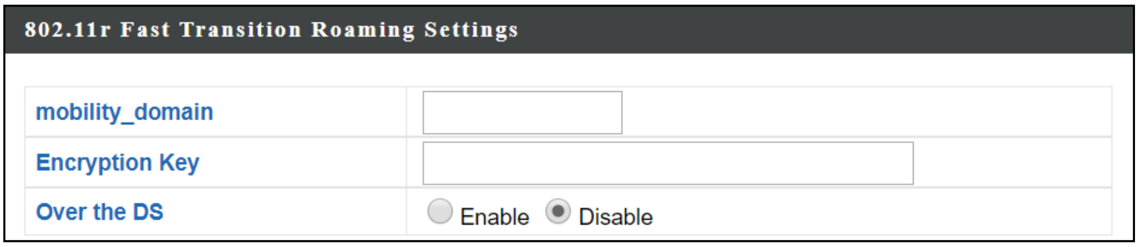
WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

Below is a figure showing the configurable fields:



Authentication Method	WPA-PSK ▼
802.11r Fast Roaming	● Enable ○ Disable
WPA Type	WPA/WPA2 Mixed Mode-PSK ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase ▼
Pre-shared Key	

Fast Roaming Settings will also be shown:



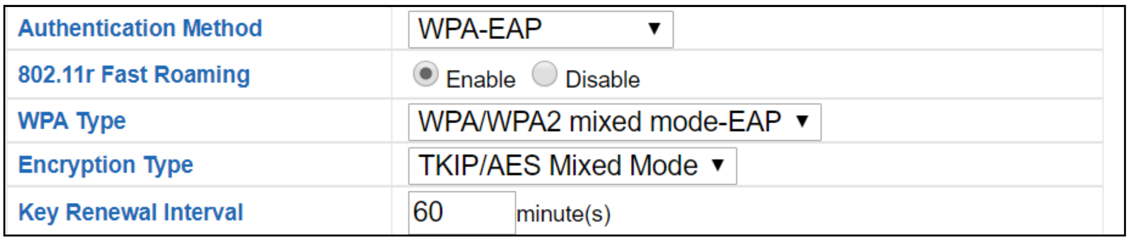
802.11r Fast Transition Roaming Settings

mobility_domain	
Encryption Key	
Over the DS	○ Enable ● Disable

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.

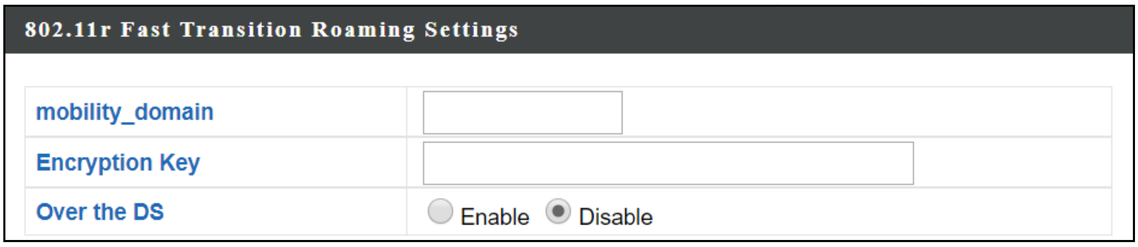
802.11r Fast Transition Roaming Settings	
Mobility_domain	Specify the mobility domain (2.4GHz or 5GHz)
Encryption Key	Specify the encryption key
Over the DS	Enable or disable this function.

IV-3-1-3-5 WPA-EAP



Authentication Method	WPA-EAP ▼
802.11r Fast Roaming	● Enable ○ Disable
WPA Type	WPA/WPA2 mixed mode-EAP ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)

Fast Roaming Settings will also be shown:



802.11r Fast Transition Roaming Settings

mobility_domain	
Encryption Key	
Over the DS	○ Enable ● Disable

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.

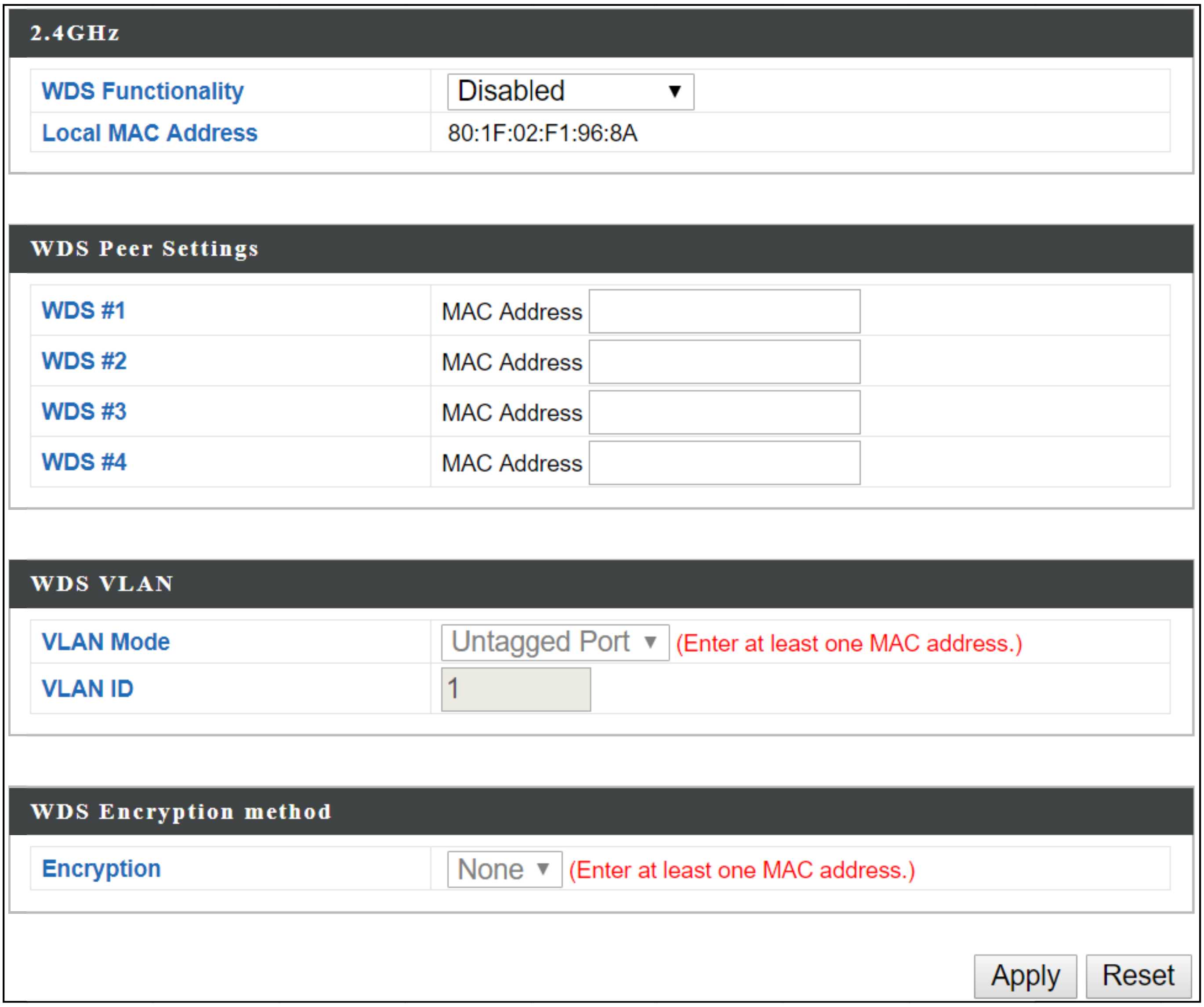
Press “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

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

WDS Peer Settings

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

WDS VLAN

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

WDS Encryption method

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

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.

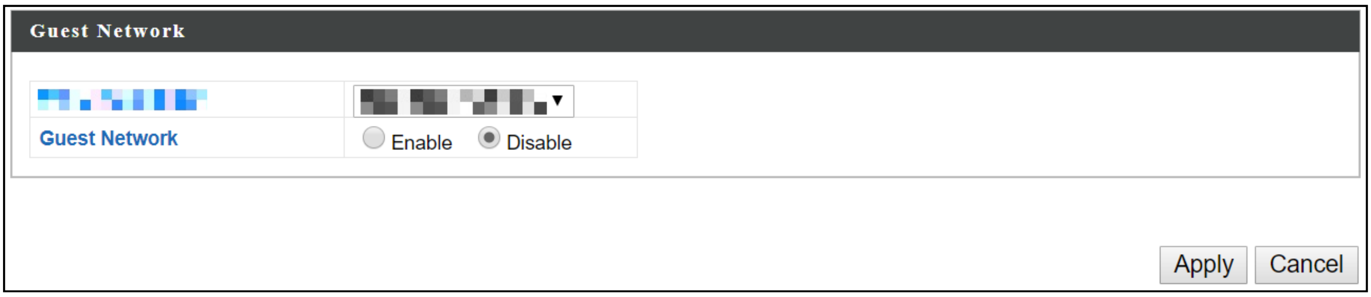
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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.



