CAP1300

User Manual

09-2017 / 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 five different modes.

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

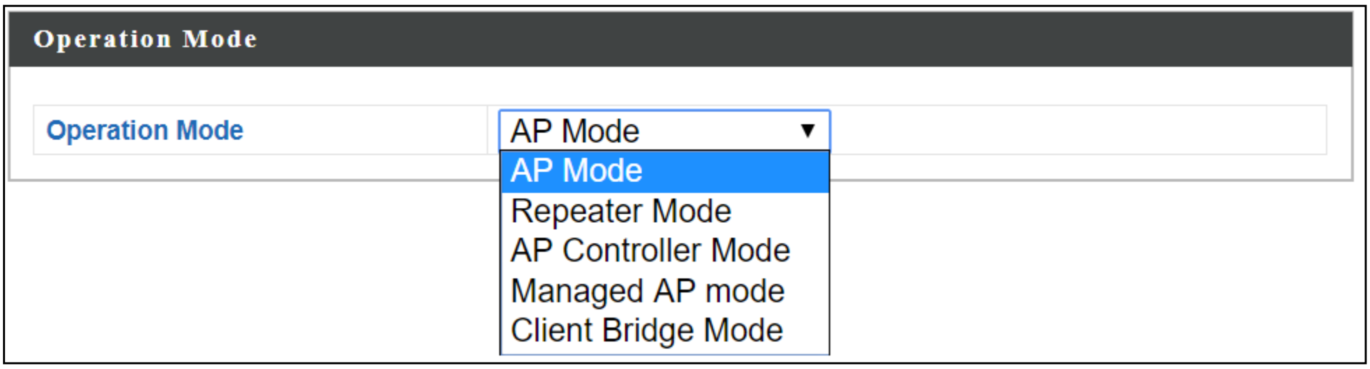
Repeater Mode is a wireless repeater (also called wireless range extender) that takes an existing signal from a wireless router or wireless access point and rebroadcasts it to create a second network.

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

AP Controller Mode acts as the designated master of an AP array (group of linked access points).

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.

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



Operation Mode

Operation Mode: AP Mode

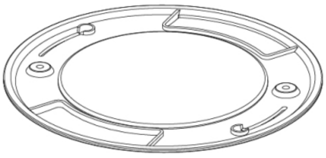
This user manual is mainly split into two parts:

- **AP Mode** (blue) – includes AP / Repeater / Managed AP / Client Bridge Mode settings
- **Edimax Pro NMS** (grey) – includes AP Controller Mode settings

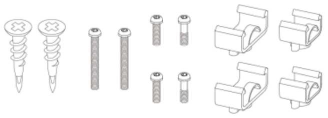
I Product Information

I-1 Package Contents

1



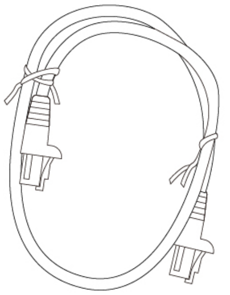
2



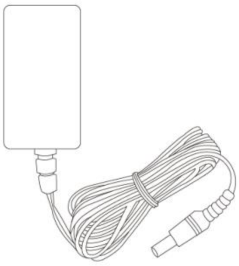
3

4

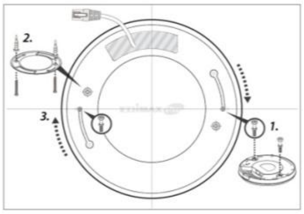
5



6



7



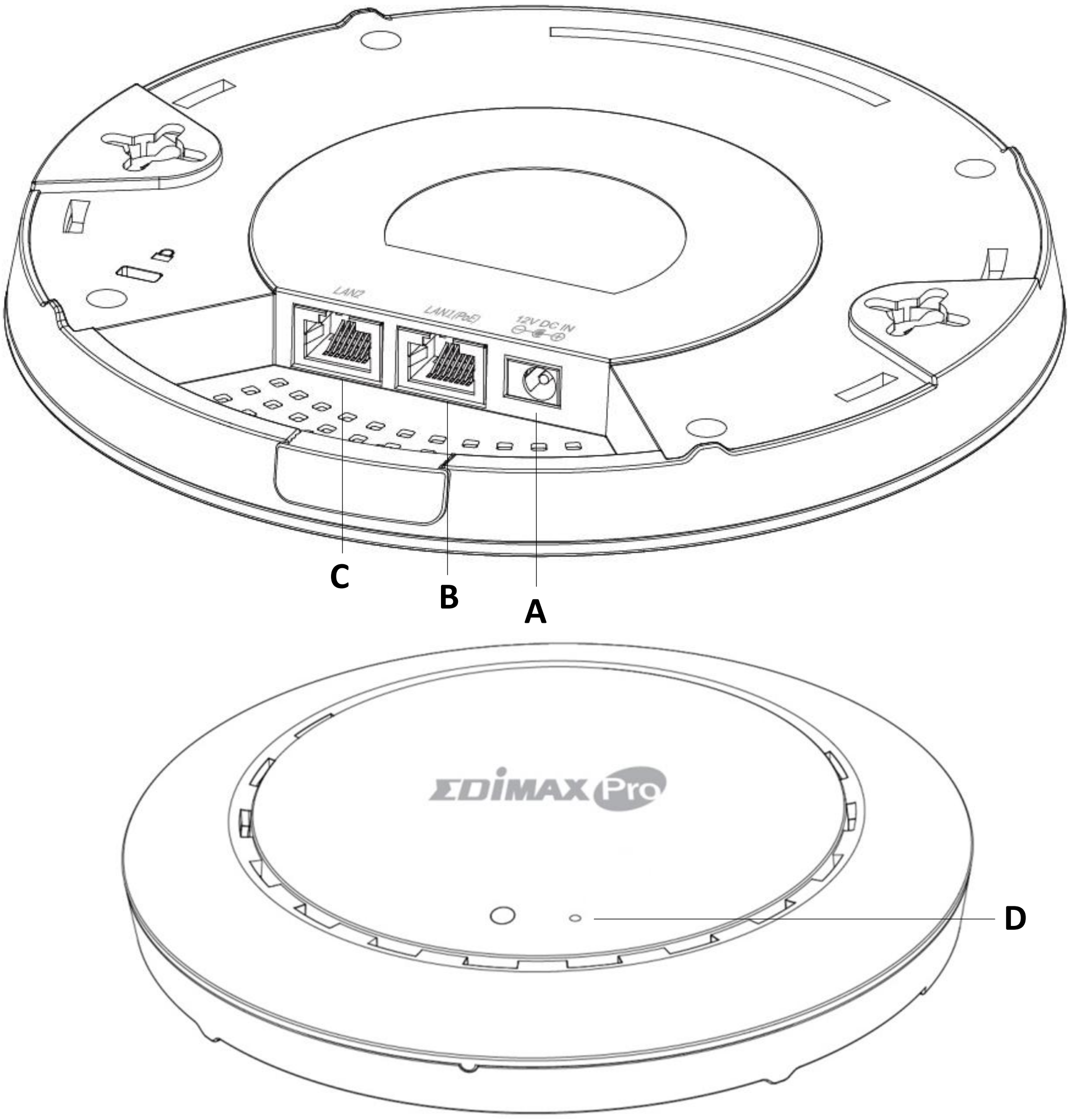
8

1. CAP1300 Access Point
2. Ceiling Mount Bracket
3. T-Rail Mounting Kit & Screws
4. CD
5. Quick Installation Guide
6. Ethernet Cable
7. Power Adapter
8. Ceiling Mount Screw Template

I-2 System Requirements

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

I-3 Hardware Overview



A	12V DC IN	12V DC port to connect the power adapter
B	LAN 1 (PoE)	LAN port with Power over Ethernet (PoE) IN
C	LAN 2	LAN port
D	Reset	Reset the device to factory default settings

I-4 LED Status

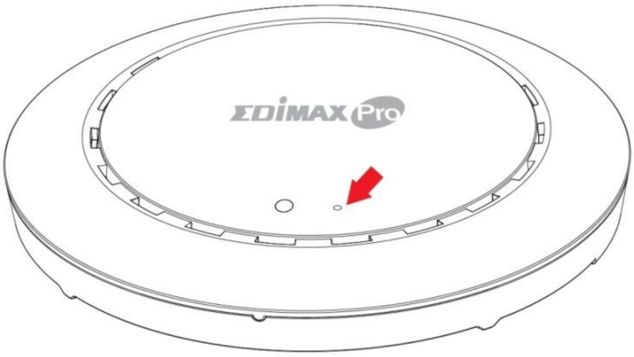
LED Color	LED Status	Description
Blue	On	The device is on.
	Flashing Slowly	Upgrading firmware.
	Flashing Quickly	Resetting to factory defaults.
Amber	On	Starting up.
	Flashing	Error.
Off	Off	The device is off.

I-5 Reset

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

1. Press and hold the reset button on the device 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 device to restart. The device is ready for setup when the LED is blue.

I-6 Safety Information

In order to ensure the safe operation of the device and its users, please read and act in accordance with the following safety instructions.

1. The device is designed for indoor use only; do not place it outdoor.

2. Do not place the device in or near hot/humid places, such as in a kitchen or a bathroom.

3. Do not pull any connected cable with force; carefully disconnect it from the device.

4. Handle the device with care. Accidental damage will void the warranty of the device.

5. The device contains small parts which are a danger to small children under 3 years old. Please keep it out of reach of children.

6. Do not place the device on paper, cloth, or other flammable materials. The device may become hot during use.

7. There are no user-serviceable parts inside the device. If you experience problems with it, please contact your dealer of purchase and ask for help.

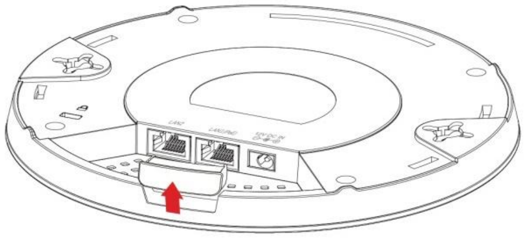
8. The device is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.

9. If smoke is visible or an obvious burning smell is coming from the device or the power adapter, disconnect the device and power adapter immediately as far as it is safe to do so. Call your dealer of purchase for help.

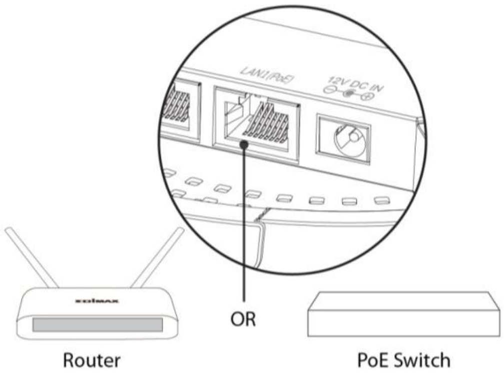
II Hardware Installation

II-1 Router/PoE Switch

1. If you need to, remove the cap from the underside of the device. This creates extra space for your cables to pass through.



2. Connect a router or a PoE switch to the device's **LAN 1** port using an Ethernet cable.

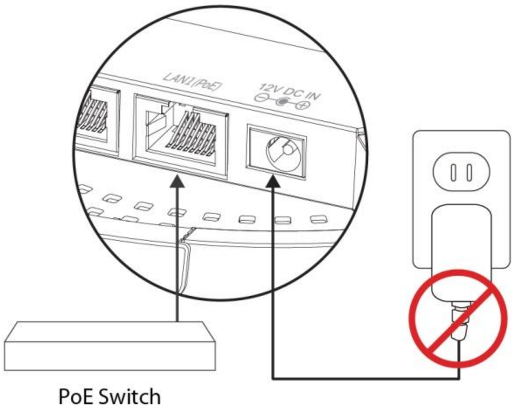


3. Power up the device:

a) If router is used, connect the power adapter to the device's 12V DC port and plug the power adapter into a power supply; or

b) If PoE (Power over Ethernet) switch is used, make sure the Ethernet cable is connected to **LAN1** port from the switch. The device will be powered by the PoE switch.

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



4. Connect a local network client or switch to the device's **LAN 2** port as required.

II-2 Mounting

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

II-2-1 Wooden Ceiling

Please refer to the figure below:

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

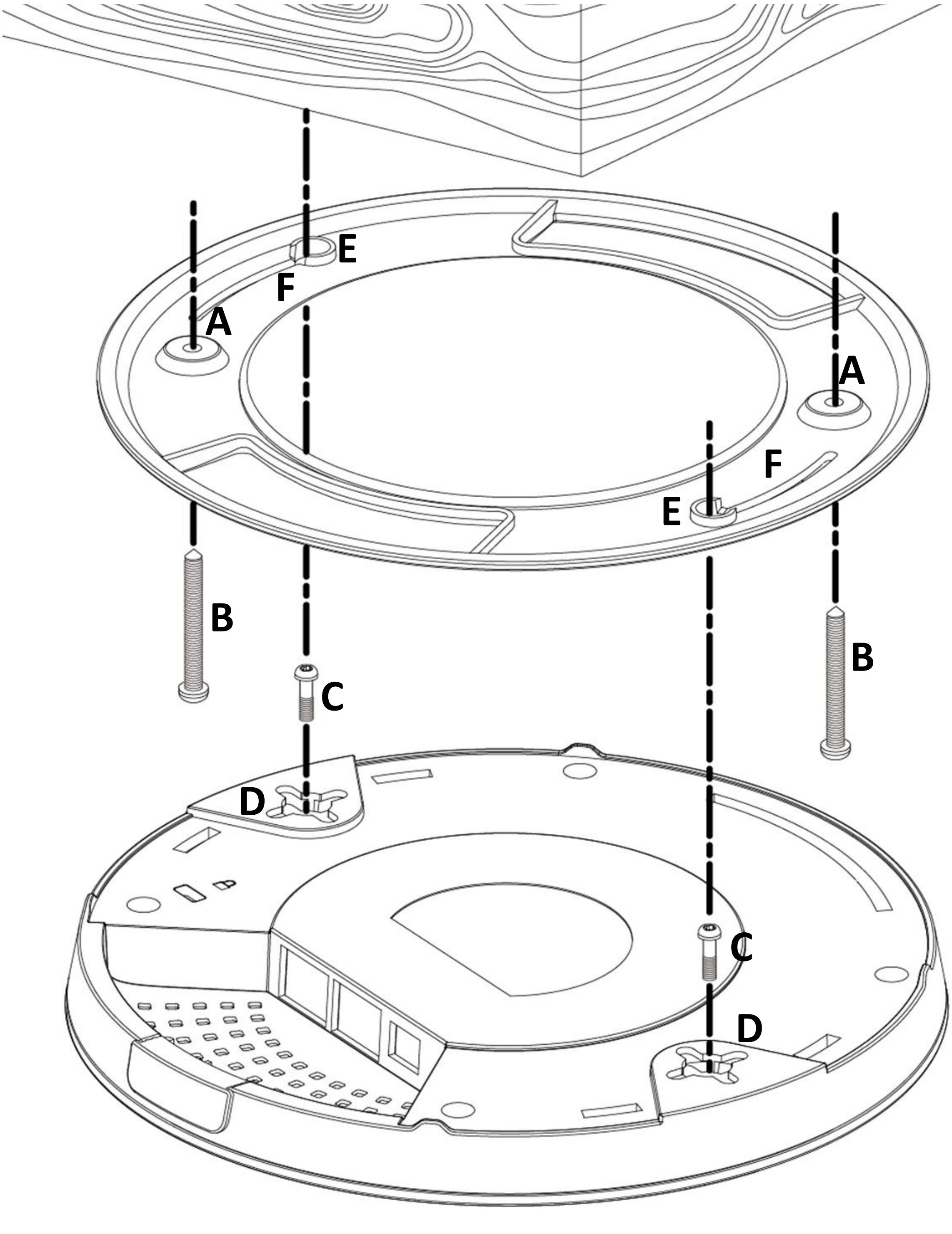
2. Where necessary, drill a hole (of radius smaller than the radius of the provided screws) on each of the marked screw positions.

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

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

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

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


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

II-2-2 Other Ceiling

Please refer to the figure below:

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

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

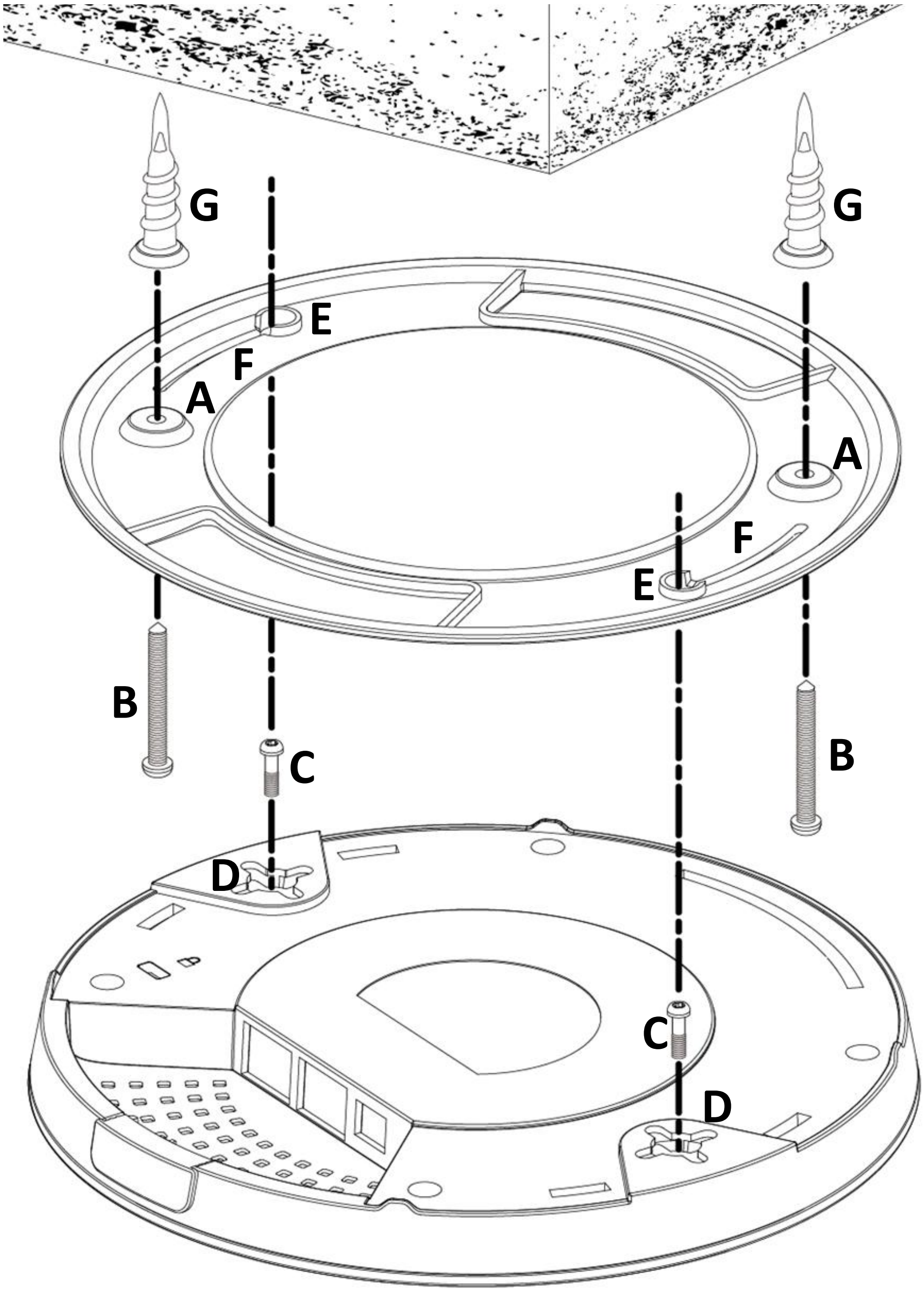
3. Insert the anchors **G** into the holes (use a screw driver where necessary) at the marked screw positions.

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

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

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

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


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

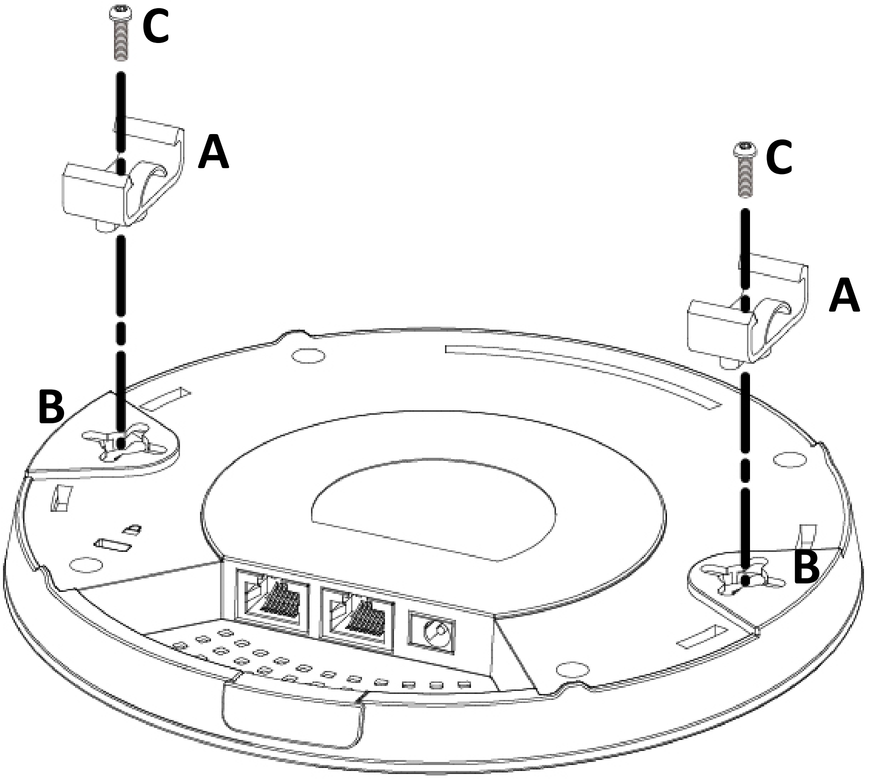
II-2-3 T-Rail Mount

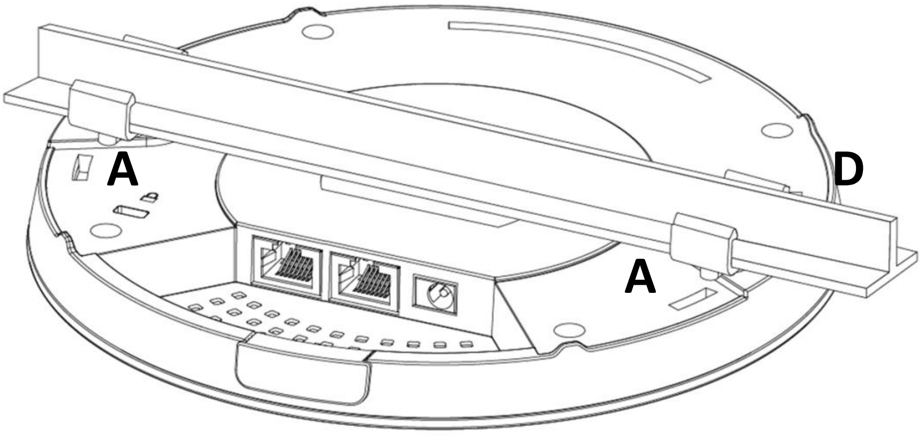
To mount the device to a T-Rail, please follow the instructions below and refer to the diagrams below.

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

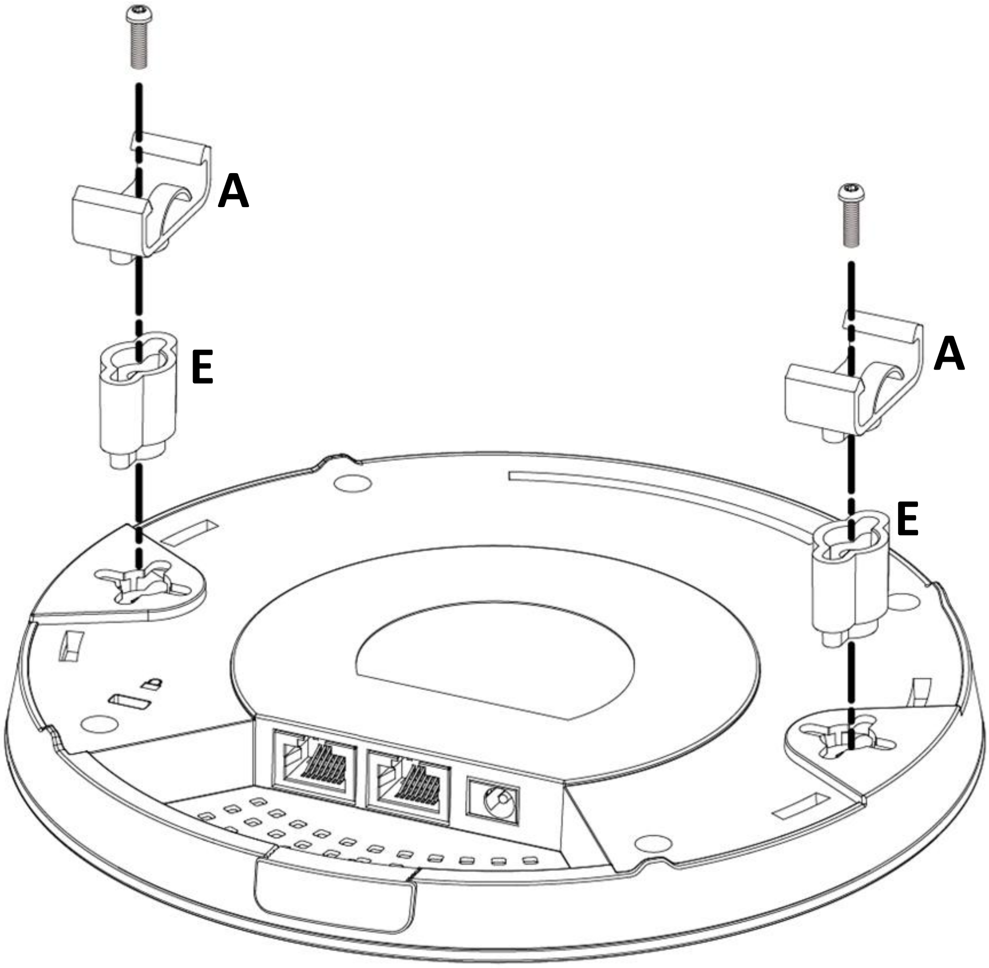
2. Attach the selected T-Rail brackets **A** to holes **B** using bracket fixing screws **C**.

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





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



III Quick Setup & Mode Selection

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

Follow the quick setup below before selecting the desired operation mode. For *AP Controller Mode*, please refer to ***VIII Quick Setup - NMS***.

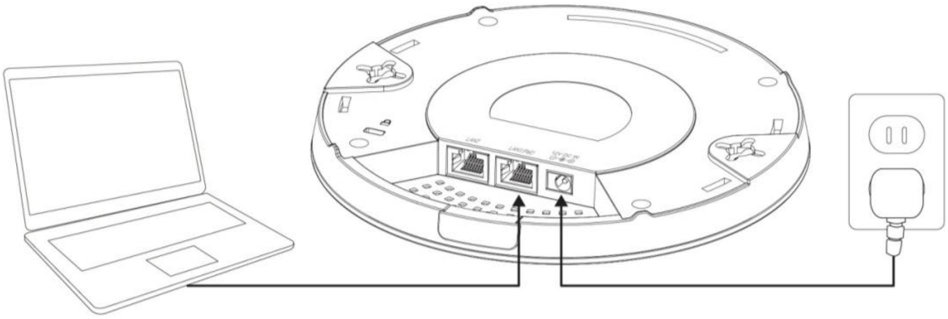
III-1 Default Mode: Access Point Mode

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 ***XI-1***.

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

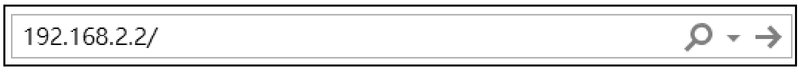
2. Connect the device to a computer via Ethernet cable.

3. Connect the power adapter to the device's 12V DC port and plug the power adapter into a power supply.



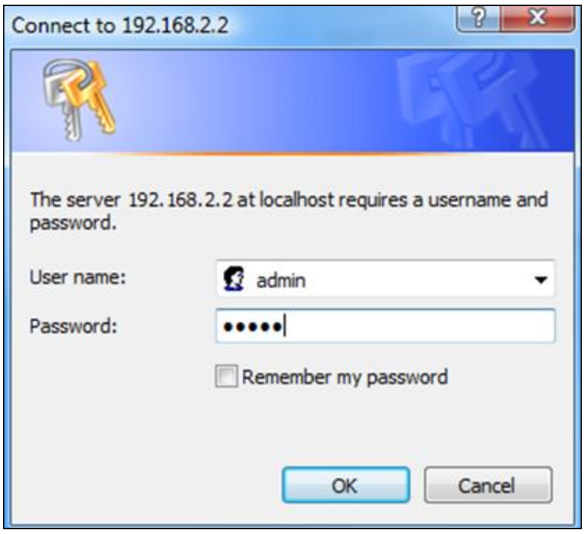
4. Please wait a moment for the device to start up. The device is ready when the LED is **blue**.

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

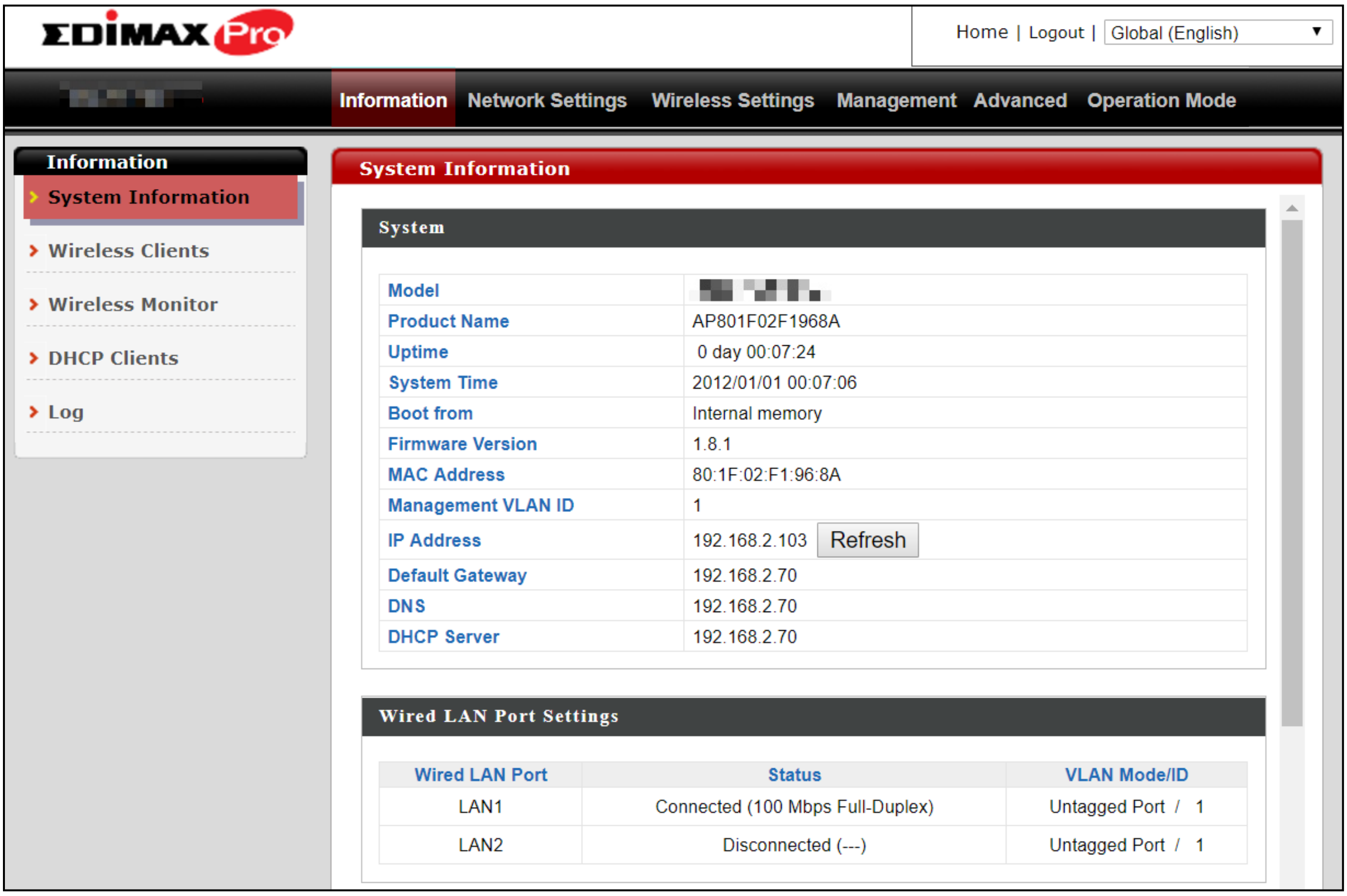
The server 192.168.2.2 at localhost requires a username and password.

User name: admin

Password: •••••

□ Remember my password

7. “System Information” home screen will be shown:



System Information

System

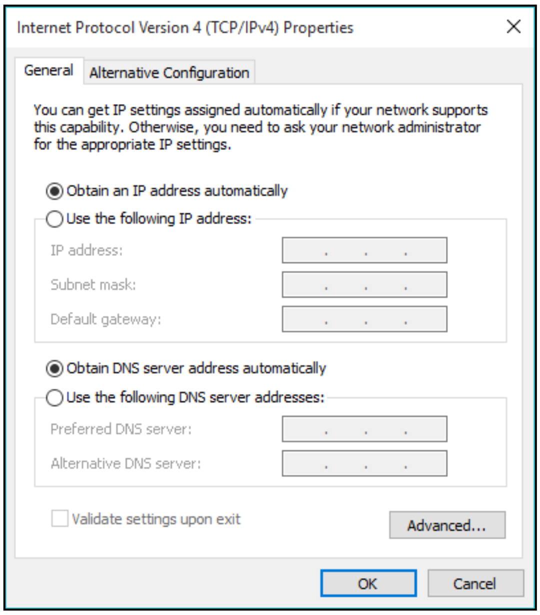
Model	[redacted]
Product Name	AP801F02F1968A
Uptime	0 day 00:07:24
System Time	2012/01/01 00:07:06
Boot from	Internal memory
Firmware Version	1.8.1
MAC Address	80:1F:02:F1:96:8A
Management VLAN ID	1
IP Address	192.168.2.103 Refresh
Default Gateway	192.168.2.70
DNS	192.168.2.70
DHCP Server	192.168.2.70

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

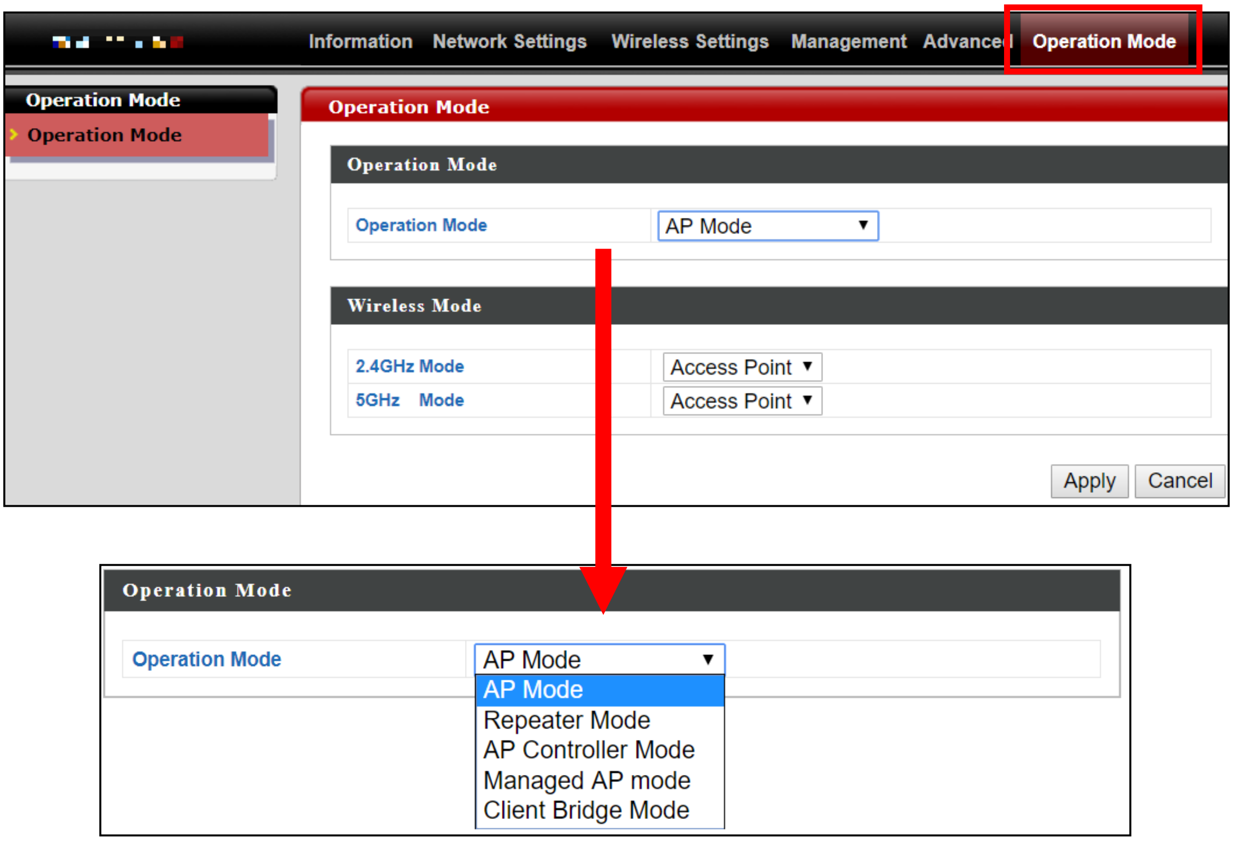
○ Use the following DNS server addresses:

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” 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

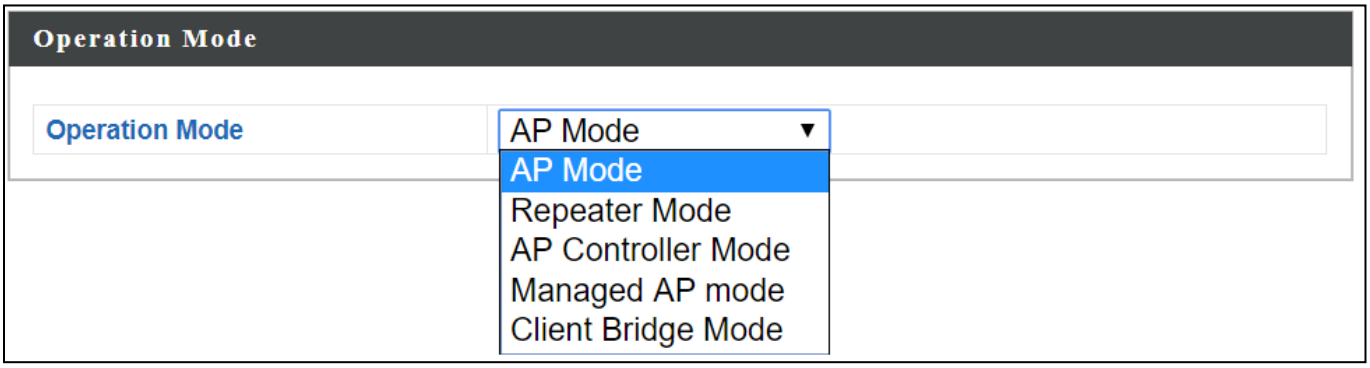
Operation Mode

Operation Mode: AP Mode

III-2 Repeater Mode

From the quick setup above,

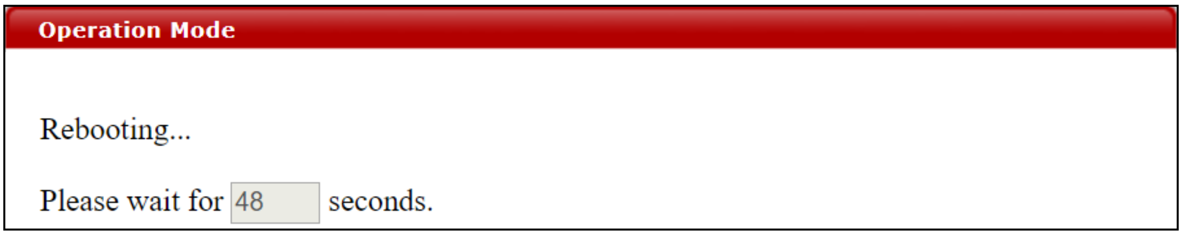
1. Select **Repeater Mode** from the operation mode drop down menu:



Operation Mode

Operation Mode: AP Mode

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

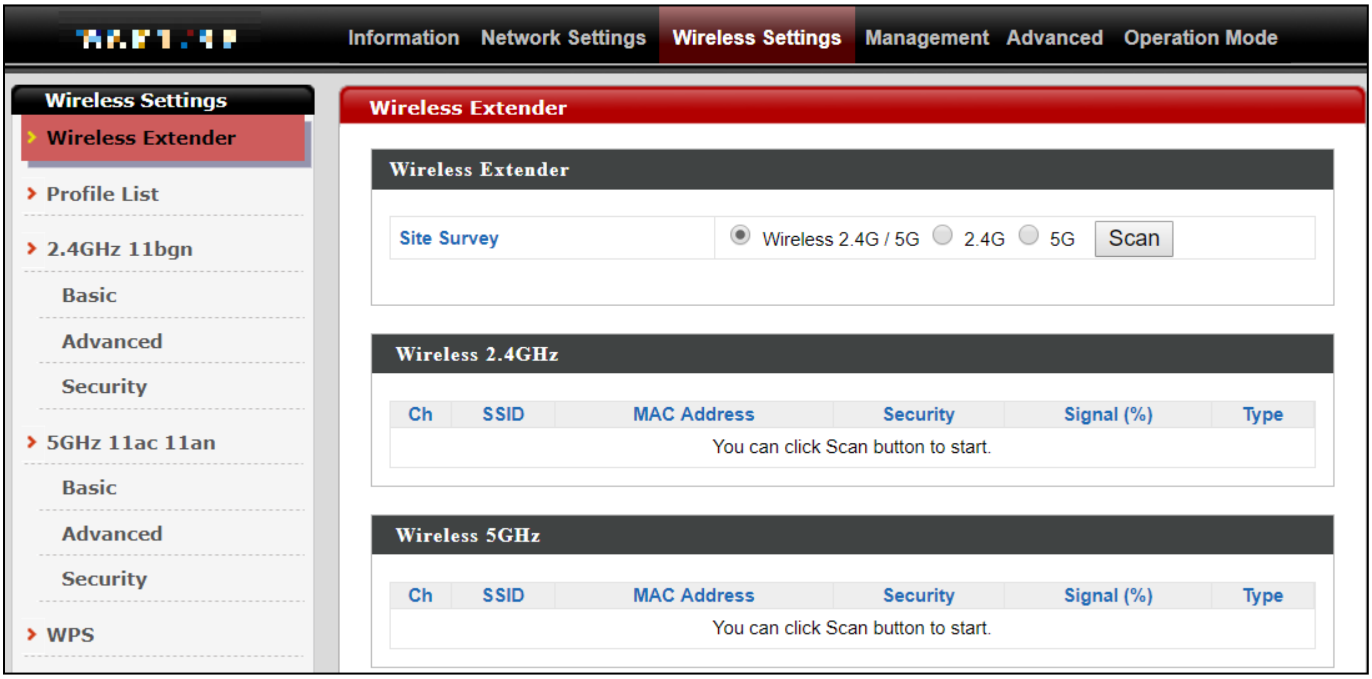


Operation Mode

Rebooting...

Please wait for 48 seconds.

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



Wireless Extender

Wireless Extender

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

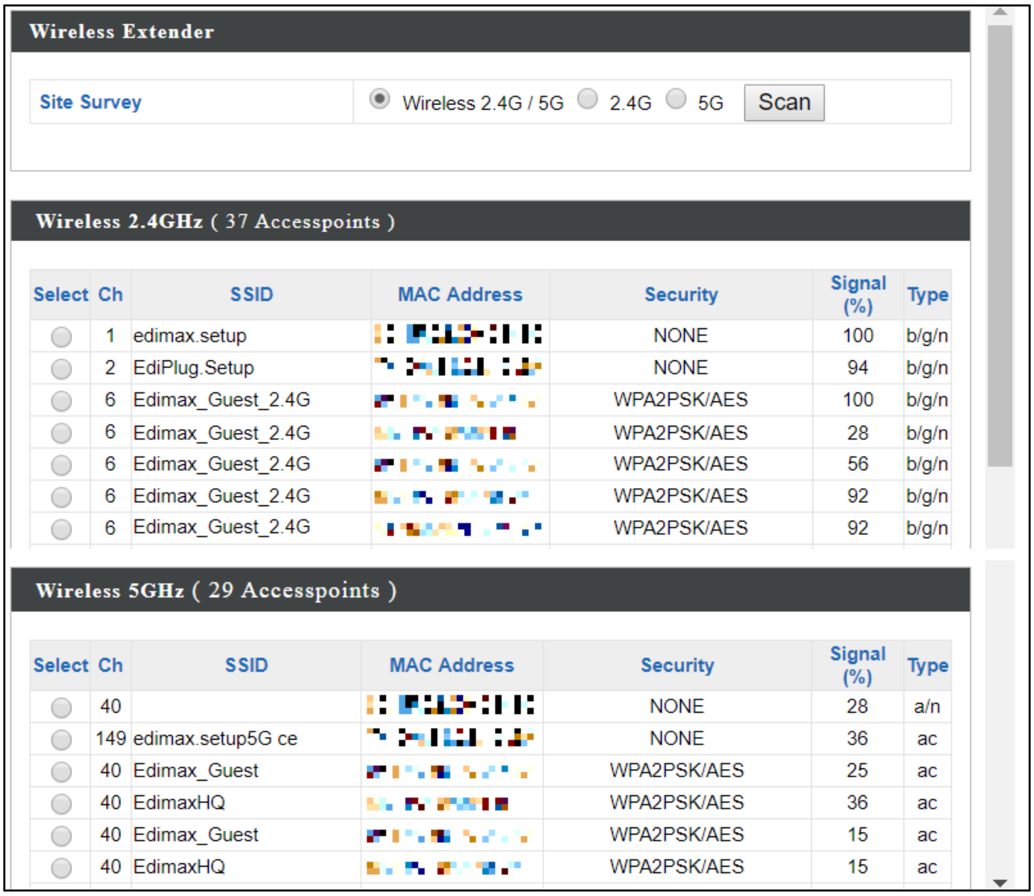
Wireless 2.4GHz

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]

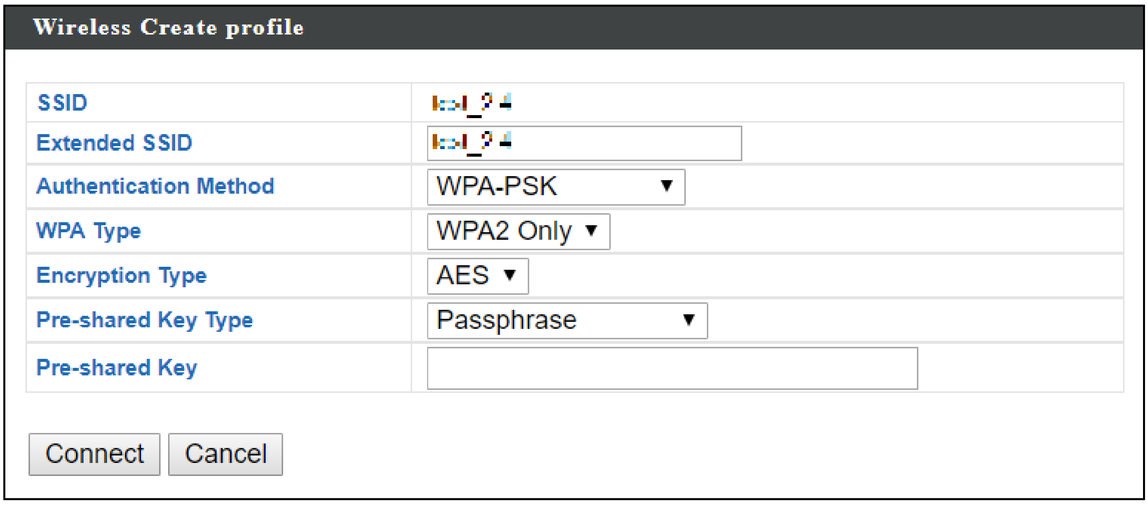
Wireless 2.4GHz (37 Accesspoints)

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.

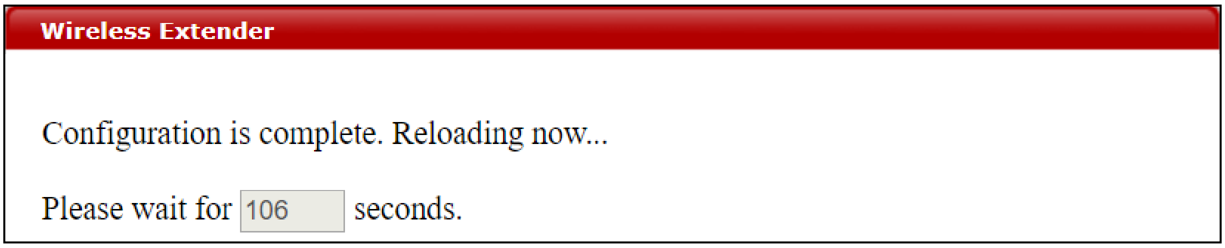


Wireless Create profile

SSID	[redacted]
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:

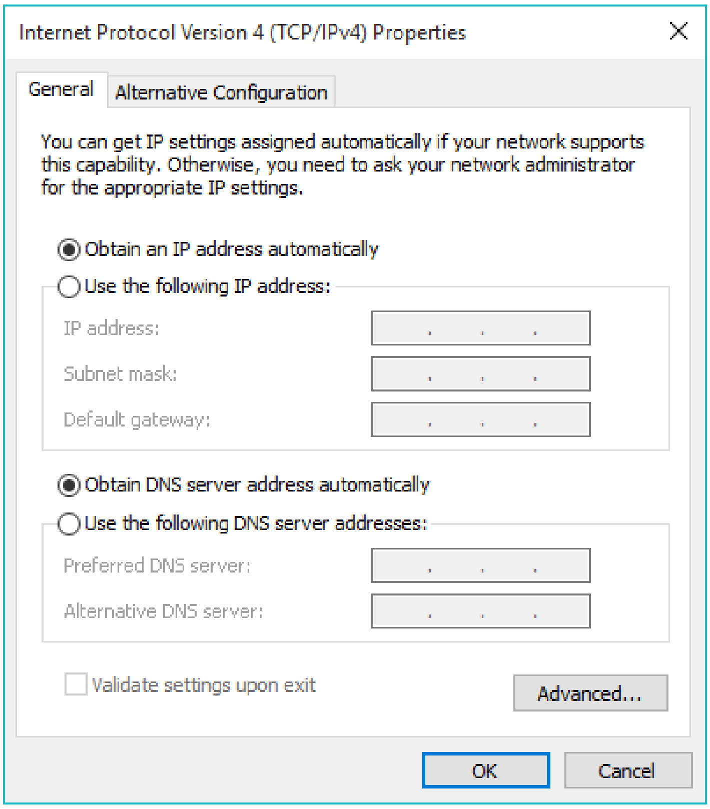


Wireless Extender

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

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

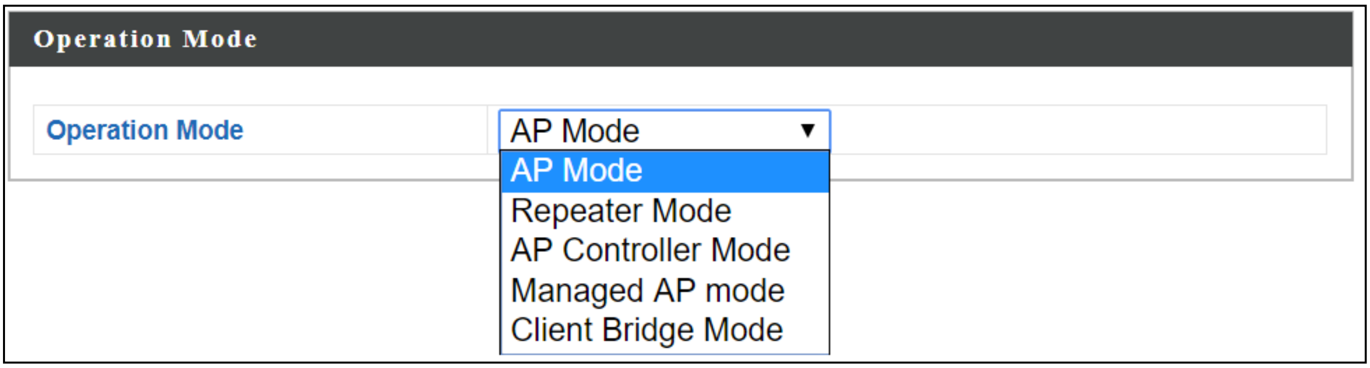
8. To access the web user interface, check your router/root AP's settings to determine the device's new IP address. Enter the new IP address into the browser for the web user interface.

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

III-3 Client Bridge Mode

From the quick setup above,

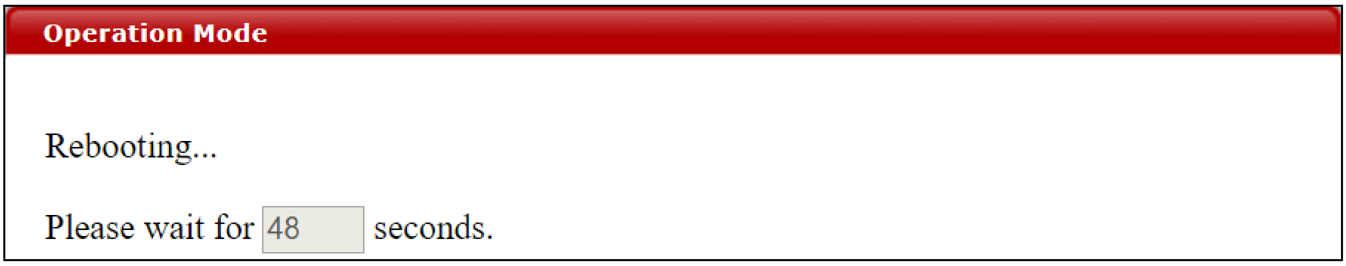
1. Select **Client Bridge Mode** from the operation mode drop down menu:



Operation Mode

Operation Mode: AP Mode ▼

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

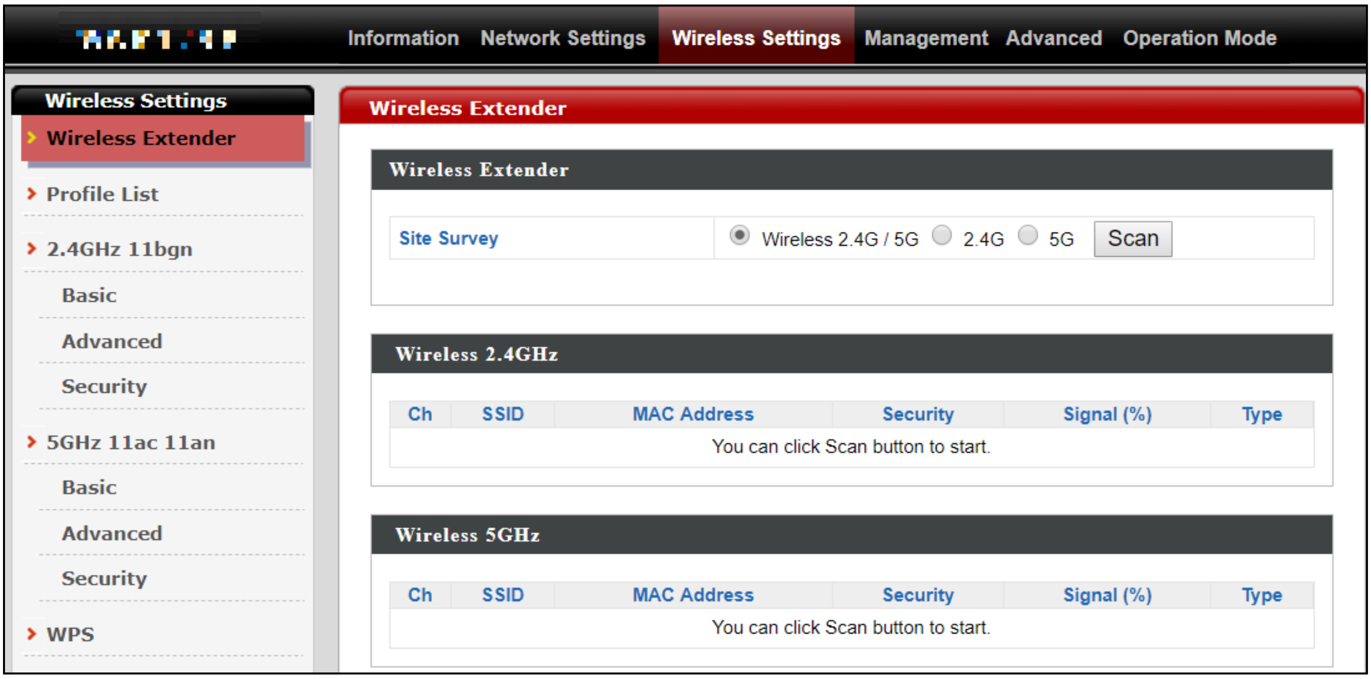


Operation Mode

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

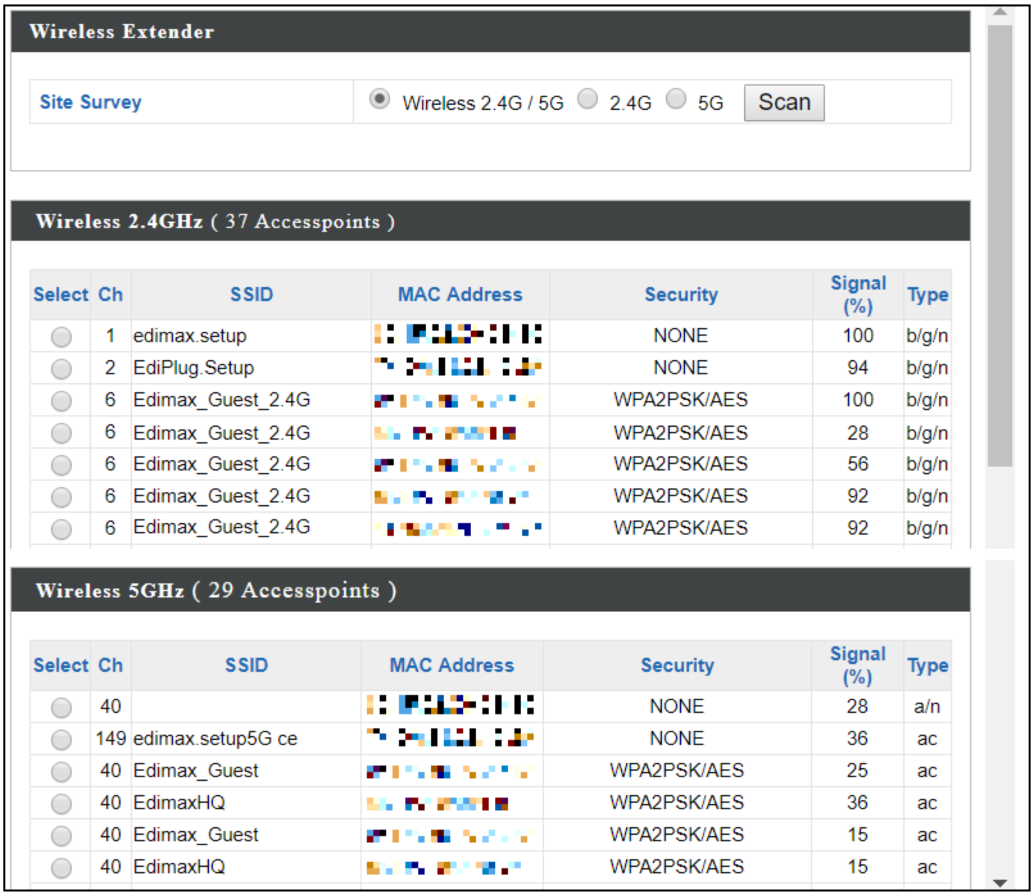
Wireless 2.4GHz

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]

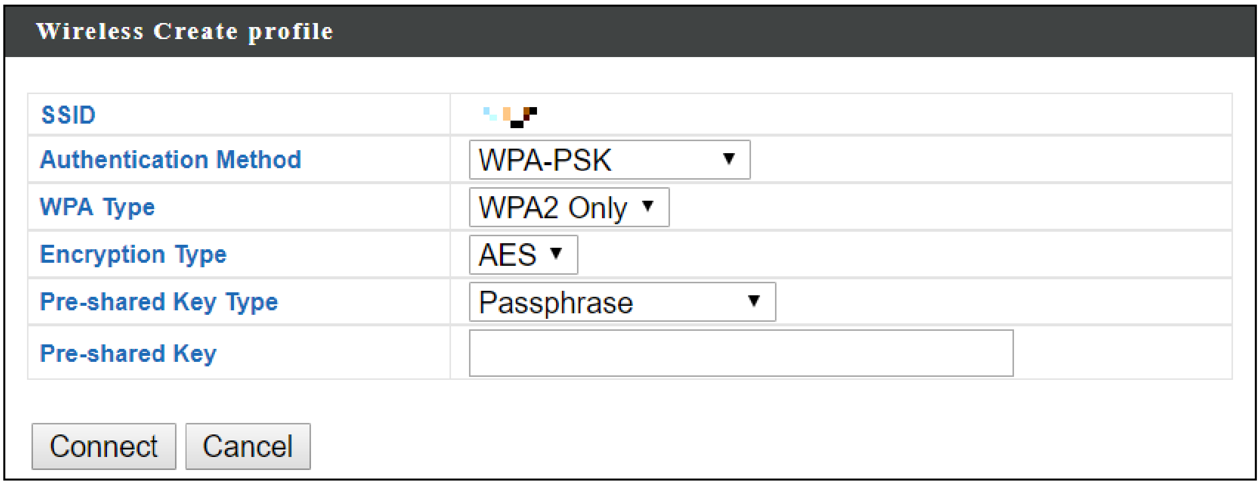
Wireless 2.4GHz (37 Accesspoints)

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.

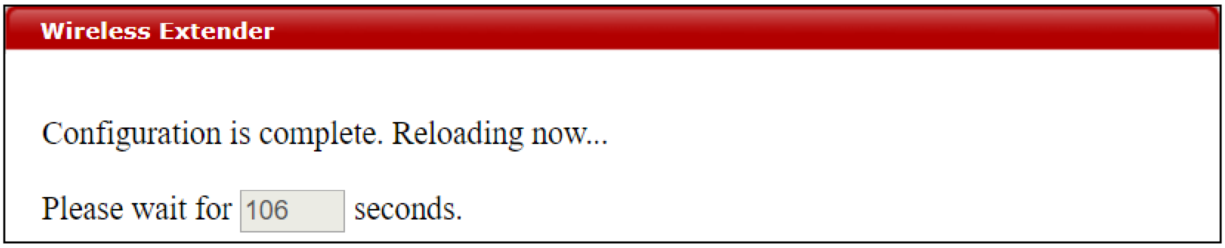


Wireless Create profile

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:

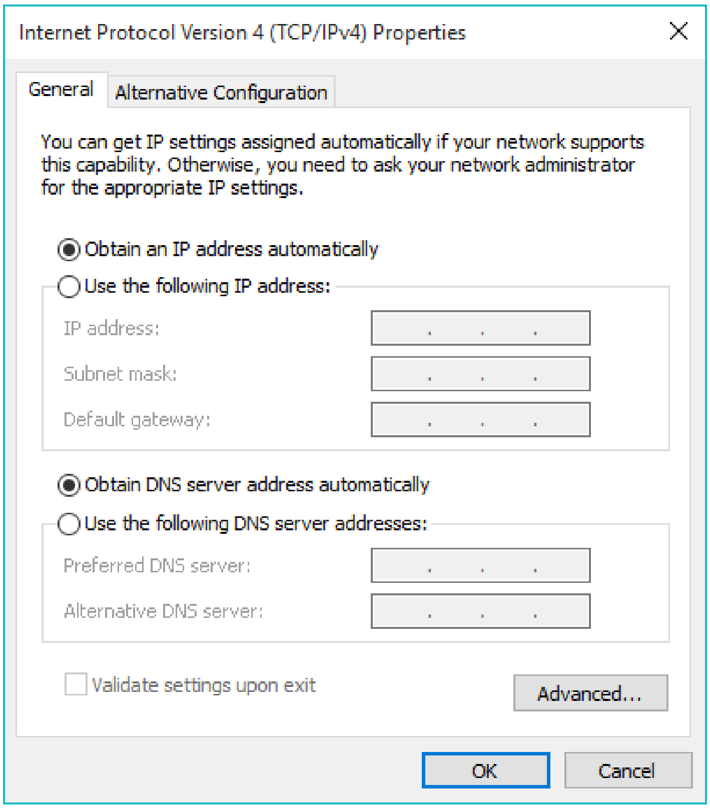


Wireless Extender

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

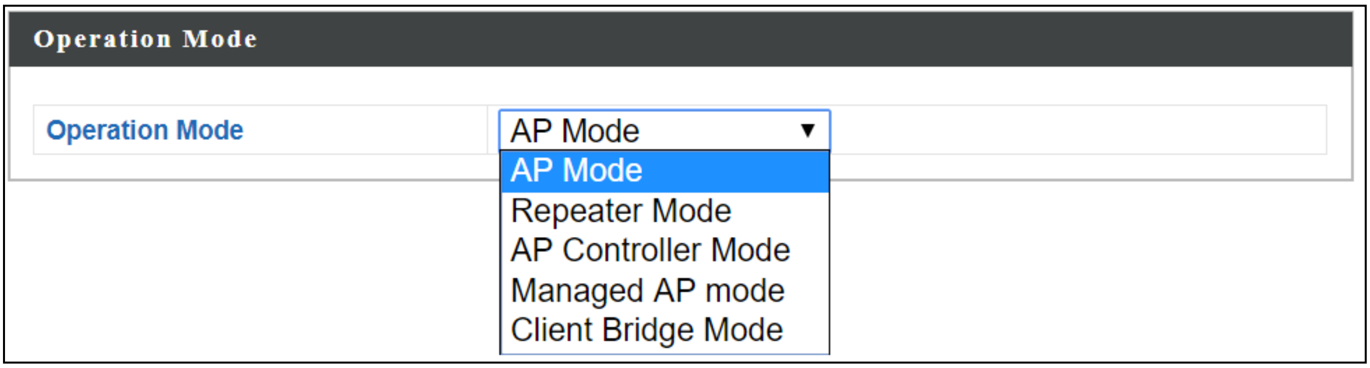
8. To access the web user interface, check your router/root AP's settings to determine the device's new IP address. Enter the new IP address into the browser for the web user interface.

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

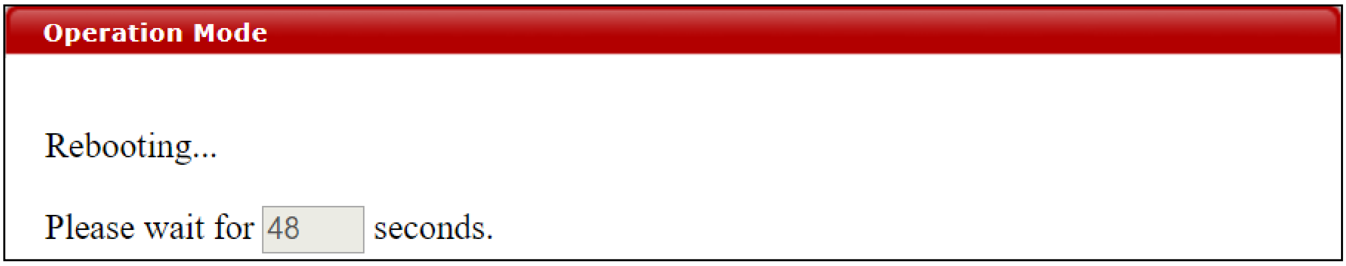
III-4 Managed AP Mode

From the quick setup above,

1. Select **Managed AP Mode** from the operation mode drop down menu:



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



Rebooting...

Please wait for 48 seconds.

For use a Managed AP in an AP array, the access point will automatically switch mode when an AP Controller is configured in the network.

AP, Managed AP, Repeater & Client Bridge Modes

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

Please refer to ***Edimax Pro NMS*** section for AP Controller Mode setting.
For operation mode selection, please follow the quick setup in ***III Quick Setup & Mode Selection***.

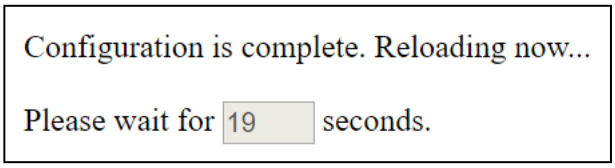
IV Basic Settings

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:



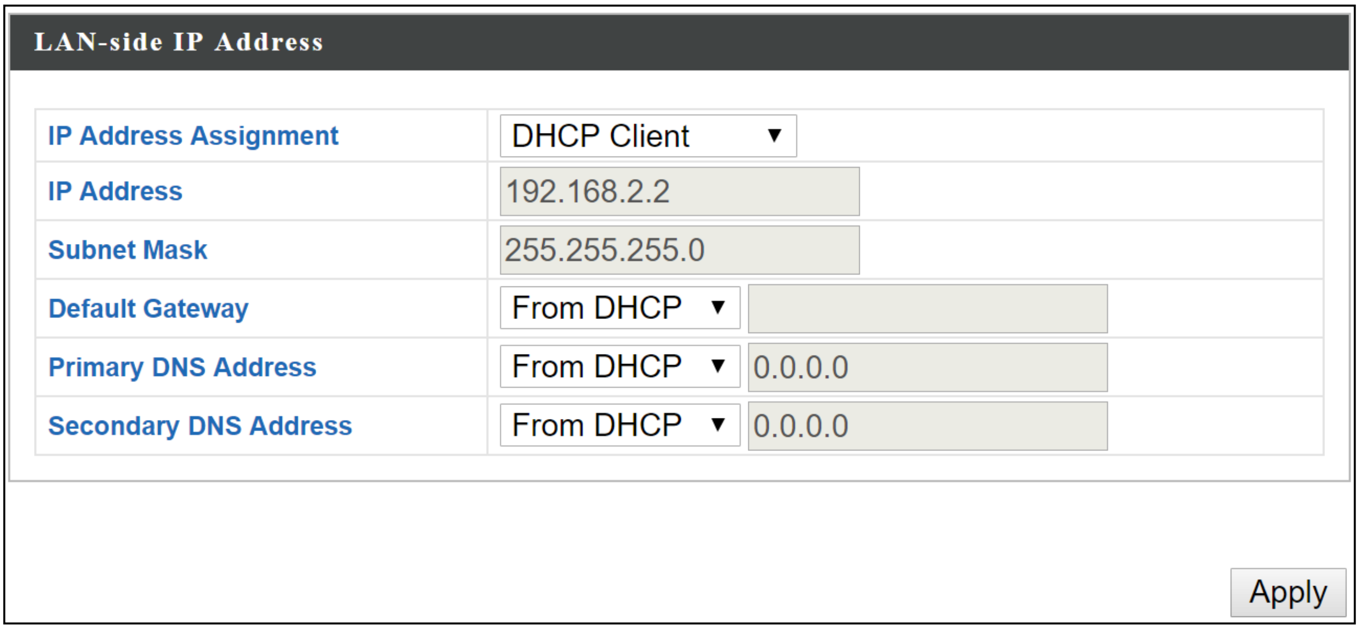
Configuration is complete. Reloading now...

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

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

If you are unable to configure any settings here, please make sure the operation mode of the Access Point is in "AP Mode". Please refer to *VI-6 Operation Mode* ***for more information.***

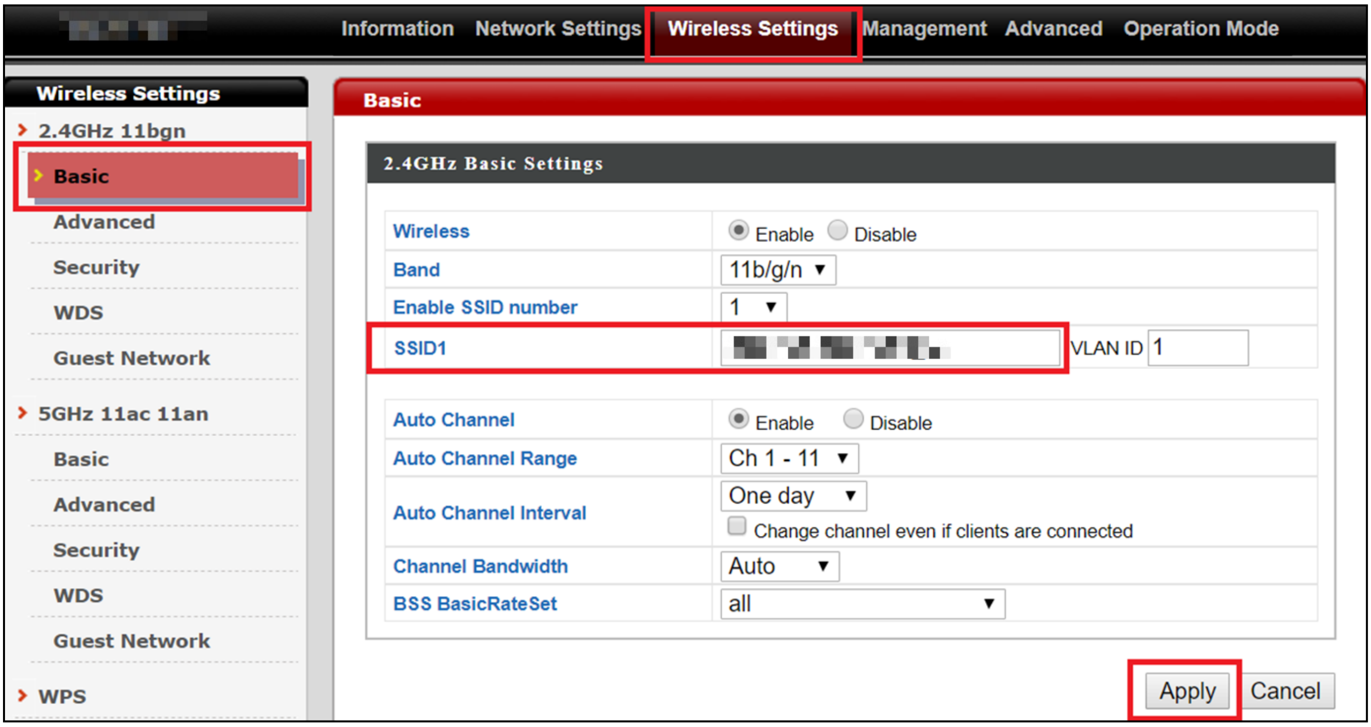
2. Enter the IP address settings you wish to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click "Apply" to save the changes and wait a few moments for the access point to reload.

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

Changing SSID for 2.4GHz wireless network

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

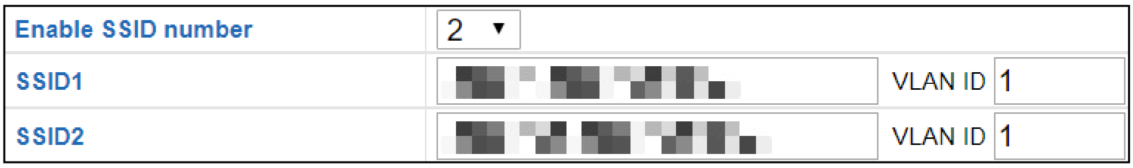
2. Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".



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".***

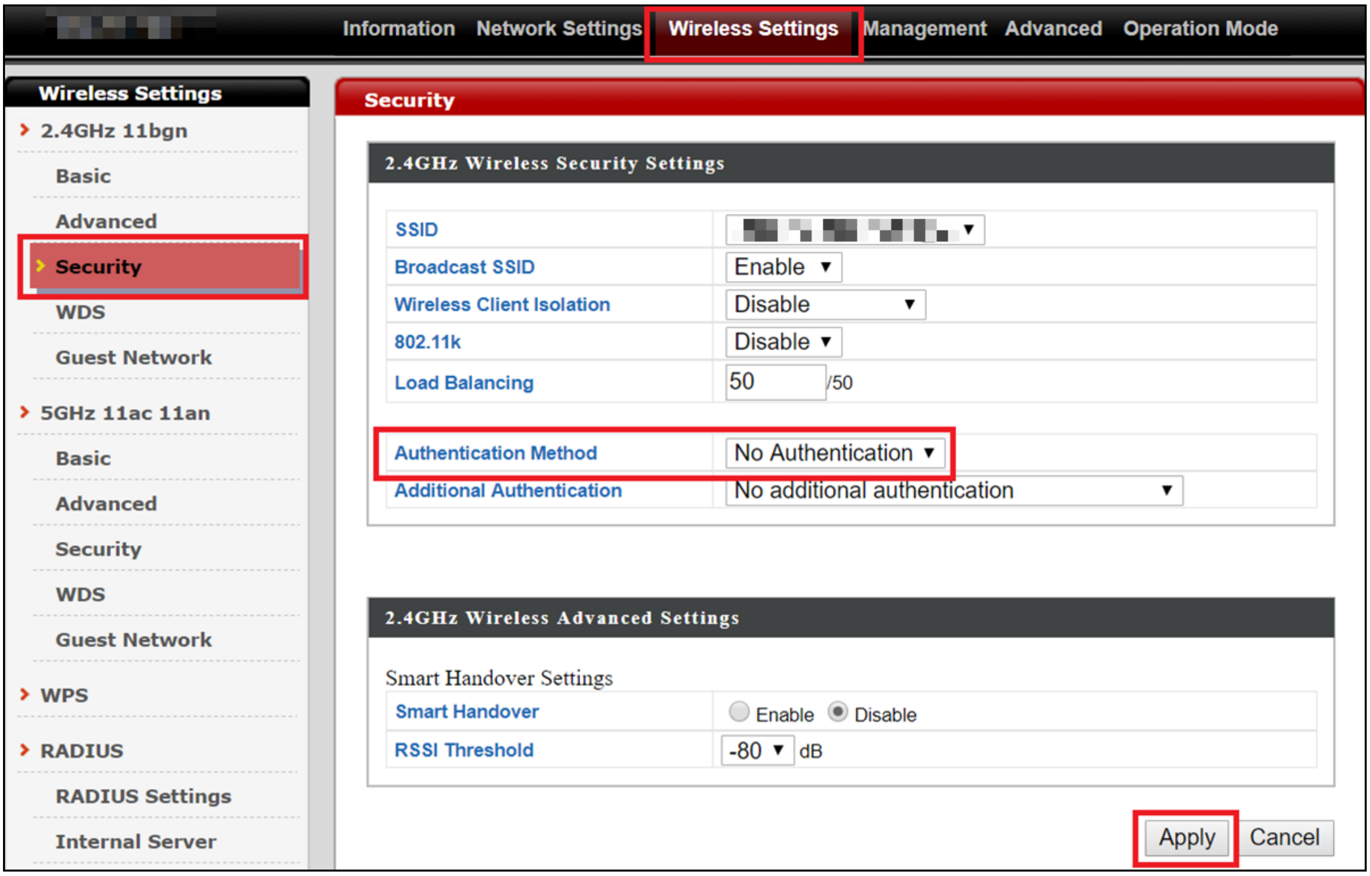


Enable SSID number	2 ▼		
SSID1	[redacted]	VLAN ID	1
SSID2	[redacted]	VLAN ID	1

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 ▾

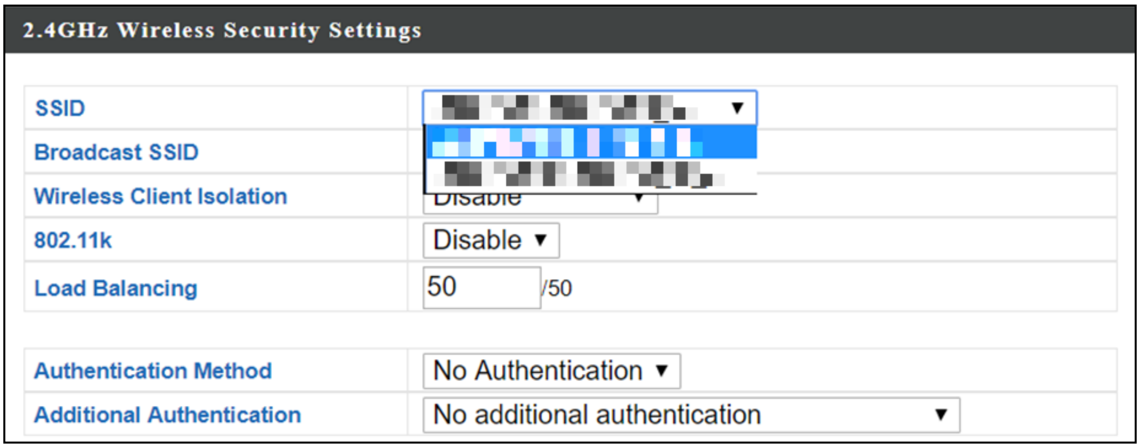
2.4GHz Wireless Advanced Settings

Smart Handover Settings

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

For more information on authentication method, please refer to VI-3-3-3 on page 65.

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



2.4GHz Wireless Security Settings

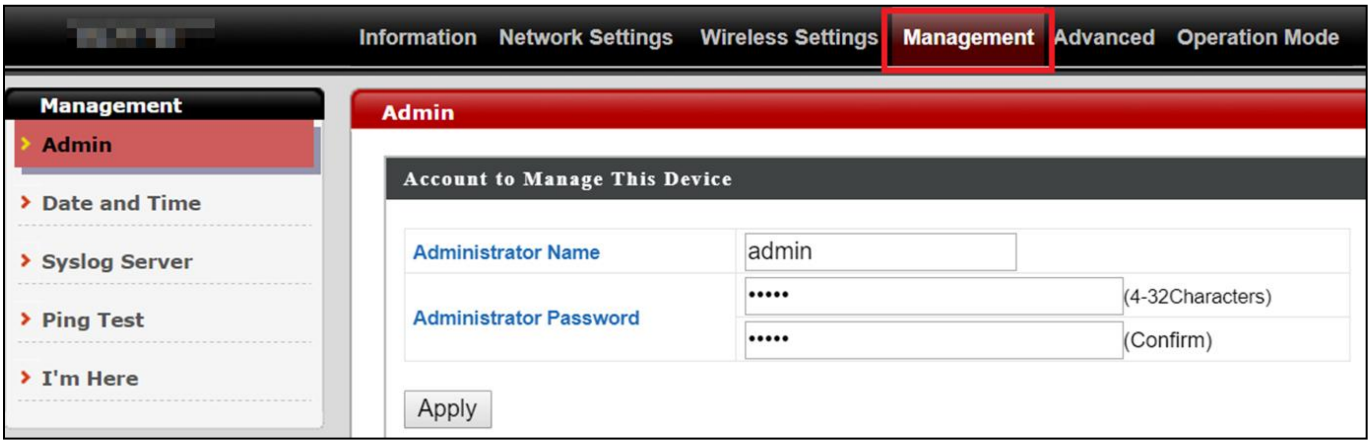
SSID	[redacted] ▾
Broadcast SSID	
Wireless Client Isolation	Disable
802.11k	Disable ▾
Load Balancing	50 /50
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

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

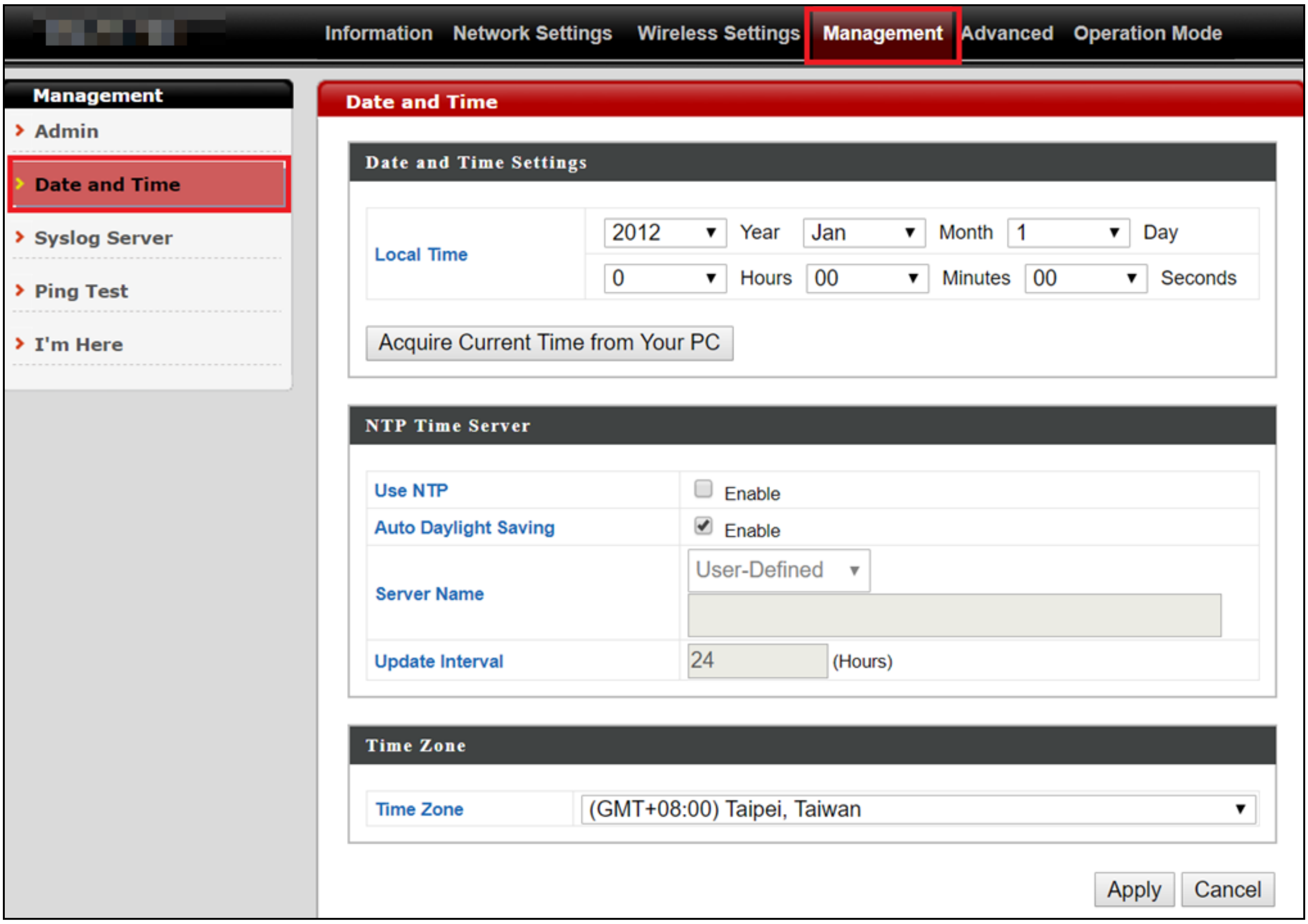
Administrator Password: ••••• (4-32Characters)

••••• (Confirm)

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

Changing Date and Time

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



Local Time: 2012 Year, Jan Month, 1 Day; 0 Hours, 00 Minutes, 00 Seconds

Use NTP: □ Enable

Auto Daylight Saving: ☑ Enable

Server Name: User-Defined

Update Interval: 24 (Hours)

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

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 device to the same time as your PC.

The basic settings of your access point are now configured.

V Wi-Fi Protected Setup (WPS)

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

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

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

3. 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.

4. The devices will establish a connection.

VI 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.

Please use Edimax Pro NMS on your Controller AP to configure your Managed AP(s).

The browser-based configuration interface enables you to configure the device's advanced features. The CAP1300 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:

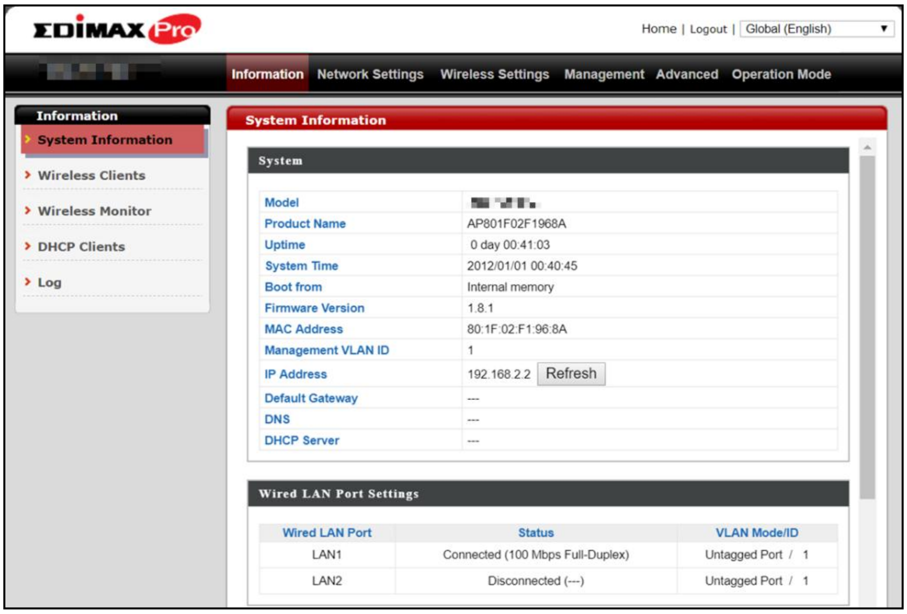
1. Connect a computer to your access point using an Ethernet cable.

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 ***IV Basic Settings***).

If you cannot remember your password, reset the access point back to its factory default settings. Refer to I-5 Reset.

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



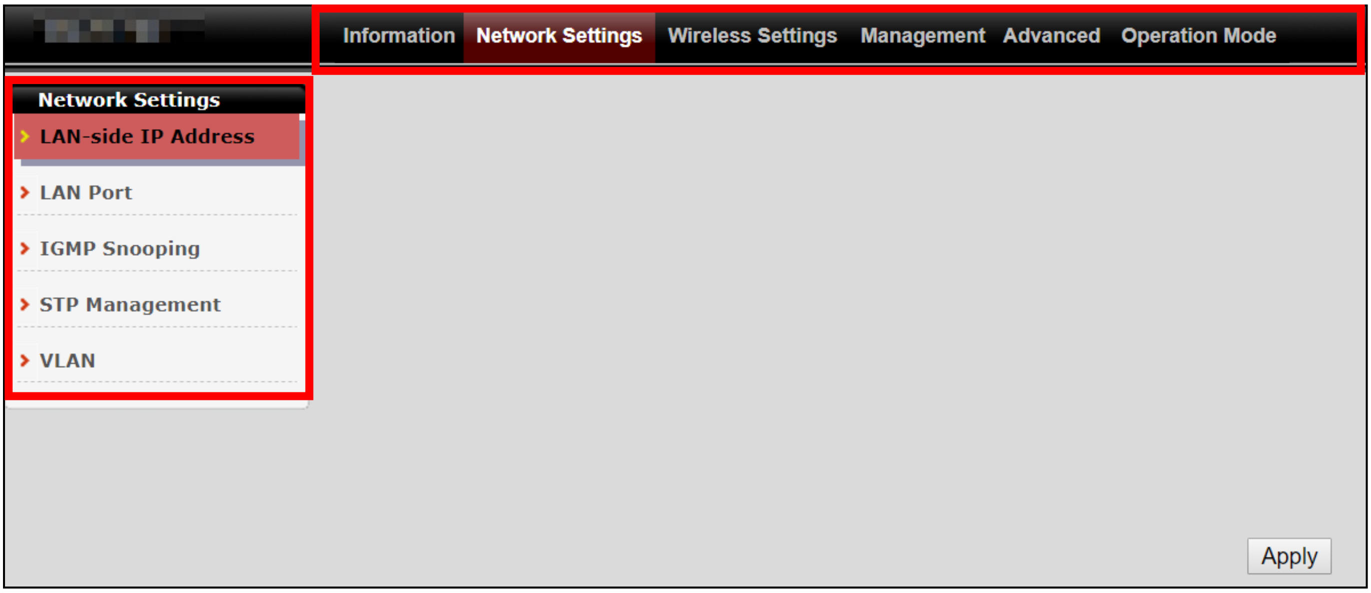
System

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
Default Gateway	---
DNS	---
DHCP Server	---

Wired LAN Port Settings

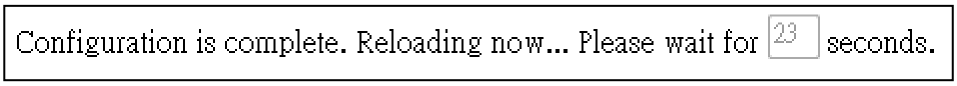
Wired LAN Port	Status	VLAN Mode/ID
LAN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1

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.

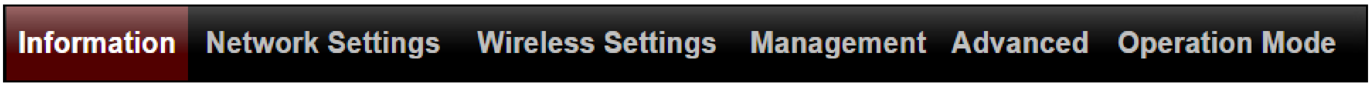
Please wait a few seconds for the access point to reload after you “Apply” changes. A countdown will be shown as exemplified below.



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

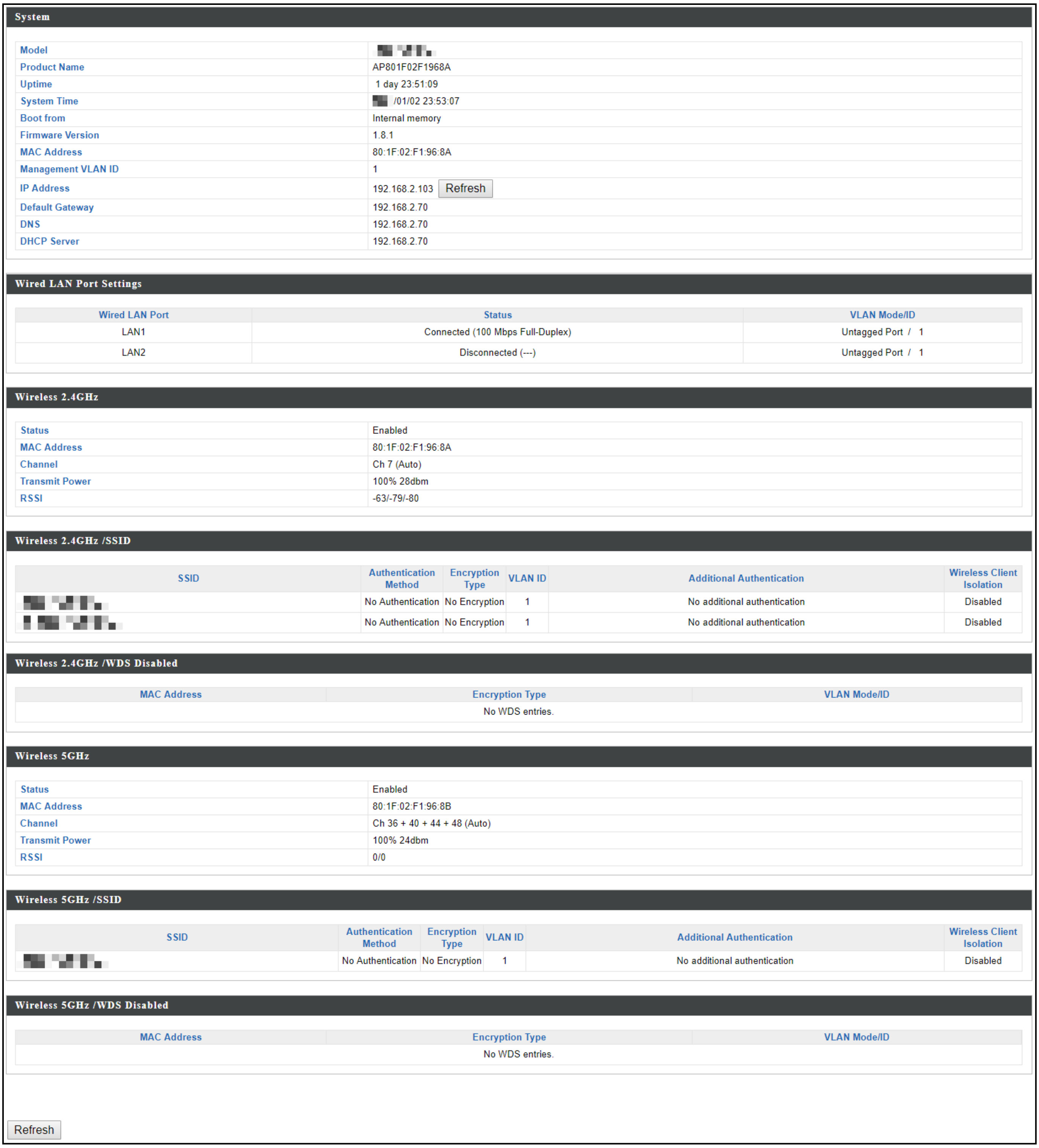
7. Please refer to the following chapters for full descriptions of the browser based configuration interface.