Guest Network

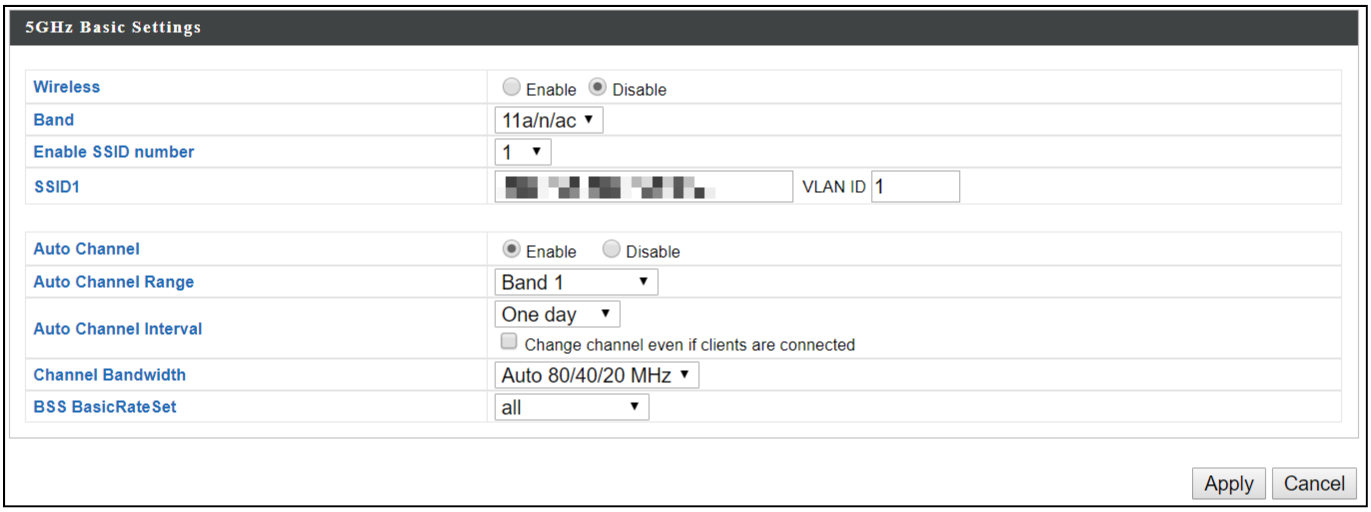
[redacted]	[redacted] ▼
Guest Network	○ Enable ● Disable

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.

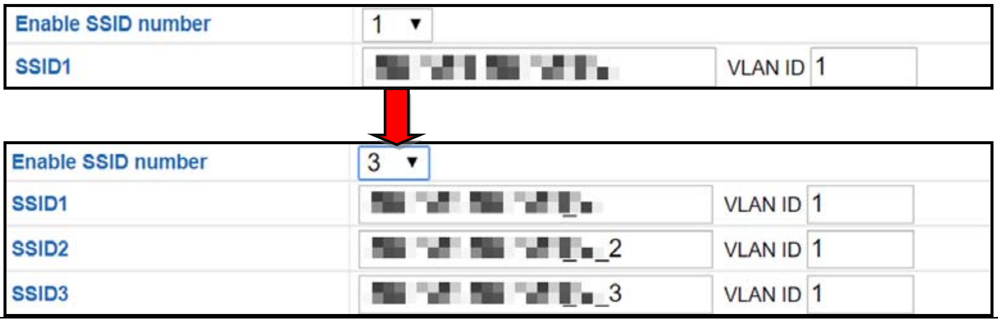
IV-3-2-1 Basic

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



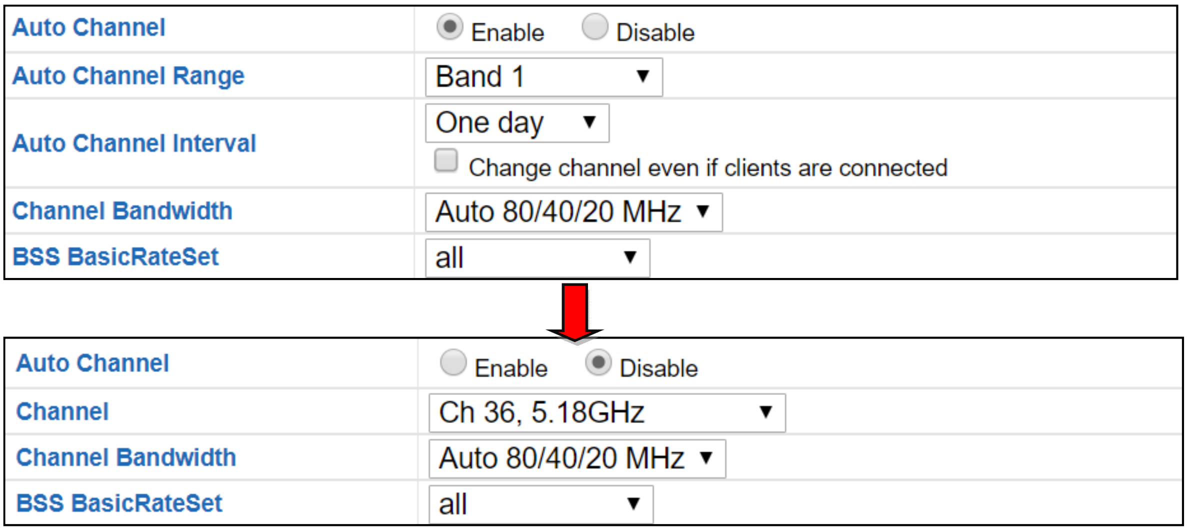
5GHz Basic Settings

Wireless	○ Enable ● Disable
Band	11a/n/ac ▾
Enable SSID number	1 ▾
SSID1	[redacted] VLAN ID 1
Auto Channel	● Enable ○ Disable
Auto Channel Range	Band 1 ▾
Auto Channel Interval	One day ▾ □ Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz ▾
BSS BasicRateSet	all ▾

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.  Enable SSID number: 1 ▾ SSID1: [redacted] VLAN ID 1 Enable SSID number: 3 ▾ SSID1: [redacted] VLAN ID 1 SSID2: [redacted]_2 VLAN ID 1 SSID3: [redacted]_3 VLAN ID 1
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:



Auto Channel	● Enable ○ Disable
Auto Channel Range	Band 1 ▼
Auto Channel Interval	One day ▼ □ Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz ▼
BSS BasicRateSet	all ▼

Auto Channel	○ Enable ● Disable
Channel	Ch 36, 5.18GHz ▼
Channel Bandwidth	Auto 80/40/20 MHz ▼
BSS BasicRateSet	all ▼

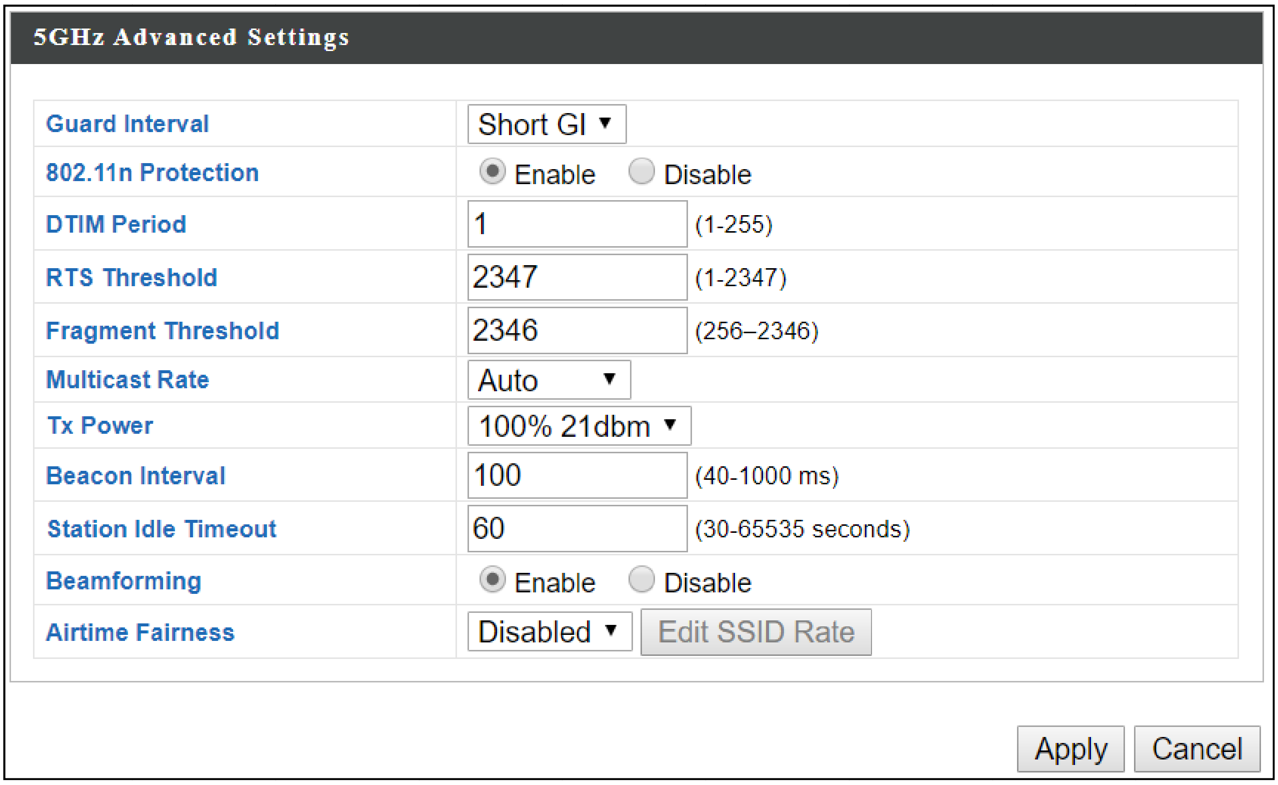
Channel	Select a wireless channel.
Channel Bandwidth	Select the channel bandwidth: 20MHz (lower performance but less interference); or Auto 40/20 MHz; or Auto 80/40/20 MHz (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates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

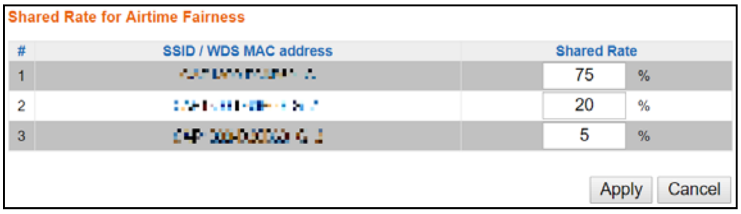
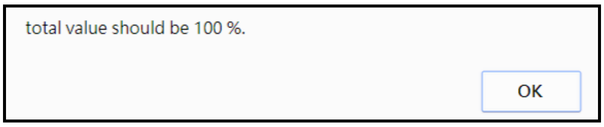
Changing these settings can adversely affect the performance of your access point.