VI-1 Information



VI-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.	

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 **VI-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.

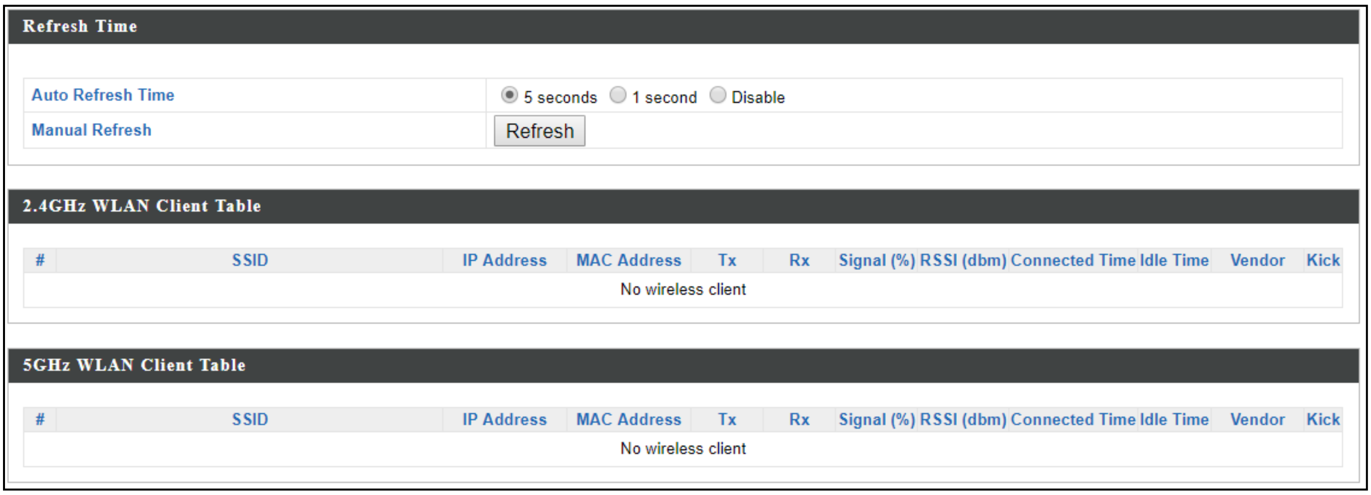
Wireless 2.4GHZ (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID. See **VI-3 Wireless Settings**.
Encryption Type	Displays the encryption type for the specified SSID. See **VI-3 Wireless Settings**.
VLAN ID	Displays the VLAN ID for the specified SSID. See **VI-2-5 VLAN**.
Additional Authentication	Displays the additional authentication type for the specified SSID. See **VI-3 Wireless Settings**.
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID. See **VI-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 **VI-3-3-4 WDS**.
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See **VI-3-3-4 WDS**.

Select “Refresh” to refresh all information.

VI-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

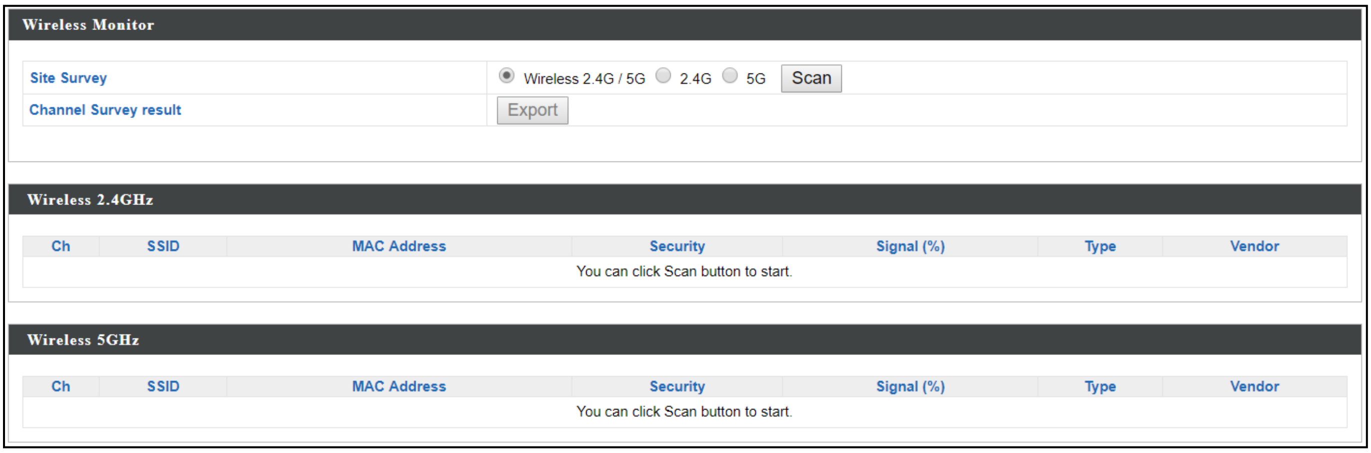
#	SSID	IP Address	MAC Address	Tx	Rx	Signal (%)	RSSI (dbm)	Connected Time	Idle Time	Vendor	Kick
No wireless client											

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.

VI-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

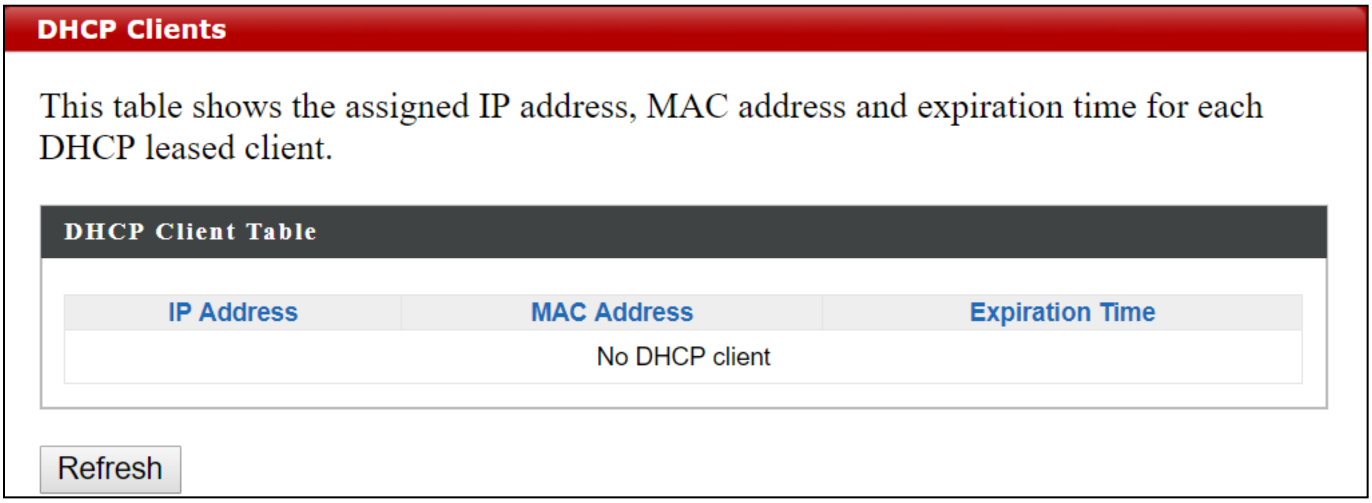
Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

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.

VI-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.

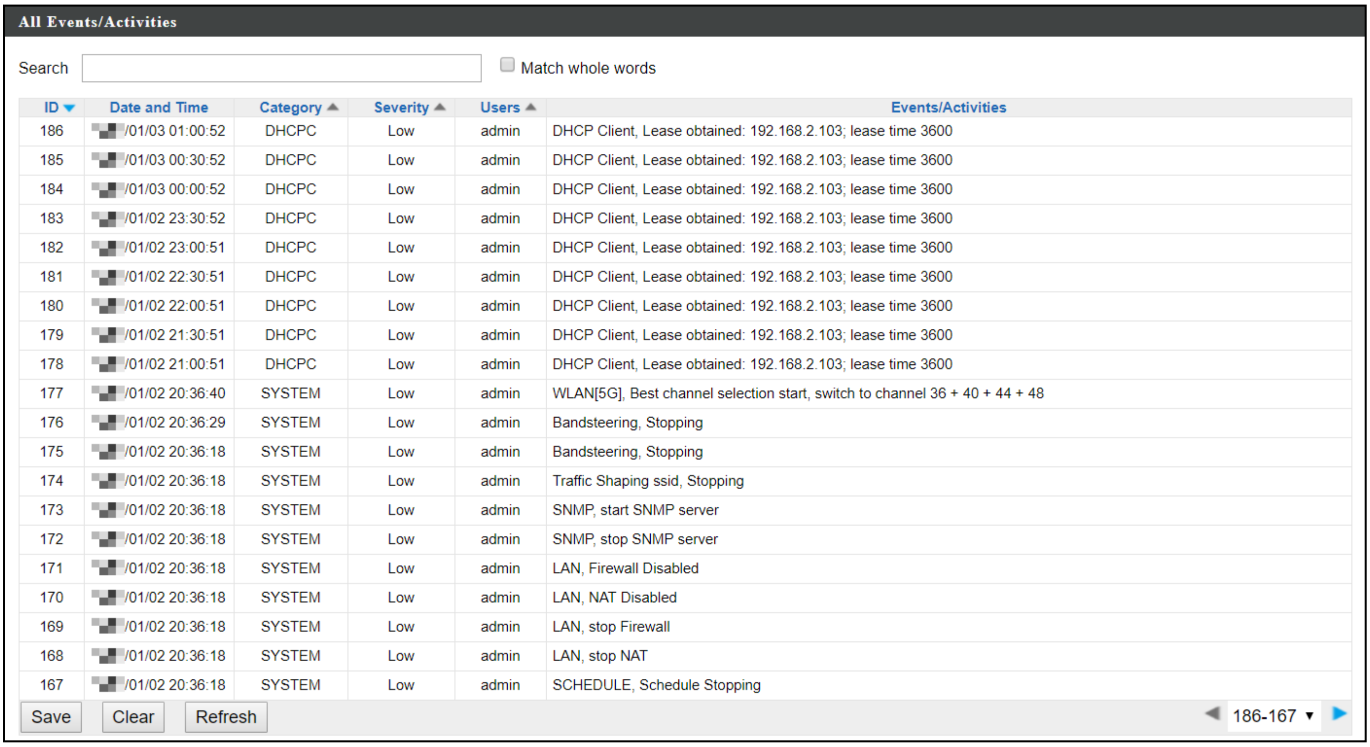
DHCP Client Table

IP Address	MAC Address	Expiration Time
	No DHCP client	

VI-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

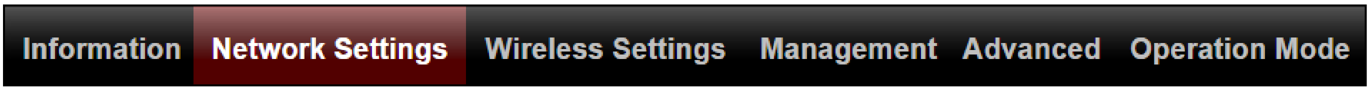
Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

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

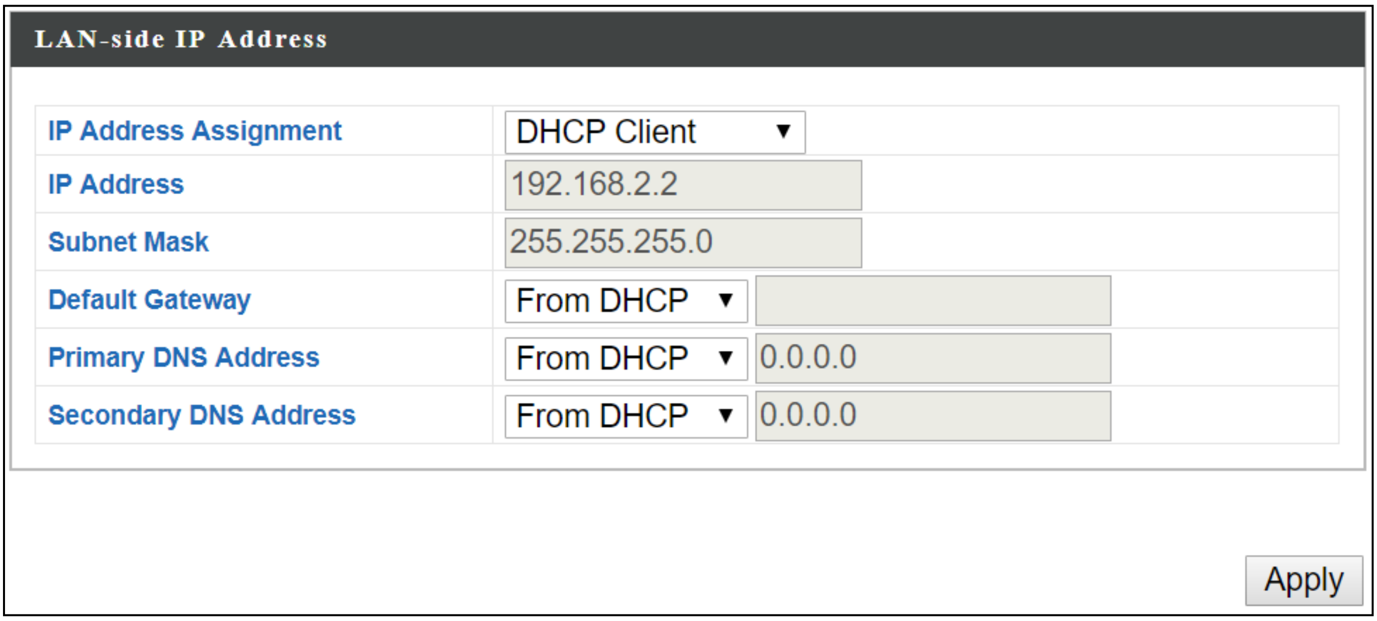
VI-2 Network Settings



VI-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.

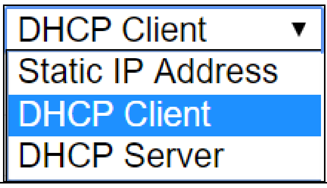
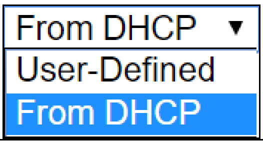
The access point’s default IP address is 192.168.2.2.



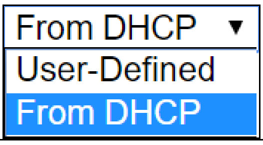
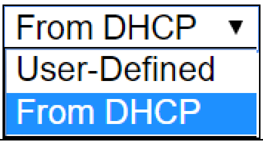
LAN-side IP Address

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.  From DHCP ▼ User-Defined From DHCP

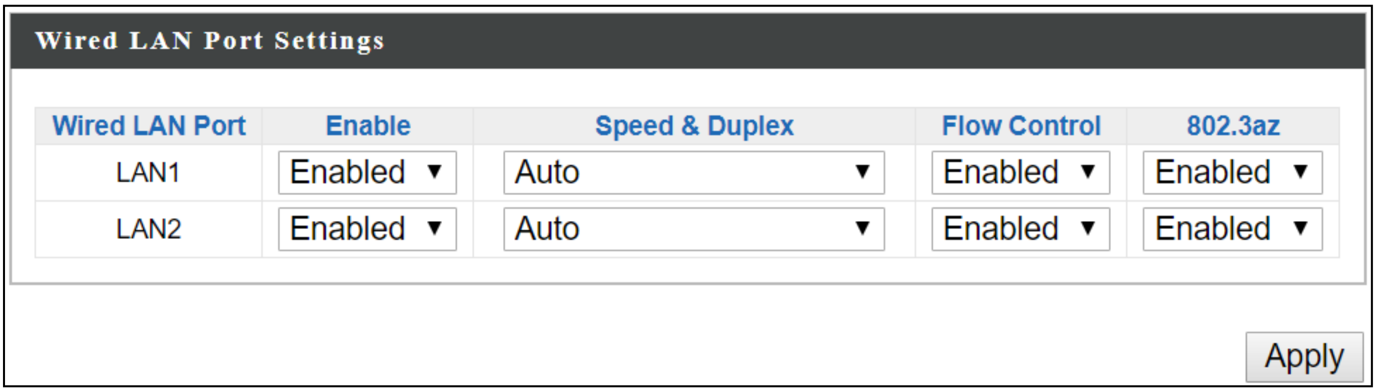
DHCP users can select to get DNS servers’ IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

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.  From DHCP ▼ User-Defined From DHCP
Secondary DNS Address	Users can manually enter a value when DNS server’s primary address is set to “User-Defined”.  From DHCP ▼ User-Defined From DHCP

Press “Apply” to confirm the settings.

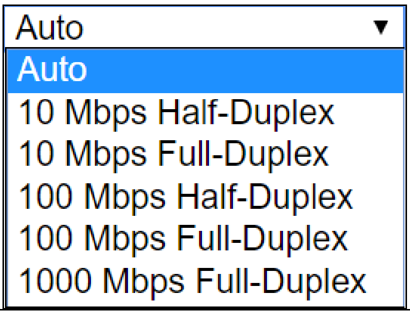
VI-2-2 LAN Port

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



Wired LAN Port Settings

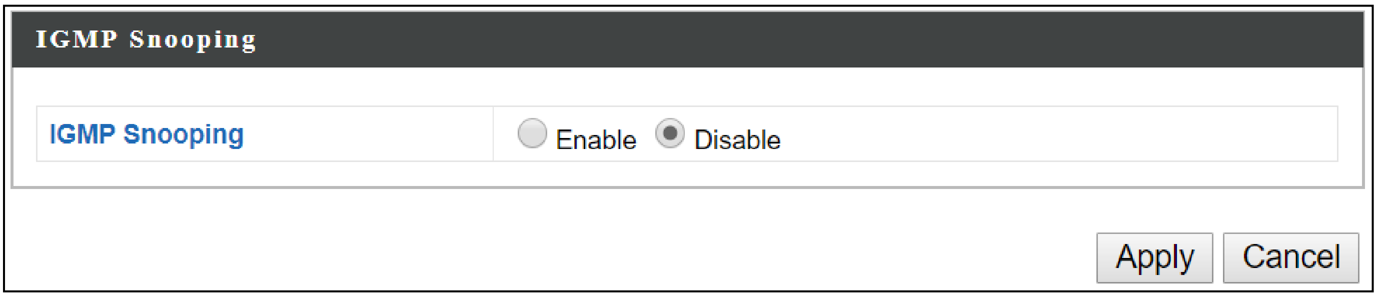
Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
LAN1	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼
LAN2	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼

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.

VI-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 need which 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.



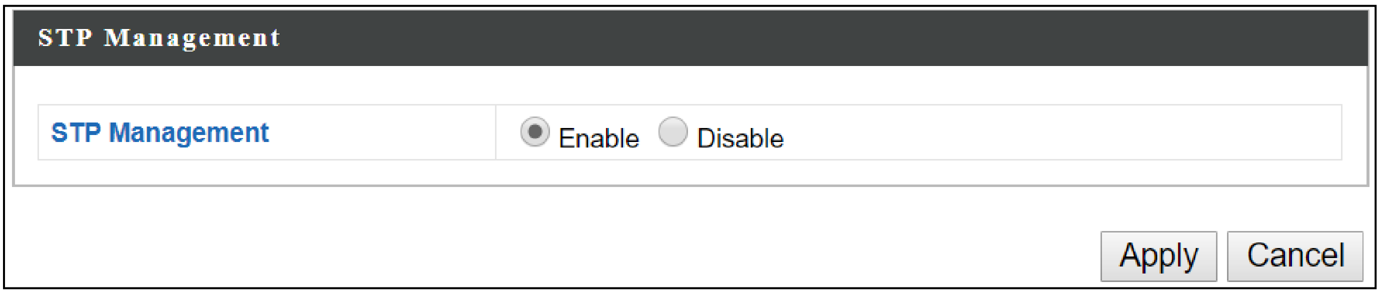
IGMP Snooping

IGMP Snooping ○ Enable ● Disable

Press “Apply” to confirm the settings.

VI-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

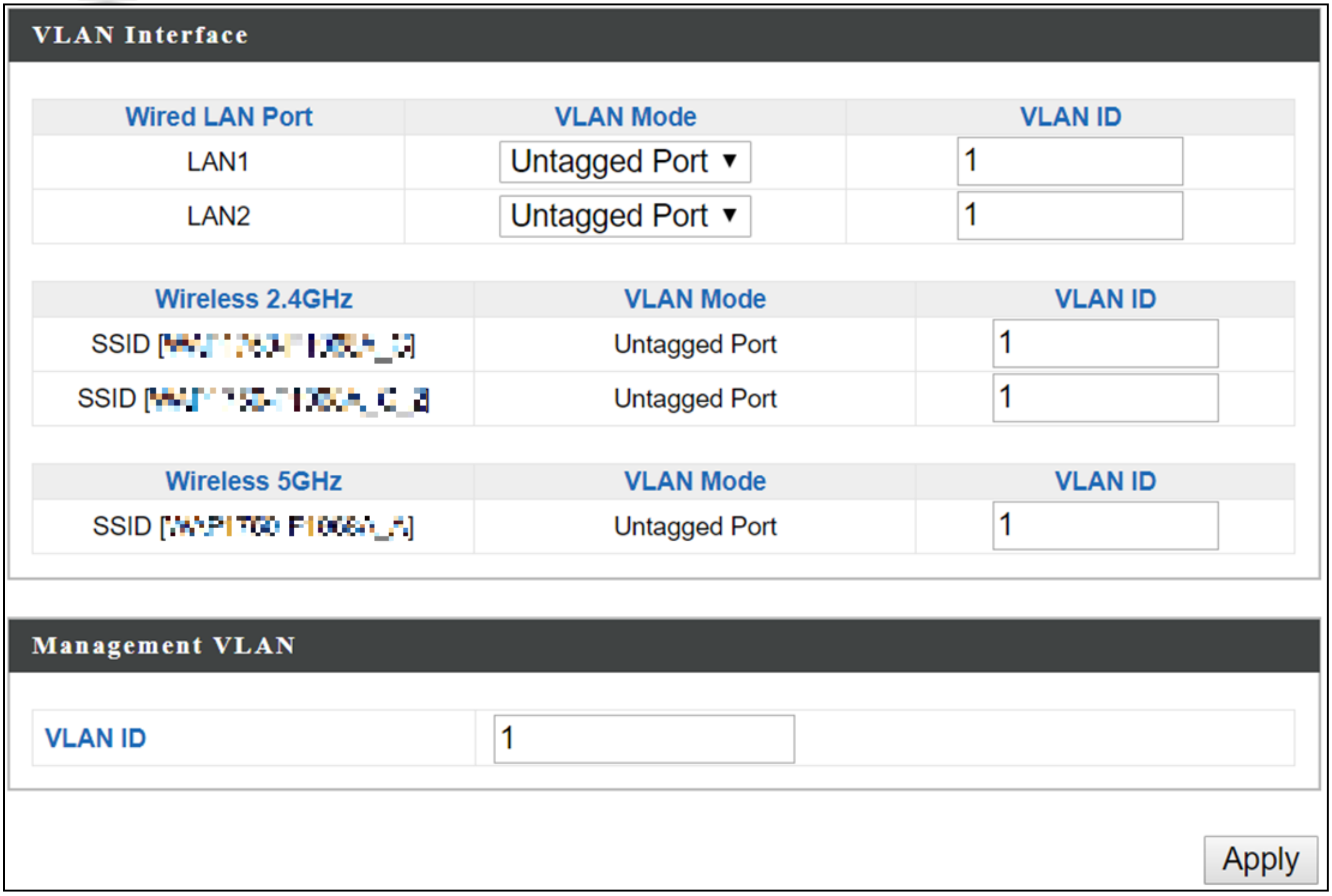
STP Management	● Enable ○ Disable

Press “Apply” to confirm the settings.

VI-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

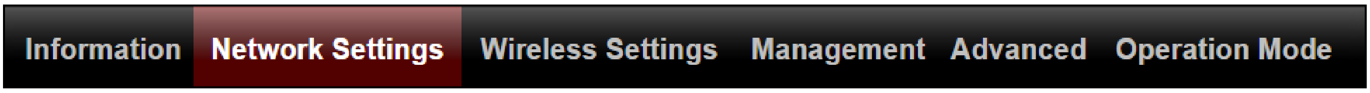
VLAN ID	1

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.

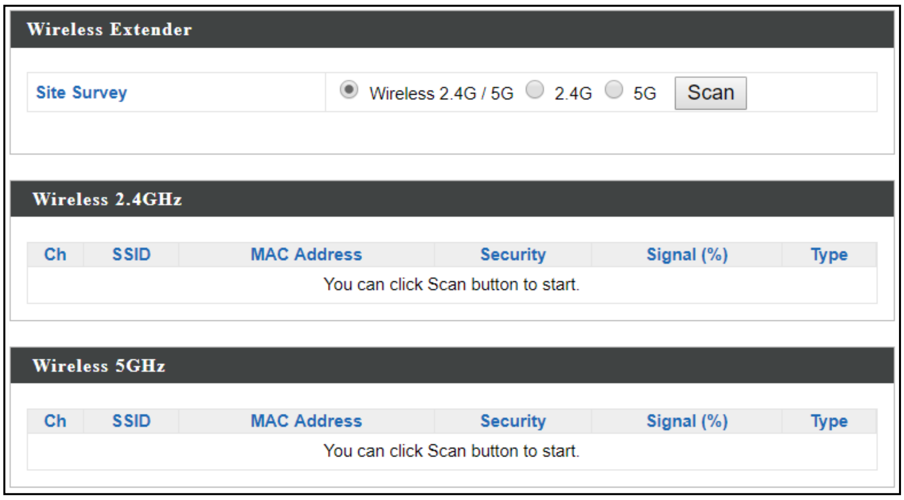
Press “Apply” to confirm the settings.

VI-3 Wireless Settings



VI-3-1 Wireless Extender

This page allows you to scan for available wireless network (both 2.4GHz and 5GHz frequencies) to connect to for repeater / client bridge modes.



Wireless Extender

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

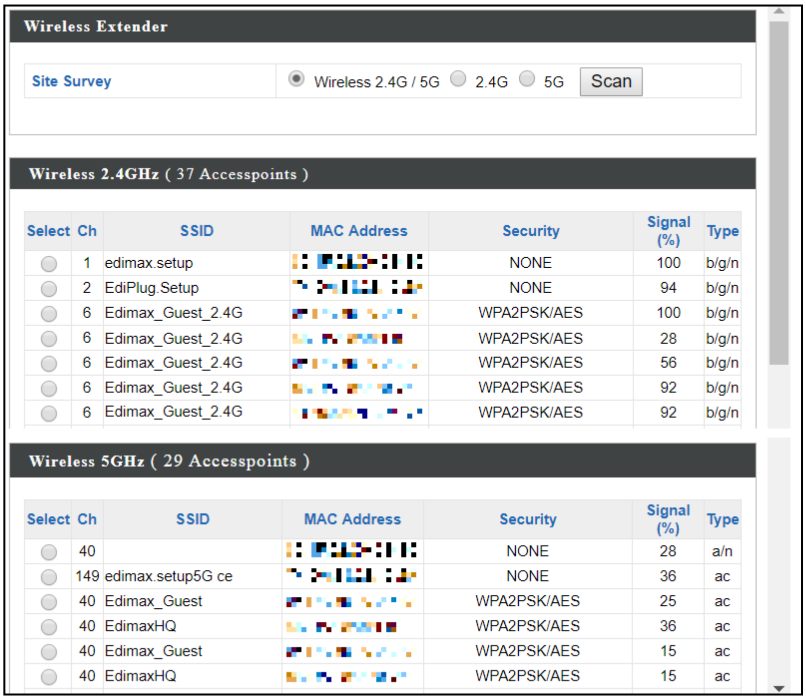
Wireless 2.4GHz

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.					

Click “Scan” to show available wireless network:



Wireless Extender

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

Wireless 2.4GHz (37 Accesspoints)

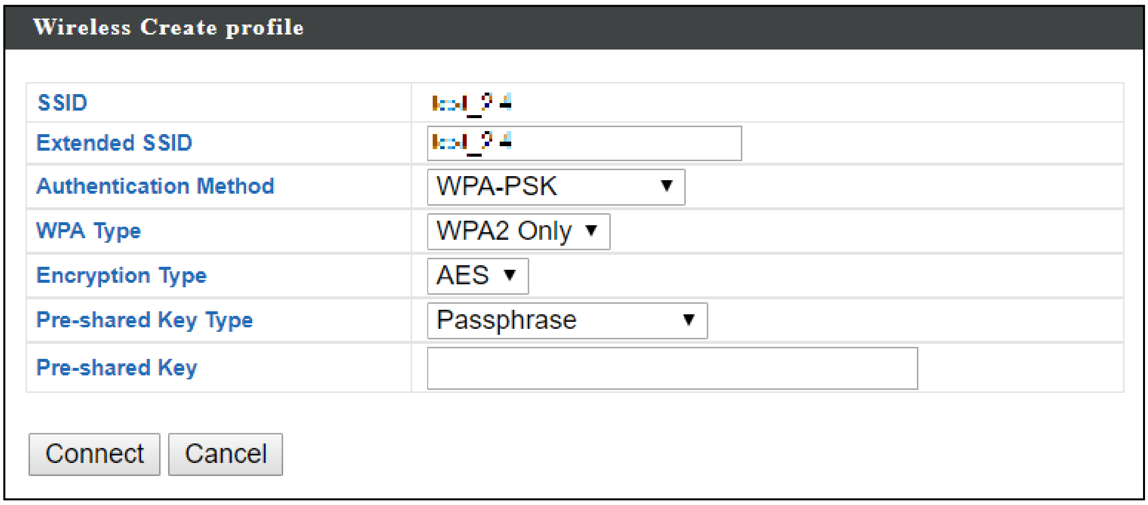
Select	Ch	SSID	MAC Address	Security	Signal (%)	Type
○	1	edimax.setup	[redacted]	NONE	100	b/g/n
○	2	EdiPlug.Setup	[redacted]	NONE	94	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	100	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	28	b/g/n
○	6	Edimax_Guest_2.4G	[redacted]	WPA2PSK/AES	56	b/g/n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

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

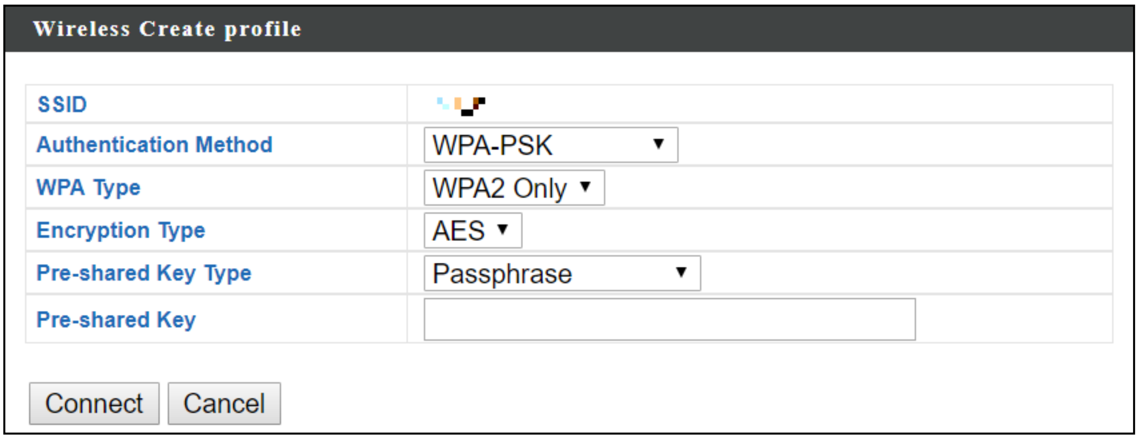
Repeater Mode source SSID connection page:



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	

Client Bridge Mode source SSID connection page:



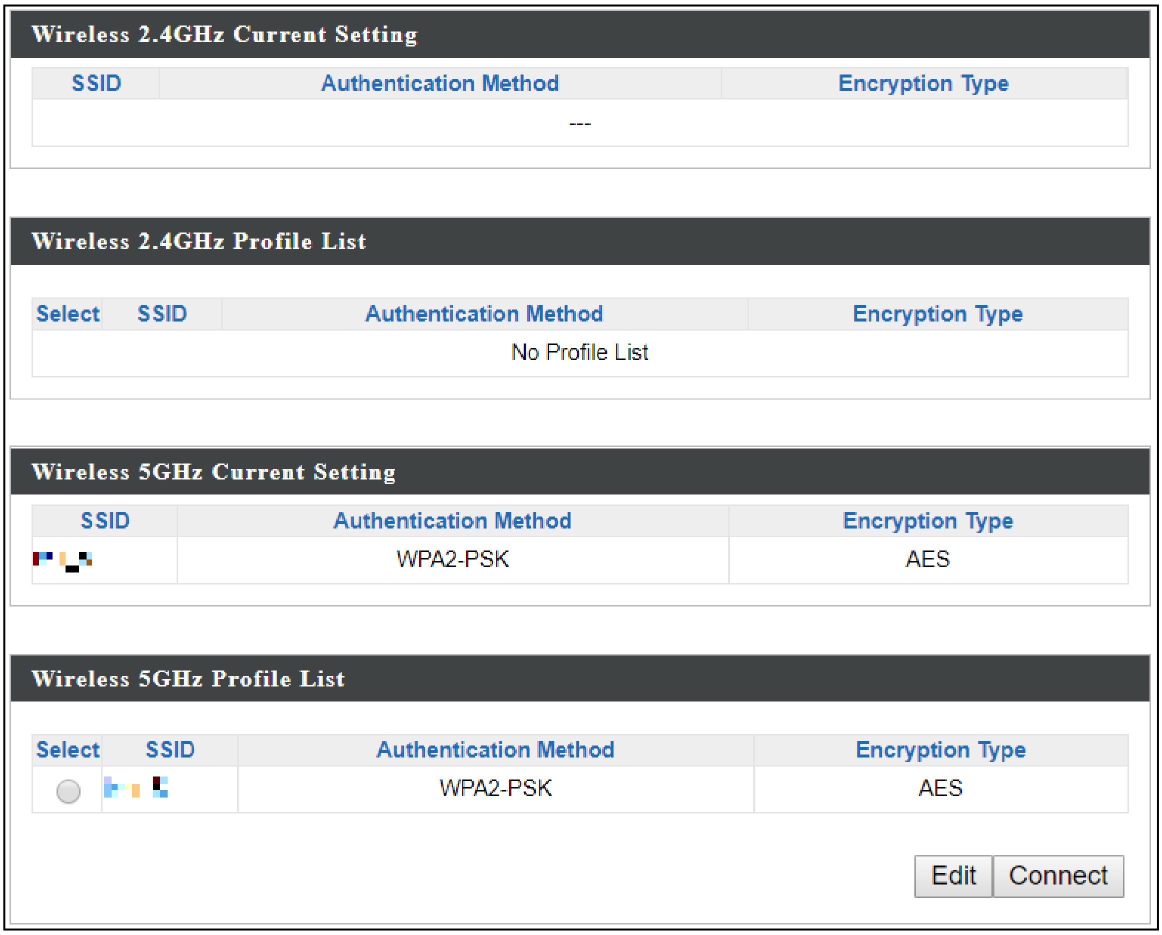
Wireless Create profile

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

Edit the connection page according to your preference and enter the security details for the source SSID (e.g. Pre-shared Key). Click "Connect" to connect to the SSID.

For more information on setting up Repeater / Client Bridge Modes, please refer to ***III Quick Setup & Mode Selection***.

VI-3-2 Profile List



Wireless 2.4GHz Current Setting

SSID	Authentication Method	Encryption Type

Wireless 2.4GHz Profile List

Select	SSID	Authentication Method	Encryption Type
		No Profile List	

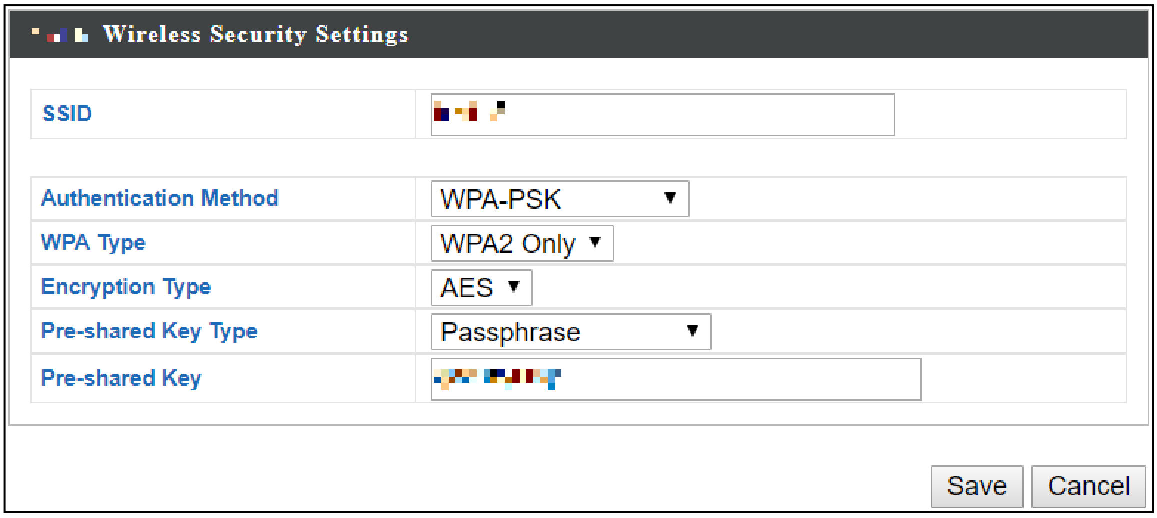
Wireless 5GHz Current Setting

SSID	Authentication Method	Encryption Type
[redacted]	WPA2-PSK	AES

Wireless 5GHz Profile List

Select	SSID	Authentication Method	Encryption Type
○	[redacted]	WPA2-PSK	AES

To edit a connection, check the circle icon and press “Edit”. The edit page is shown below:



[redacted] Wireless Security Settings

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

Press “Save” to save the configuration, or “Cancel” to forfeit the changes.

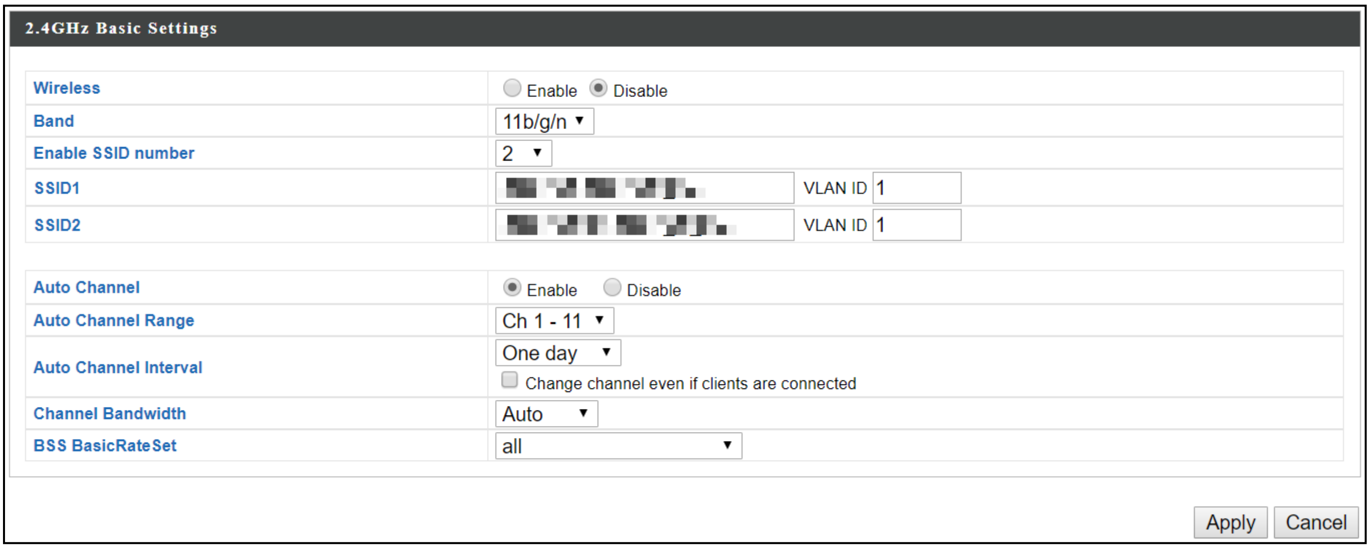
If you wish to use a different source SSID connection, check the circle icon (of the source SSID) and press “Connect”.

VI-3-3 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.

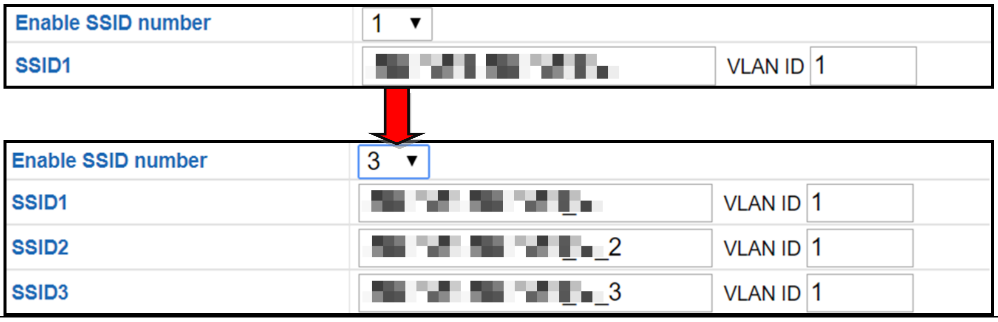
VI-3-3-1 Basic

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



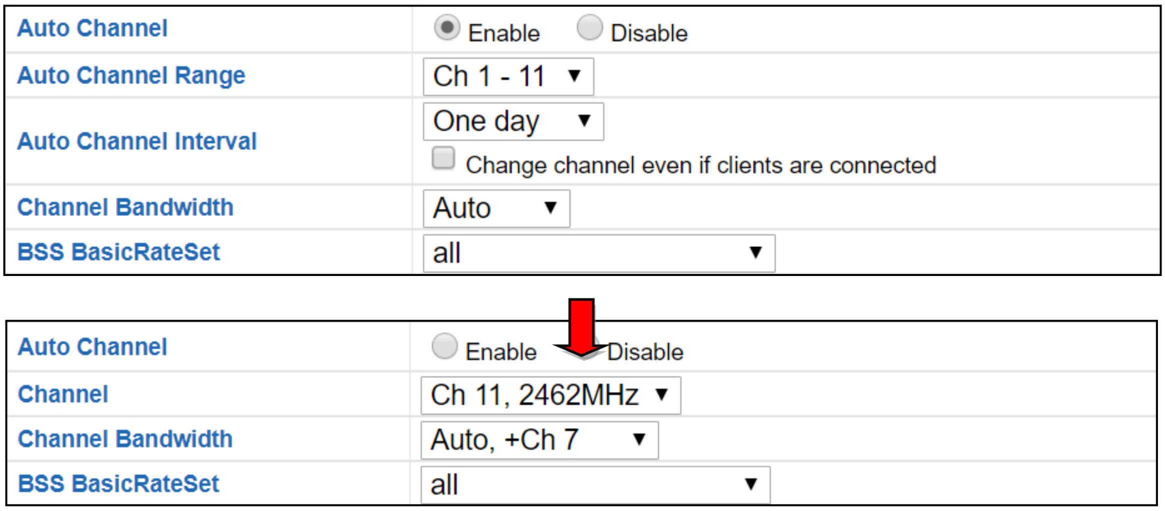
2.4GHz Basic Settings

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 ▼

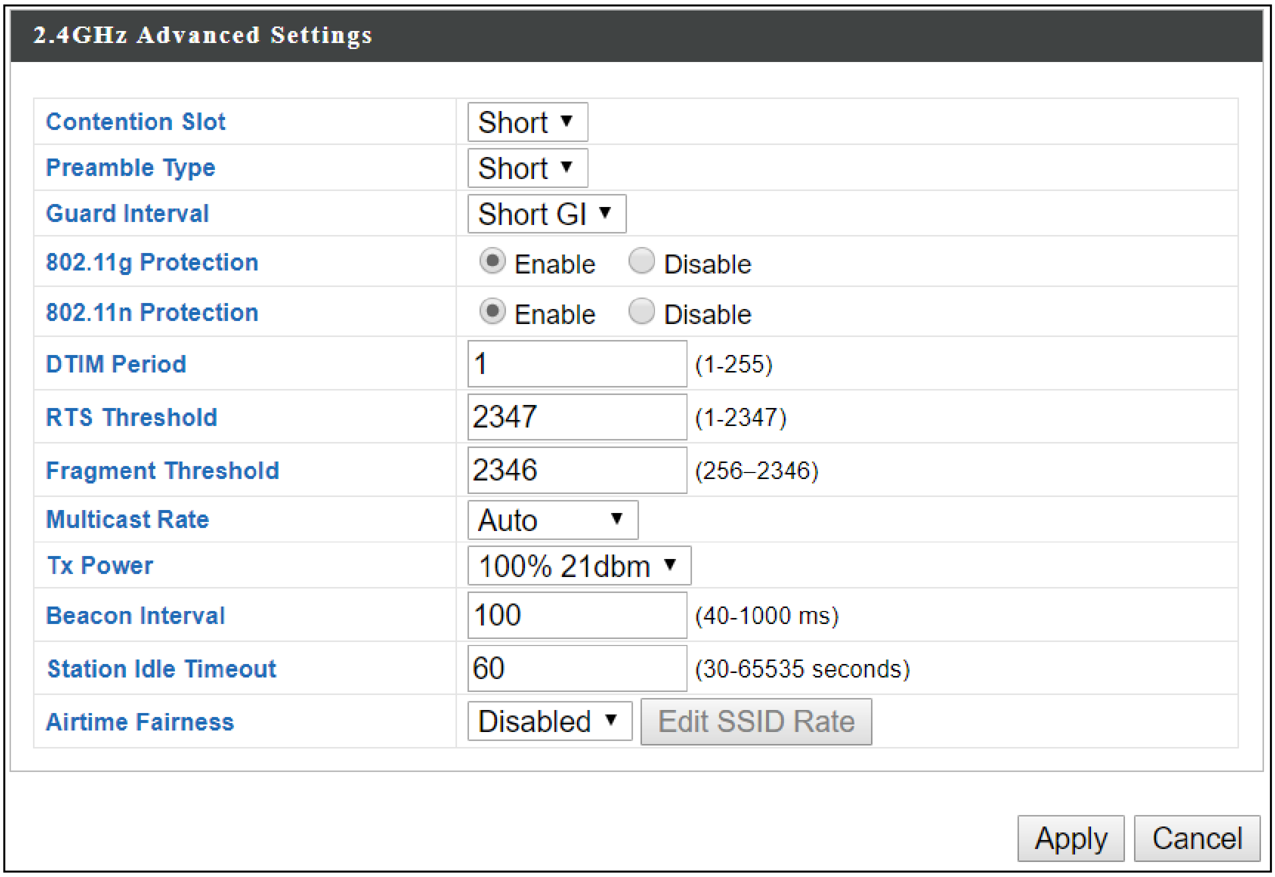
Channel	Select a wireless channel from 1 – 11.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference); or 40MHz (higher performance but potentially higher interference); or Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service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

VI-3-3-2 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.

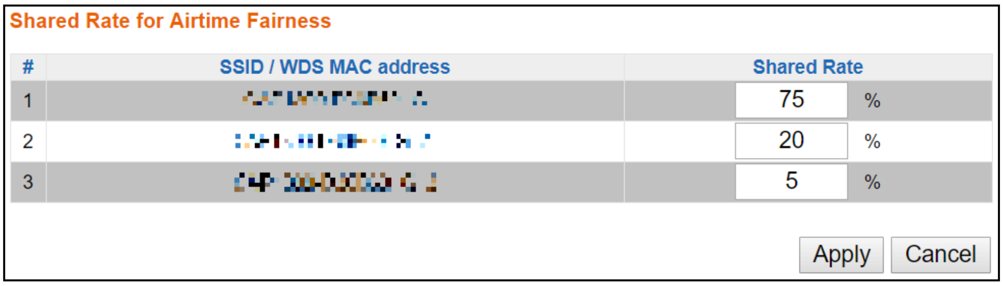
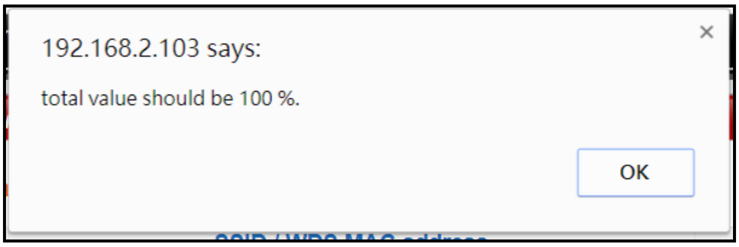


2.4GHz Advanced Settings

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 ***VI-3-8 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.

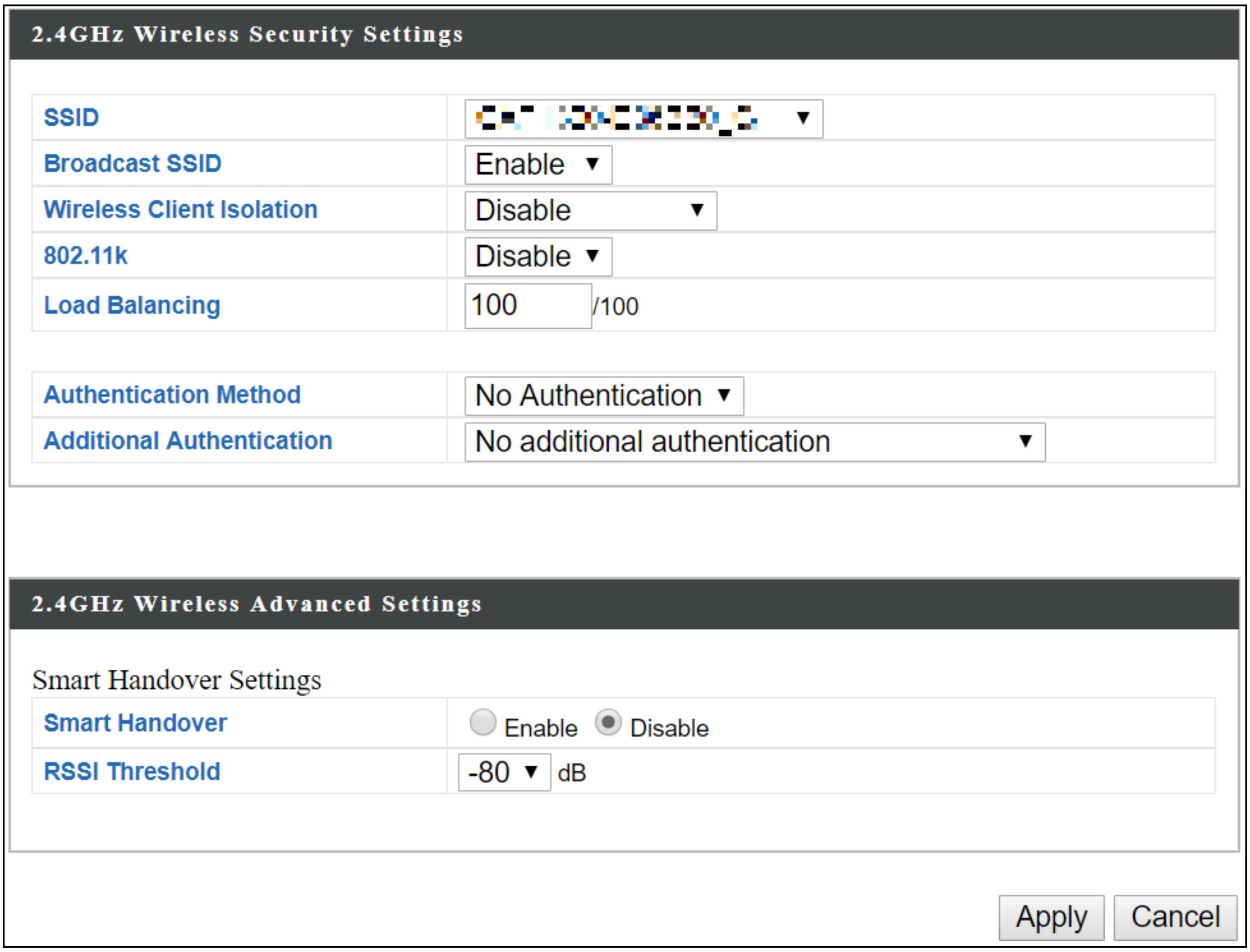
Airtime Fairness	Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate. Set airtime fairness to “Auto”, “Static” or “Disable”. When “Auto” is selected, the share rate is automatically managed. When “Static” is selected, press “Edit SSID Rate” to enter a % for each SSID’s share rate as shown below:  Shared Rate for Airtime Fairness # | SSID / WDS MAC address | Shared Rate 1 | [redacted] | 75 % 2 | [redacted] | 20 % 3 | [redacted] | 5 % The % field has to add up to 100% or the system will display a message:  192.168.2.103 says: 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.

VI-3-3-3 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.

VI-3-3-3-1 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** VI-3-5 WPS **for WPS settings.

MAC Address Filter

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

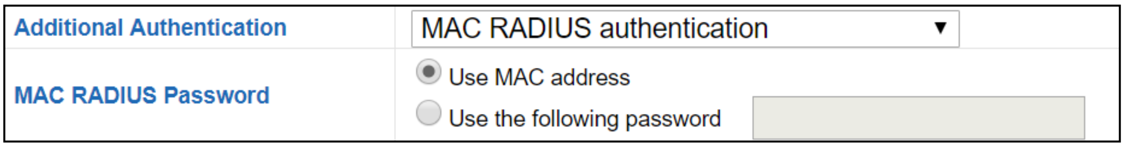
See** VI-3-7 MAC Filter **to configure MAC filtering.

MAC-RADIUS Authentication

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

See** VI-3-6 RADIUS **to configure RADIUS servers.

WPS must be disabled to use MAC-RADIUS authentication. See** VI-3-5 WPS **for WPS settings.

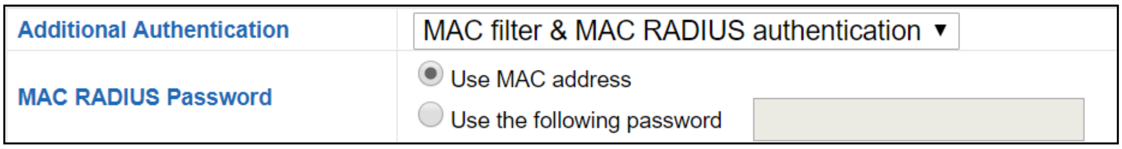


Additional Authentication: MAC RADIUS authentication ▼

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.



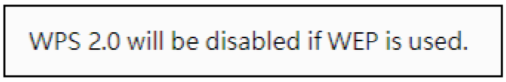
Additional Authentication: MAC filter & MAC RADIUS authentication ▼

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 **VI-3-6 RADIUS**.

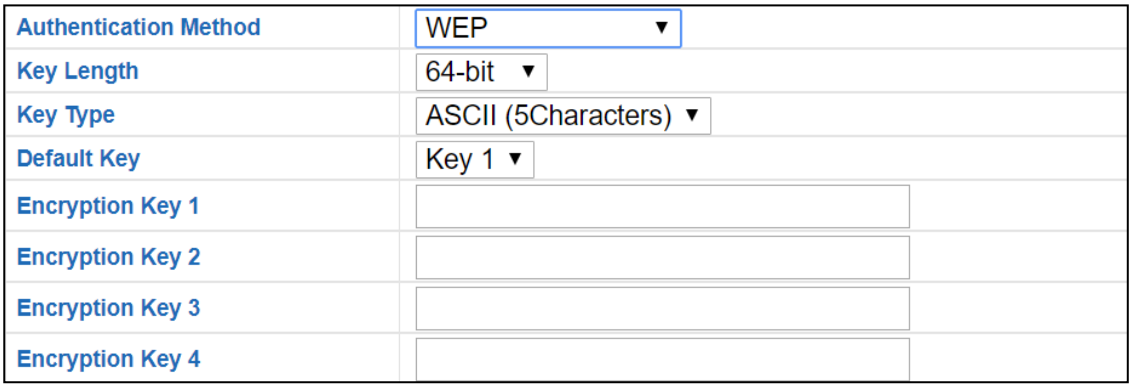
VI-3-3-3-2 WEP

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:



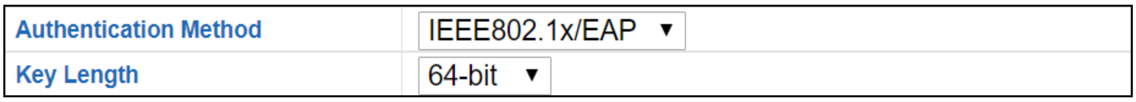
Authentication Method	WEP ▼
Key Length	64-bit ▼
Key Type	ASCII (5Characters) ▼
Default Key	Key 1 ▼
Encryption Key 1	
Encryption Key 2	
Encryption Key 3	
Encryption Key 4	

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.

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

Below is a figure showing the configurable fields:



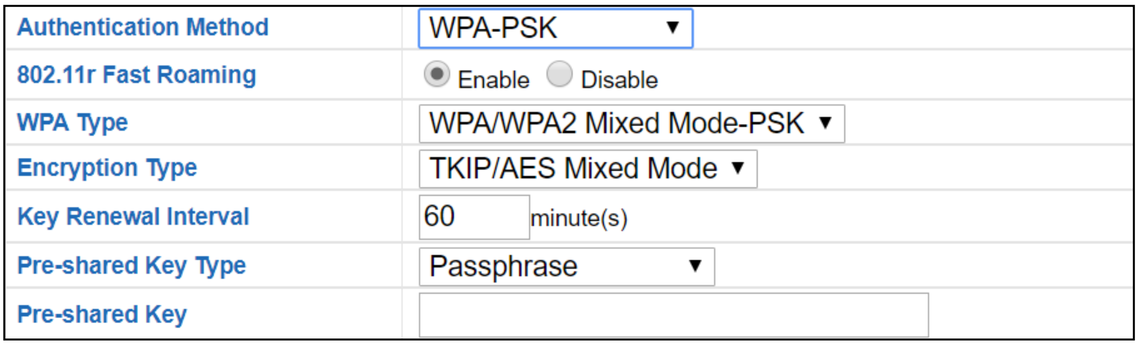
Authentication Method	IEEE802.1x/EAP ▼
Key Length	64-bit ▼

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

VI-3-3-3-4 WPA-PSK

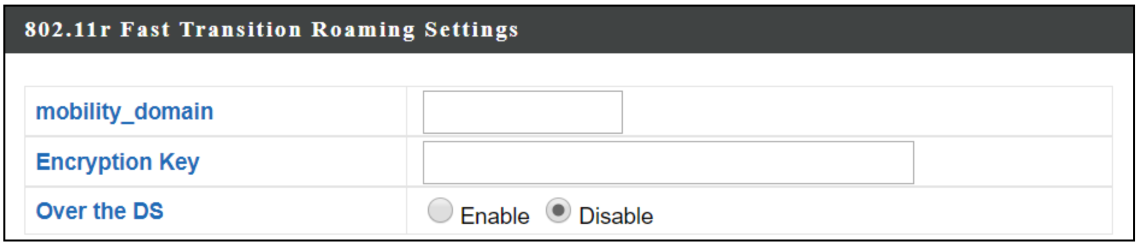
WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

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:



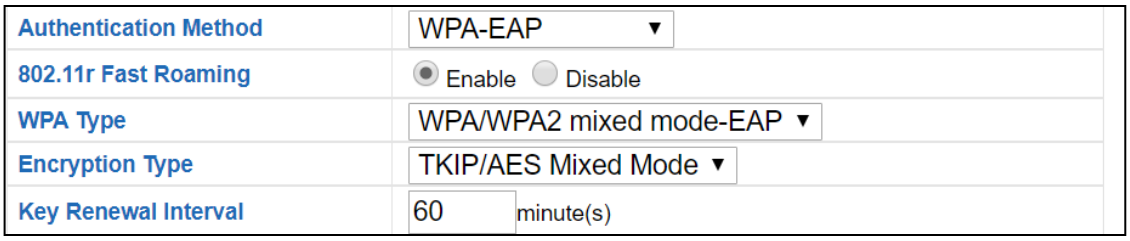
802.11r Fast Transition Roaming Settings

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.

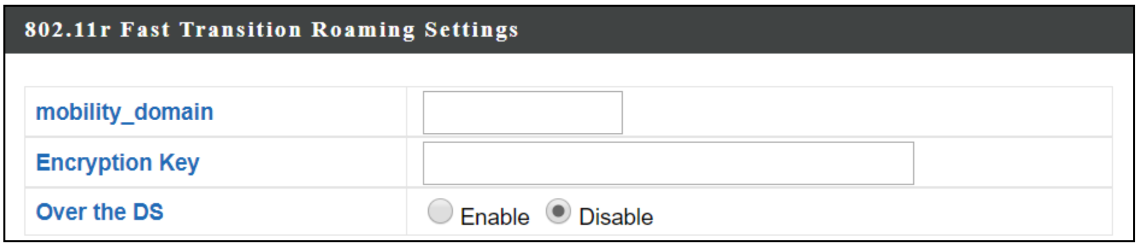
802.11r Fast Transition Roaming Settings	
Mobility_domain	Specify the mobility domain (2.4GHz or 5GHz)
Encryption Key	Specify the encryption key
Over the DS	Enable or disable this function.

VI-3-3-3-5 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.

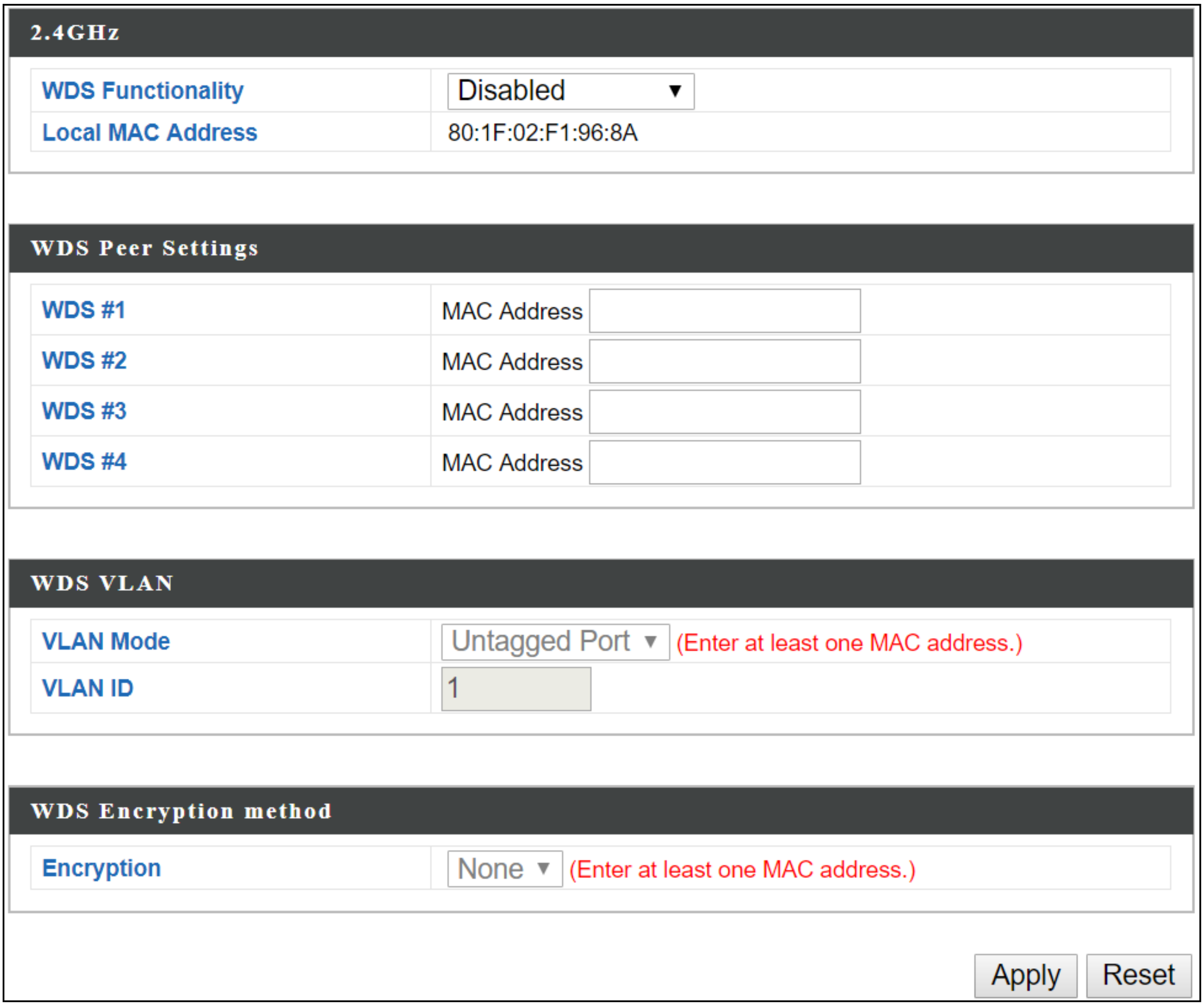
Press “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

VI-3-3-4 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.

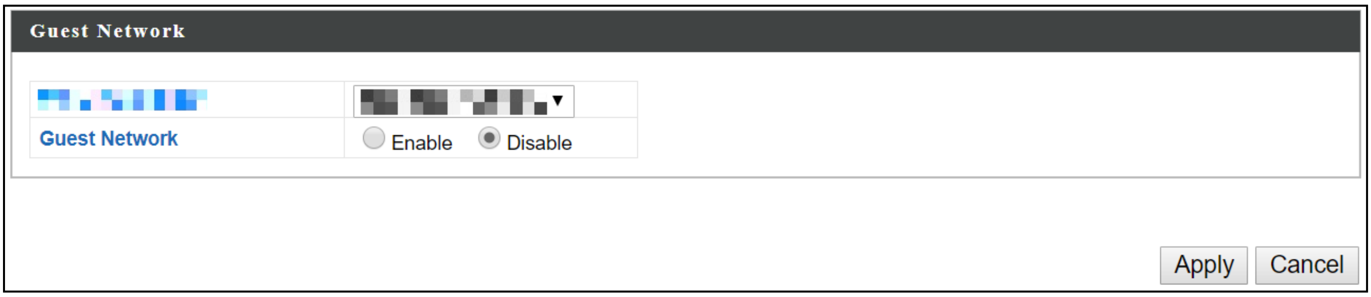
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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.

VI-3-3-5 Guest Network

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



Guest Network

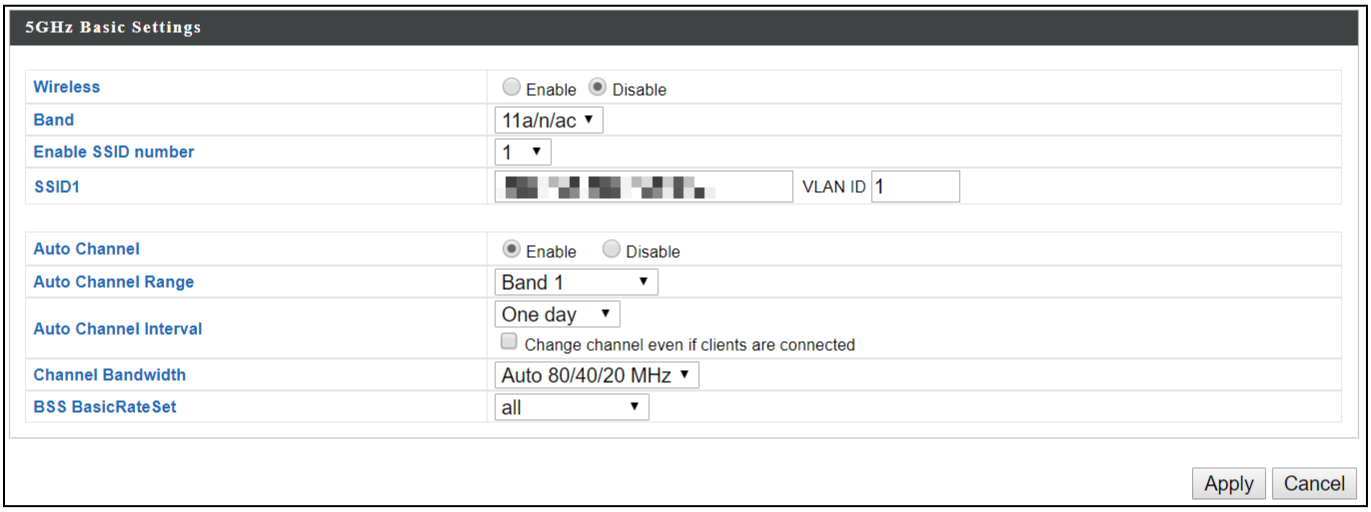
[redacted]	[redacted] ▾
Guest Network	○ Enable ● Disable

VI-3-4 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.

VI-3-4-1 Basic

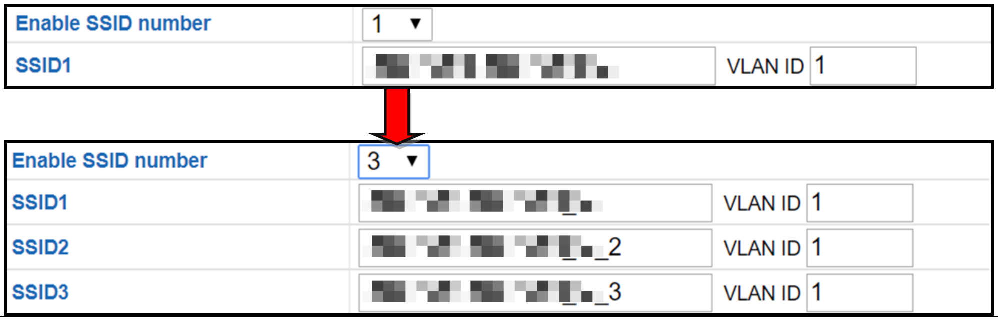
The “Basic” screen displays basic settings for your access point’s 5GHz Wi-Fi network (s).



5GHz Basic Settings

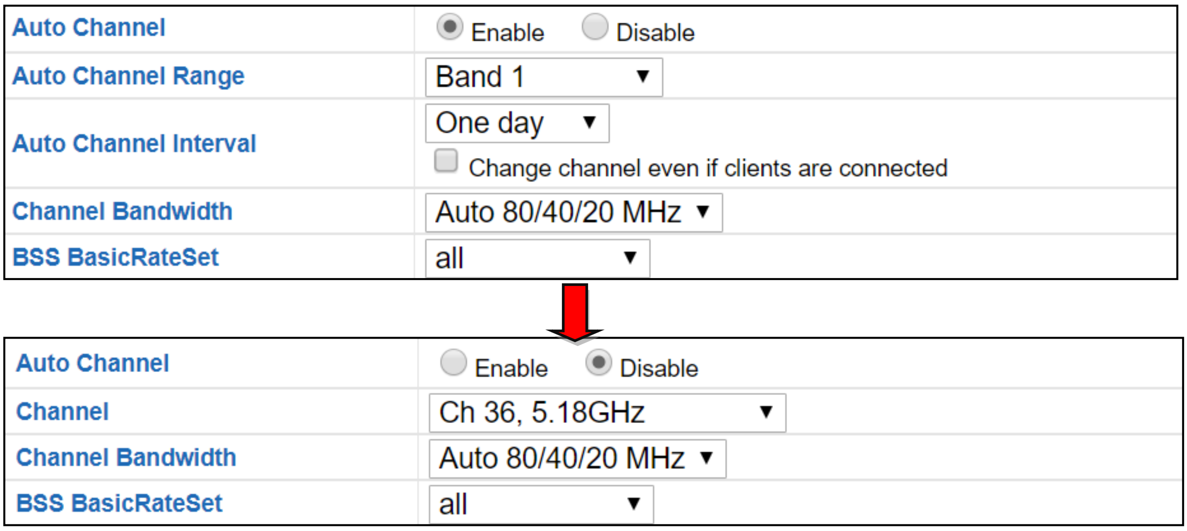
Wireless: ○ Enable ● Disable
Band: 11a/n/ac ▾
Enable SSID number: 1 ▾
SSID1: [redacted] VLAN ID 1

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	Select a range to which auto channel selection can choose

Channel Range	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 ▼

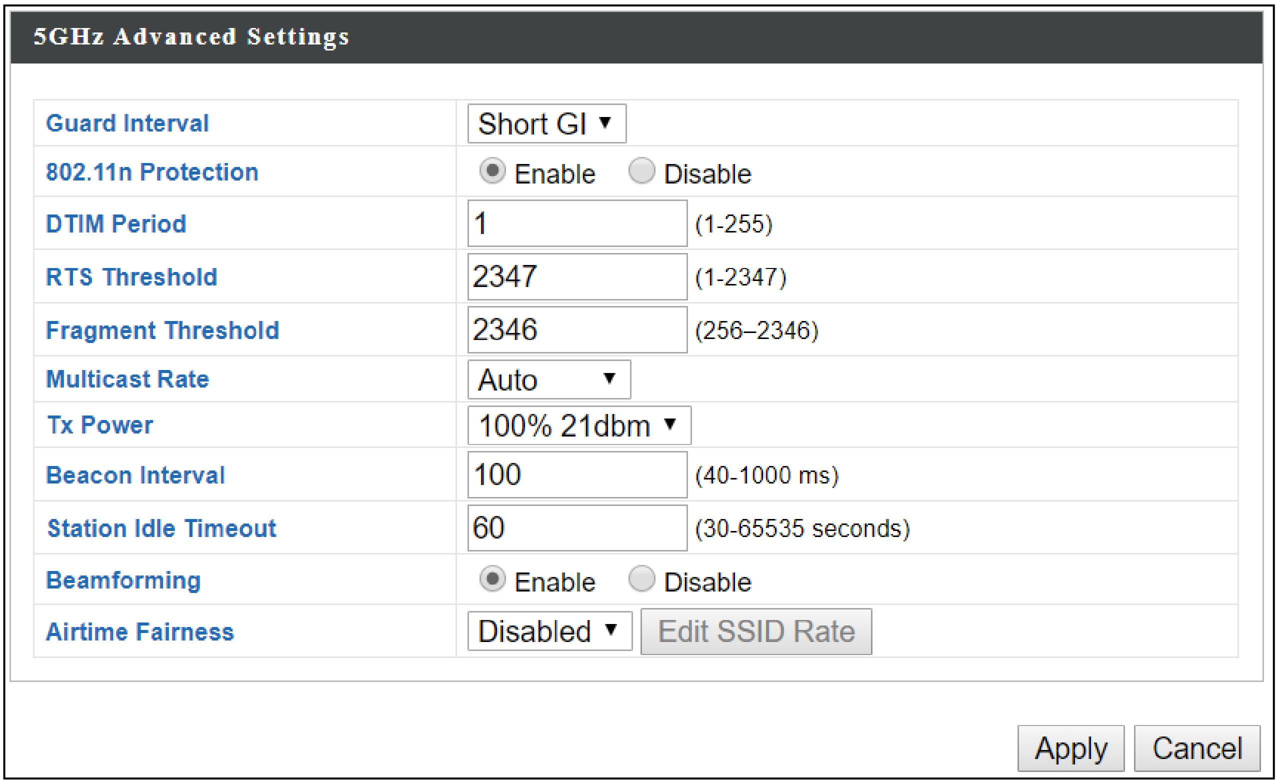
Channel	Select a wireless channel.
Channel Bandwidth	Select the channel bandwidth: 20MHz (lower performance but less interference); or Auto 40/20 MHz; or Auto 80/40/20 MHz (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates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

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

VI-3-4-2 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.

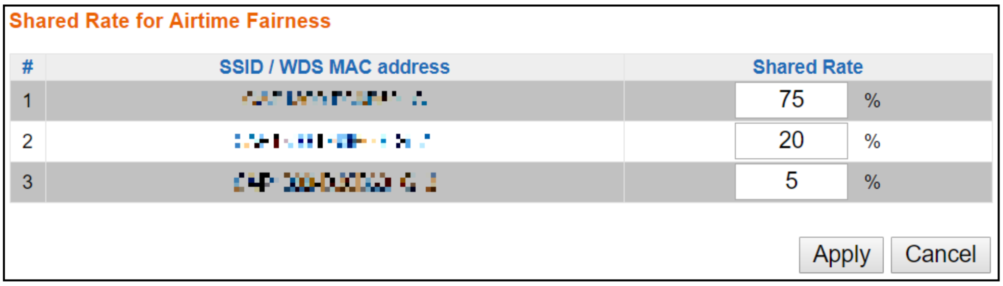
Airtime Fairness

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”.

When “Auto” is selected, the share rate is automatically managed.

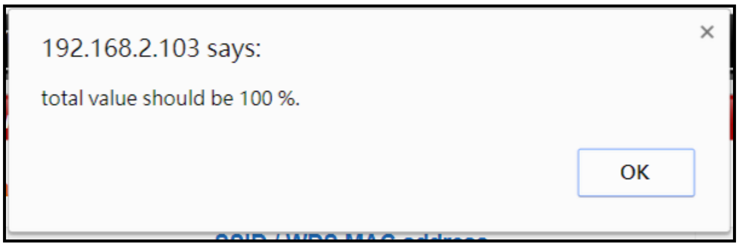
When “Static” is selected, press “Edit SSID Rate” to enter a % for each SSID’s share rate as shown below:



Shared Rate for Airtime Fairness

#	SSID / WDS MAC address	Shared Rate
1	[redacted]	75 %
2	[redacted]	20 %
3	[redacted]	5 %

The % field has to add up to 100% or the system will display a message:



192.168.2.103 says:

total value should be 100 %.

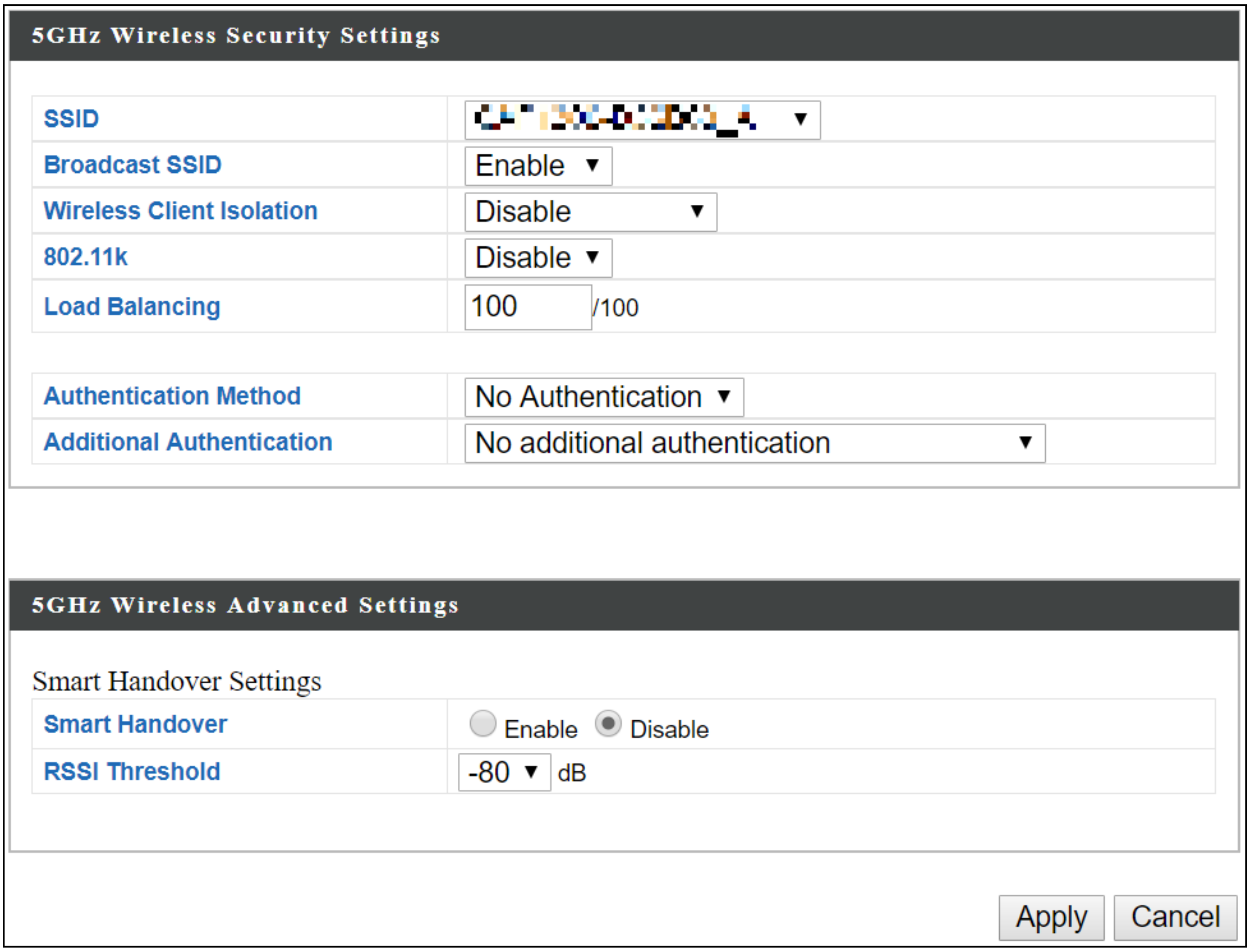
Airtime fairness is disabled if “Disable” is selected.

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

VI-3-4-3 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 **VI-3-3-3 Security** for your method.

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

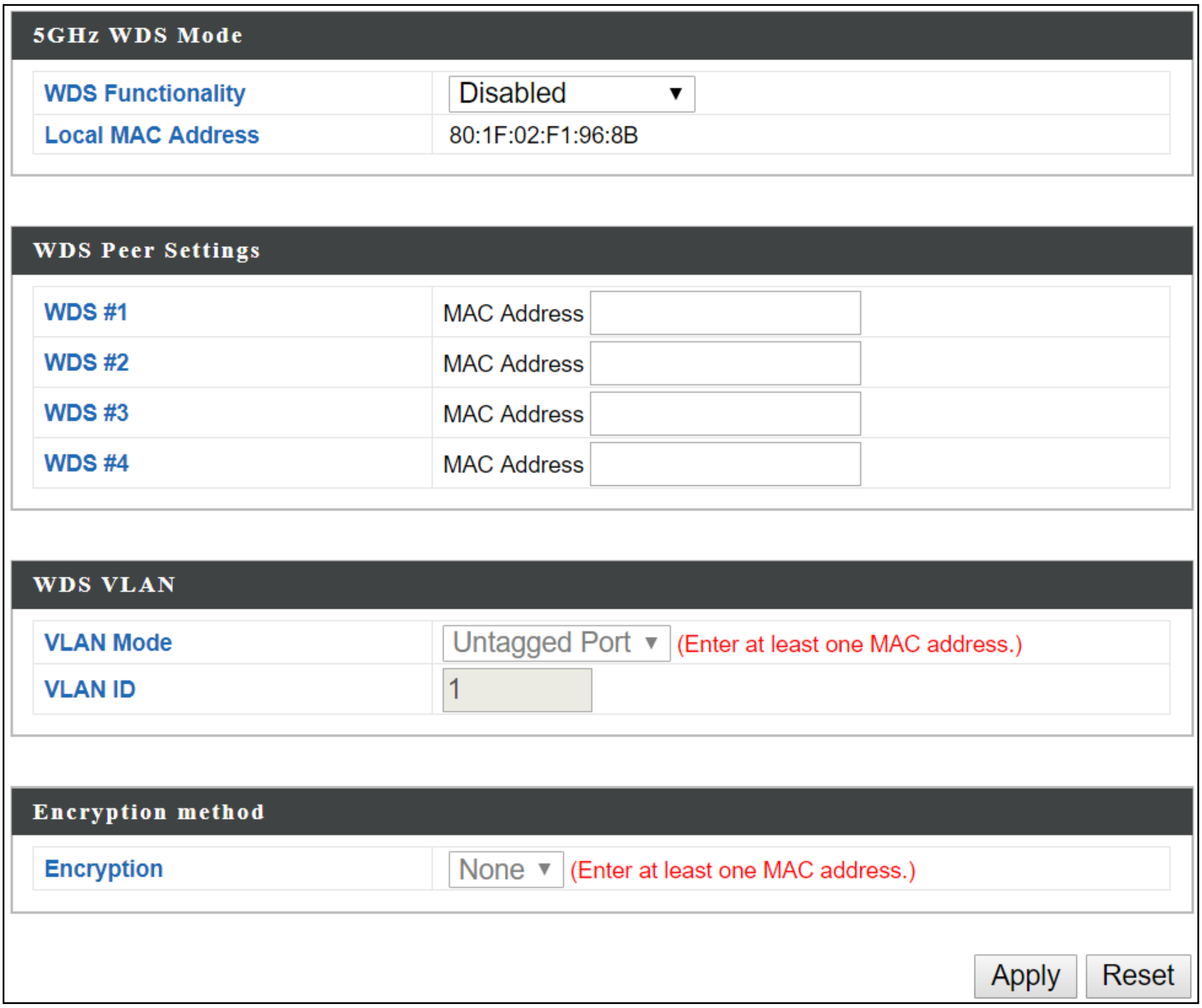
Please refer back to **VI-3-3-3 Security** for more information on authentication and additional authentication types.

VI-3-4-4 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.

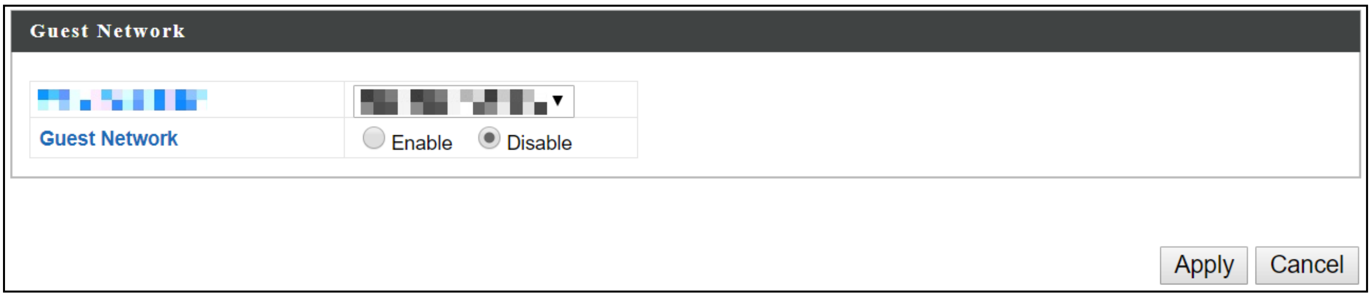
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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.

VI-3-4-5 Guest Network

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



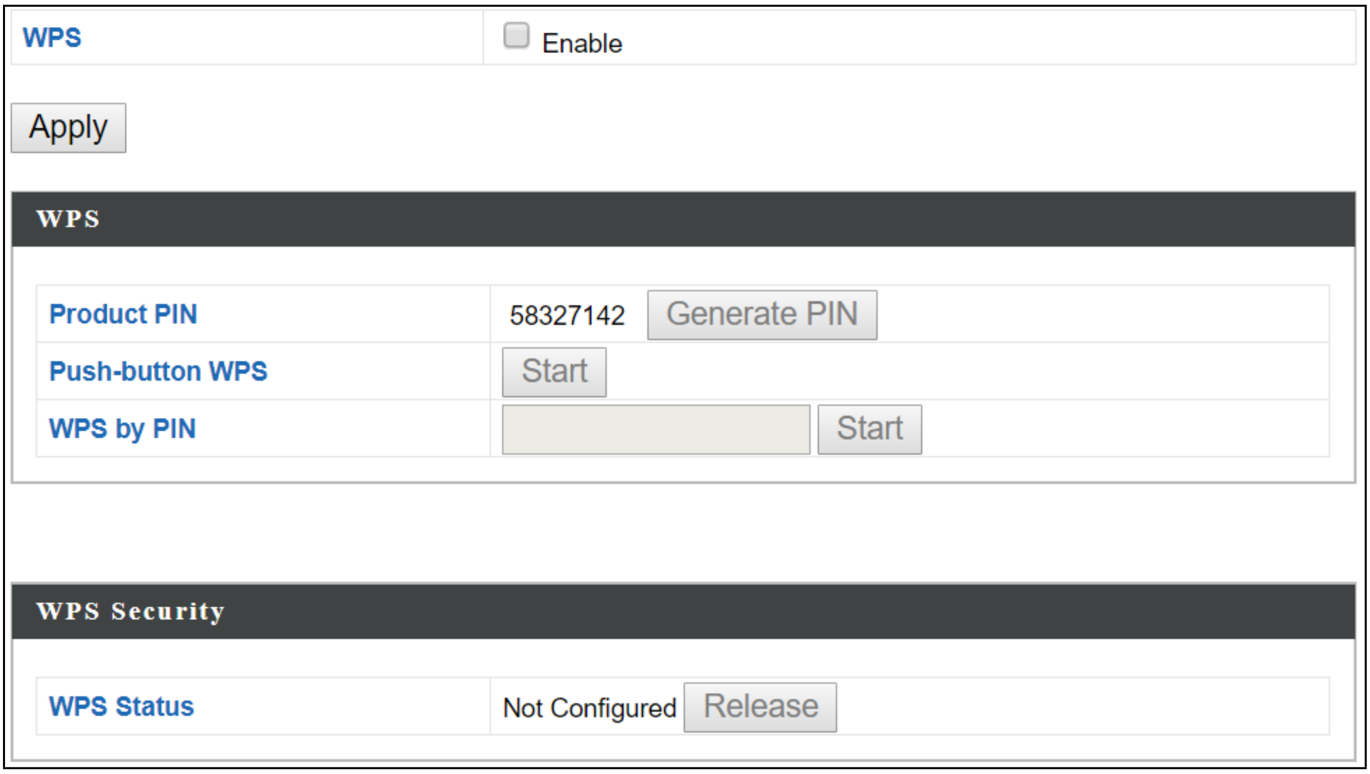
Guest Network

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

VI-3-5 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

Apply

WPS

Product PIN	58327142 Generate PIN
Push-button WPS	Start
WPS by PIN	Start

WPS Security

WPS Status	Not Configured Release

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 ***VI-3-6 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.

VI-3-6 RADIUS

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

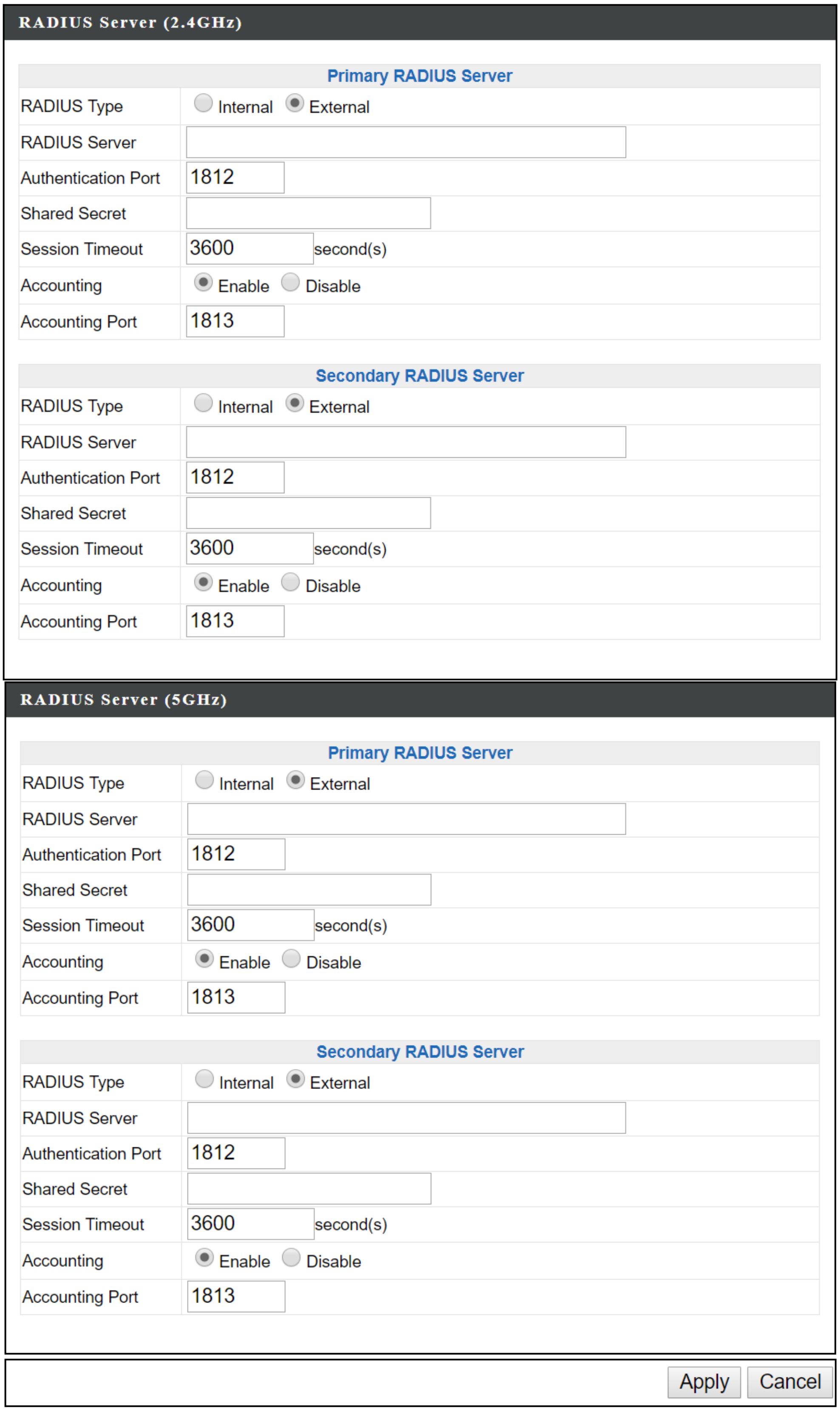
A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

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*** *VI-3-3-3* ***or*** *VI-3-4-3****).***

VI-3-6-1 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

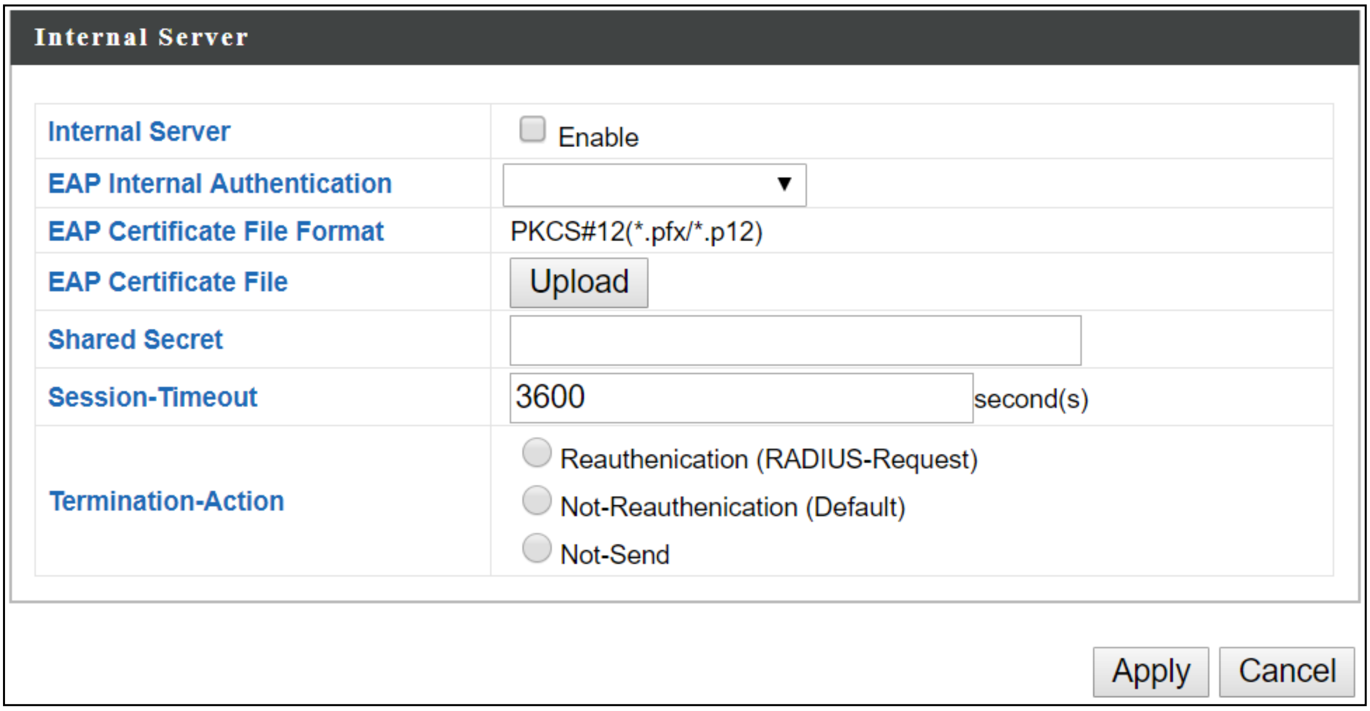
RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in ***VI-3-3-3*** or ***VI-3-4-3***.
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.