5GHz Advanced Settings

Guard Interval	Short GI ▼
802.11n Protection	● Enable ○ Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256–2346)
Multicast Rate	Auto ▼
Tx Power	100% 21dbm ▼
Beacon Interval	100 (40-1000 ms)
Station Idle Timeout	60 (30-65535 seconds)
Beamforming	● Enable ○ Disable
Airtime Fairness	Disabled ▼ Edit SSID Rate

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.

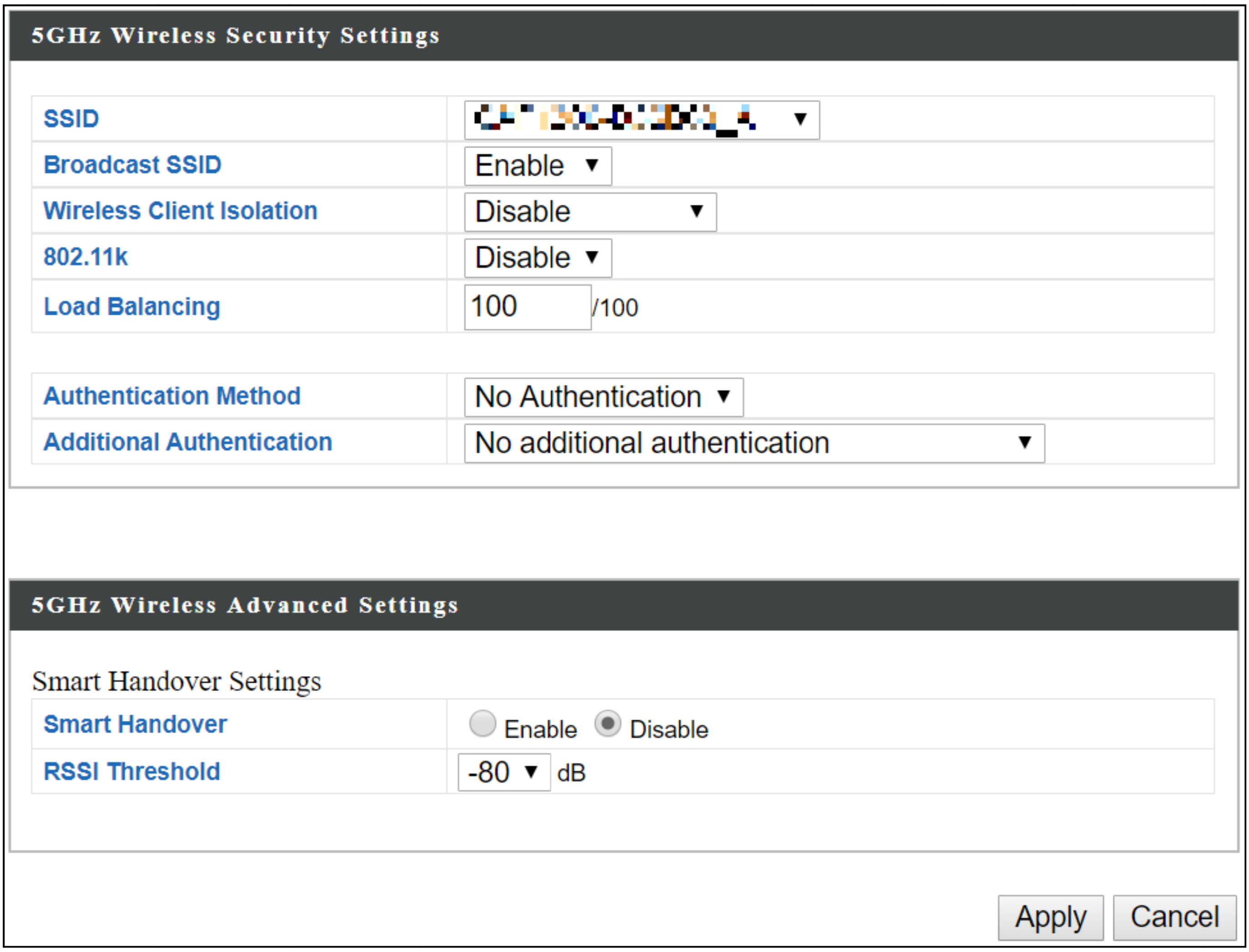
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. 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:  Shared Rate for Airtime Fairness # | SSID / WDS MAC address | Shared Rate 1 | [redacted] | 75 % 2 | [redacted] | 20 % 3 | [redacted] | 5 % Apply Cancel The % field must add up to 100% or a message will be displayed:  total value should be 100 %. OK 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.



5GHz Wireless Security Settings

SSID	[redacted] ▼
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
802.11k	Disable ▼
Load Balancing	100 /100
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

5GHz Wireless Advanced Settings

Smart Handover Settings

Smart Handover	○ Enable ● Disable
RSSI Threshold	-80 ▼ dB

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.

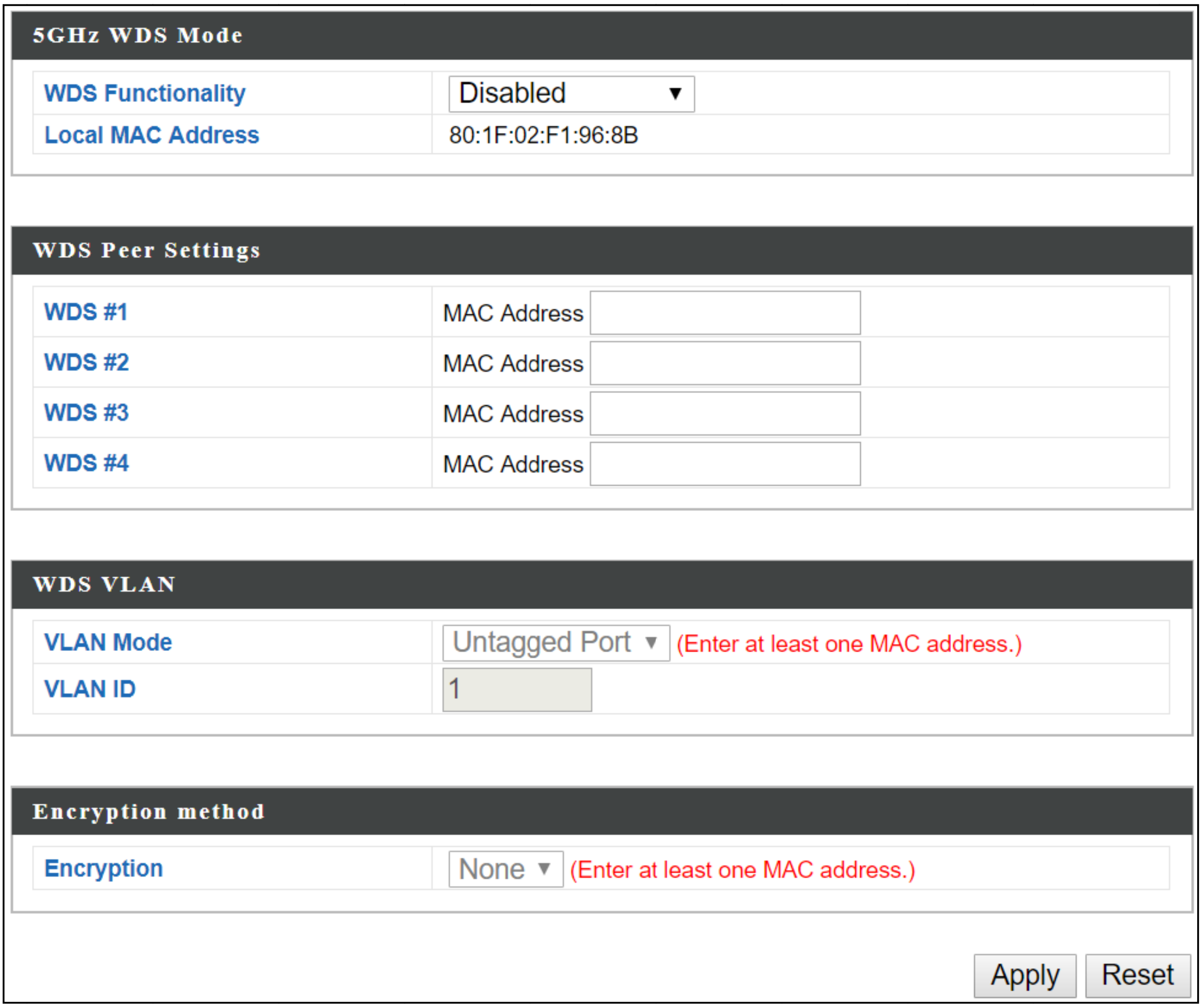
Please refer back to **IV-3-1-3 Security** for more information on authentication and additional authentication types.