VI-3-6-2 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** VI-3-3-3 **&** VI-3-4-3**).



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

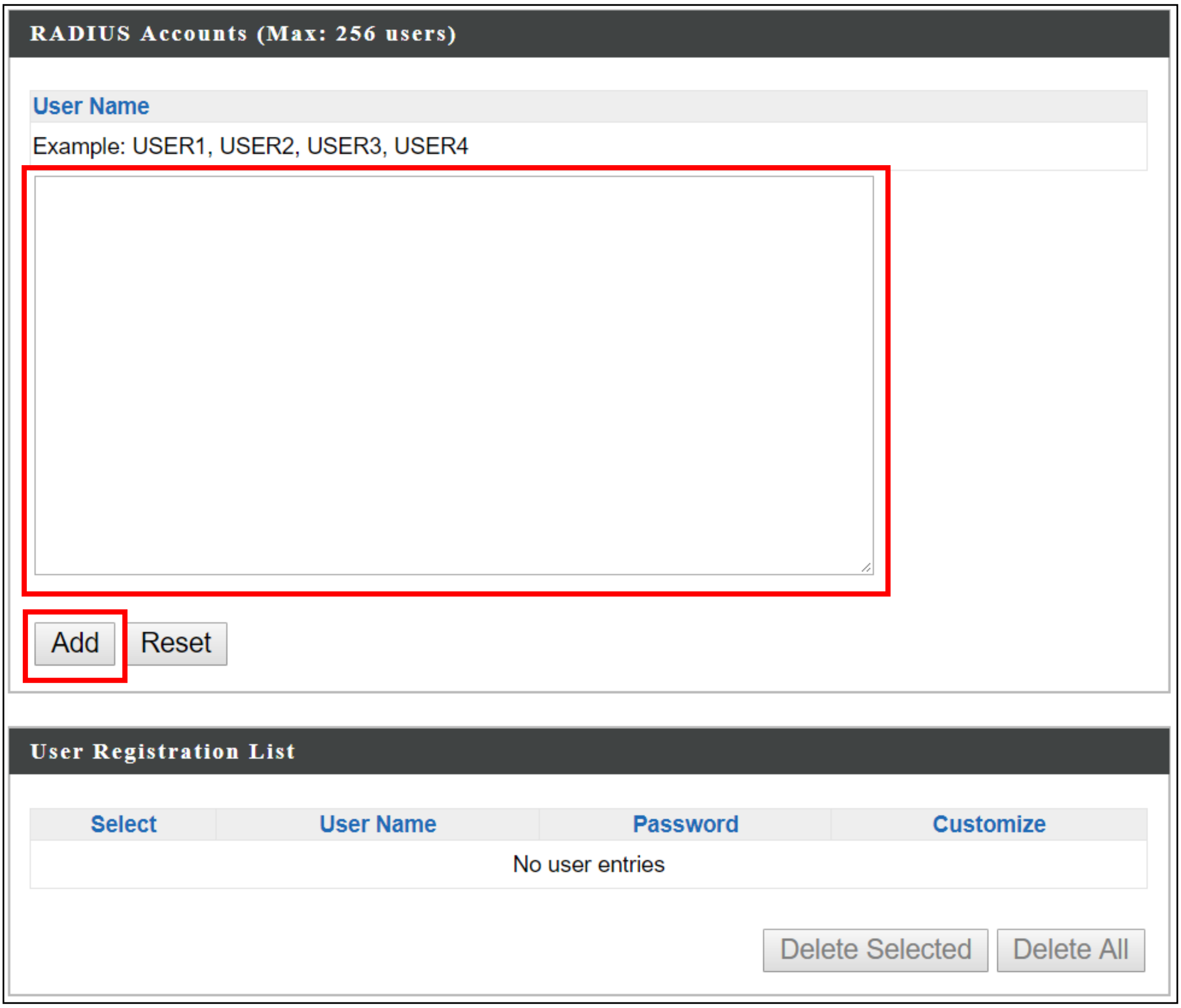
Internal Server	Check/uncheck to enable/disable the access point's internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click "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 ***VI-3-3-3*** or ***VI-3-4-3***.
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.

VI-3-6-3 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)

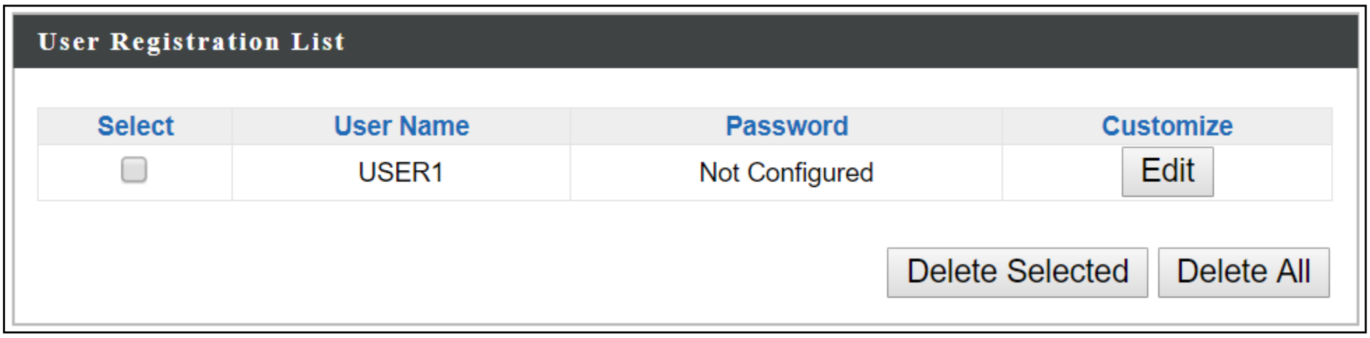
User Name

Example: USER1, USER2, USER3, USER4

User Registration List

Select	User Name	Password	Customize
No user entries			

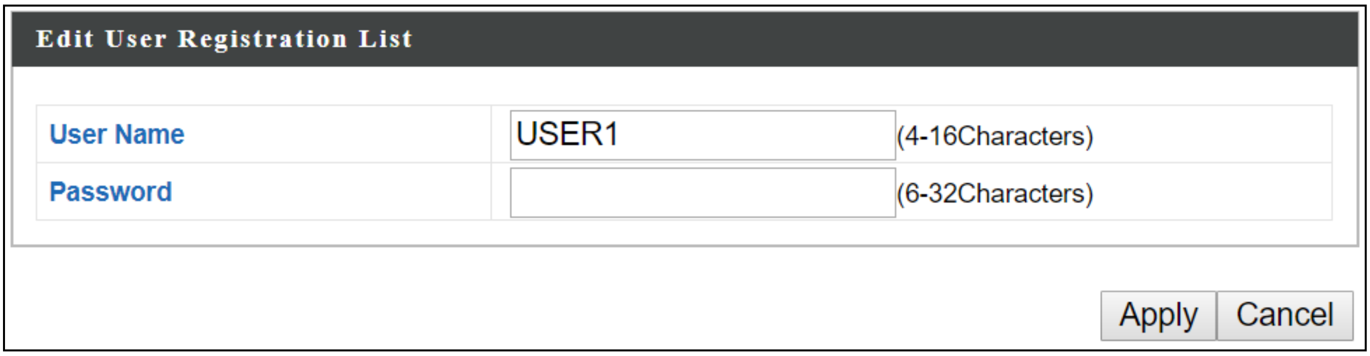
Enter a username in the box below and click "Add" to add the username.



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.

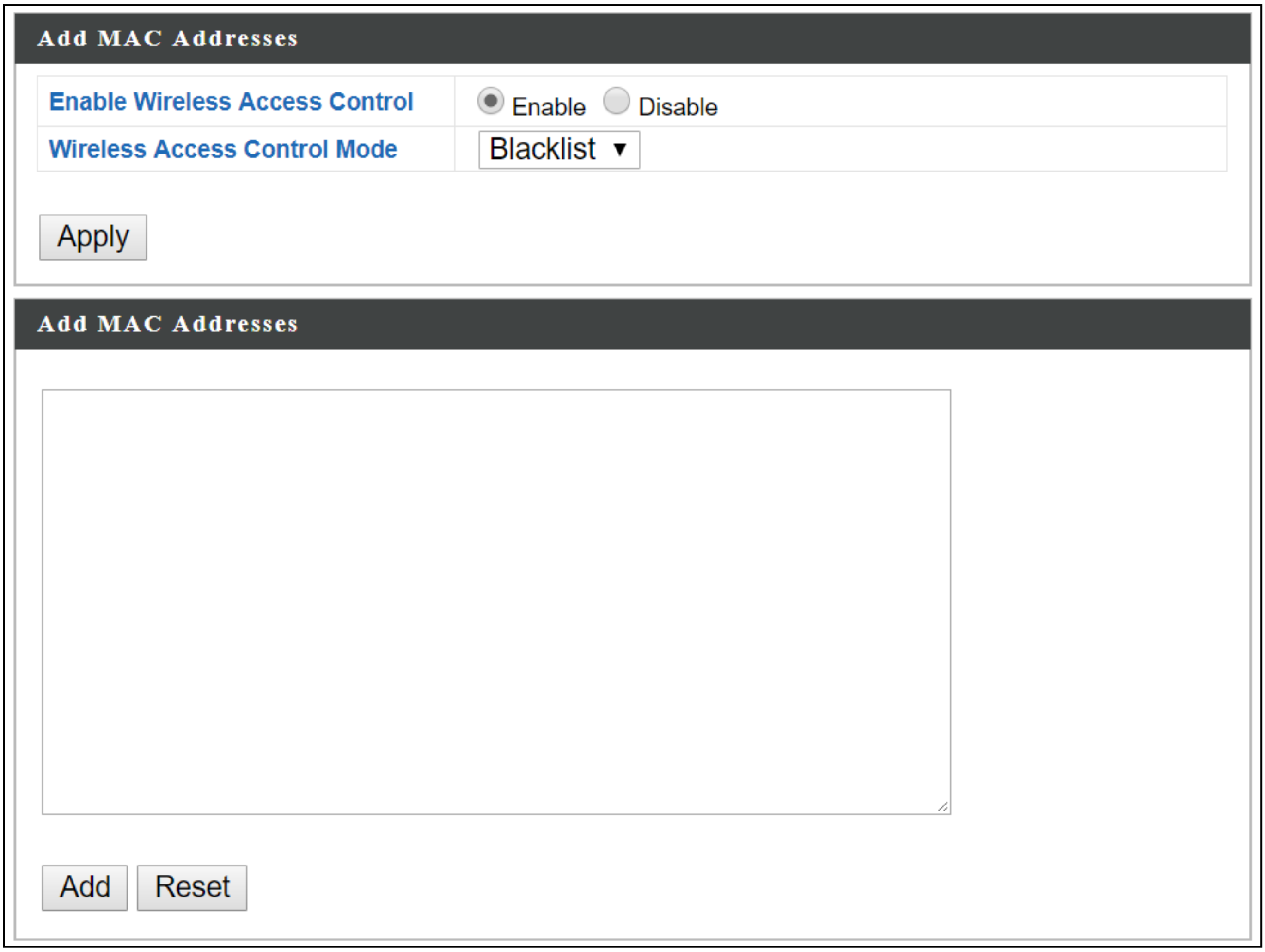
VI-3-7 MAC Filter

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*** *VI-3-3-3* ***or*** *VI-3-4-3****).***

The MAC address filtering table is displayed below:



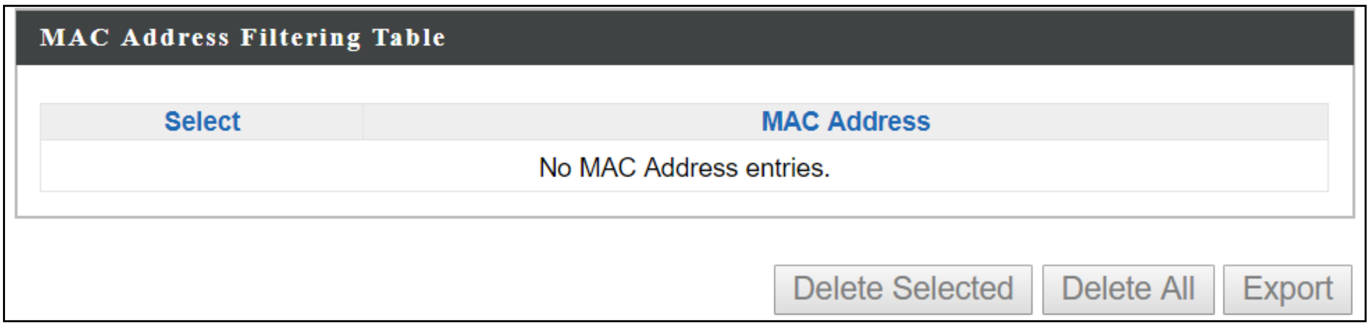
Add MAC Addresses

Enable Wireless Access Control	● Enable ○ Disable
Wireless Access Control Mode	Blacklist ▾

Add MAC Addresses

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.



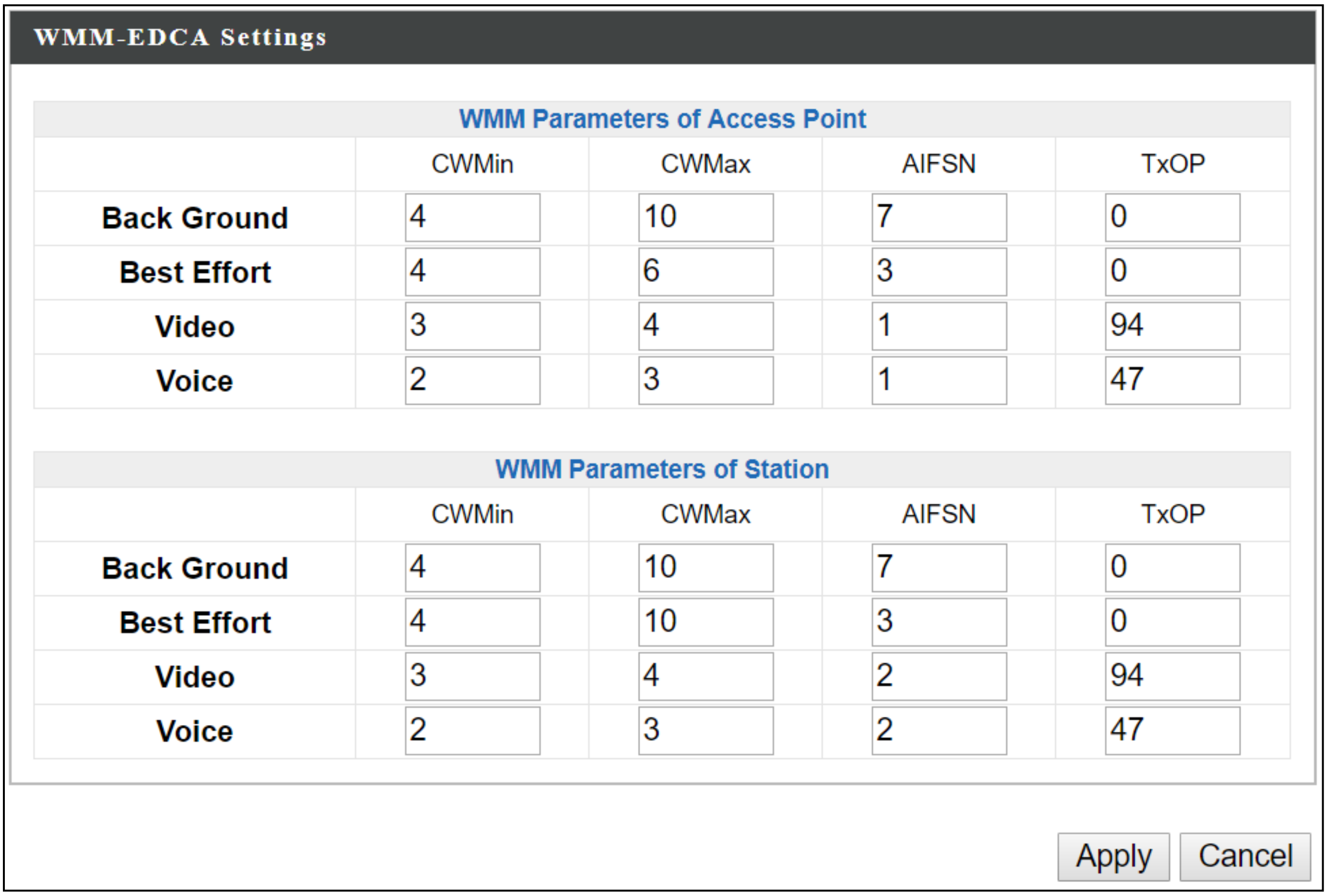
MAC Address Filtering Table

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.

VI-3-8 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:

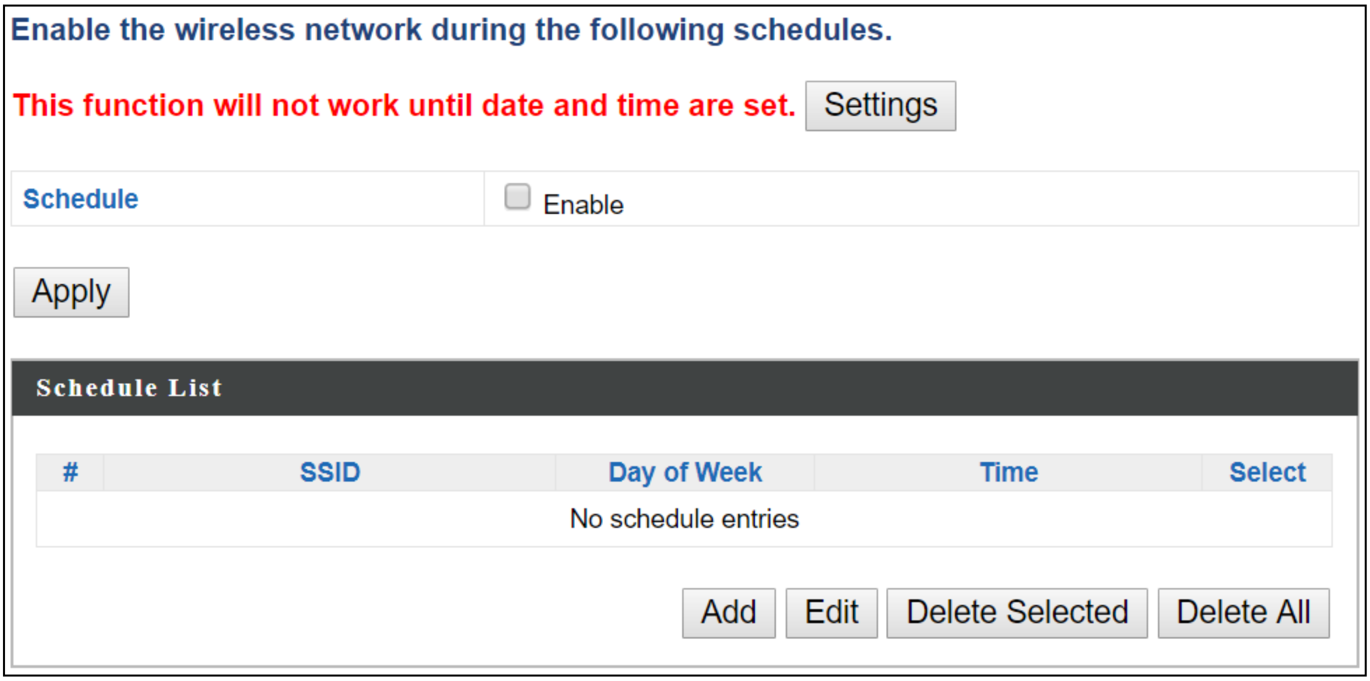
CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value 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.

VI-3-9 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.

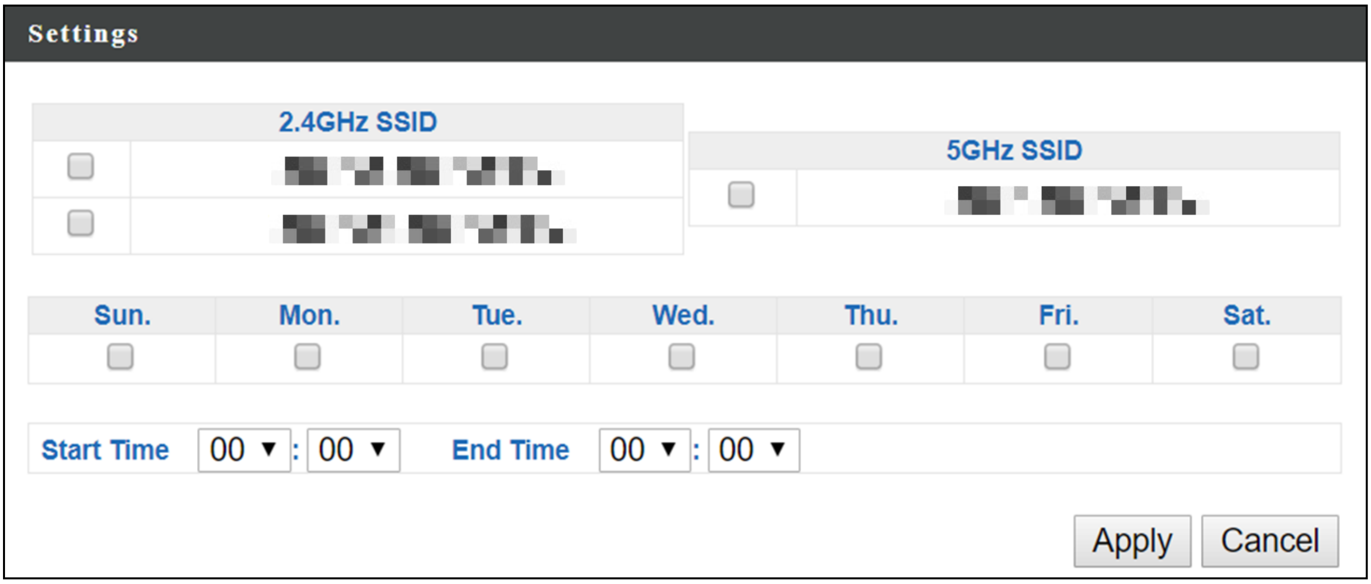
This function will not work until date and time are set.

Schedule	□ Enable

#	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

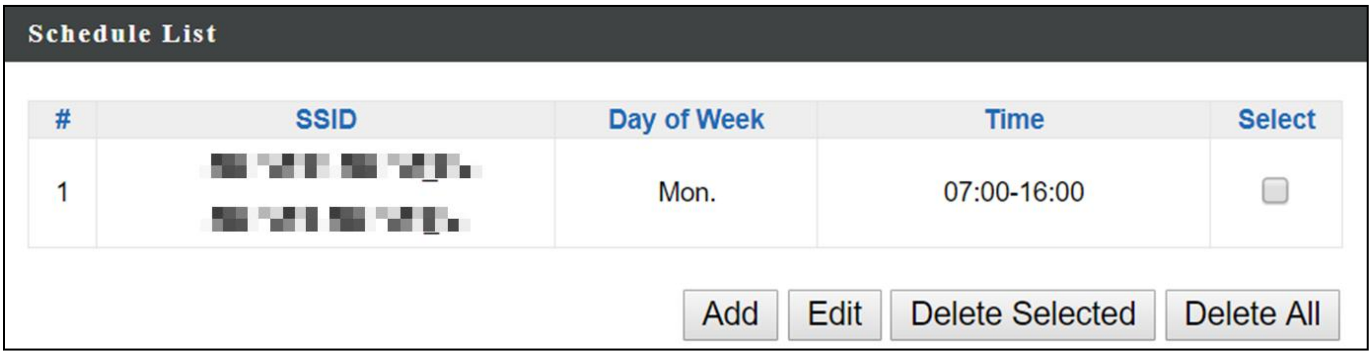
2.4GHz SSID	
□	[redacted]
□	[redacted]

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

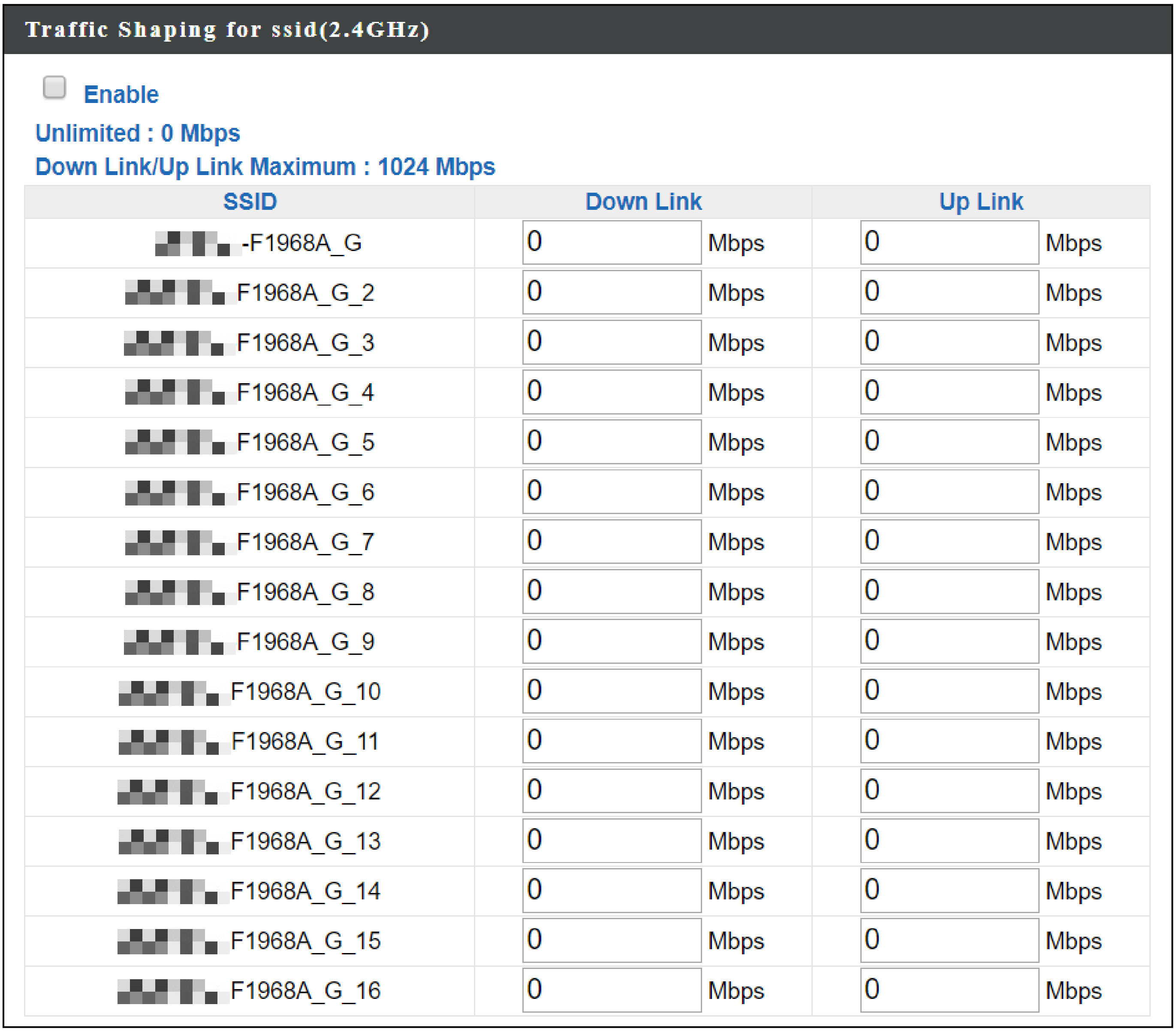
#	SSID	Day of Week	Time	Select
1	[redacted]	Mon.	07:00-16:00	□

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.

VI-3-10 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.



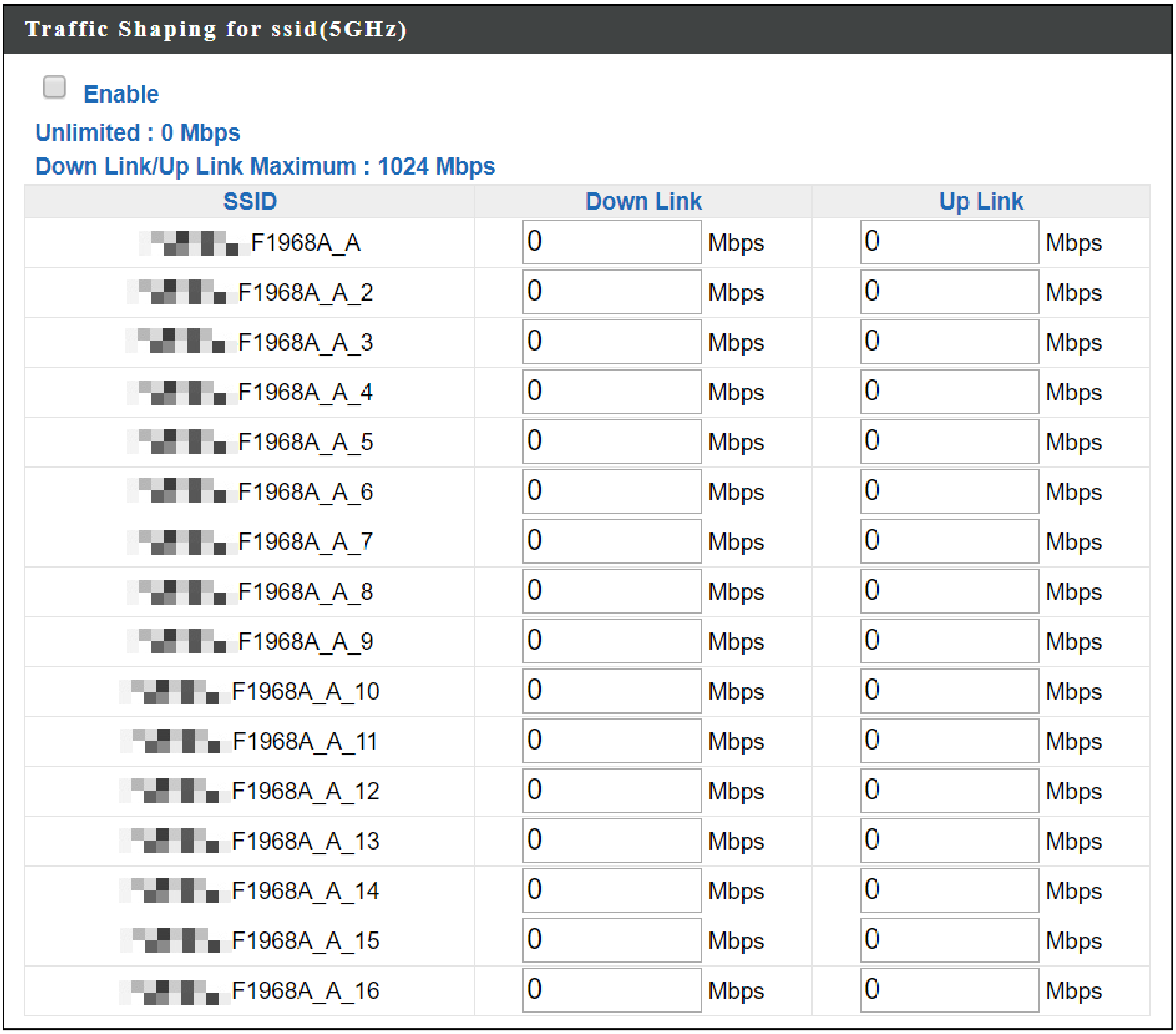
Traffic Shaping for ssid(2.4GHz)

□ 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

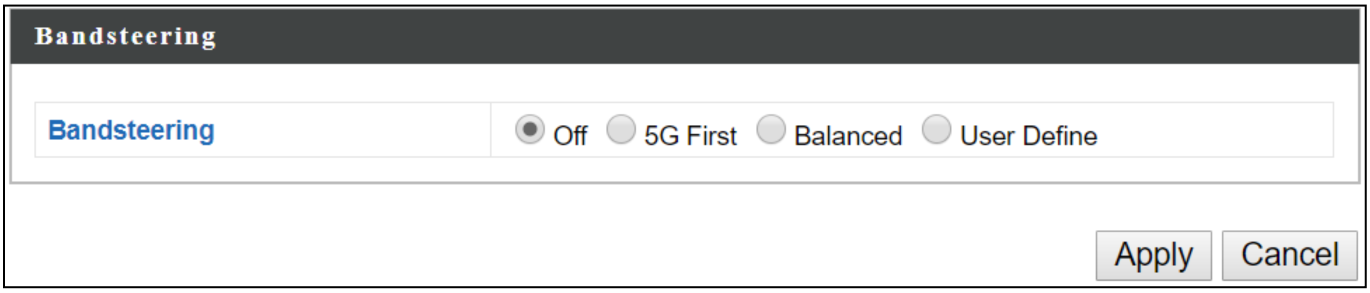
Unlimited : 0 Mbps

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

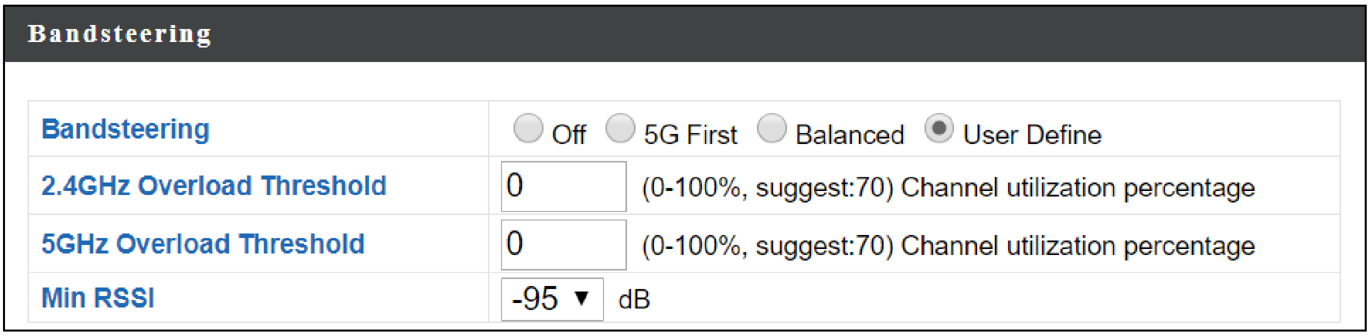
VI-3-11 Bandsteering

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

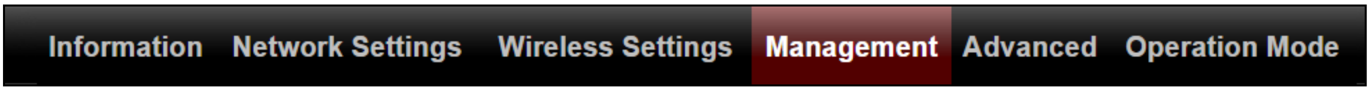
Bandsteering	● Off ○ 5G First ○ Balanced ○ User Define



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

VI-4 Management

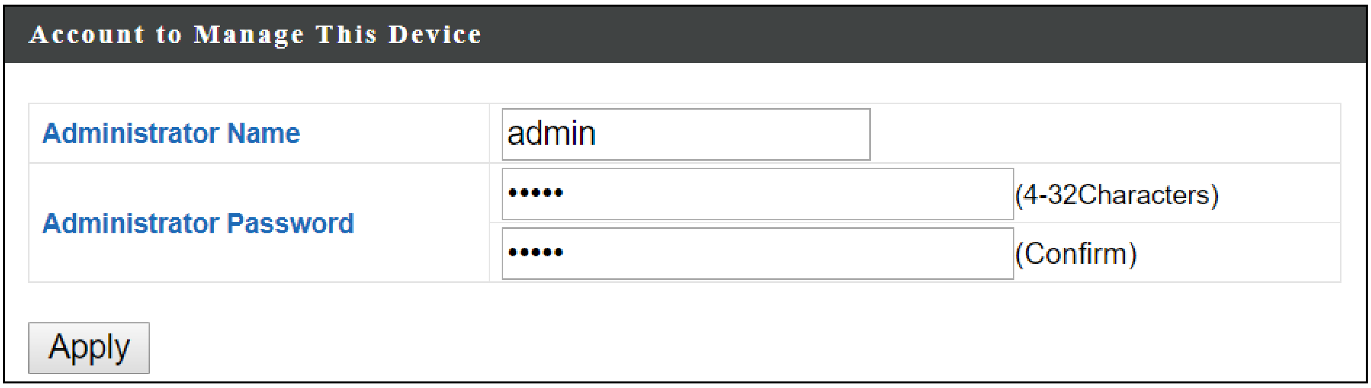


(Configurable for AP Mode only)

VI-4-1 Admin

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

> ⚠ ***If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see** I-5 Reset **for how to reset the access point.***

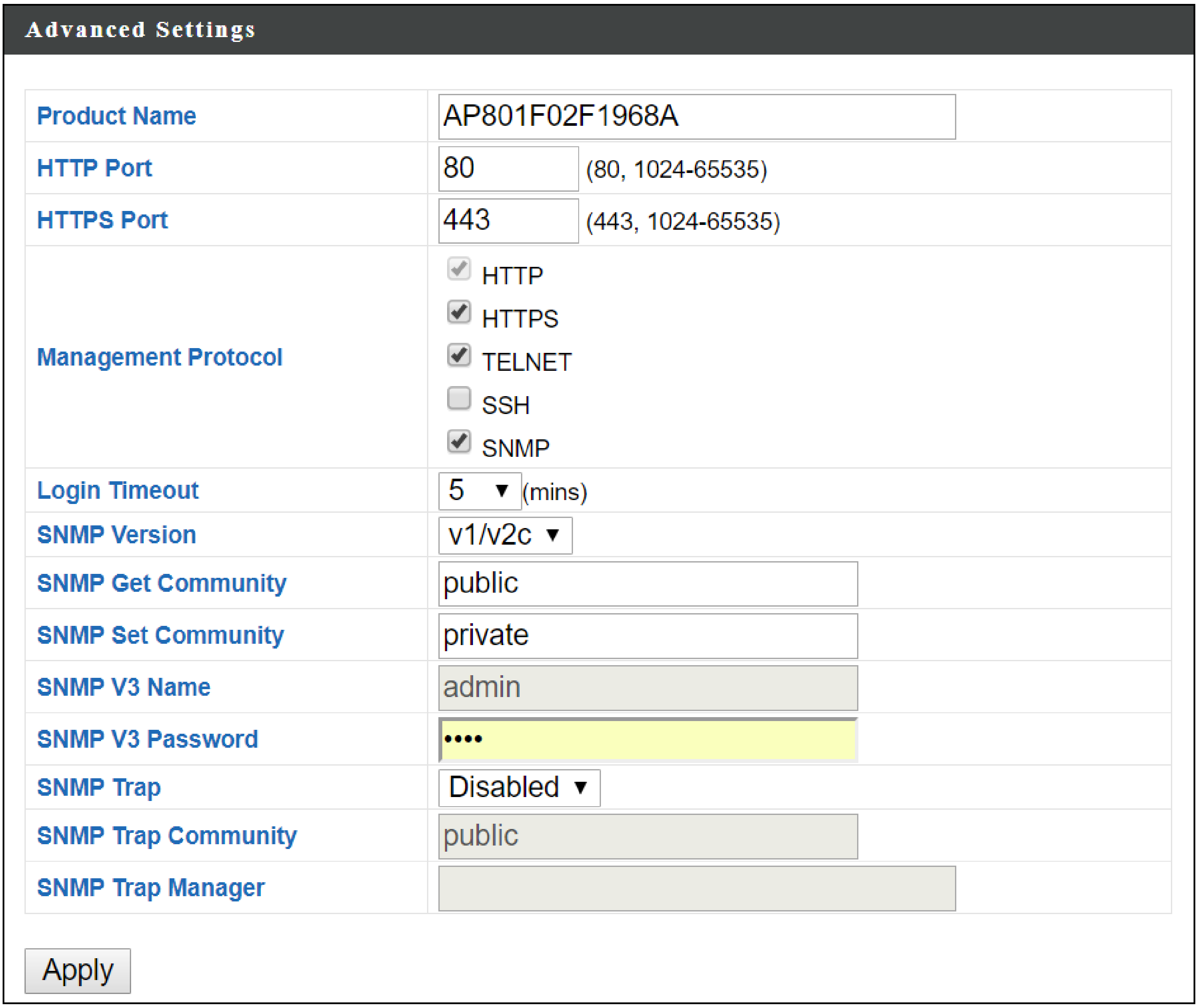


Account to Management This Device

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

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

Press “Apply” to apply the configuration.



Advanced Settings

Product Name	AP801F02F1968A
HTTP Port	80 (80, 1024-65535)
HTTPS Port	443 (443, 1024-65535)
Management Protocol	☑ HTTP ☑ HTTPS ☑ TELNET ☐ SSH ☑ SNMP
Login Timeout	5 ▼ (mins)
SNMP Version	v1/v2c ▼
SNMP Get Community	public
SNMP Set Community	private
SNMP V3 Name	admin
SNMP V3 Password	••••
SNMP Trap	Disabled ▼
SNMP Trap Community	public
SNMP Trap Manager	

Apply

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

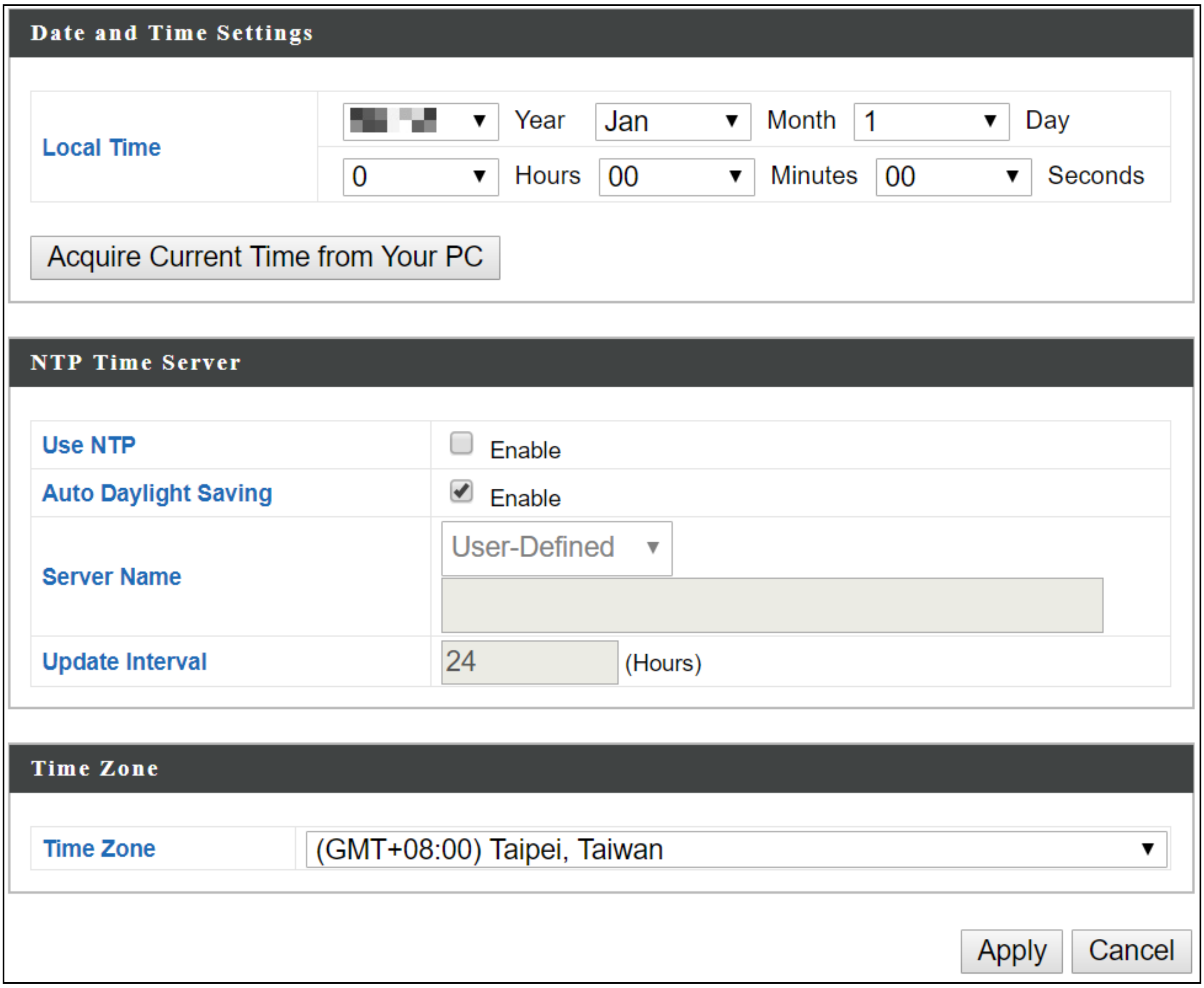
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (2-128 alphanumeric characters) of the SNMP manager.

HTTP
Internet browser HTTP protocol management interface
TELNET
Client terminal with telnet protocol management interface
SNMP
Simple Network Management Protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (USM) architecture.

Press “Apply” to apply the configuration.

VI-4-2 Date and Time

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



Date and Time Settings

Local Time: [redacted] Year, Jan Month, 1 Day, 0 Hours, 00 Minutes, 00 Seconds

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

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

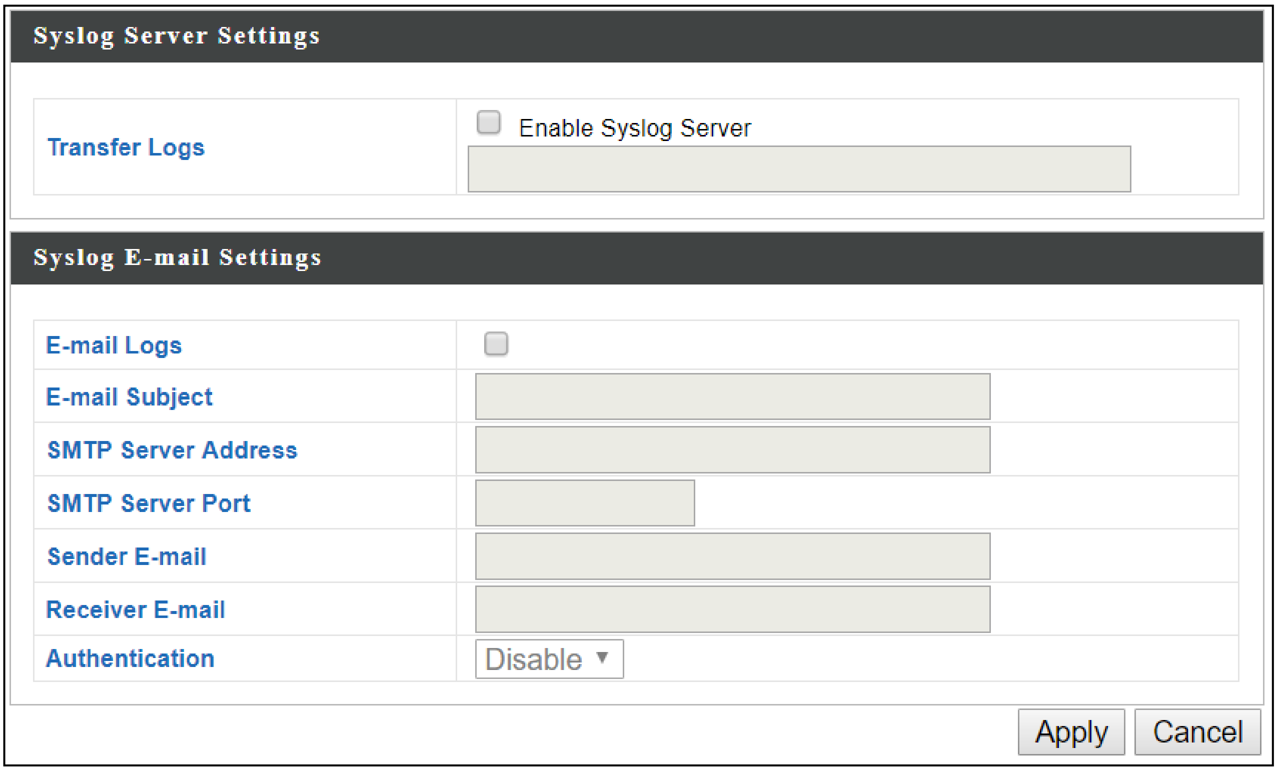
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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

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

VI-4-3 Syslog Server

The system log can be sent to a server.



Syslog Server Settings

Transfer Logs: □ Enable Syslog Server

Syslog E-mail Settings

E-mail Logs: □

E-mail Subject

SMTP Server Address

SMTP Server Port

Sender E-mail

Receiver E-mail

Authentication: Disable ▾

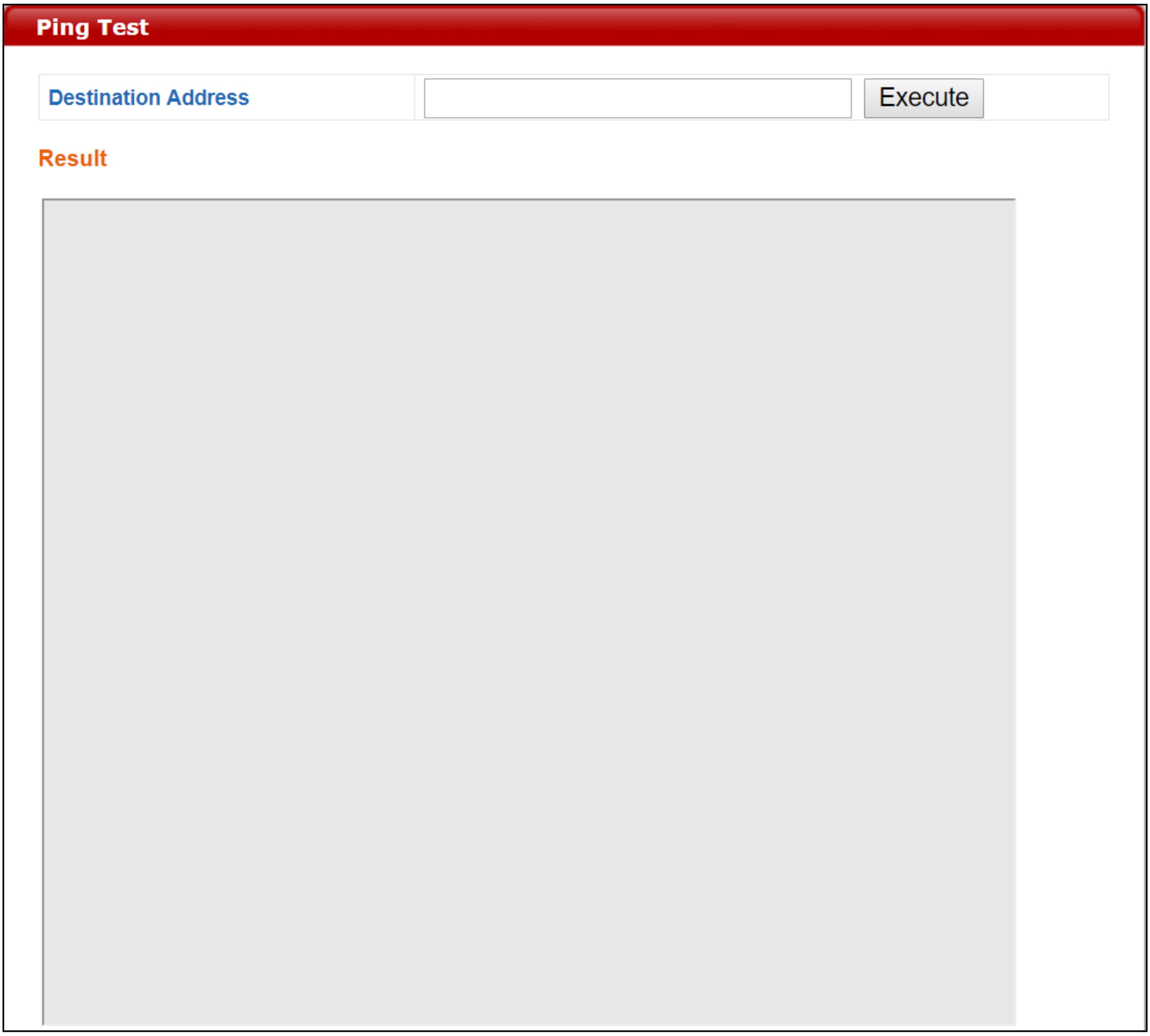
Syslog Server Settings	
Transfer Logs	Check the box to enable the use of a syslog server. Enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.

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

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

VI-4-4 Ping Test

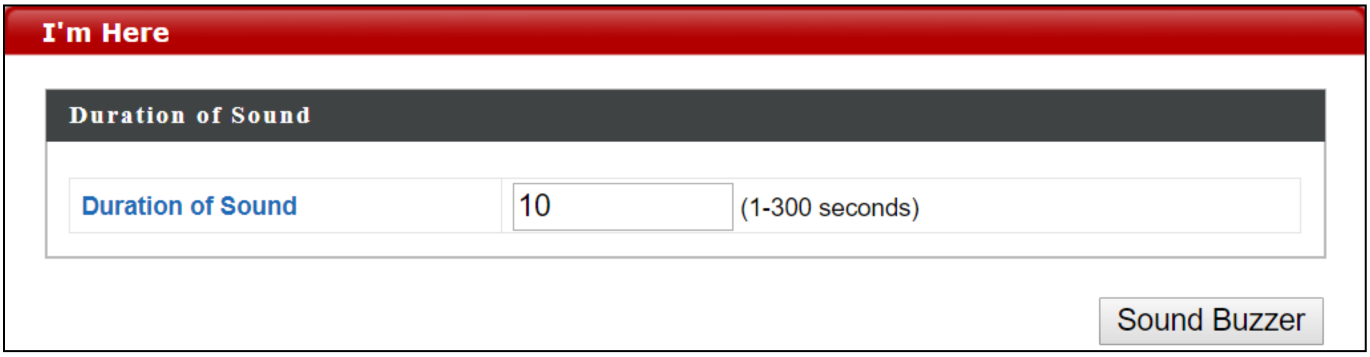
The access point includes a built-in ping test function. Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.



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

VI-4-5 I'm Here

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



I'm Here

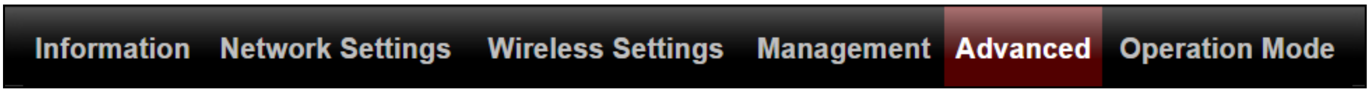
Duration of Sound

Duration of Sound: 10 (1-300 seconds)

⚠ ***The buzzer is loud!***

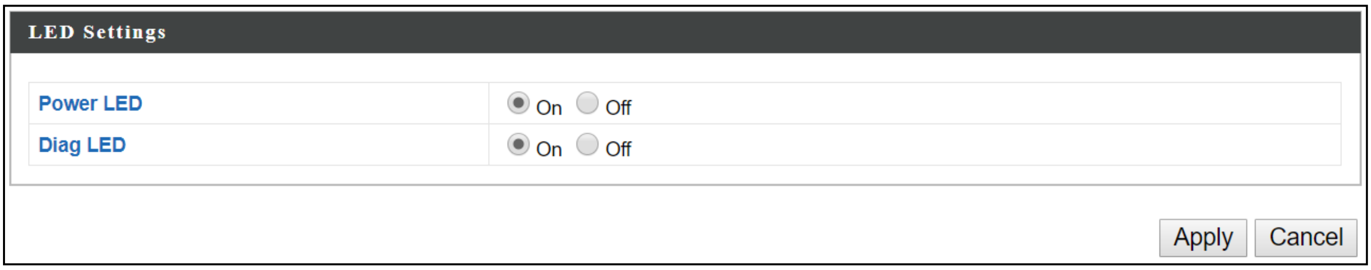
Duration of Sound	Set the duration for which the buzzer will sound when the "Sound Buzzer" button is clicked.
Sound Buzzer	Activate the buzzer sound for a duration specified above.

VI-5 Advanced



VI-5-1 LED Settings

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



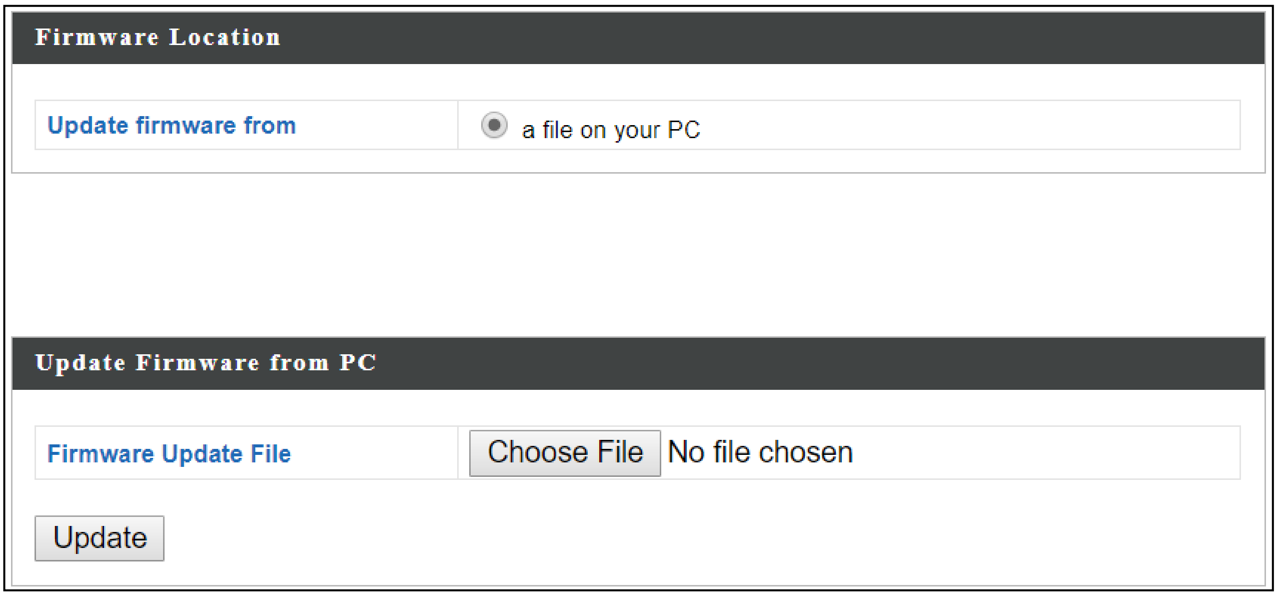
LED Settings

Power LED	● On ○ Off
Diag LED	● On ○ Off

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

VI-5-2 Update Firmware

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



Firmware Location

Update firmware from	● a file on your PC

Update Firmware from PC

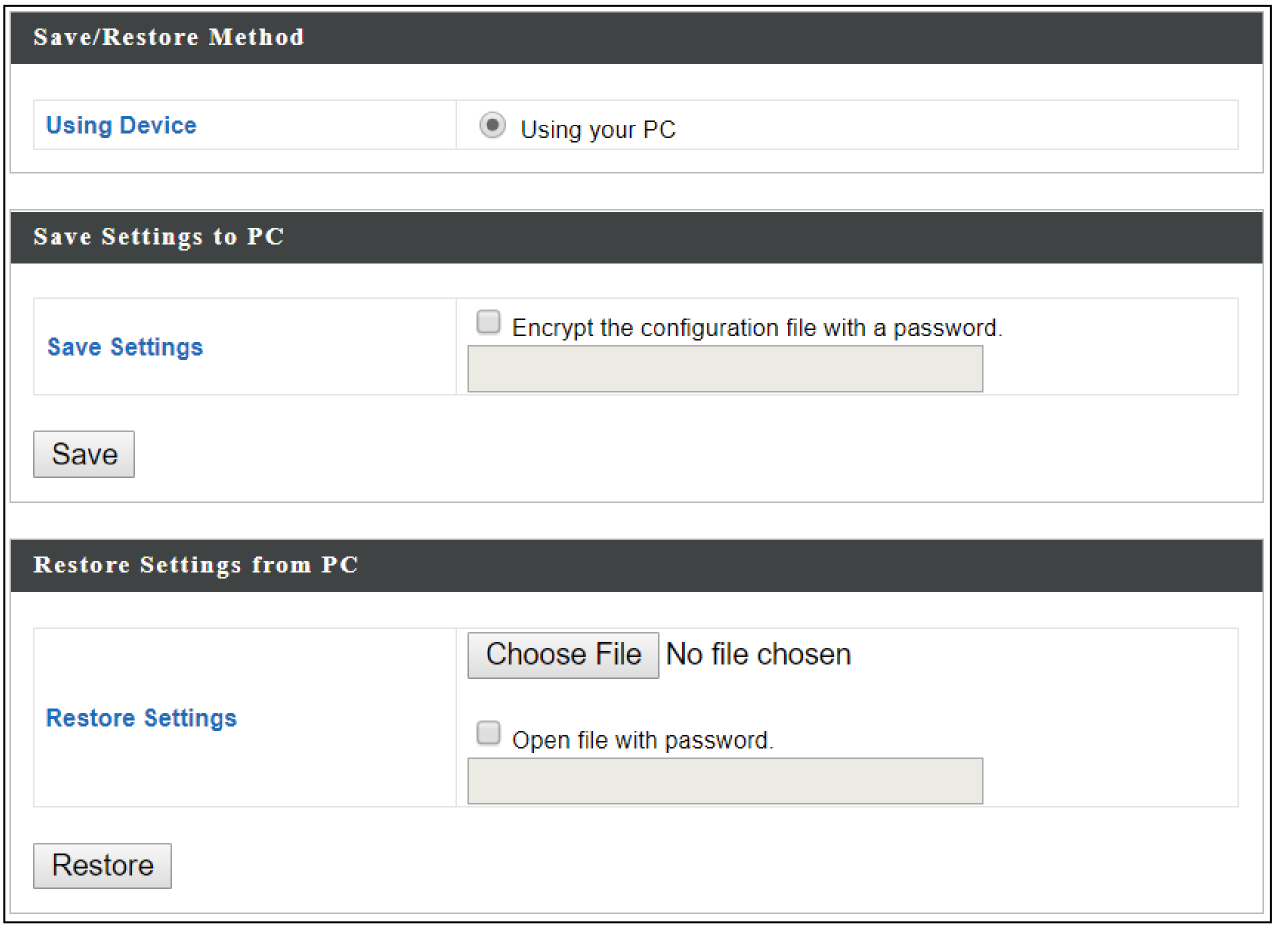
Firmware Update File	Choose File No file chosen

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

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

VI-5-3 Save / Restore Settings

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



Using Device: ● Using your PC

Save Settings: □ Encrypt the configuration file with a password.

Restore Settings: No file chosen

□ Open file with password.

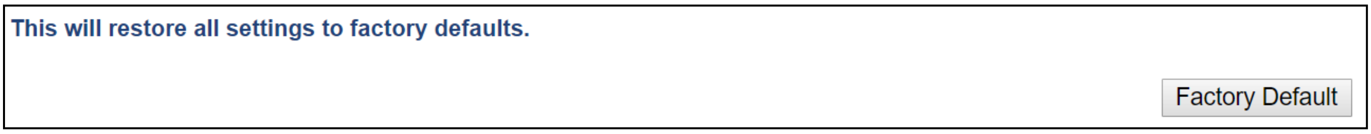
Save Settings to PC	
Save Settings	**Encryption**: If you wish to encrypt the configuration file with a password, check the "Encrypt the configuration file with a password" box and enter a password. Click "Save" to save current settings. A new window will open to allow you to specify a location to save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

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

	Click “Restore” to replace your current settings.

VI-5-4 Factory Default

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



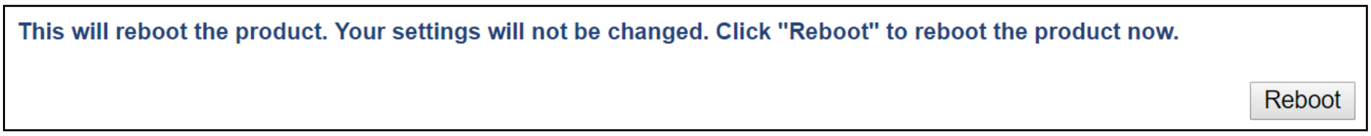
This will restore all settings to factory defaults.

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

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

VI-5-5 Reboot

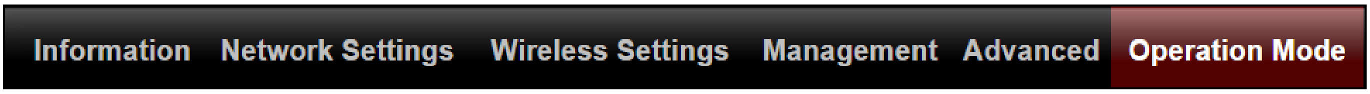
If the access point malfunctions or is not responding, rebooting the device may be an option to consider. You can reboot the access point remotely using this feature.



This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.

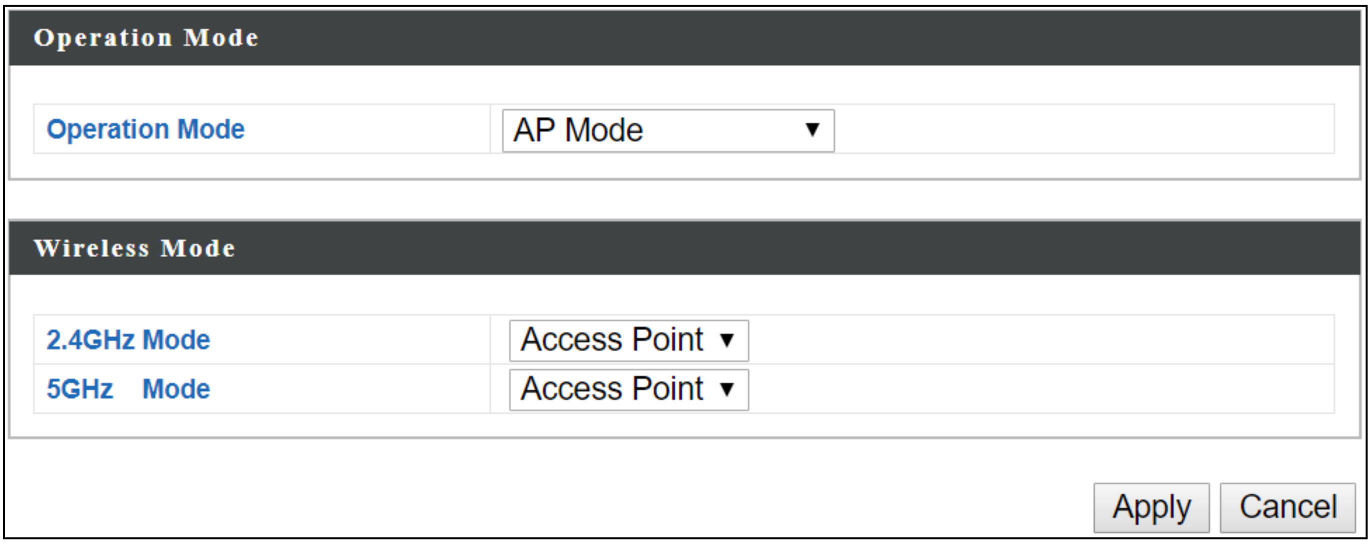
Reboot	Click “Reboot” to reboot the device. A countdown will indicate the progress of the reboot.

VI-6 Operation Mode



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

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

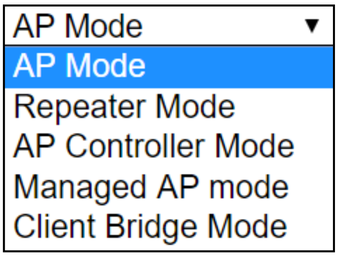


Operation Mode

Operation Mode	AP Mode ▼

Wireless Mode

2.4GHz Mode	Access Point ▼
5GHz Mode	Access Point ▼



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

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

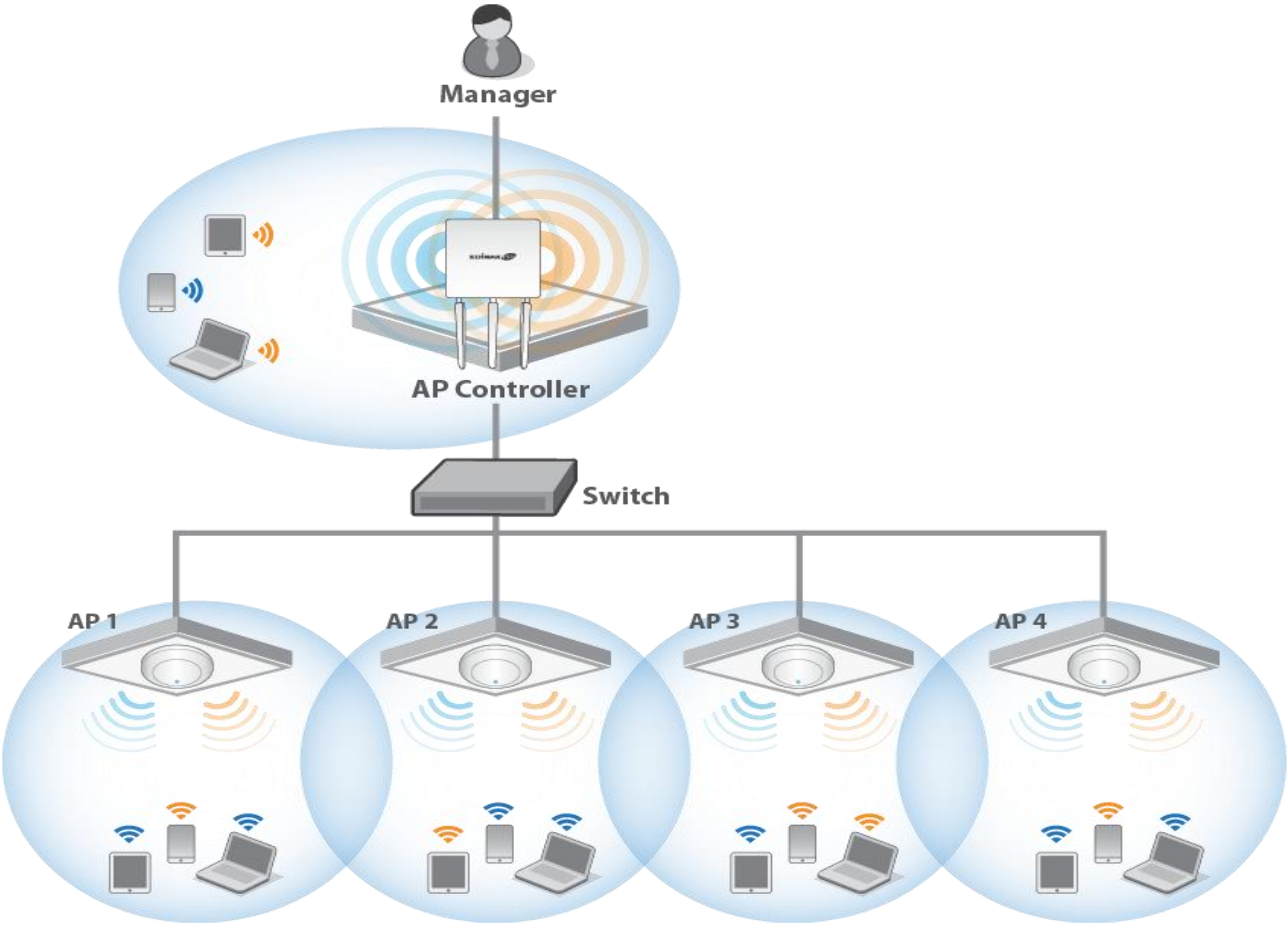
Press “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

Edimax Pro NMS

VII Product Information

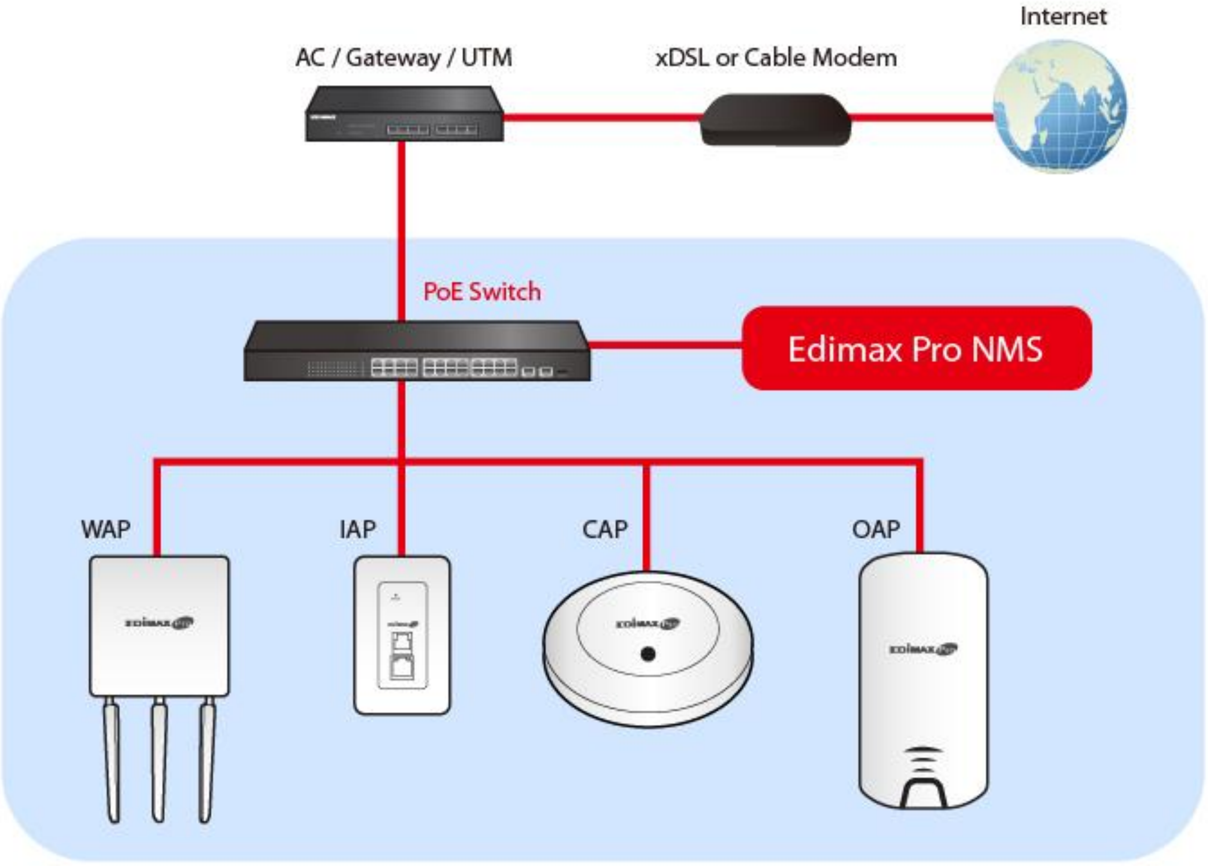
Edimax Pro Network Management Suite (NMS) supports the central management of a group of access points, otherwise known as an AP Array. NMS can be installed on one access point and support up to 16 Edimax Pro access points with no additional wireless controller required, reducing costs and facilitating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

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



VIII Quick Setup - NMS

Edimax Pro NMS (AP Controller Mode) is simple to setup. An overview of the system is shown below:

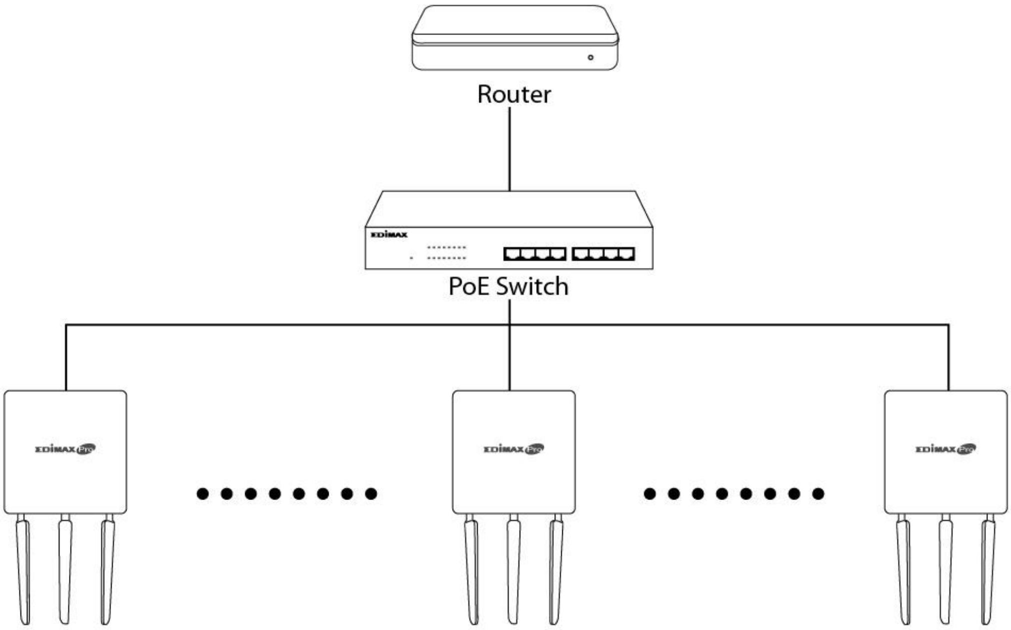


One AP (access point) is designated as the AP Controller (master) and other connected Edimax Pro APs are automatically designated as Managed APs (slaves). Using Edimax Pro NMS you can monitor, configure and manage all Managed APs (up to 16) from the single AP Controller.

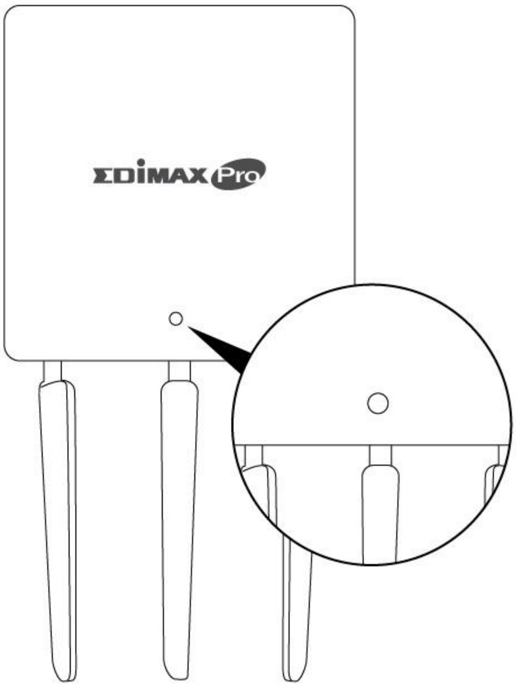
VIII-1 Hardware Deployment

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

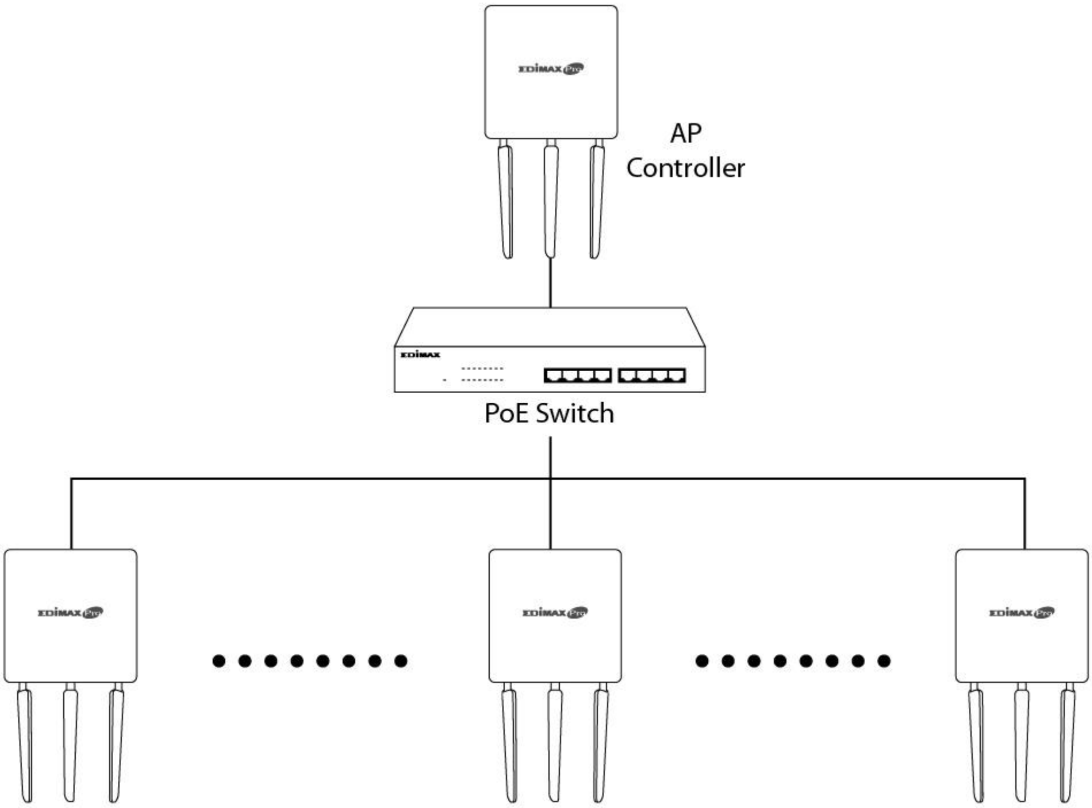
1. Connect all APs to an Ethernet or PoE switch which is connected to a gateway/router.



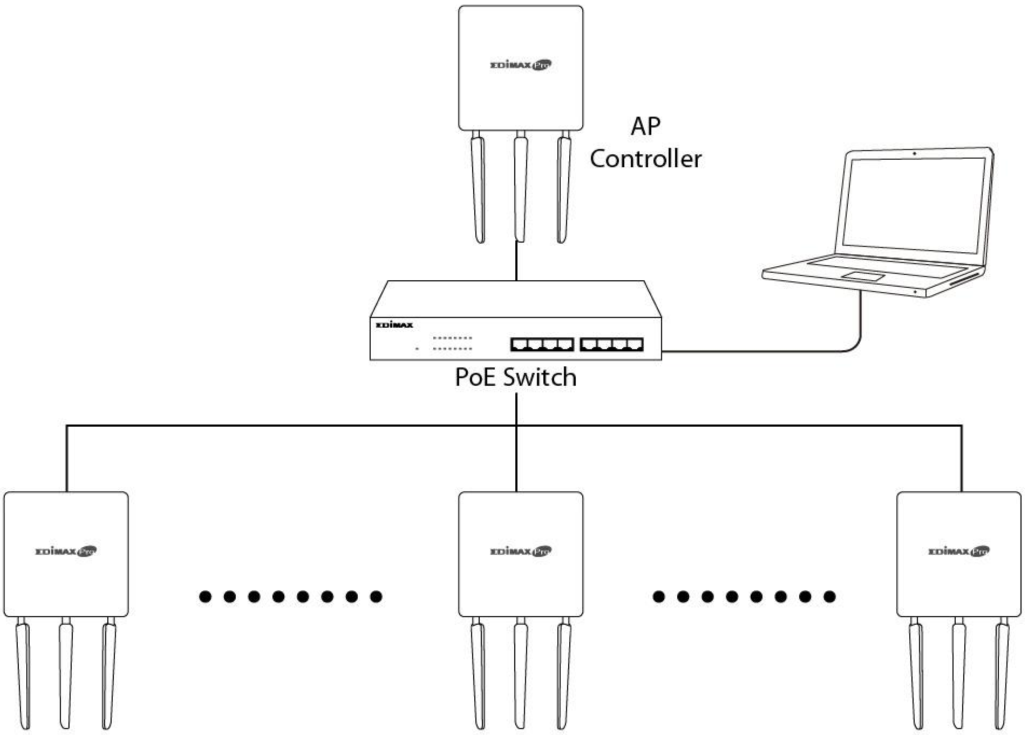
2. Ensure all APs are powered on (check their LEDs).



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



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



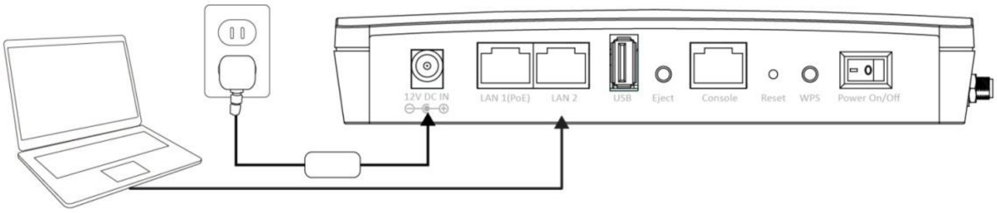
VIII-2 Software Setup

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 ***XI-1***.

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

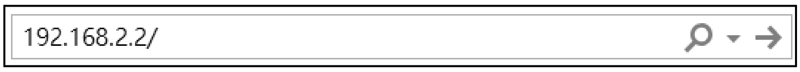
2. Disconnect the designated AP Controller from the PoE switch and connect it to your computer via Ethernet cable.

3. Connect the power adapter to the device's 12V DC port and plug the power adapter into a power supply.



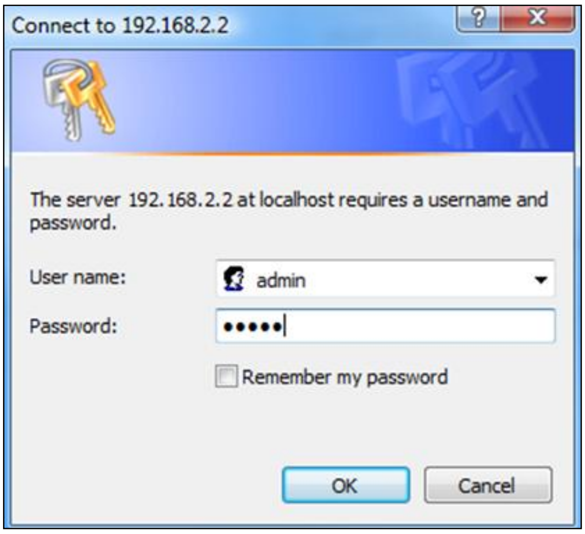
4. Please wait a moment for the device to start up. The device is ready when the LED is **blue**.

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

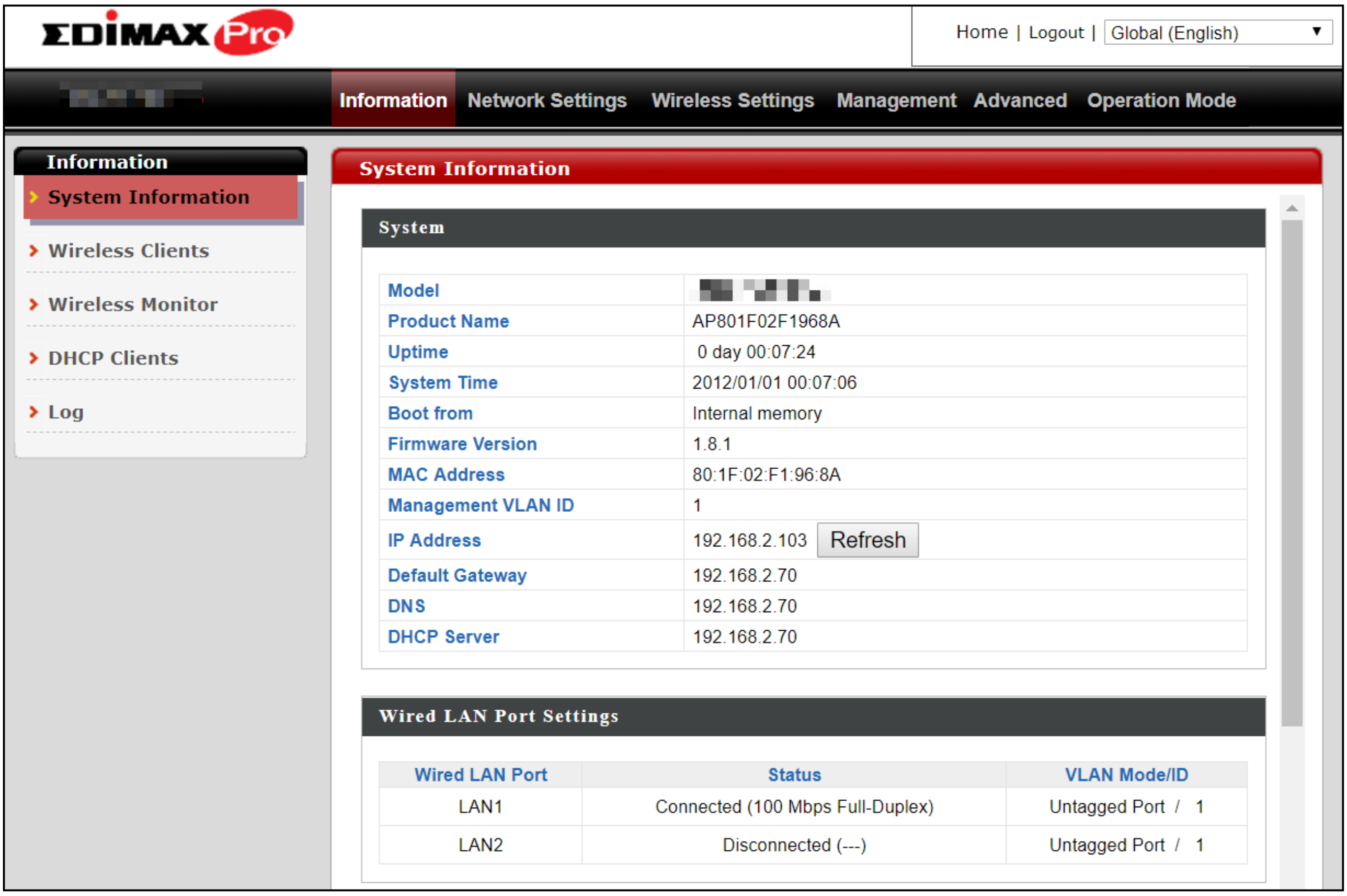
The server 192.168.2.2 at localhost requires a username and password.

User name: admin

Password: •••••

□ Remember my password

7. “System Information” home screen will be shown:



System Information

System

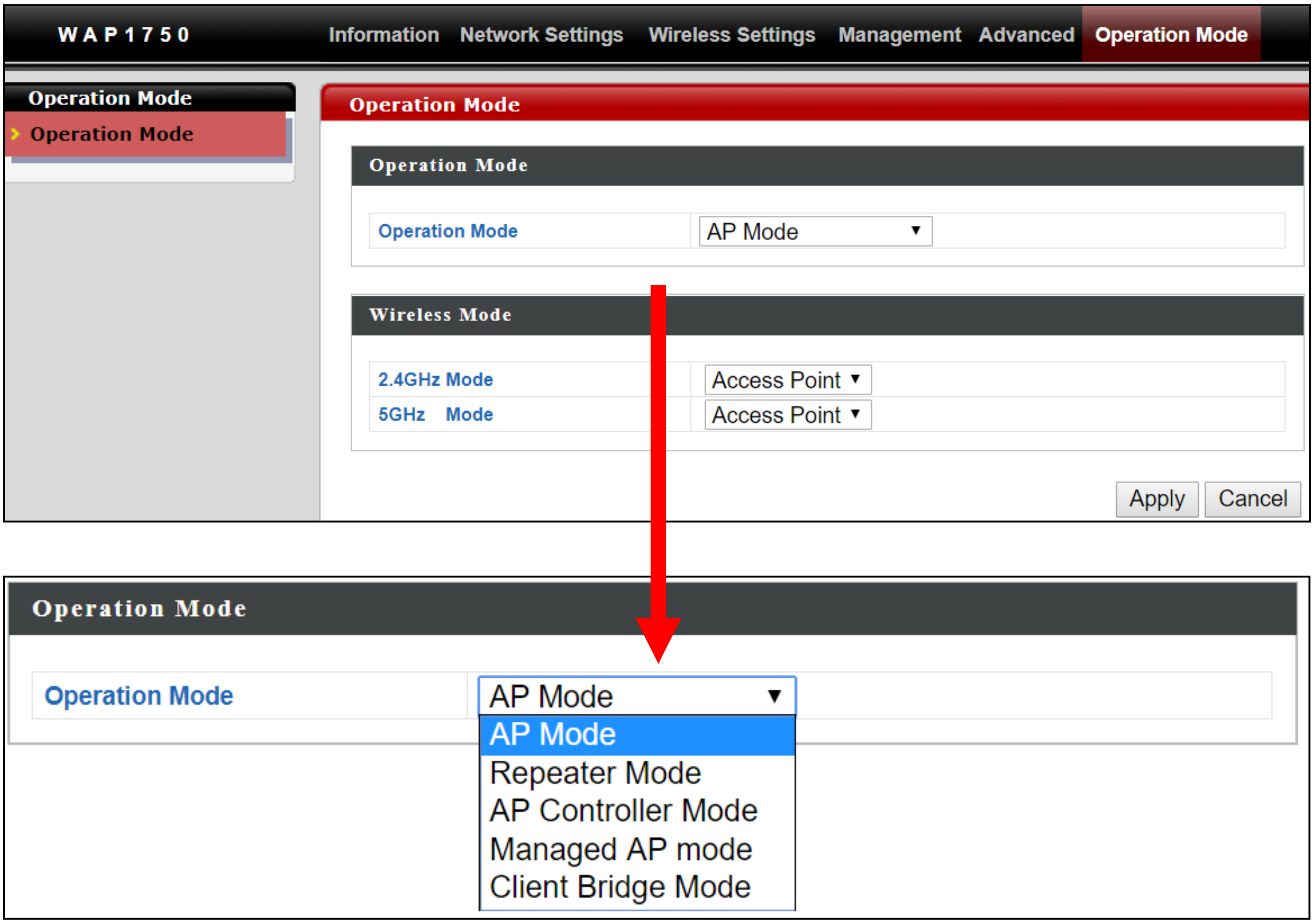
Model	[redacted]
Product Name	AP801F02F1968A
Uptime	0 day 00:07:24
System Time	2012/01/01 00:07:06
Boot from	Internal memory
Firmware Version	1.8.1
MAC Address	80:1F:02:F1:96:8A
Management VLAN ID	1
IP Address	192.168.2.103 Refresh
Default Gateway	192.168.2.70
DNS	192.168.2.70
DHCP Server	192.168.2.70

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

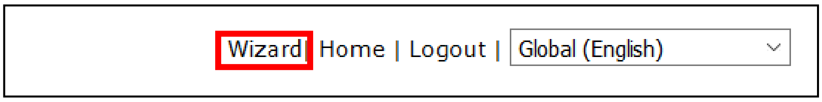
8. By default, the device is in **AP Mode**.