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	Disabled ▼
Local MAC Address	80:1F:02:F1:96:8B

WDS Peer Settings

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

WDS VLAN

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

Encryption method

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

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.

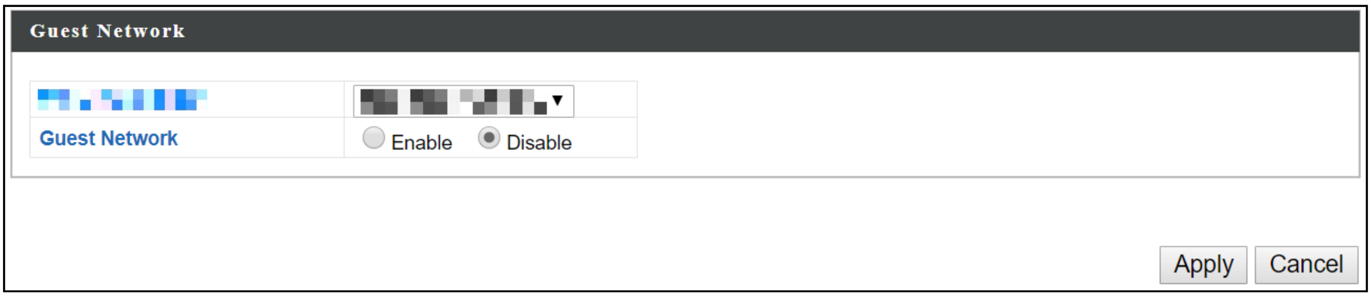
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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.



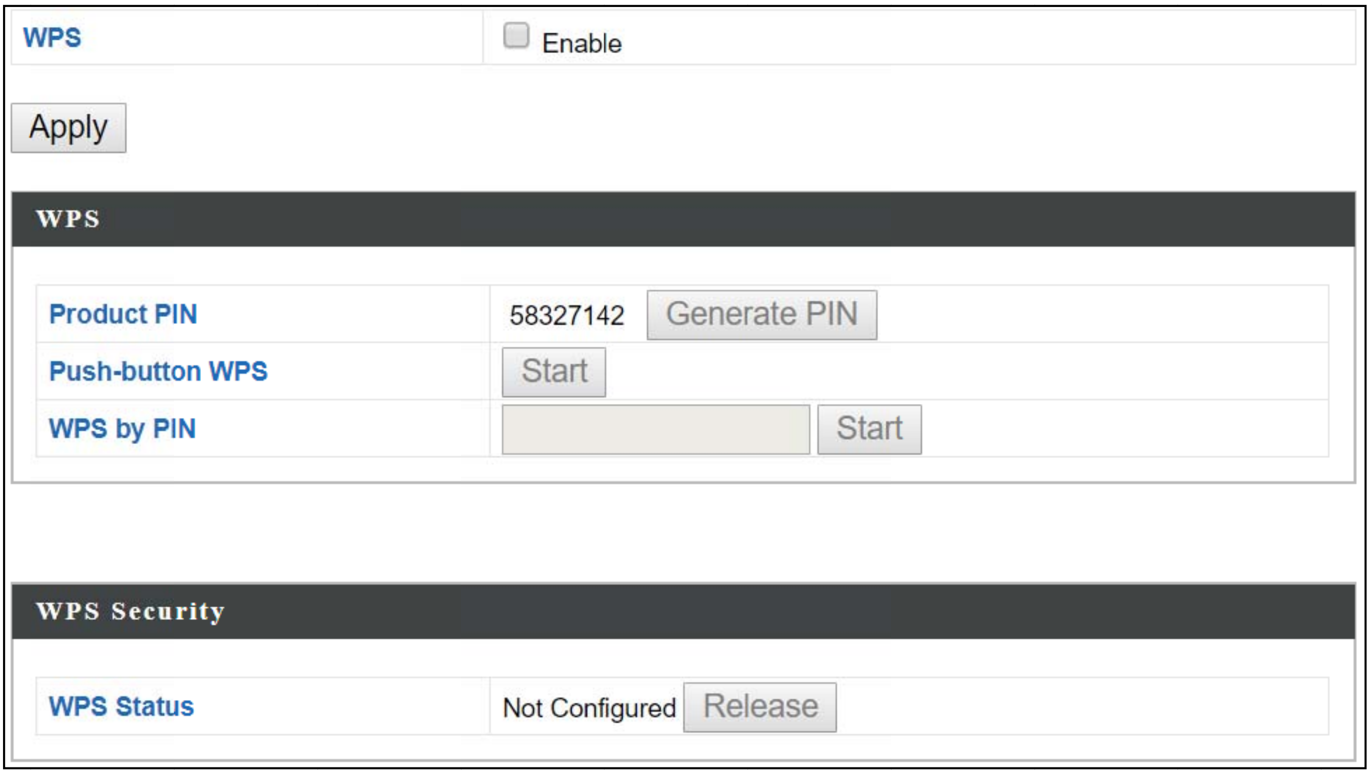
Guest Network

[redacted]	[redacted] ▾
Guest Network	○ Enable ● Disable

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 □ Enable

WPS

Product PIN	58327142
Push-button WPS	
WPS by PIN	

WPS Security

WPS Status	Not Configured

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.

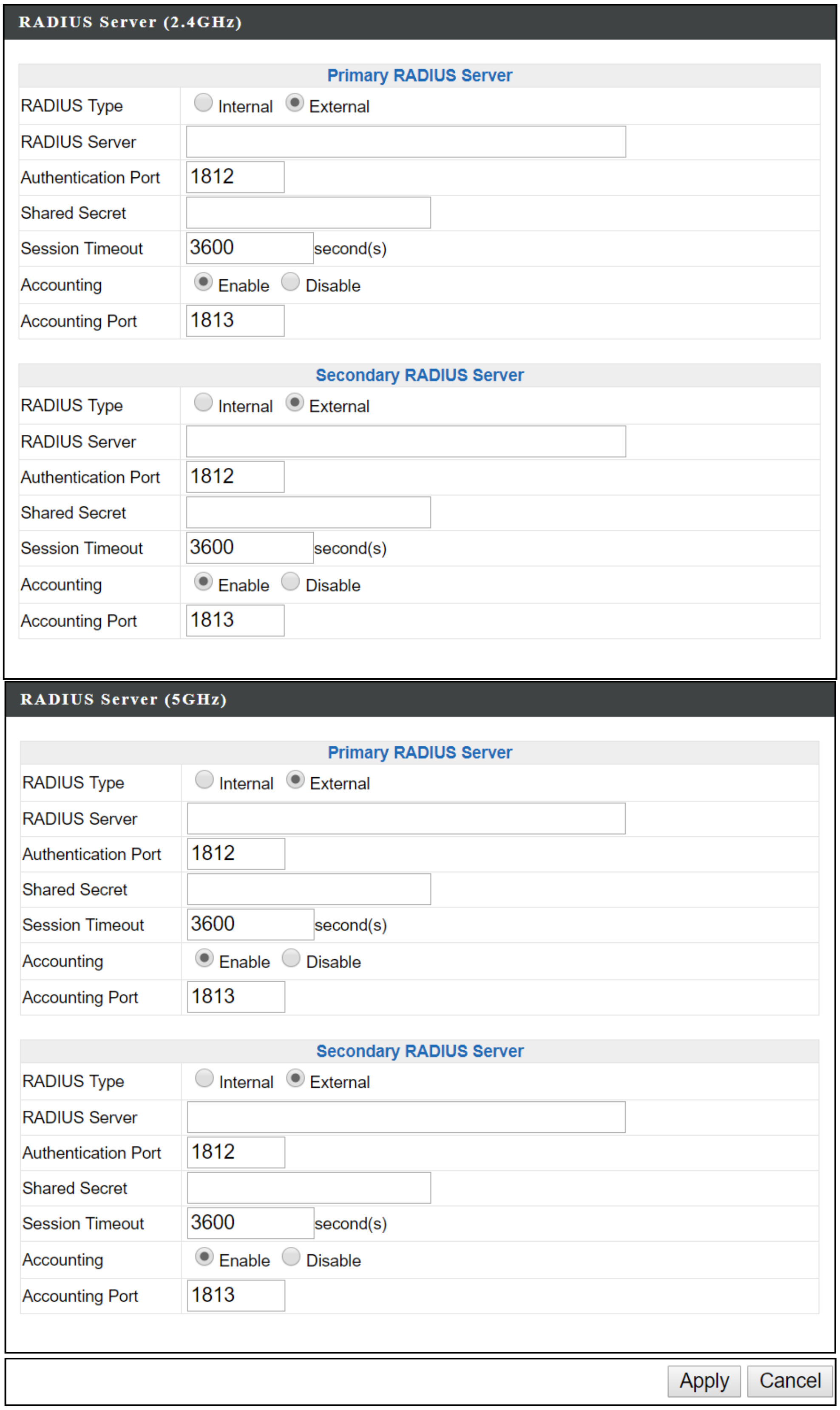
A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

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 Server (2.4GHz)