9. Go to “Operation Mode” to select AP Controller Mode.

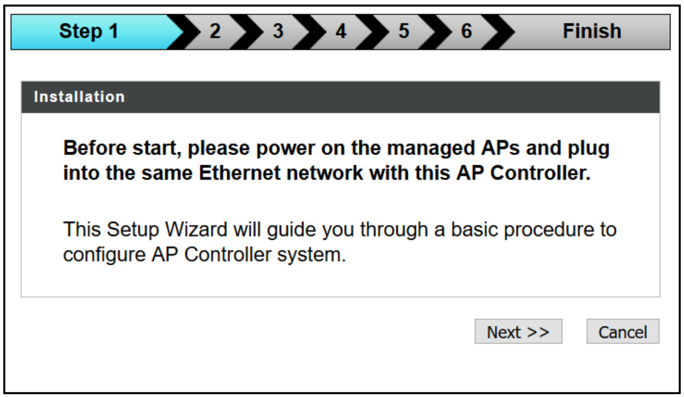


10. Once selected, press “Apply” to apply the settings.
Wait for the device to reboot.

11. Edimax Pro NMS includes a wizard to quickly setup the SSID & security for Managed APs. Go back to the web user interface, locate and click “Wizard” in the top right corner to begin the wizard.



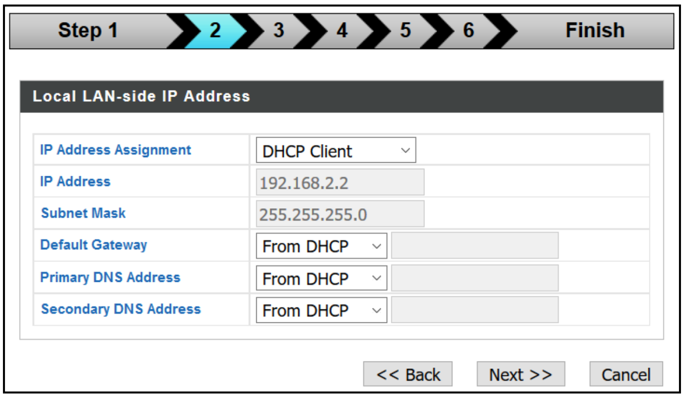
12. Follow the on-screen instructions to complete **Steps 1-6** and click **"Finish"** to save the settings.



Installation

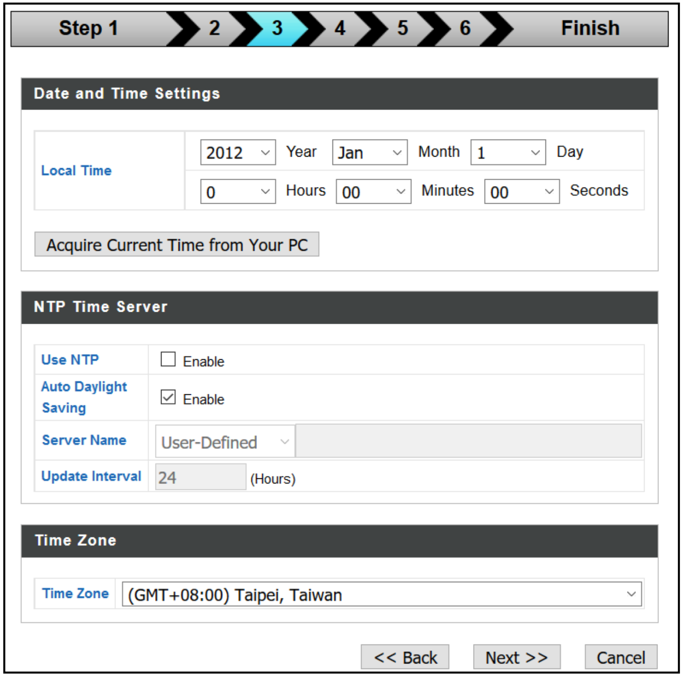
Before start, please power on the managed APs and plug into the same Ethernet network with this AP Controller.

This Setup Wizard will guide you through a basic procedure to configure AP Controller system.



Local 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
Secondary DNS Address	From DHCP



Date and Time Settings

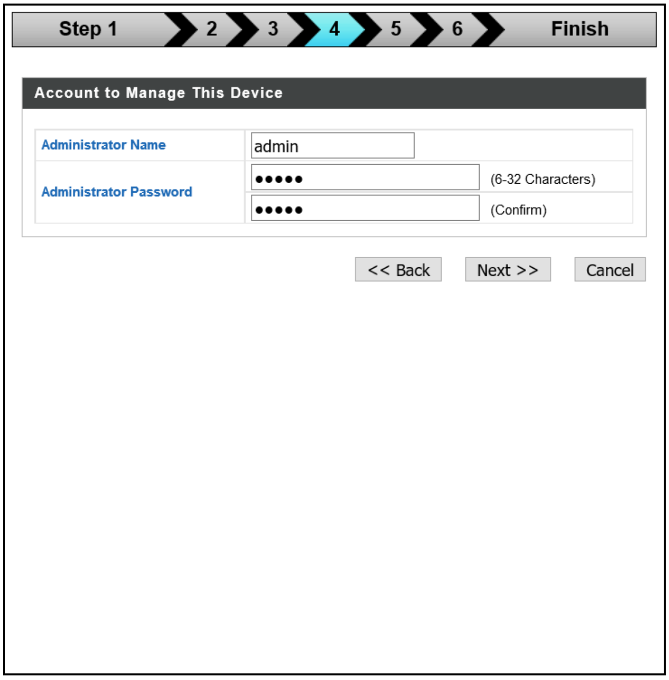
Local Time	2012 Year Jan Month 1 Day 0 Hours 00 Minutes 00 Seconds

NTP Time Server

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

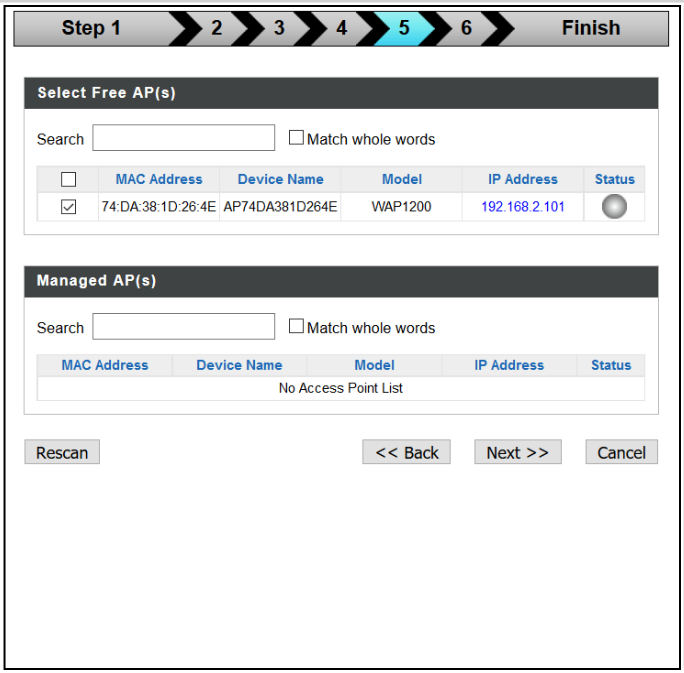
Time Zone

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



Account to Manage This Device

Administrator Name	admin
Administrator Password	●●●●● (6-32 Characters) ●●●●● (Confirm)



Select Free AP(s)

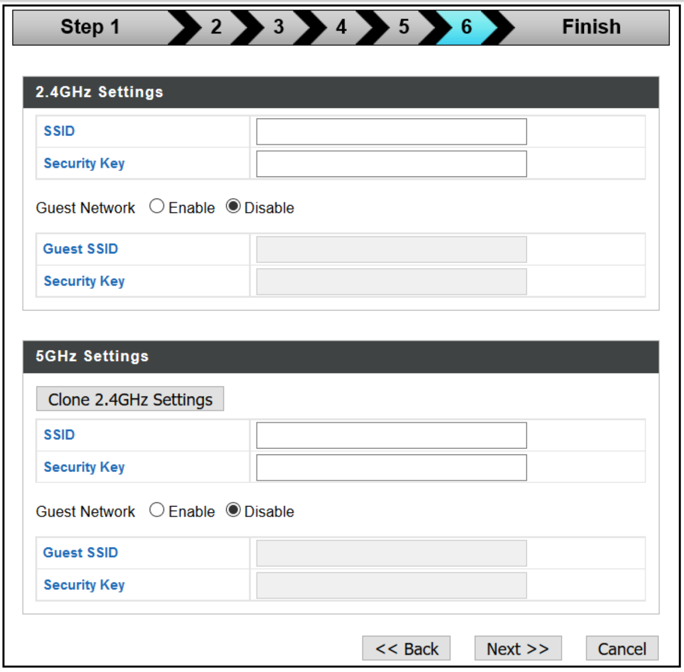
Search □Match whole words

□	MAC Address	Device Name	Model	IP Address	Status
☑	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	●

Managed AP(s)

Search □Match whole words

MAC Address	Device Name	Model	IP Address	Status
No Access Point List				



2.4GHz Settings

SSID	
Security Key	

Guest Network ○ Enable ● Disable

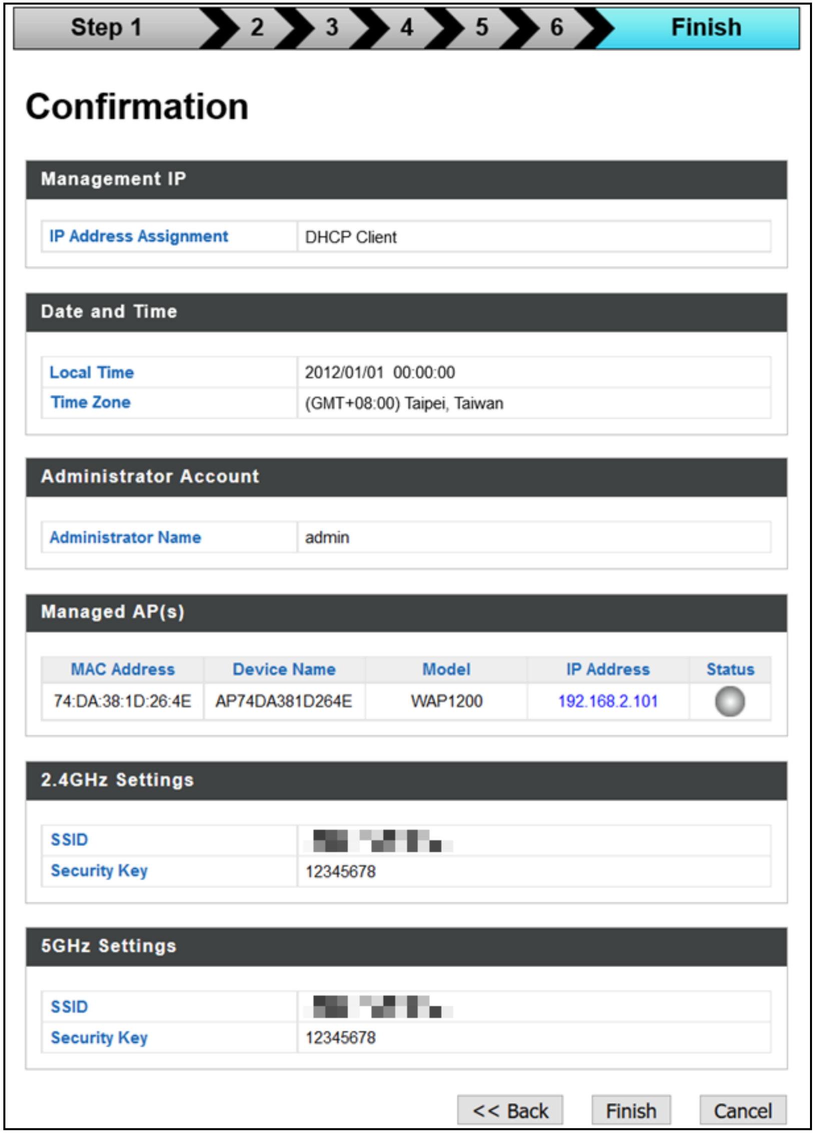
Guest SSID	
Security Key	

5GHz Settings

SSID	
Security Key	

Guest Network ○ Enable ● Disable

Guest SSID	
Security Key	



Confirmation

Management IP

IP Address Assignment	DHCP Client

Date and Time

Local Time	2012/01/01 00:00:00
Time Zone	(GMT+08:00) Taipei, Taiwan

Administrator Account

Administrator Name	admin

Managed AP(s)

MAC Address	Device Name	Model	IP Address	Status
74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	●

2.4GHz Settings

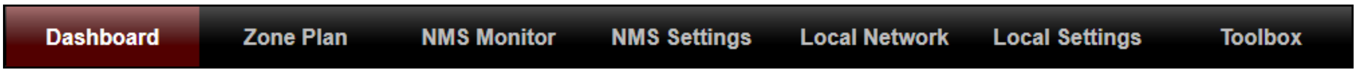
SSID	[redacted]
Security Key	12345678

5GHz Settings

SSID	[redacted]
Security Key	12345678

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

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



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

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

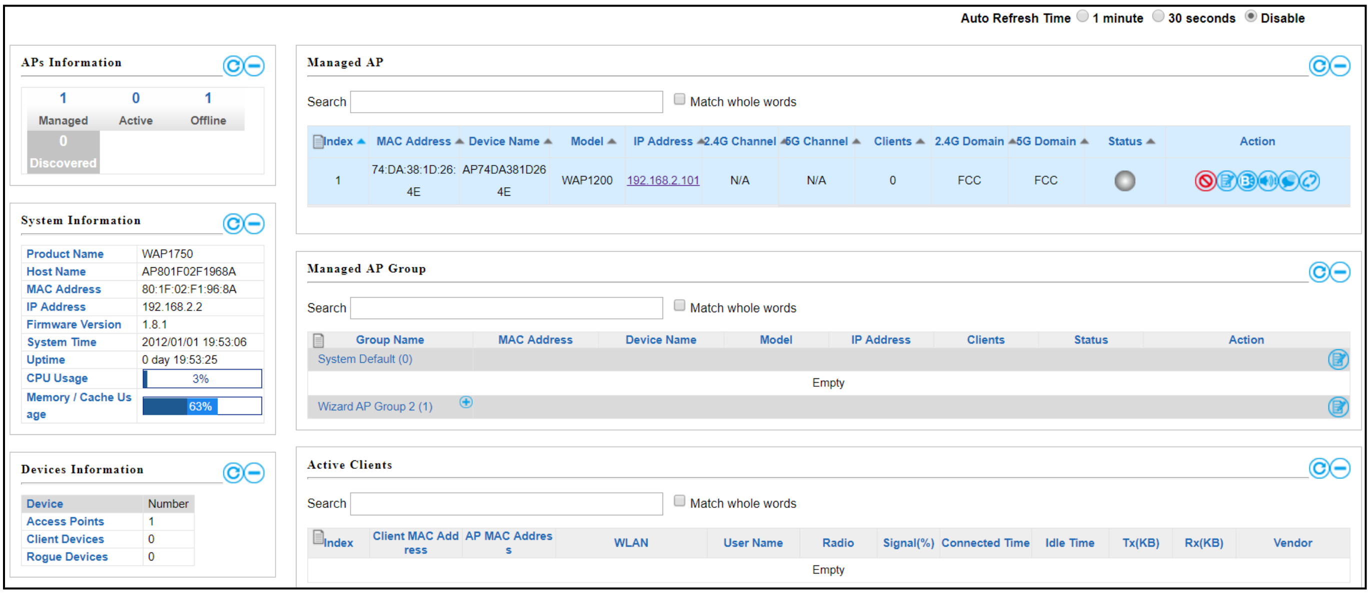
Use ***Toolbox*** to diagnose network status including *Ping*, *Traceroute*, and *IP Scan*.

IX Webpage Layout - NMS

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

Dashboard

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



Auto Refresh Time ○ 1 minute ○ 30 seconds ● Disable

APs Information

1	0	1
Managed	Active	Offline
0 Discovered		

System Information

Product Name	WAP1750
Host Name	AP801F02F1968A
MAC Address	80:1F:02:F1:96:8A
IP Address	192.168.2.2
Firmware Version	1.8.1
System Time	2012/01/01 19:53:06
Uptime	0 day 19:53:25
CPU Usage	3%
Memory / Cache Usage	63%

Devices Information

Device	Number
Access Points	1
Client Devices	0
Rogue Devices	0

Managed AP

Search □ Match whole words

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	2.4G Domain	5G Domain	Status	Action
1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	N/A	N/A	0	FCC	FCC	●	

Managed AP Group

Search □ Match whole words

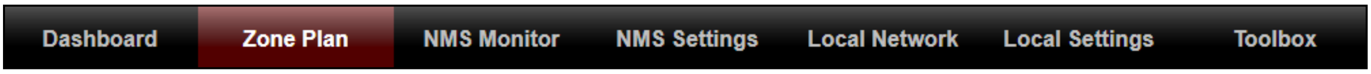
Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (0)							
Empty							
Wizard AP Group 2 (1)							

Active Clients

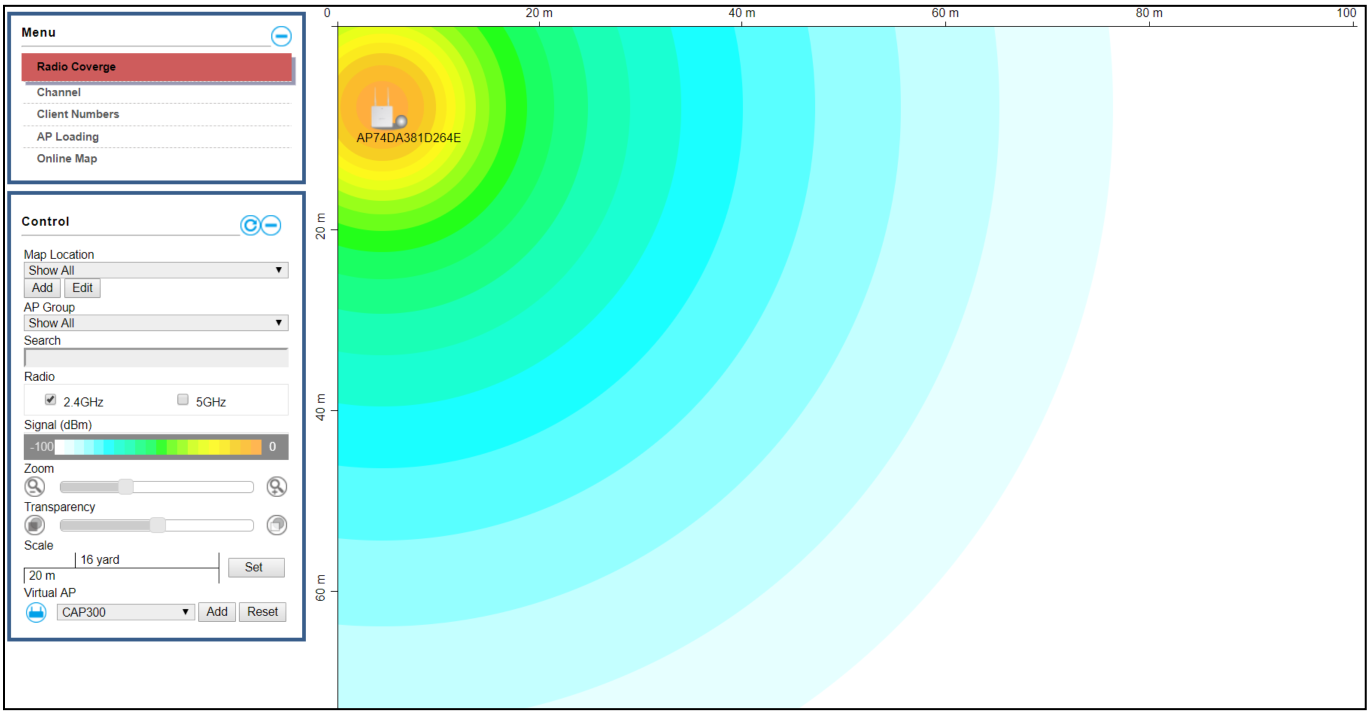
Search □ Match whole words

Index	Client MAC Address	AP MAC Address	WLAN	User Name	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
Empty											

Zone Plan



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



Map Location: Show All

AP Group: Show All

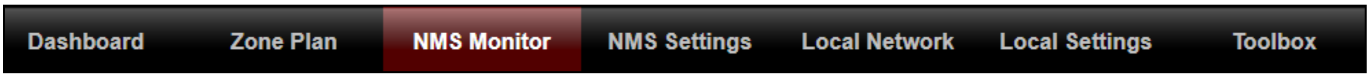
Radio: ☑ 2.4GHz ☐ 5GHz

Signal (dBm): -100 0

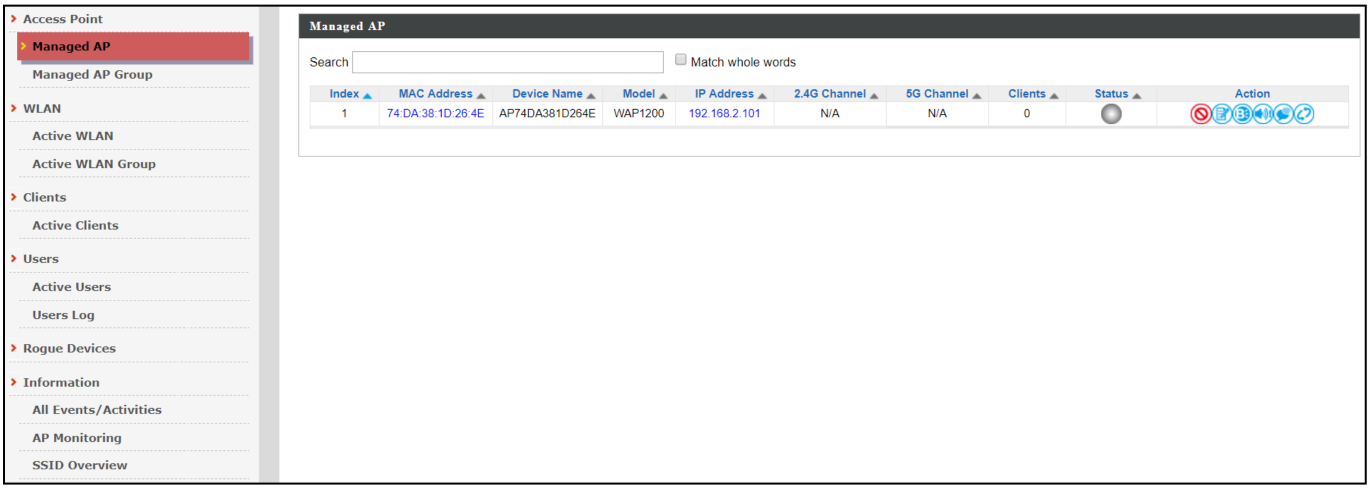
Scale: 16 yard 20 m

Virtual AP: CAP300

NMS Monitor



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

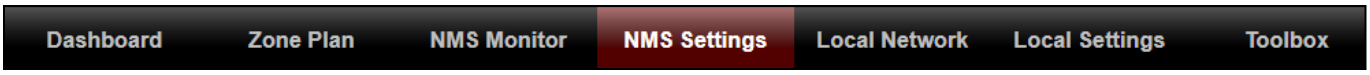


Managed AP

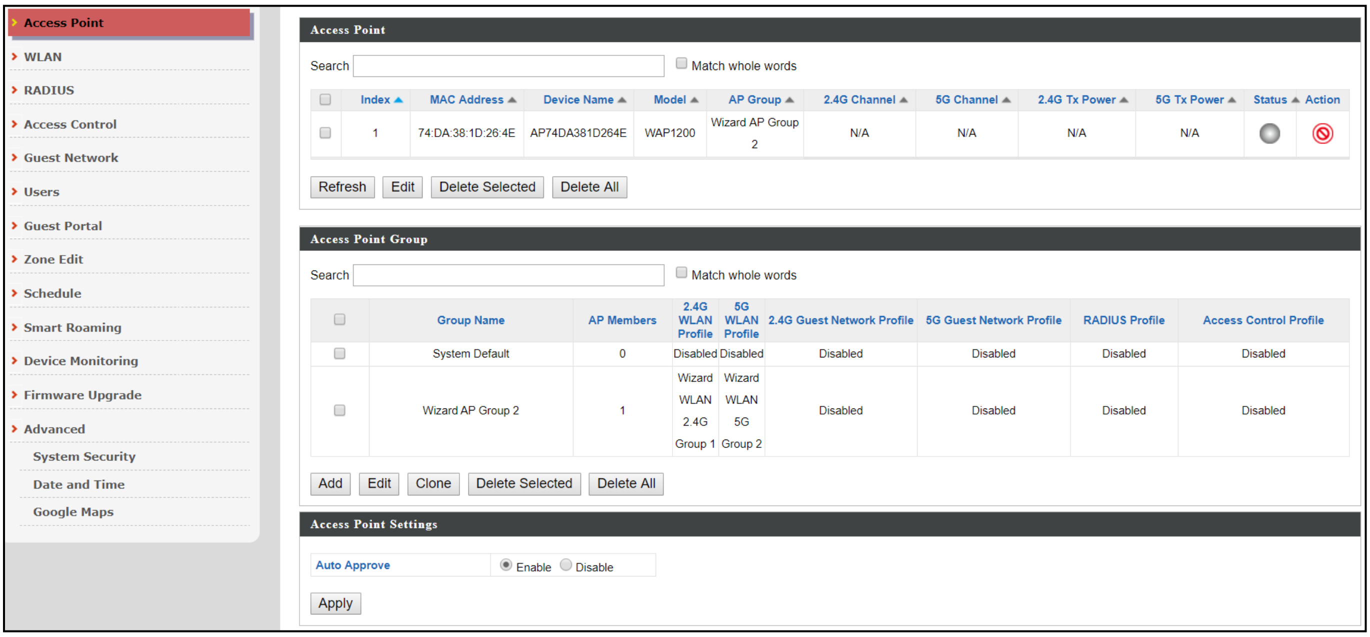
Search □ Match whole words

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	N/A	N/A	0	●	

NMS Settings



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



Access Point

Search □ Match whole words

□	Index ▲	MAC Address ▲	Device Name ▲	Model ▲	AP Group ▲	2.4G Channel ▲	5G Channel ▲	2.4G Tx Power ▲	5G Tx Power ▲	Status ▲	Action
□	1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	Wizard AP Group 2	N/A	N/A	N/A	N/A	●	🚫

Access Point Group

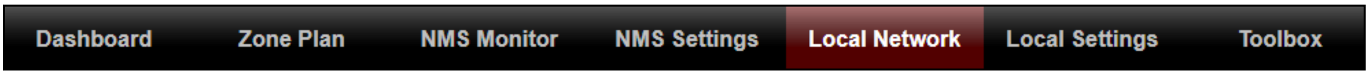
Search □ Match whole words

□	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
□	System Default	0	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
□	Wizard AP Group 2	1	Wizard WLAN 2.4G Group 1	Wizard WLAN 5G Group 2	Disabled	Disabled	Disabled	Disabled

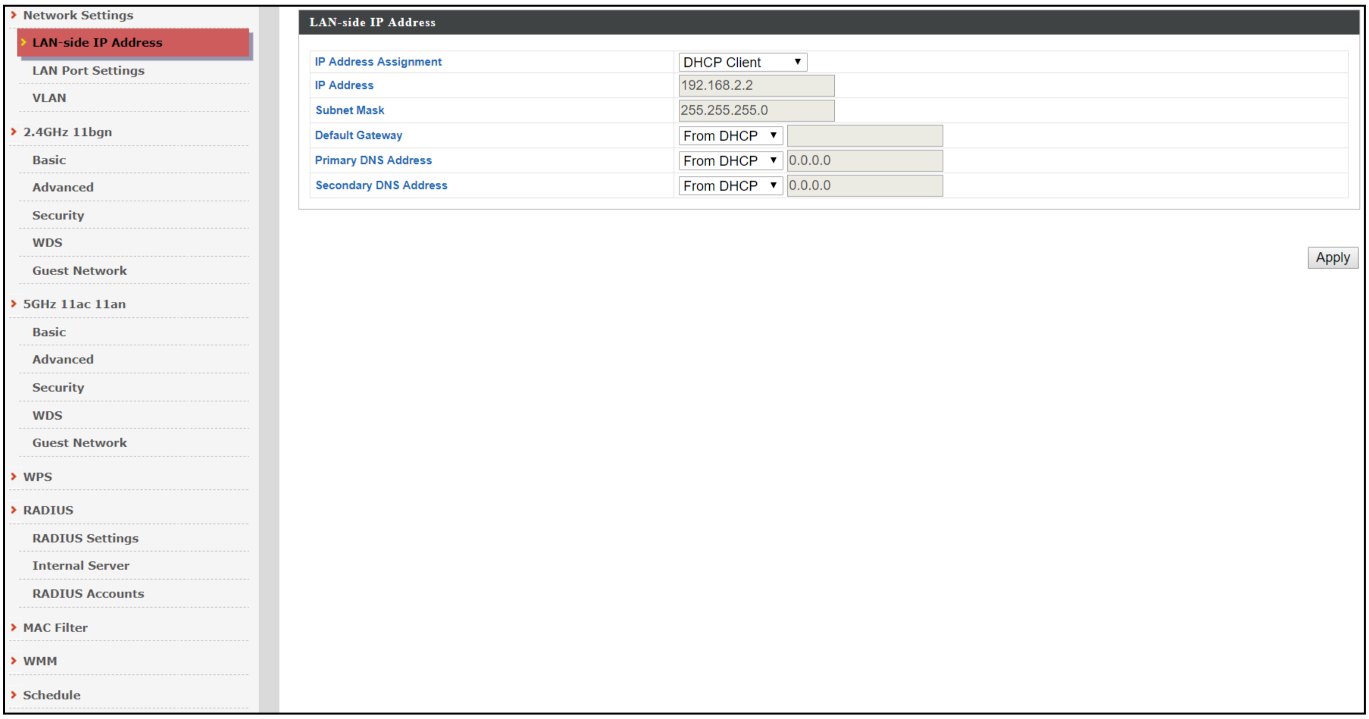
Access Point Settings

Auto Approve ● Enable ○ Disable

Local Network



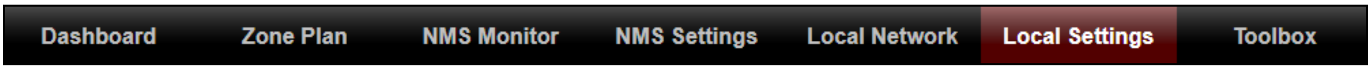
Local Network settings are for your AP Controller. You can configure the IP address and DHCP server of the AP Controller in addition to 2.4GHz & 5Ghz Wi-Fi and security, with WPS, RADIUS server, MAC filtering and WMM settings also available.



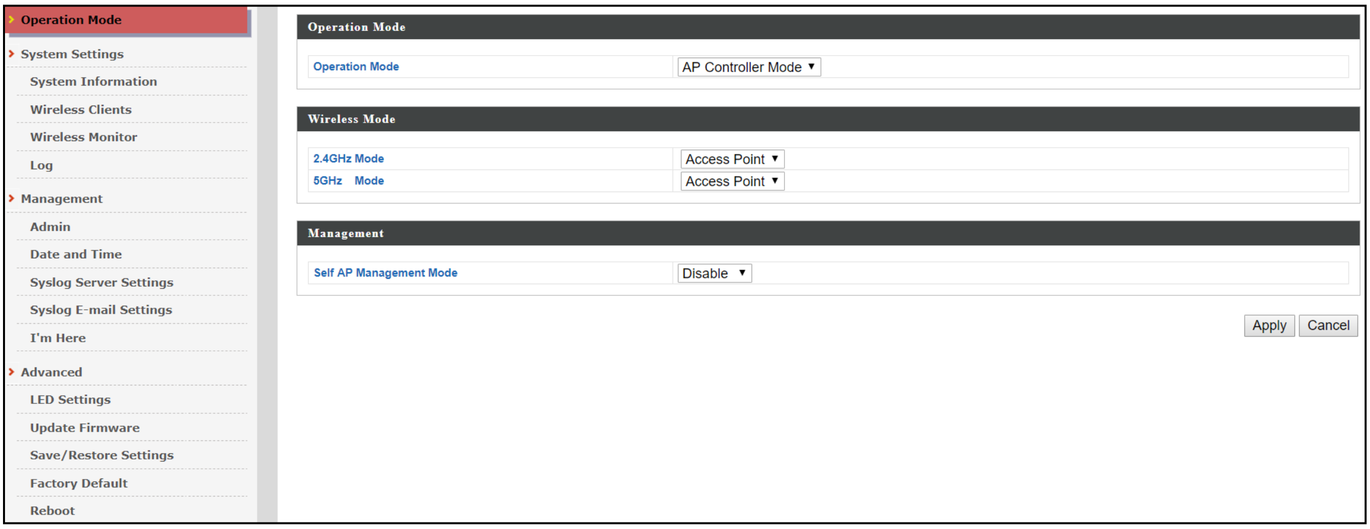
LAN-side IP Address

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

Local Settings



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



Operation Mode

Operation Mode: AP Controller Mode

Wireless Mode

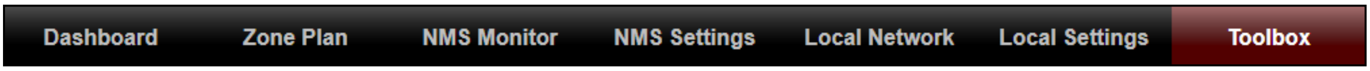
2.4GHz Mode: Access Point

5GHz Mode: Access Point

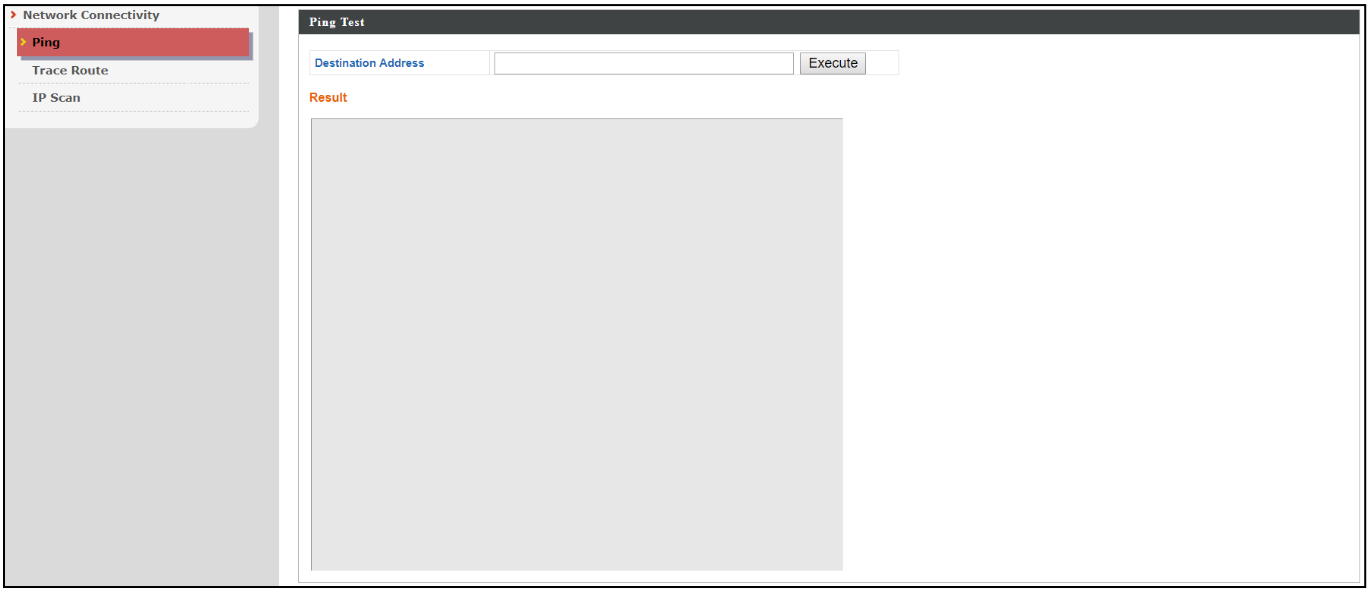
Management

Self AP Management Mode: Disable

Toolbox



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



X NMS Features

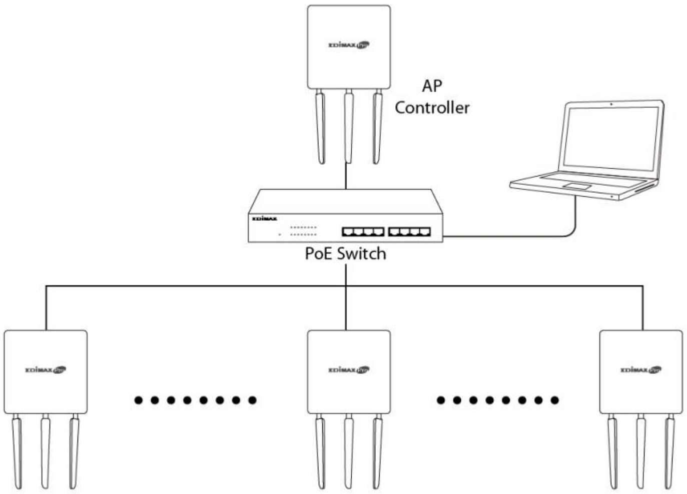
Descriptions of the functions of each main panel can be found below. When using Edimax NMS, click "Apply" to save changes:

X-1 Login, Logout & Restart

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

<u>Login</u>

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



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

192.168.2.2/

Your computer's IP address must be in the same subnet as the AP Controller. Refer to *XI-1 Configuring your IP address* ***for more help.***

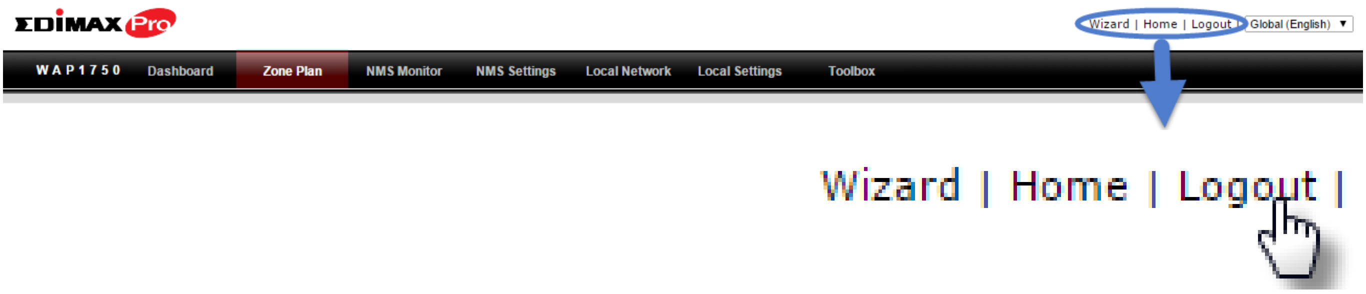
If you changed the AP Controller's IP address, or if your gateway/router uses a DHCP server, ensure you enter the correct IP address. Refer to your gateway/router's settings.

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

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

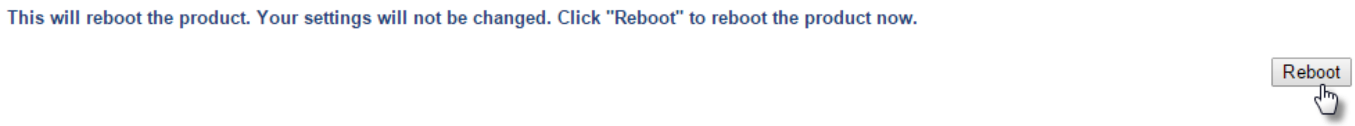
Logout

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

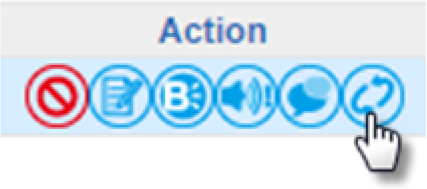


Restart

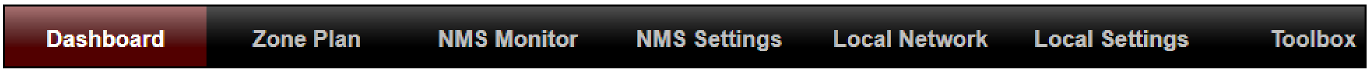
You can restart your AP Controller or any Managed AP using Edimax NMS. To restart your AP Controller go to **Local Settings → Advanced → Reboot** and click "Reboot".


This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.

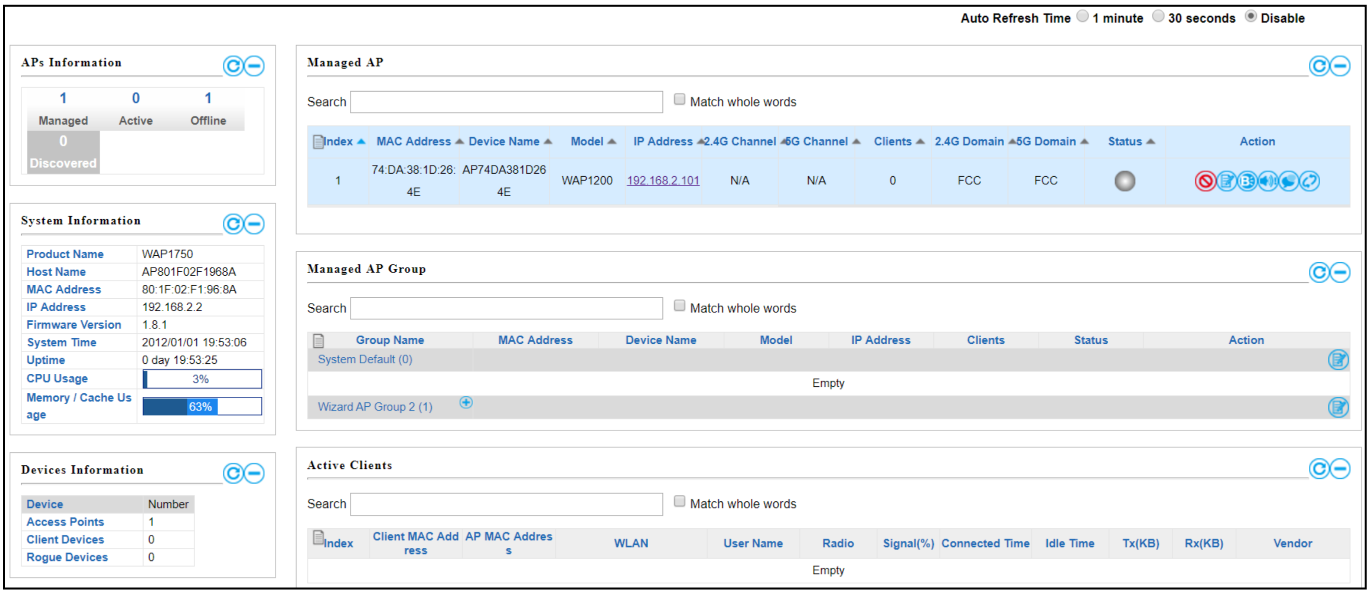
To restart Managed APs click the Restart icon for the specified AP on the Dashboard:



X-2 Dashboard



The dashboard displays an overview of your AP array:



Auto Refresh Time ○ 1 minute ○ 30 seconds ● Disable

APs Information

1	0	1
Managed	Active	Offline
0 Discovered		

System Information

Product Name	WAP1750
Host Name	AP801F02F1968A
MAC Address	80:1F:02:F1:96:8A
IP Address	192.168.2.2
Firmware Version	1.8.1
System Time	2012/01/01 19:53:06
Uptime	0 day 19:53:25
CPU Usage	3%
Memory / Cache Usage	63%

Devices Information

Device	Number
Access Points	1
Client Devices	0
Rogue Devices	0

Managed AP

Search □ Match whole words

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	2.4G Domain	5G Domain	Status	Action
1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	N/A	N/A	0	FCC	FCC	●	

Managed AP Group

Search □ Match whole words

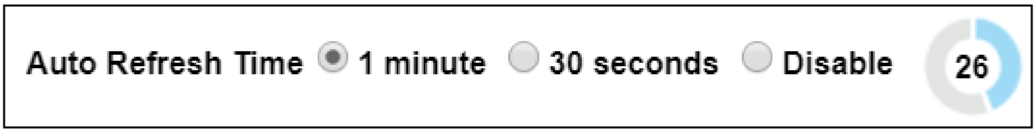
Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (0)							
Empty							
Wizard AP Group 2 (1)							

Active Clients

Search □ Match whole words

Index	Client MAC Address	AP MAC Address	WLAN	User Name	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
Empty											

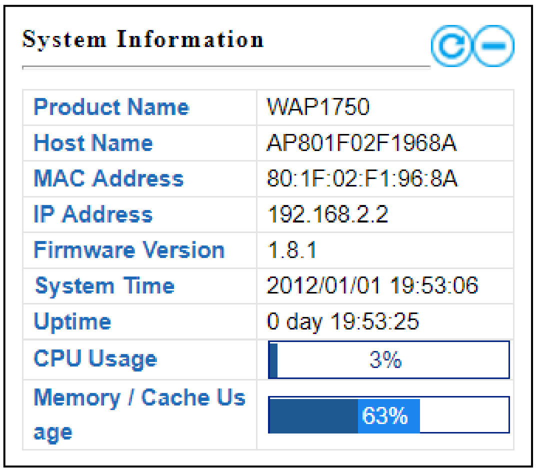
Use the blue icons above to refresh or collapse each panel in the dashboard. Click and drag to move a panel to suit your preference. You can set the dashboard to auto-refresh every 1 minute, 30 seconds or disable auto-refresh:



Auto Refresh Time ● 1 minute ○ 30 seconds ○ Disable 26

X-2-1 System Information

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

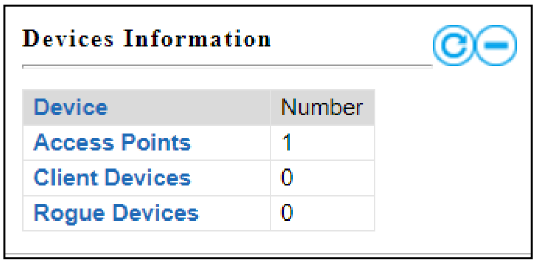


System Information

Product Name	WAP1750
Host Name	AP801F02F1968A
MAC Address	80:1F:02:F1:96:8A
IP Address	192.168.2.2
Firmware Version	1.8.1
System Time	2012/01/01 19:53:06
Uptime	0 day 19:53:25
CPU Usage	3%
Memory / Cache Usage	63%

X-2-2 Devices Information

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

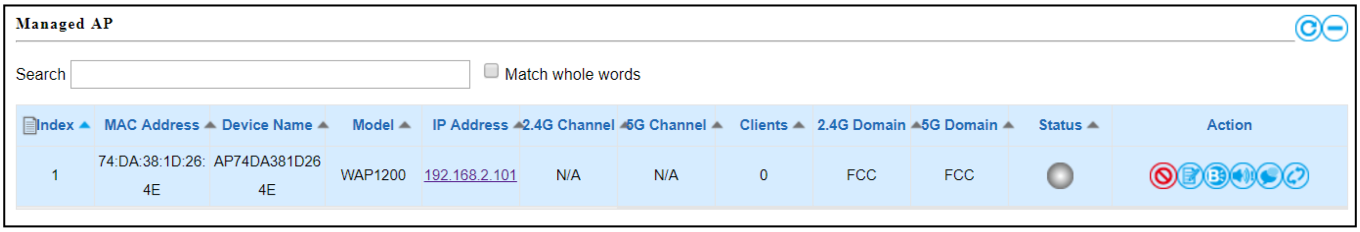


Devices Information

Device	Number
Access Points	1
Client Devices	0
Rogue Devices	0

X-2-3 Managed AP

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

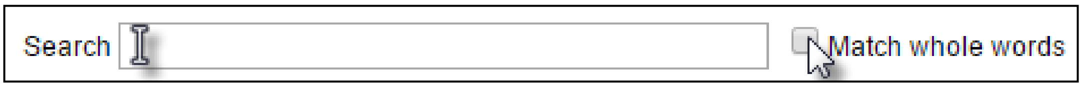


Managed AP

Search □ Match whole words

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	2.4G Domain	5G Domain	Status	Action
1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	N/A	N/A	0	FCC	FCC	●	

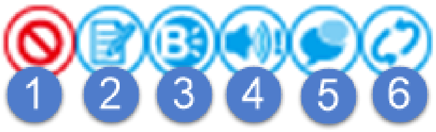
The **search** function can be used to locate a specific Managed AP. Type in the search box and the list will update:



Search □ Match whole words

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

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



1. **Disallow**

   Remove the Managed AP from the AP array and disable connectivity.