Primary RADIUS Server

RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

Secondary RADIUS Server

RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

RADIUS Server (5GHz)

Primary RADIUS Server

RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

Secondary RADIUS Server

RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

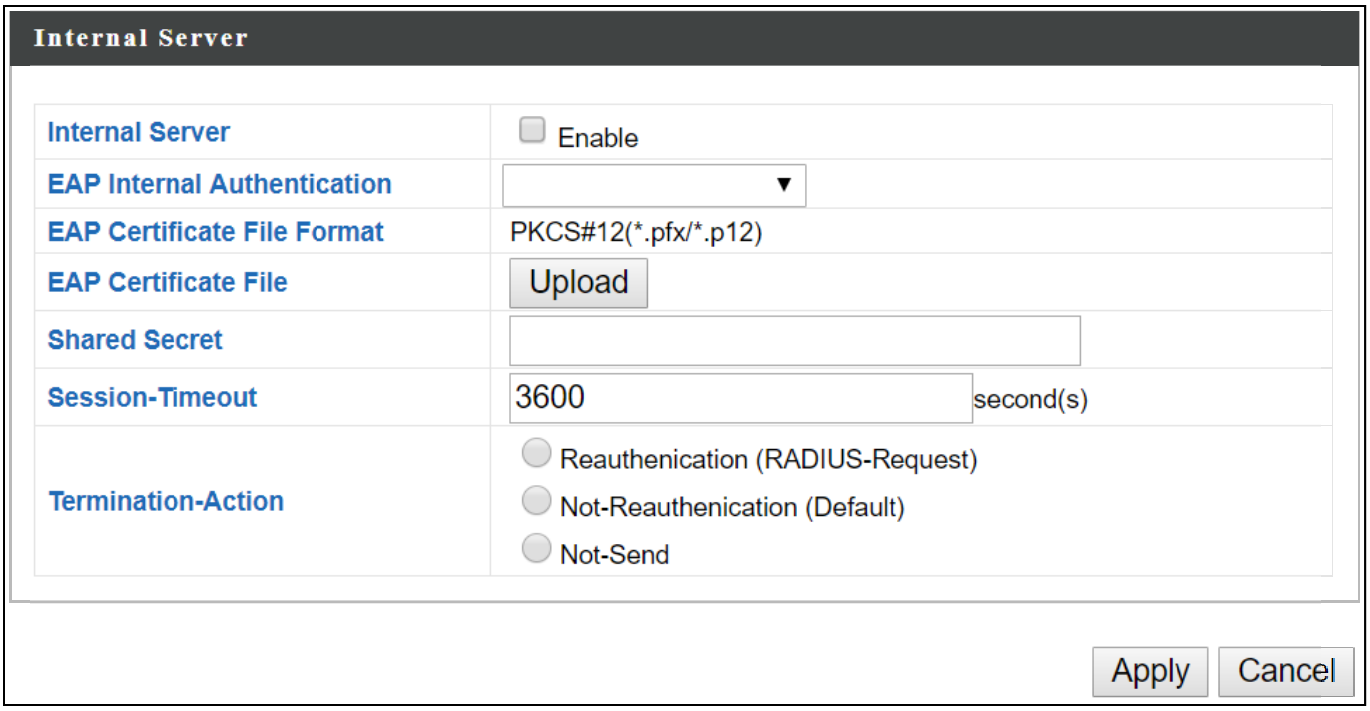
RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 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

Internal Server	□ Enable
EAP Internal Authentication	▼
EAP Certificate File Format	PKCS#12(*.pfx/*.p12)
EAP Certificate File	Upload
Shared Secret	
Session-Timeout	3600 second(s)
Termination-Action	○ Reauthenication (RADIUS-Request) ○ Not-Reauthenication (Default) ○ Not-Send

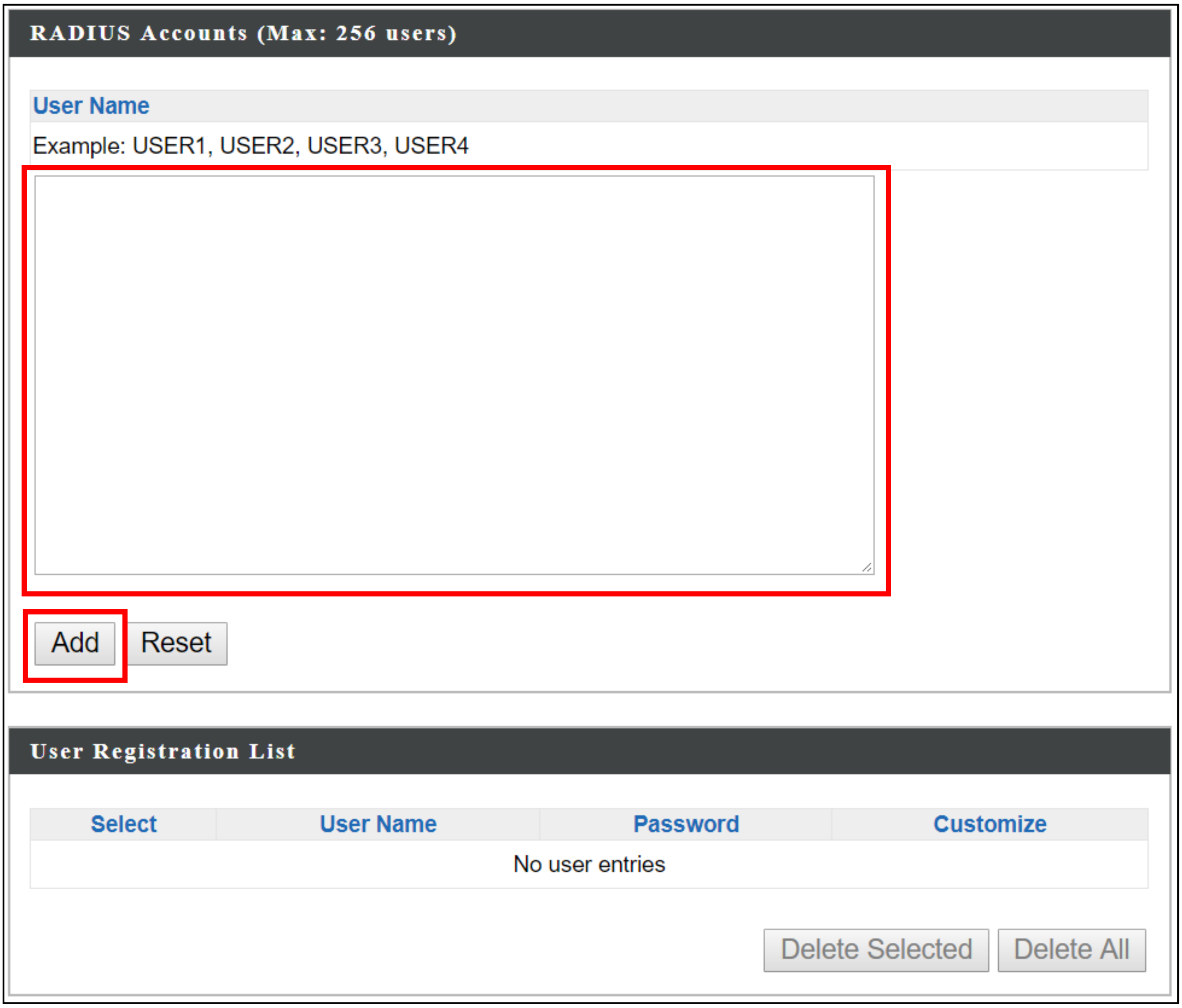
Internal Server	Check/uncheck to enable/disable the access point's internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click "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.



RADIUS Accounts (Max: 256 users)

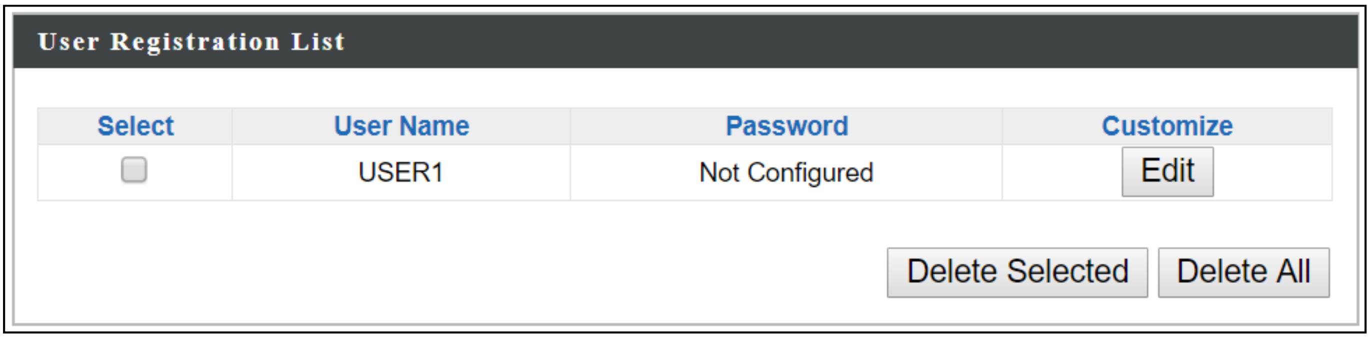
User Name

Example: USER1, USER2, USER3, USER4

User Registration List

Select	User Name	Password	Customize
No user entries			

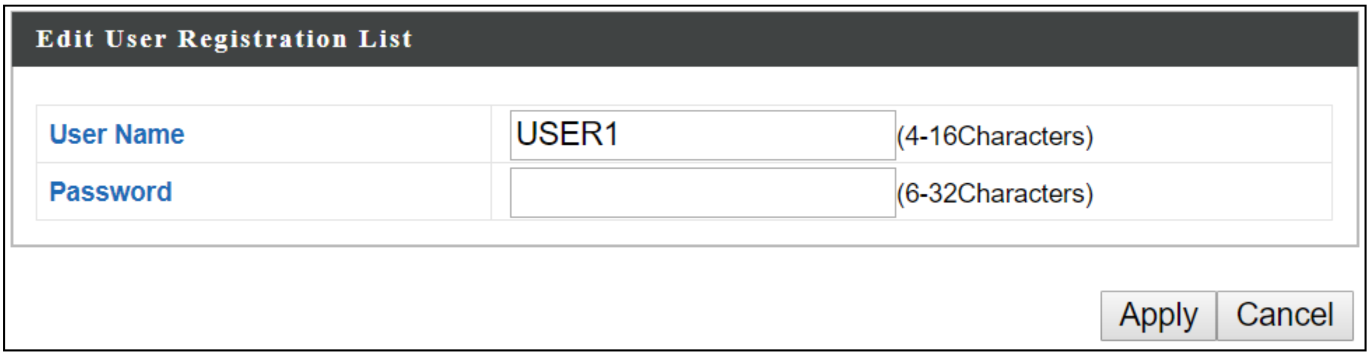
Enter a username in the box below and click "Add" to add the username.



User Registration List

Select	User Name	Password	Customize
□	USER1	Not Configured	Edit

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



Edit User Registration List

User Name	USER1	(4-16Characters)
Password		(6-32Characters)

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.

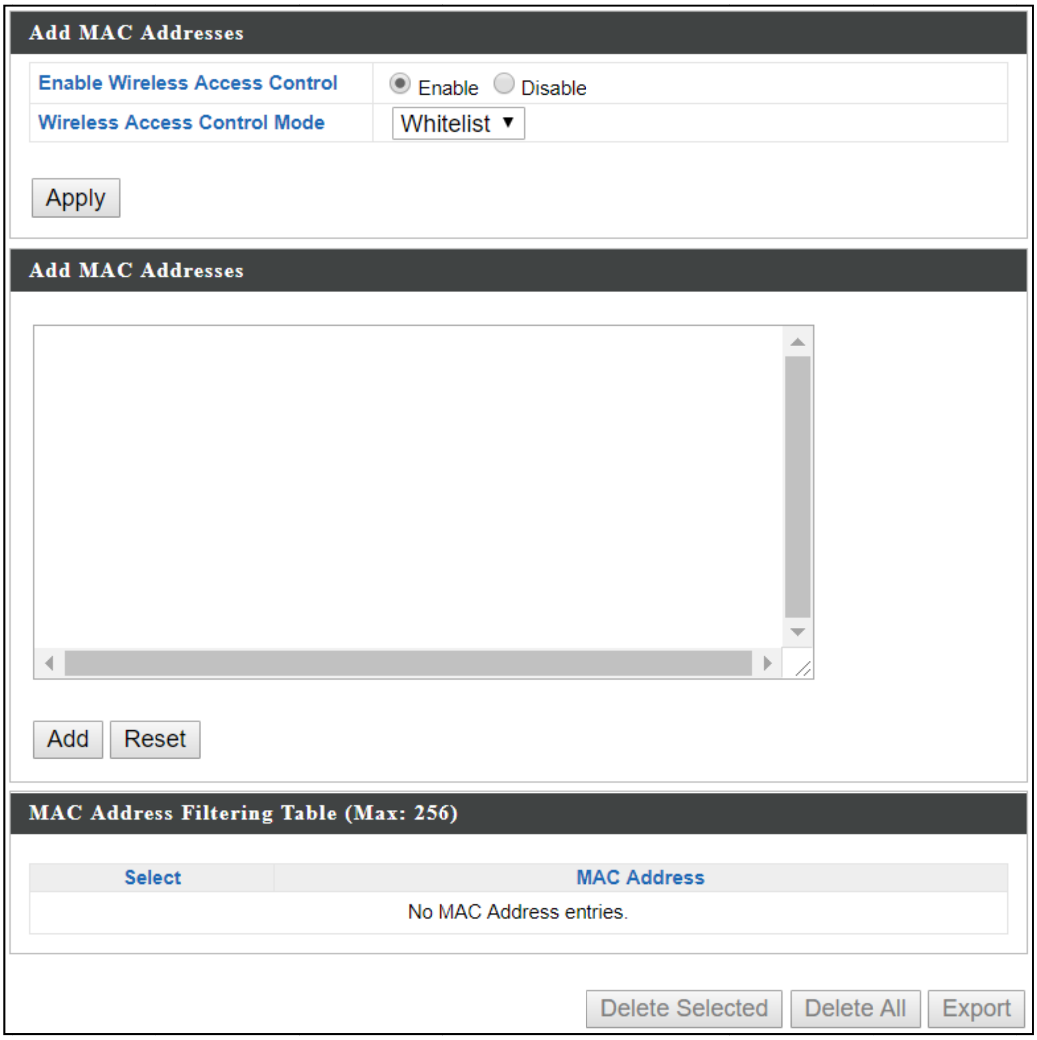
IV-3-5 MAC Filter

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 Addresses

Enable Wireless Access Control	● Enable ○ Disable
Wireless Access Control Mode	Whitelist ▼

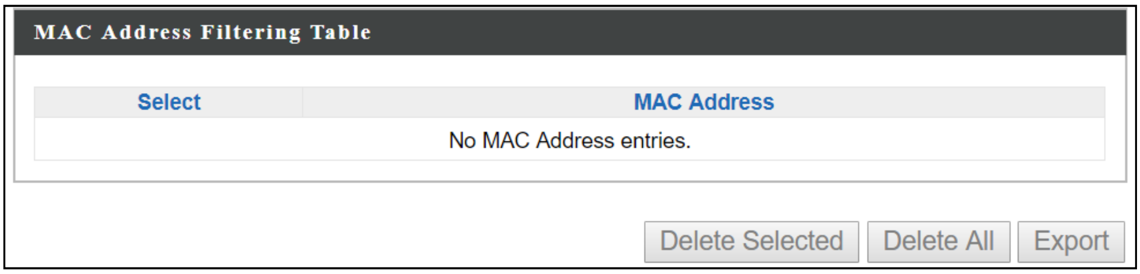
Add MAC Addresses

MAC Address Filtering Table (Max: 256)

Select	MAC Address
No MAC Address entries.	

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.



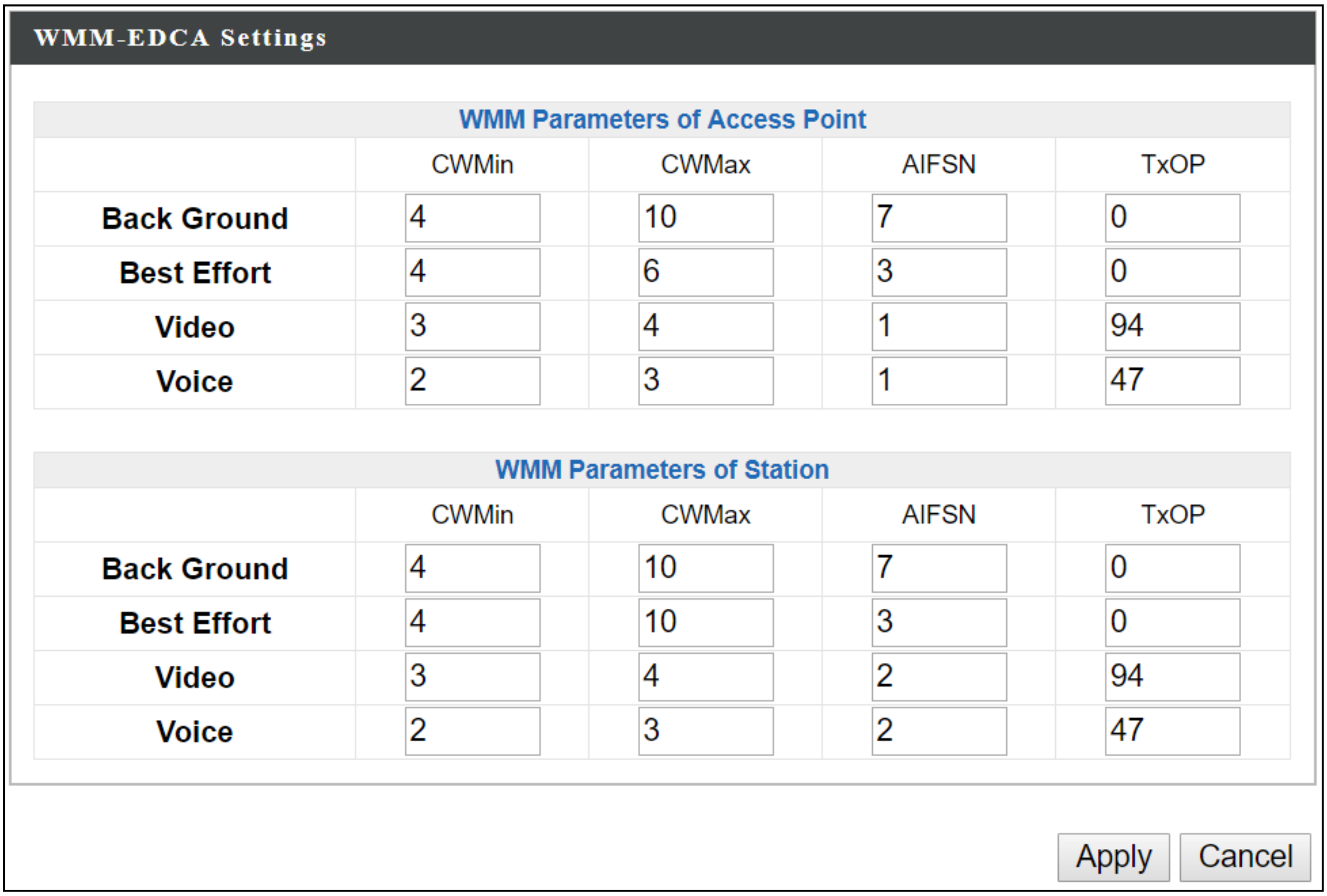
MAC Address Filtering Table

Select	MAC Address
No MAC Address entries.	

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.



WMM-EDCA Settings

WMM Parameters of Access Point

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

WMM Parameters of Station

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

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.

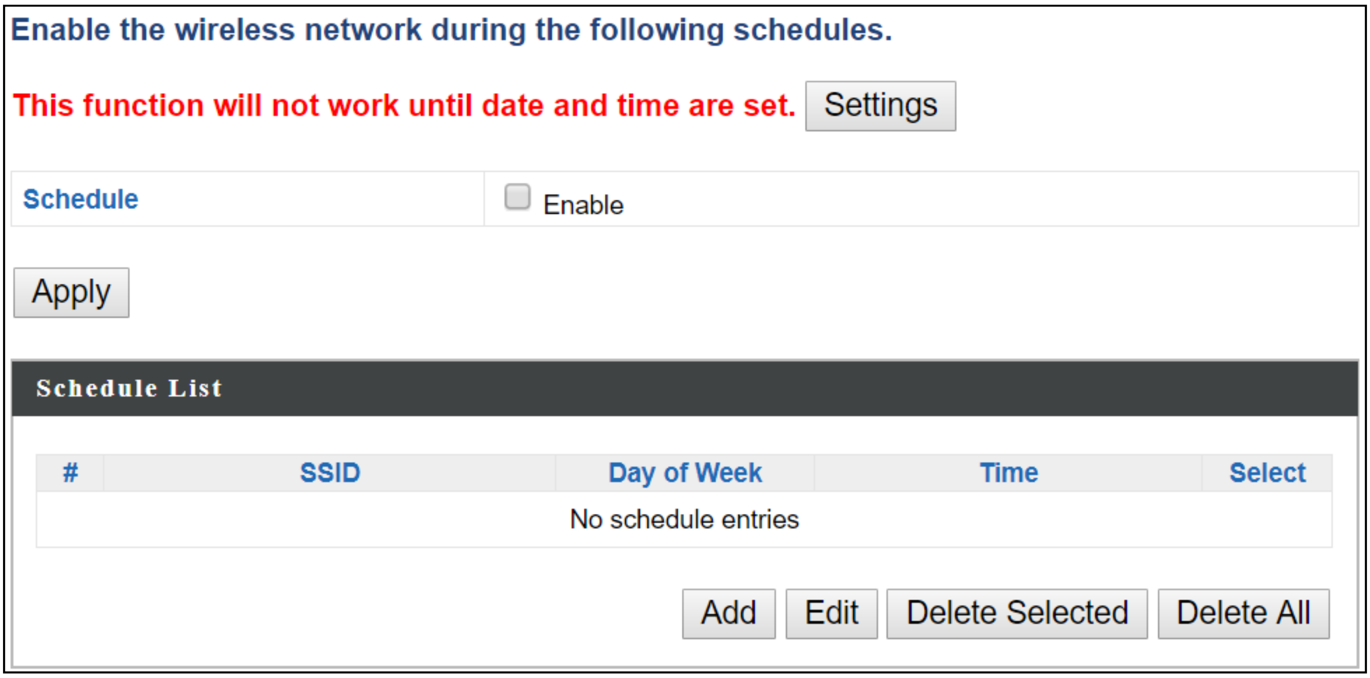
Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can be adjusted further manually:

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.



Enable the wireless network during the following schedules.

This function will not work until date and time are set.

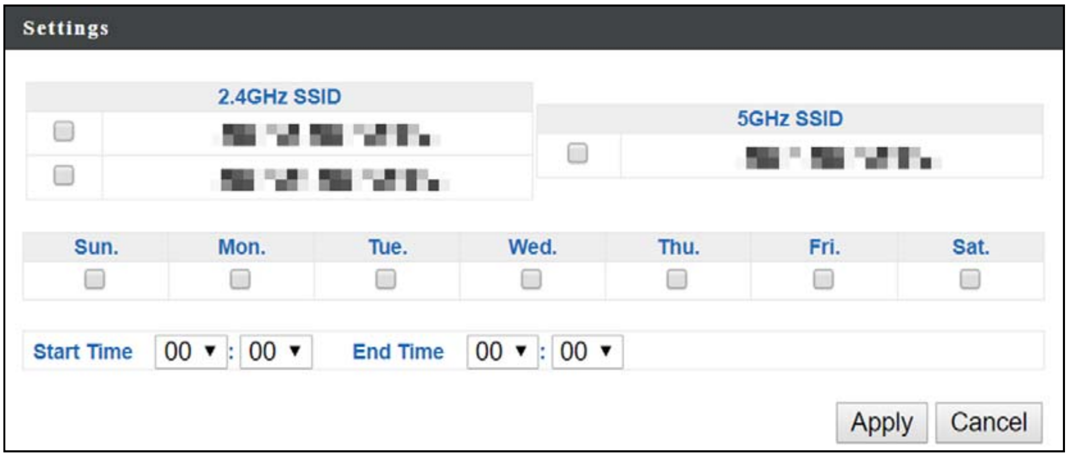
Schedule	□ Enable

Schedule List

#	SSID	Day of Week	Time	Select
No schedule entries				

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.



Settings

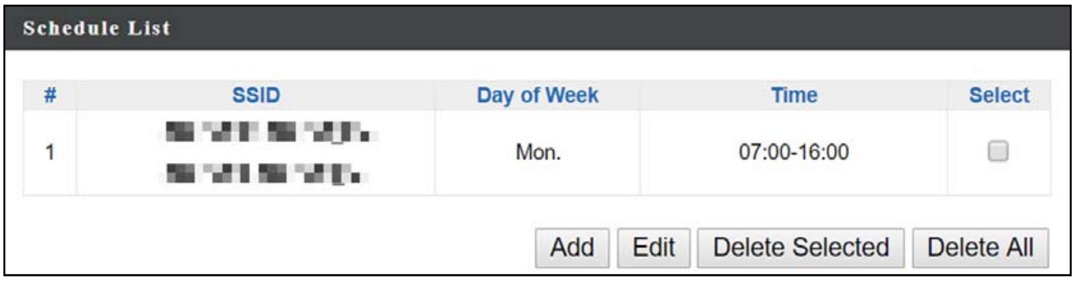
	2.4GHz SSID
□	[redacted]
□	[redacted]

	5GHz SSID
□	[redacted]

Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
□	□	□	□	□	□	□

Start Time 00 ▾ : 00 ▾ End Time 00 ▾ : 00 ▾

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



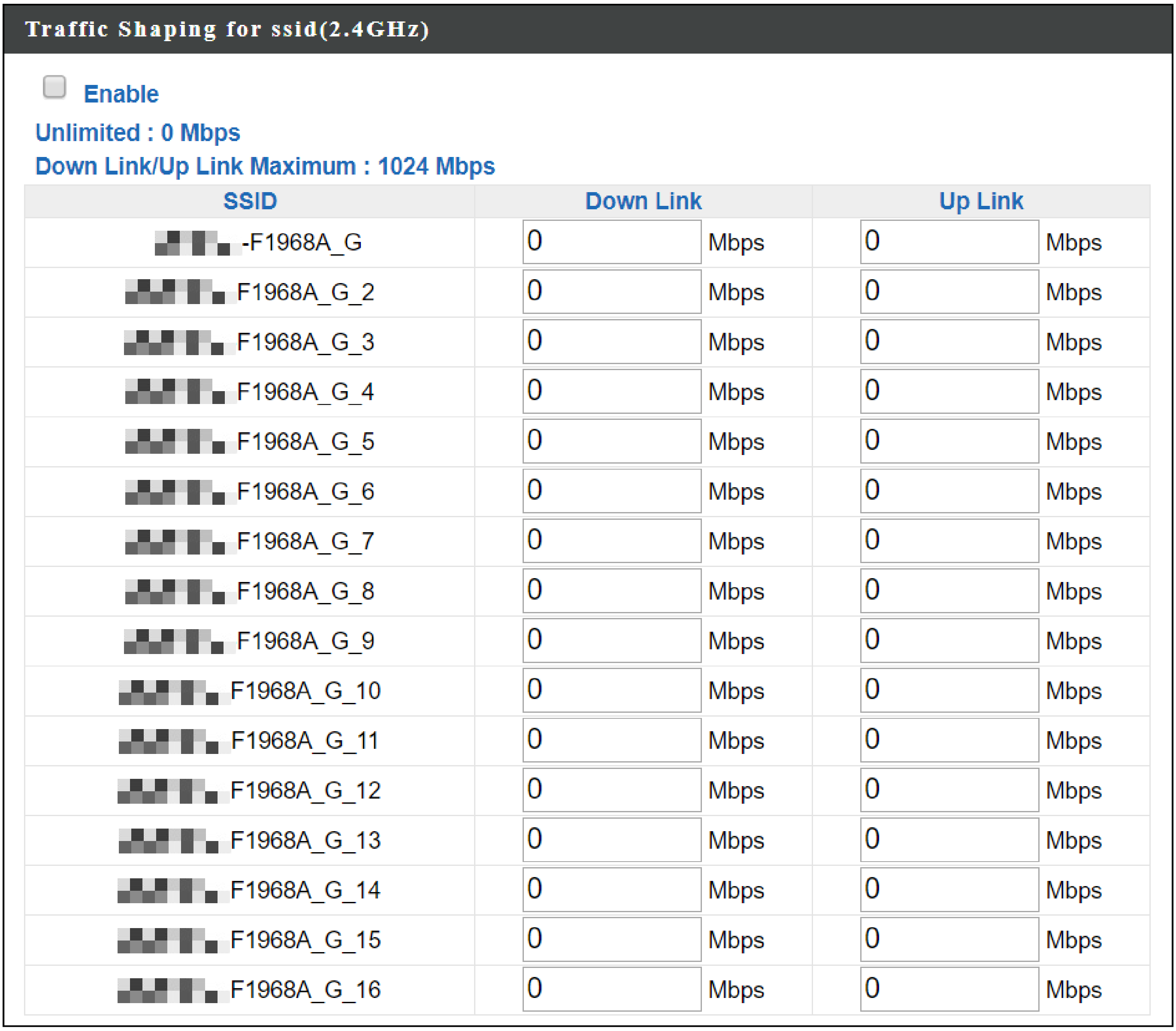
Schedule List

#	SSID	Day of Week	Time	Select
1	[redacted]	Mon.	07:00-16:00	□

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.



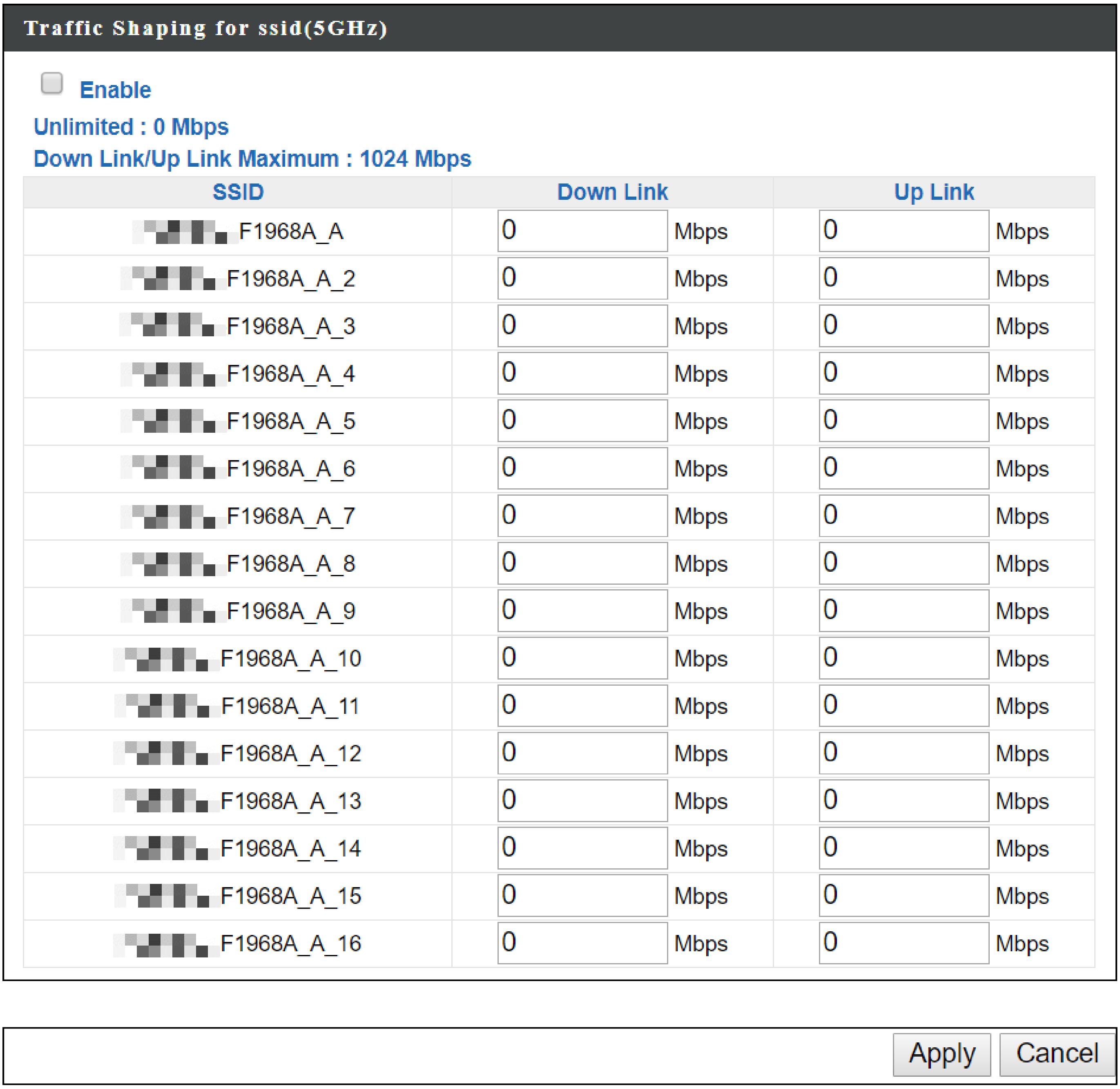
Traffic Shaping for ssid(2.4GHz)

□ 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

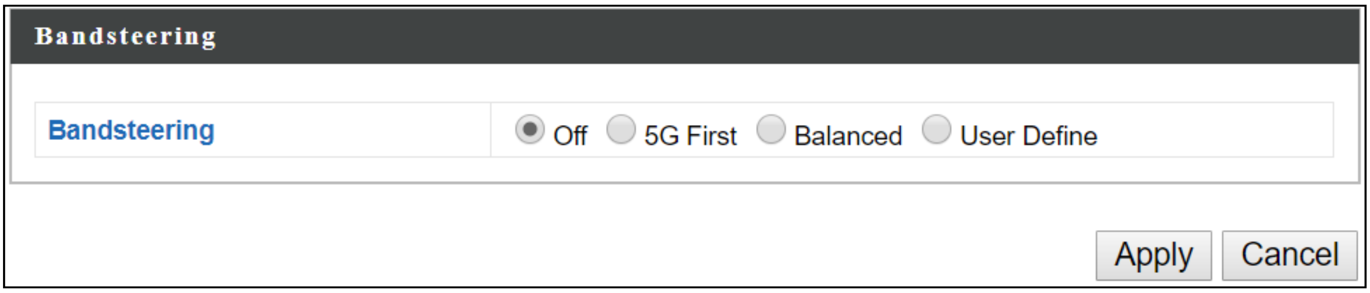
Unlimited : 0 Mbps

Down Link/Up Link Maximum : 1024 Mbps

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

IV-3-9 Bandsteering

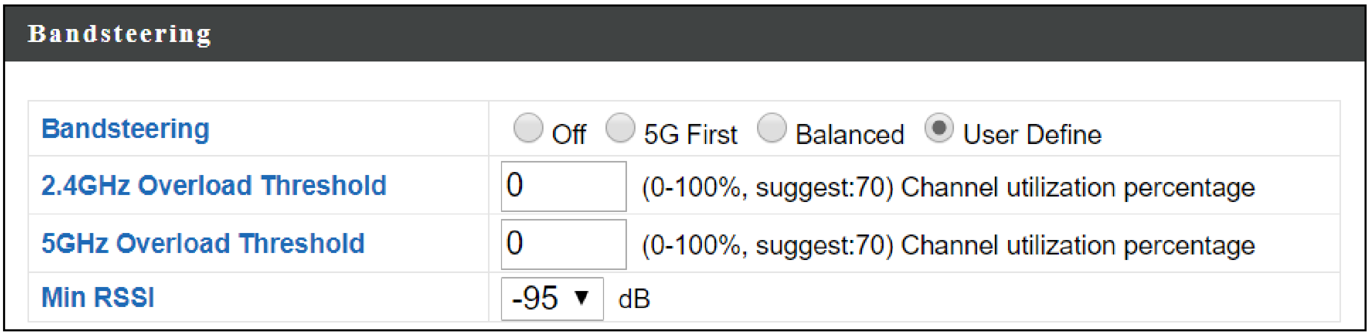
Band steering detects clients capable of 5GHz operation and steers them there to make the more crowded 2.4 GHz band available for clients only capable of connecting to 2.4GHz band. This helps improve end user experience by reducing channel utilization, especially in high density environments.



Bandsteering

Bandsteering	● Off ○ 5G First ○ Balanced ○ User Define

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



Bandsteering

Bandsteering	○ Off ○ 5G First ○ Balanced ● User Define
2.4GHz Overload Threshold	0 (0-100%, suggest:70) Channel utilization percentage
5GHz Overload Threshold	0 (0-100%, suggest:70) Channel utilization percentage
Min RSSI	-95 ▼ dB