2. **Edit**

   *Edit various settings for the Managed AP (refer to **X-5-1 Access Point**).*

3. **Blink LED**

   The Managed AP's LED will flash temporarily to help identify & locate the access point.

4. **Buzzer**

   The Managed AP's buzzer will sound temporarily to help identify/locate the access point.

5. **Network Connectivity**

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

6. **Restart**

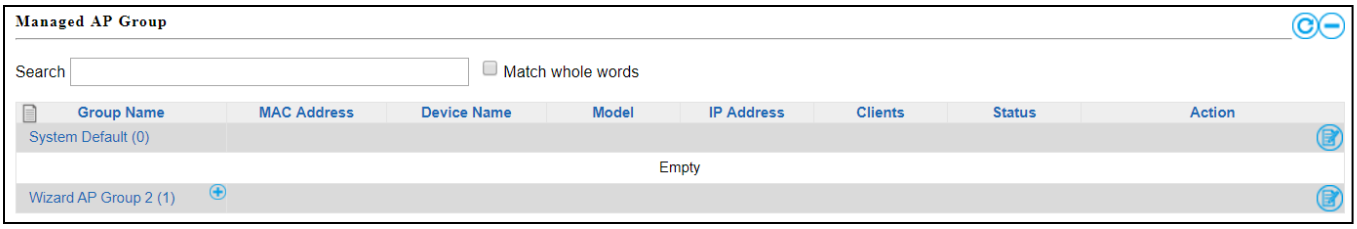
   Restarts the Managed AP.

Status Icons			
Icon	**Color**	**Status**	**Definition**
●	Grey	Disconnected	Managed AP is disconnected. *Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.*
●	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all access points in the AP array. *Please check security settings (refer to **X-5-13-1 System Security**).* All access points must have the same firmware version. *Please use the AP Controller's firmware upgrade function (refer to **X-5-12 Firmware Upgrade**).*
●	Orange	Configuring or Upgrading	*Please wait while the Managed AP makes configurations or while the firmware is upgrading.*
●	Yellow	Connecting	*Please wait while Managed AP is connecting.*
●	Green	Connected	*Managed AP is connected.*
●	Blue	Waiting for Approval	Managed AP is waiting for approval. *Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.*

X-2-4 Managed AP Group

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

To edit Managed AP Groups go to **NMS Settings → Access Point** (refer to ***X-5-1 Access Point***).

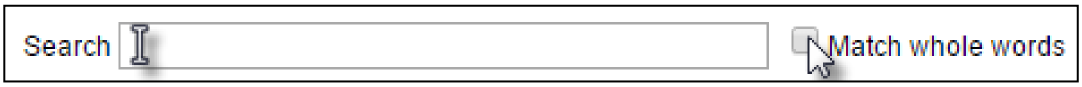


Managed AP Group

Search ☐ Match whole words

Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (0)							
			Empty				
Wizard AP Group 2 (1)							

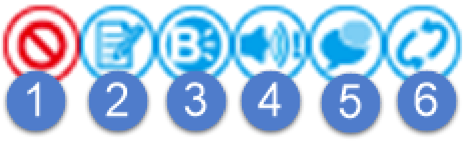
The search function can be used to locate a specific Managed AP Group. Type in the search box and the list will update:



Search ☐ Match whole words

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

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



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

2. **Edit**
   Edit various settings for the Managed AP Group (refer to ***X-5-1 Access Point****)*

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

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

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

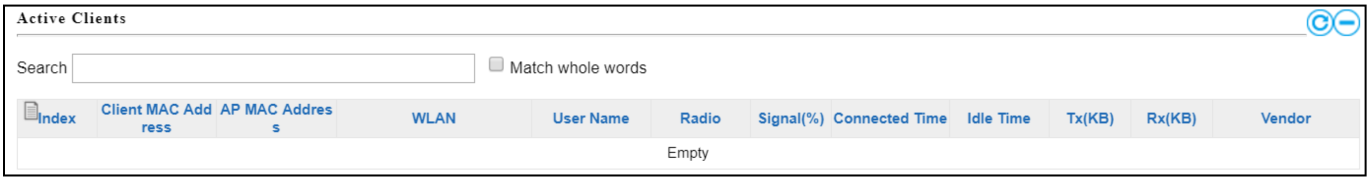
6. **Restart**
   Restarts all Managed APs in the group.

Status Icons			
Icon	**Color**	**Status**	**Definition**
●	Grey	Disconnected	Managed AP is disconnected. *Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.*
🔴	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all access points in the AP array. *Please check security settings (refer to* ***X-5-13-1 System Security****).* All access points must have the same firmware version. *Please use the AP Controller's firmware upgrade function (refer to* ***X-5-12 Firmware Upgrade****).*
🟠	Orange	Configuring or Upgrading	*Please wait while the Managed AP makes configurations or while the firmware is upgrading.*
🟡	Yellow	Connecting	*Please wait while Managed AP is connecting.*

🟢	Green	Connected	*Managed AP is connected.*
🔵	Blue	Waiting for Approval	Managed AP is waiting for approval. *Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.*

X-2-5 Active Clients

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

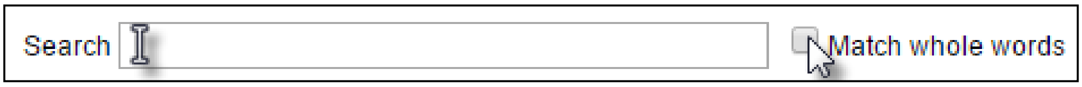


Active Clients

Search ☐ Match whole words

☐ Index	Client MAC Address	AP MAC Address	WLAN	User Name	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
					Empty						

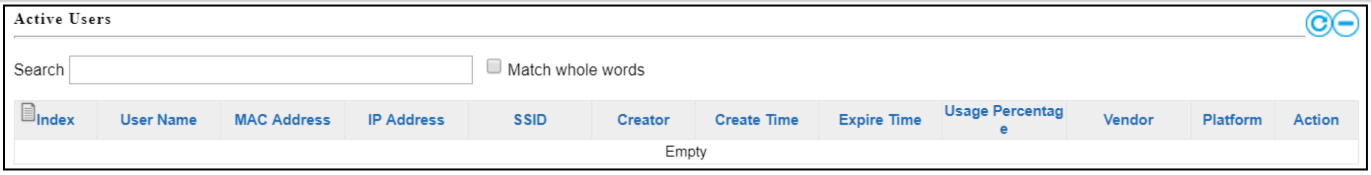
The search function can be used to locate a specific client. Type in the search box and the list will update:



Search ☐ Match whole words

X-2-6 Active Users

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

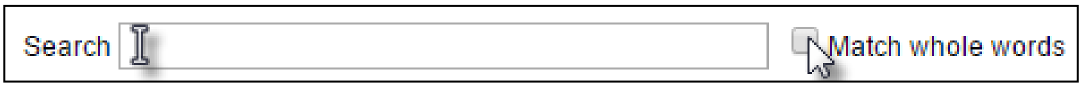


Active Users

Search □ Match whole words

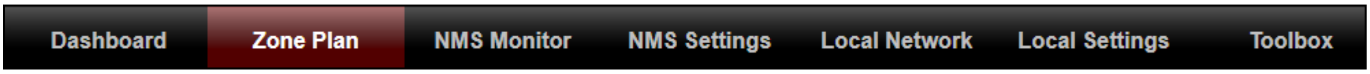
Index	User Name	MAC Address	IP Address	SSID	Creator	Create Time	Expire Time	Usage Percentage	Vendor	Platform	Action
Empty											

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

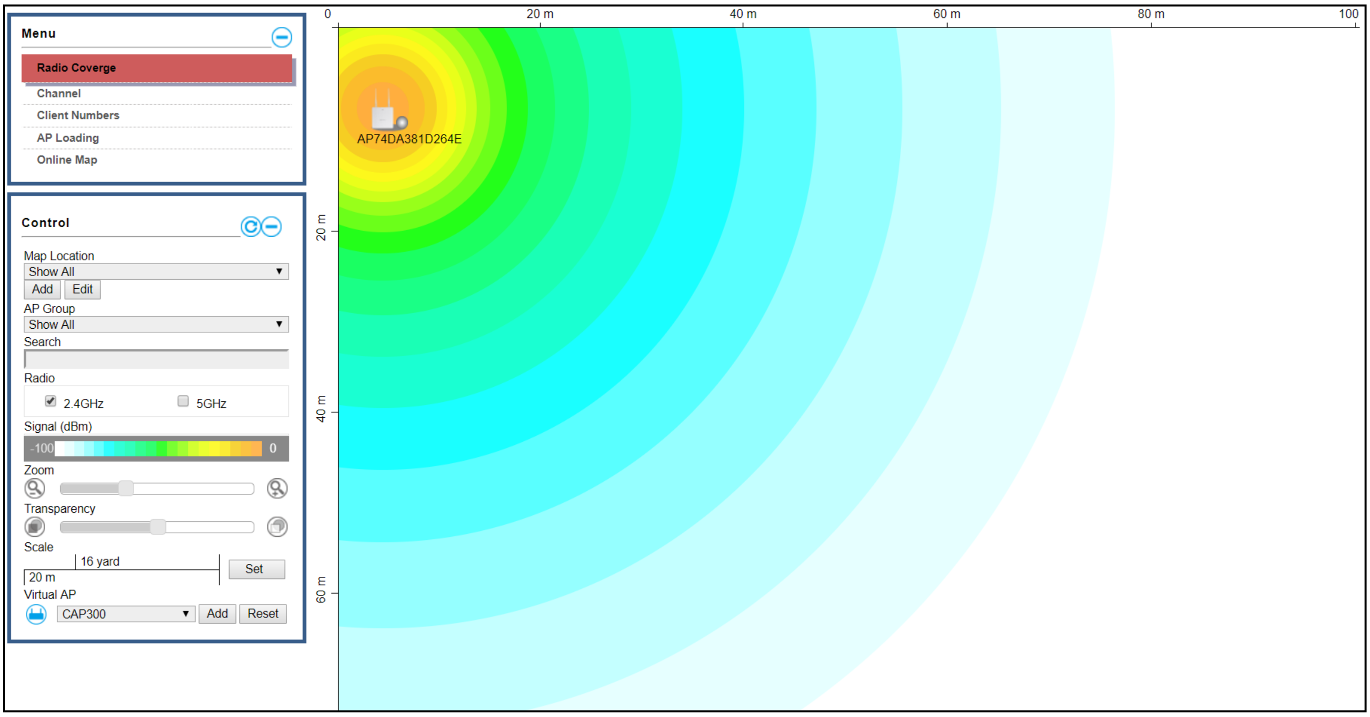


Search □ Match whole words

X-3 Zone Plan



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



Map Location: Show All

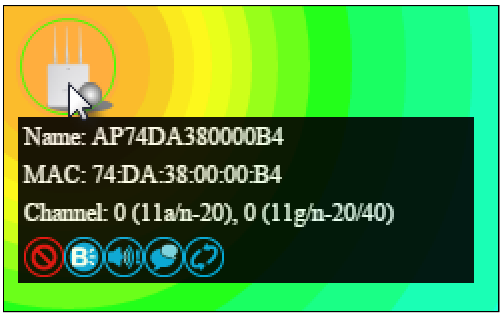
AP Group: Show All

Radio: ☑ 2.4GHz ☐ 5GHz

Scale: 16 yard, 20 m

Virtual AP: CAP300

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



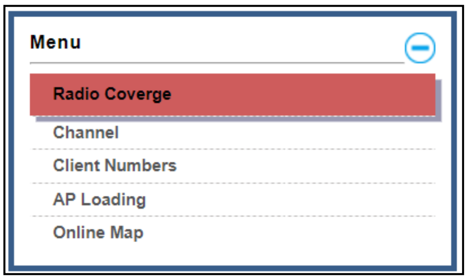
Name: AP74DA380000B4

MAC: 74:DA:38:00:00:B4

Channel: 0 (11a/n-20), 0 (11g/n-20/40)

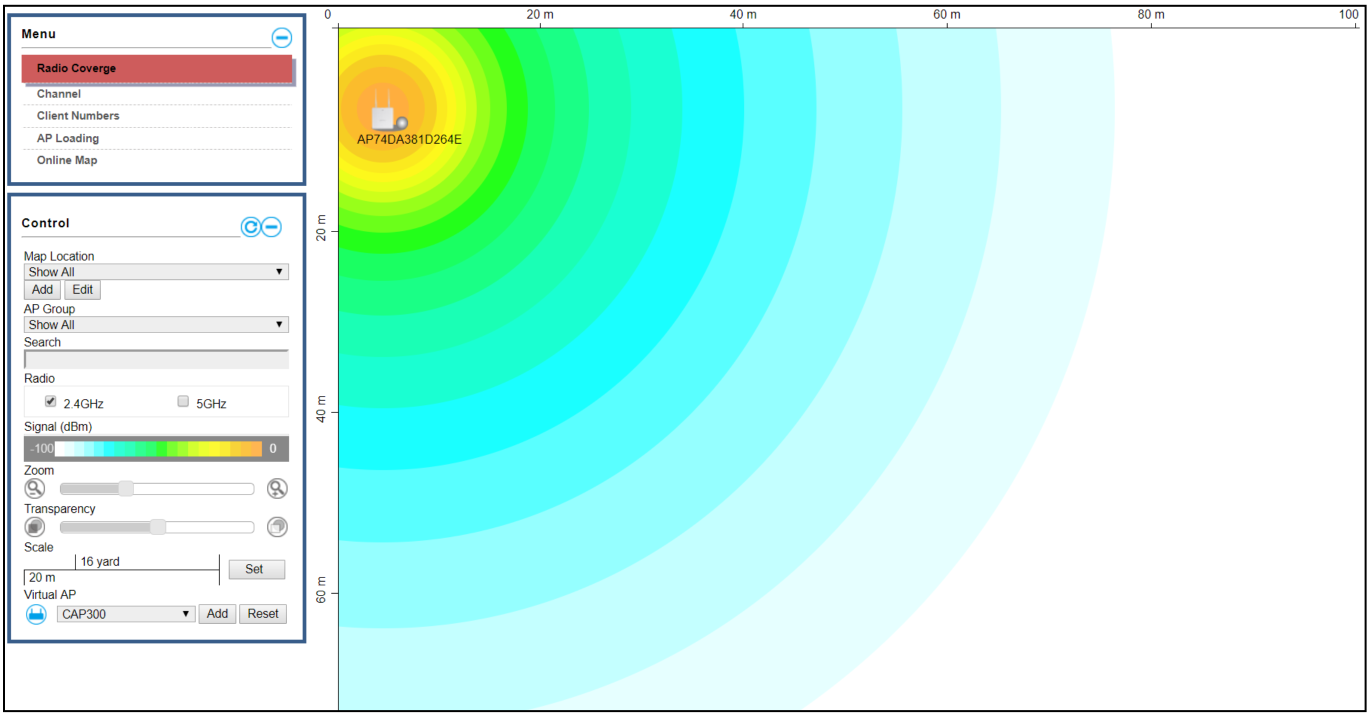
X-3-1 Menu

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



Radio Coverage

Below is displayed as Radio Coverage is selected:



Map Location: Show All

AP Group: Show All

Search:

Radio: ☑ 2.4GHz □ 5GHz

Signal (dBm): -100 0

Zoom

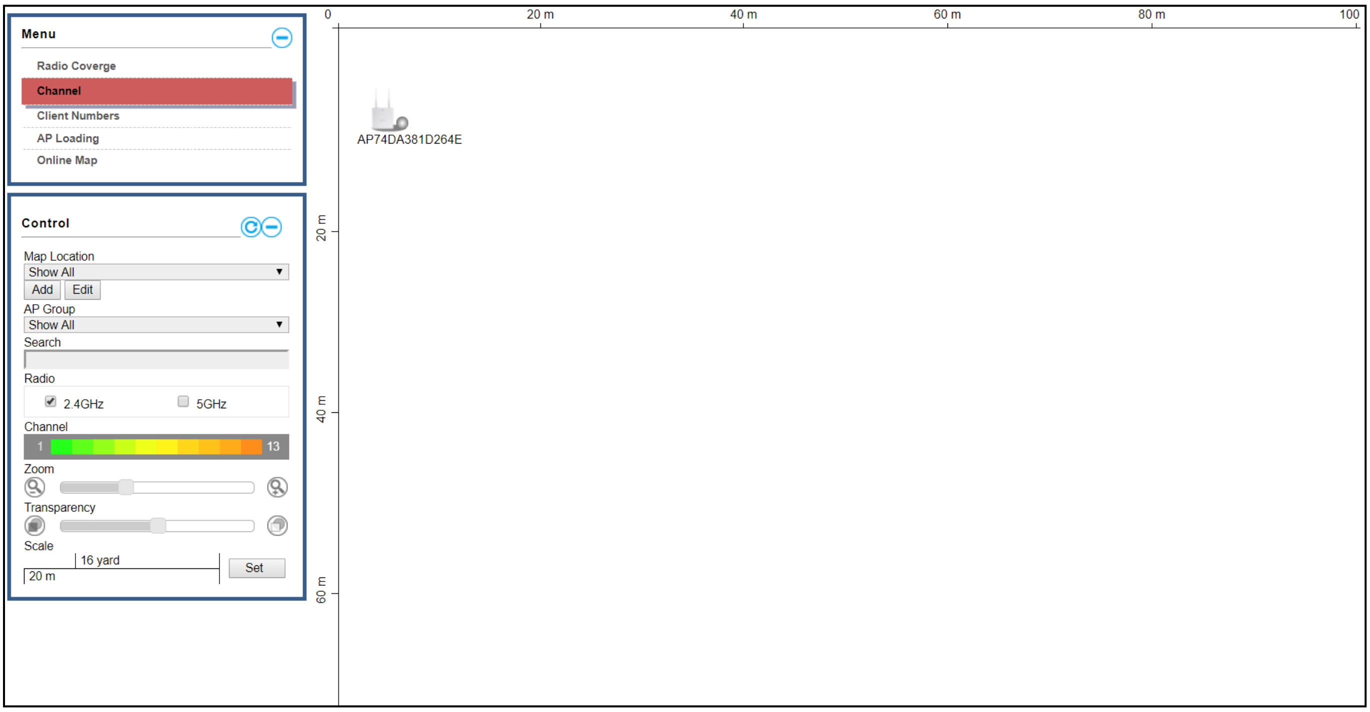
Transparency

Scale: 16 yard, 20 m

Virtual AP: CAP300

Channel

Below is displayed as Channel is selected:



Map Location: Show All

AP Group: Show All

Search:

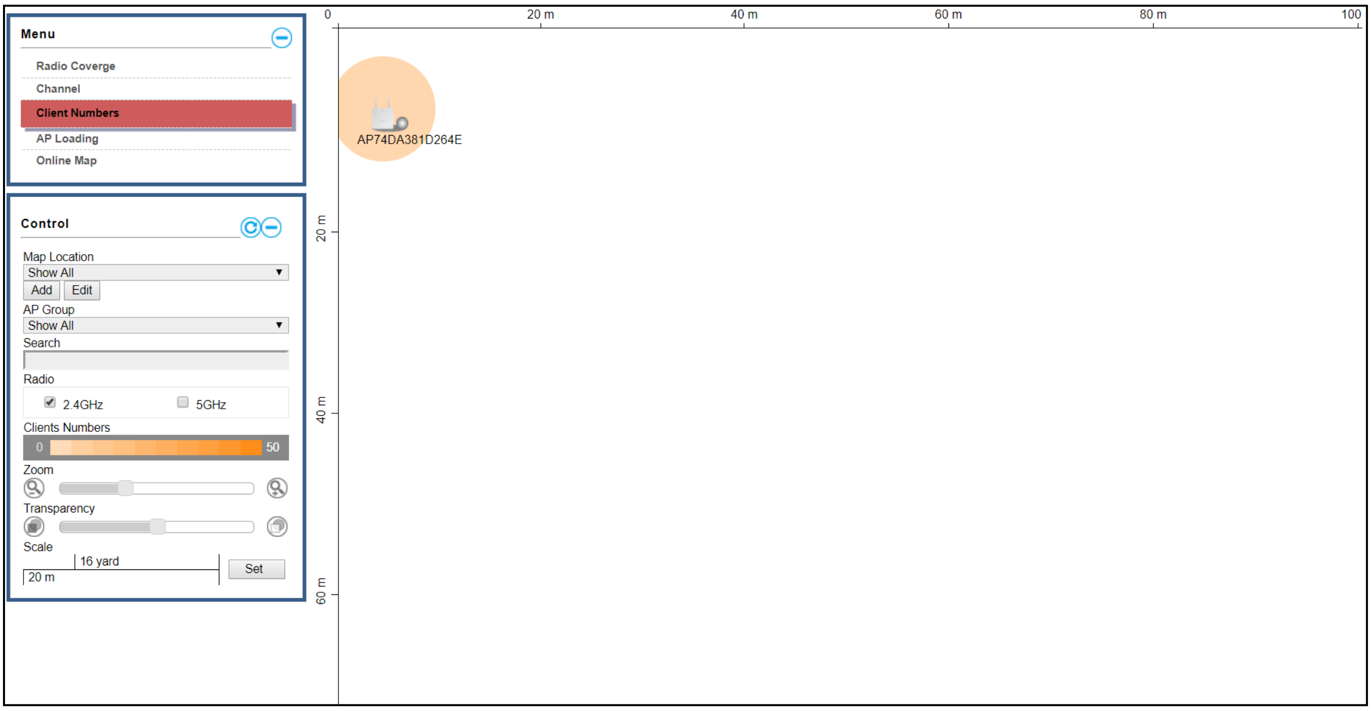
Radio: ☑ 2.4GHz ☐ 5GHz

Channel: 1 – 13

Scale: 16 yard / 20 m

Client Numbers

Below is displayed as Client Numbers is selected:



Map Location: Show All

AP Group: Show All

Search:

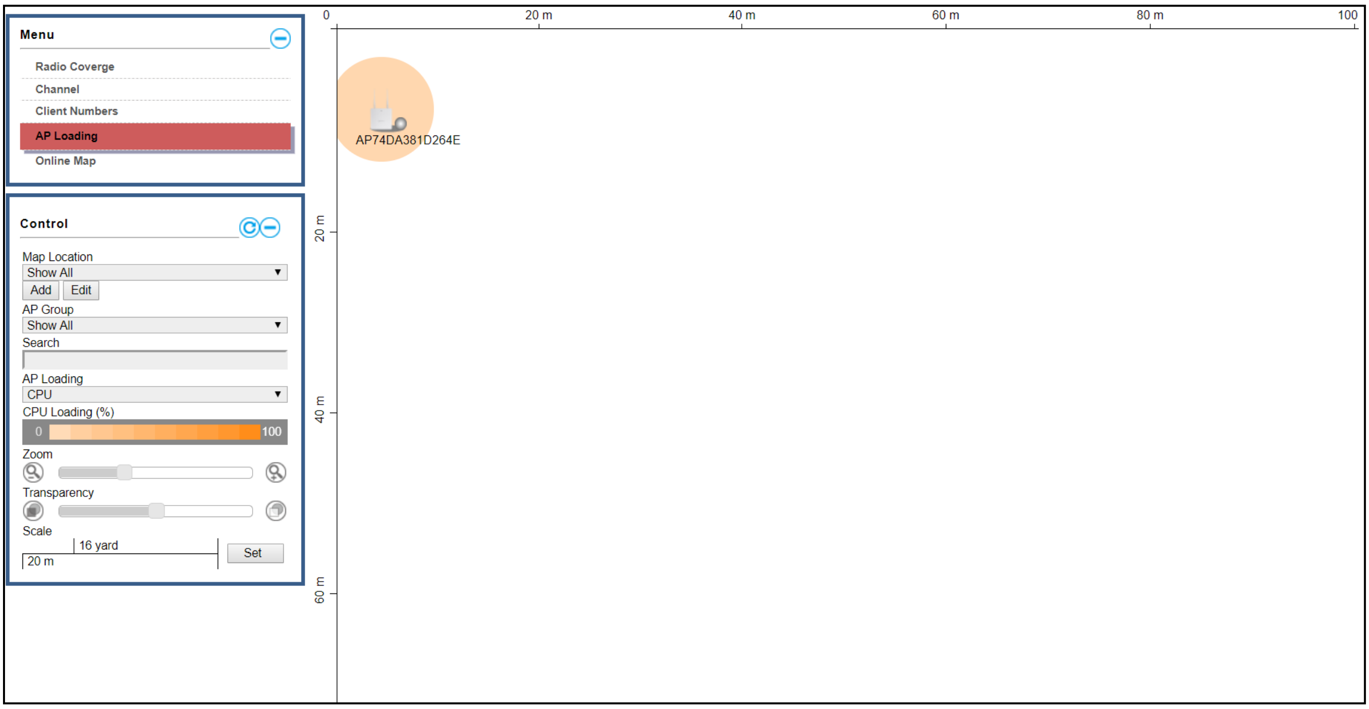
Radio: ☑ 2.4GHz ☐ 5GHz

Clients Numbers: 0 – 50

Scale: 16 yard / 20 m

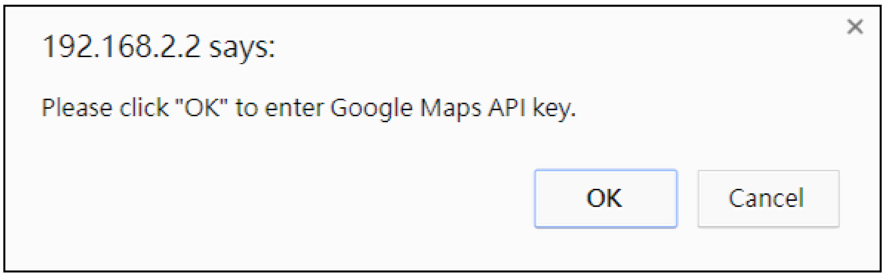
AP Loading

Below is displayed as AP Loading is selected:



Online Map

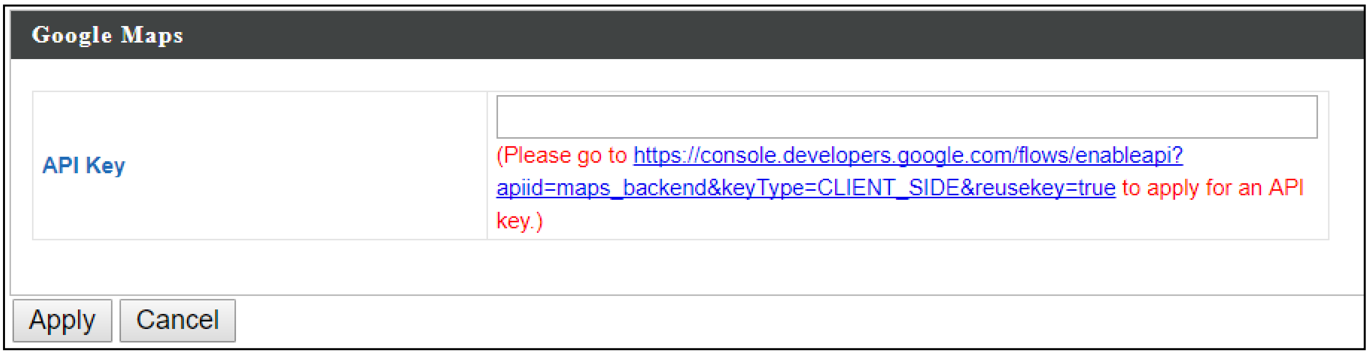
When Online Map is selected, the message below is displayed:



192.168.2.2 says:

Please click "OK" to enter Google Maps API key.

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



Google Maps

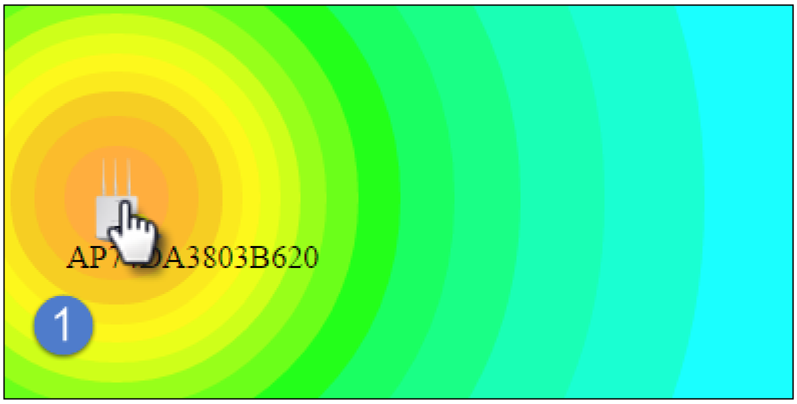
API Key	(Please go to https://console.developers.google.com/flows/enableapi?apiid=maps_backend&keyType=CLIENT_SIDE&reusekey=true to apply for an API key.)

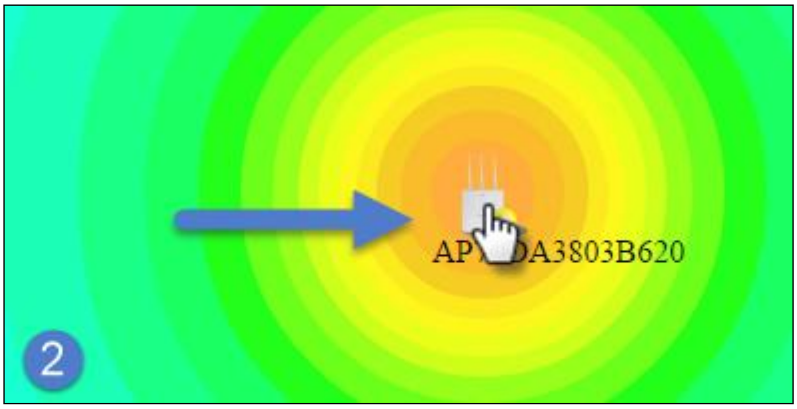
X-3-2 Control

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

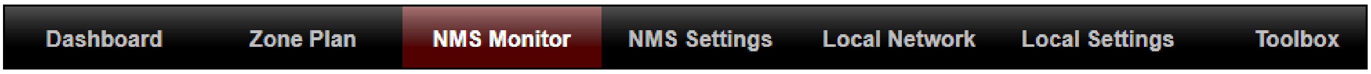
Map Location	Select a pre-defined location from the drop down menu. When you upload a location image in **NMS Settings → Zone Edit**, it will be available for selection here.
AP Group	You can select an AP Group to display in the zone map. Edit AP Groups in **NMS Settings → Access Point.**
Search	Use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

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





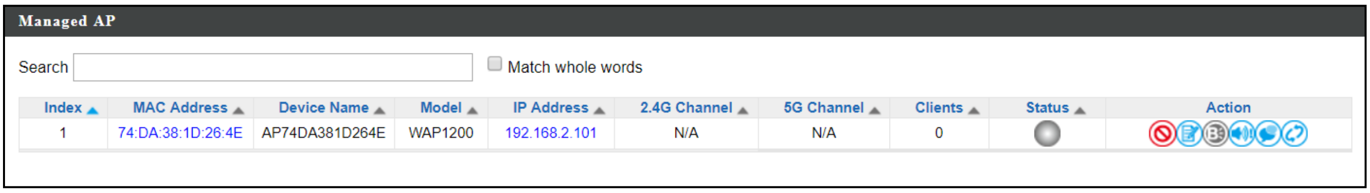
X-4 NMS Monitor



X-4-1 Access Point

X-4-1-1 Managed AP

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

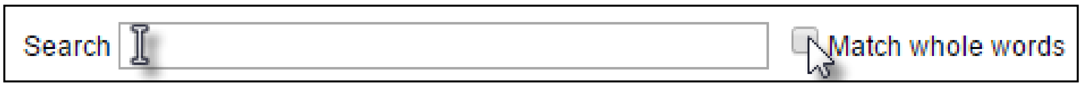


Managed AP

Search □ Match whole words

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	N/A	N/A	0	●	

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



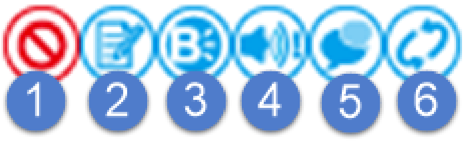
Search □ Match whole words

The **Status** icon displays the status of each Managed AP.

Status Icons			
Icon	**Color**	**Status**	**Definition**
●	Grey	Disconnected	Managed AP is disconnected. *Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.*
●	Red	Authentication Failed	System security must be the same for all access points in the AP array. *Please check security settings (refer to **X-5-13-1 System***

		Or Incompatible NMS Version	***Security****).* All access points must have the same firmware version. *Please use the AP Controller's firmware upgrade function (refer to **X-5-12 Firmware Upgrade**).*
🟠	Orange	Configuring or Upgrading	*Please wait while the Managed AP makes configurations or while the firmware is upgrading.*
🟡	Yellow	Connecting	*Please wait while Managed AP is connecting.*
🟢	Green	Connected	*Managed AP is connected.*
🔵	Blue	Waiting for Approval	Managed AP is waiting for approval. *Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.*

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



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

2. **Edit**
   *Edit various settings for the Managed AP (refer to **X-5-1 Access Point**).*

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

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

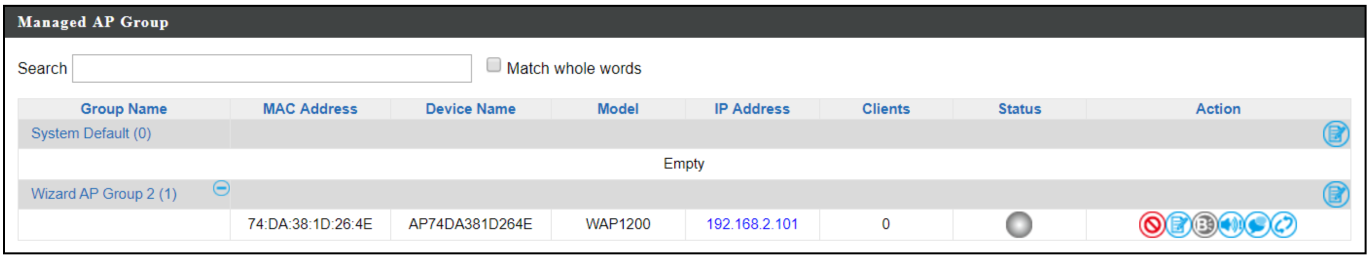
5. **Network Connectivity**
   Go to the "Network Connectivity" panel to perform a ping or traceroute.

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

X-4-1-2 Managed AP Group

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

To edit Managed AP Groups go to **NMS Settings → Access Point** (refer to **X-5-1 Access Point**).

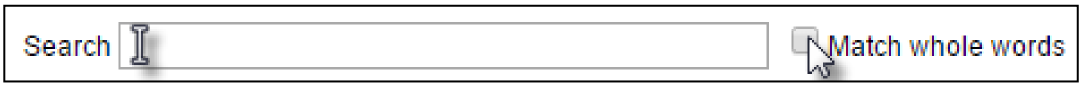


Managed AP Group

Search □ Match whole words

Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (0)							
			Empty				
Wizard AP Group 2 (1)							
	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	0	●	

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



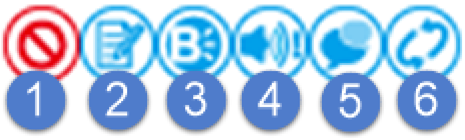
Search □ Match whole words

The **Status** icon displays the status of each Managed AP.

Status Icons			
Icon	**Color**	**Status**	**Definition**
●	Grey	Disconnected	Managed AP is disconnected. *Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.*
●	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all access points in the AP array. *Please check security settings (refer to **X-5-13-1 System Security**).* All access points must have the same firmware version. *Please use the AP*

			Controller's firmware upgrade function (refer to ***X-5-12 Firmware Upgrade****).*
🟠	Orange	Configuring or Upgrading	*Please wait while the Managed AP makes configurations or while the firmware is upgrading.*
🟡	Yellow	Connecting	*Please wait while Managed AP is connecting.*
🟢	Green	Connected	*Managed AP is connected.*
🔵	Blue	Waiting for Approval	Managed AP is waiting for approval. *Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.*

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



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

2. **Edit**
   Edit various settings for the Managed AP Group (refer to ***X-5-1 Access Point****)*

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

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

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

6. **Restart**

   Restarts all Managed APs in the group.

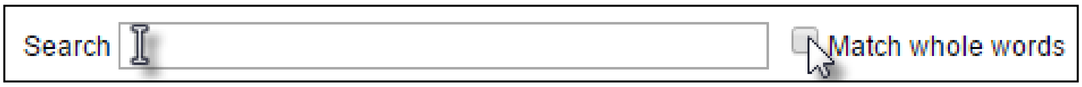
X-4-2 WLAN

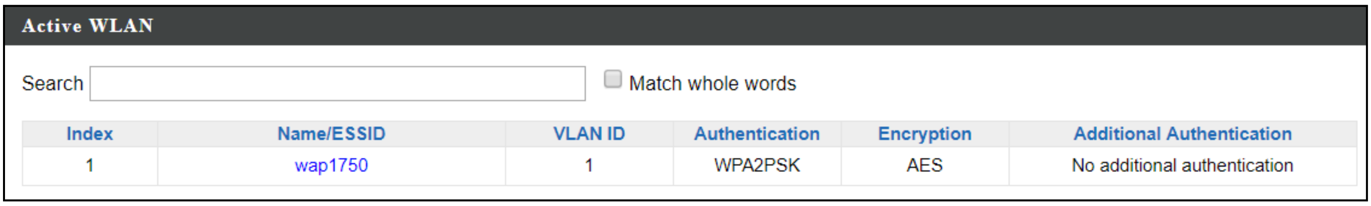
X-4-2-1 Active WLAN

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

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

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



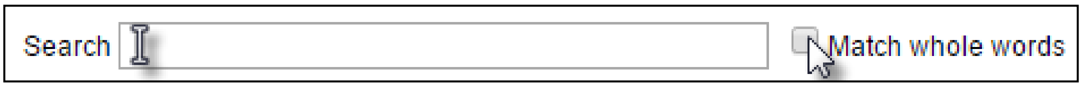


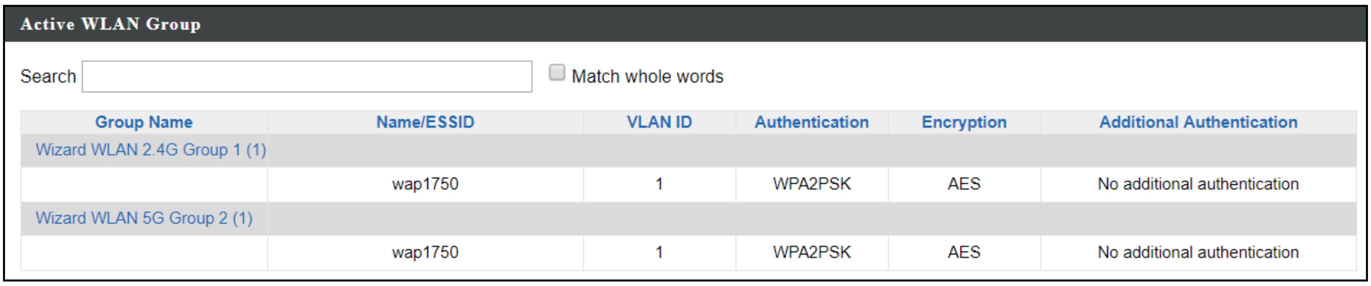
Index	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
1	wap1750	1	WPA2PSK	AES	No additional authentication

X-4-2-2 Active WLAN Group

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

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





Active WLAN Group

Search □ Match whole words

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

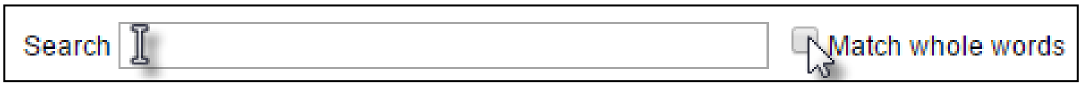
X-4-3 Clients

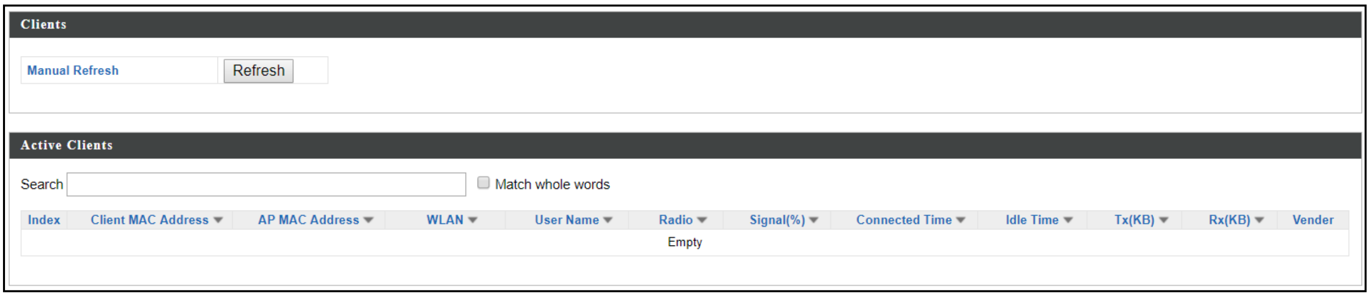
X-4-3-1 Active Clients

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

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

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



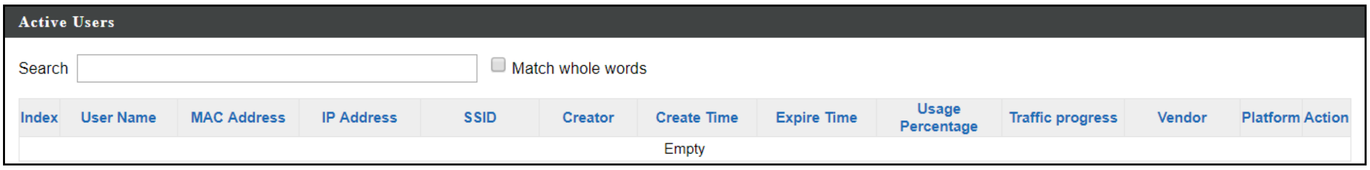


Index	Client MAC Address ▼	AP MAC Address ▼	WLAN ▼	User Name ▼	Radio ▼	Signal(%) ▼	Connected Time ▼	Idle Time ▼	Tx(KB) ▼	Rx(KB) ▼	Vender
Empty											

X-4-4 Users

X-4-4-1 Active Users

Displays information about users currently connected.



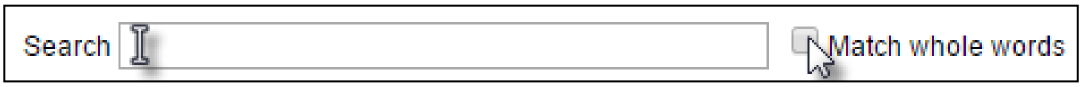
Active Users

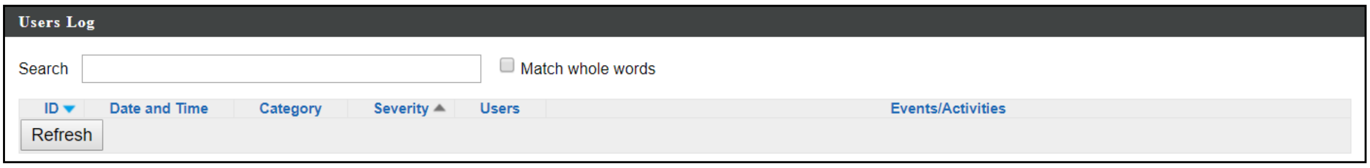
Search □ Match whole words

Index	User Name	MAC Address	IP Address	SSID	Creator	Create Time	Expire Time	Usage Percentage	Traffic progress	Vendor	Platform	Action
Empty												

X-4-4-2 Users Log

Displays the log information about users currently connected.





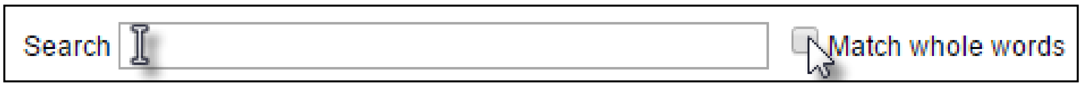
X-4-5 Rogue Devices

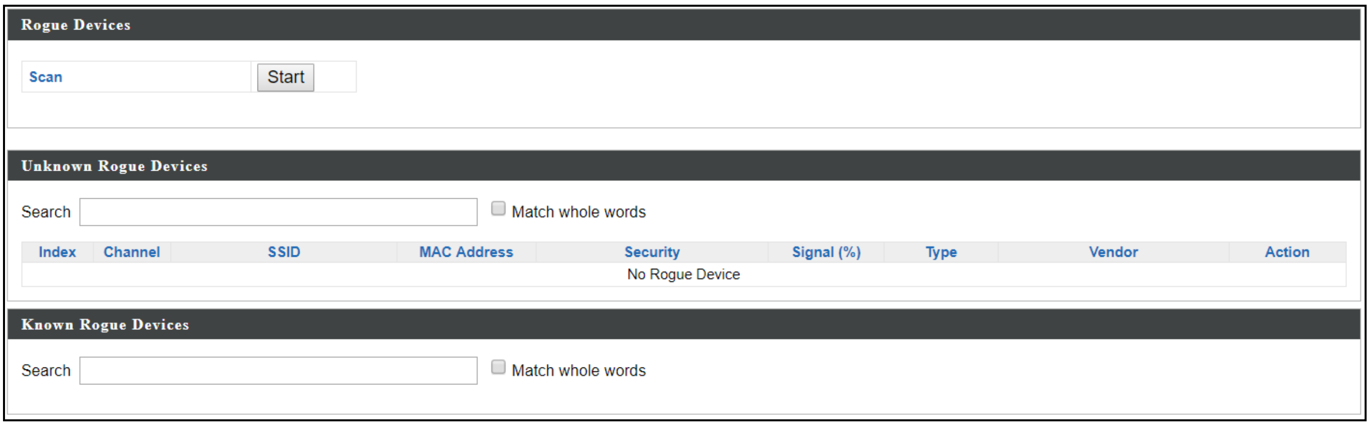
Rogue access point detection can identify any unauthorized access points which may have been installed in the network.

Click “Start” to scan for rogue devices:

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

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





Rogue Devices

Scan | Start

Unknown Rogue Devices

Search □ Match whole words

Index	Channel	SSID	MAC Address	Security	Signal (%)	Type	Vendor	Action
				No Rogue Device				

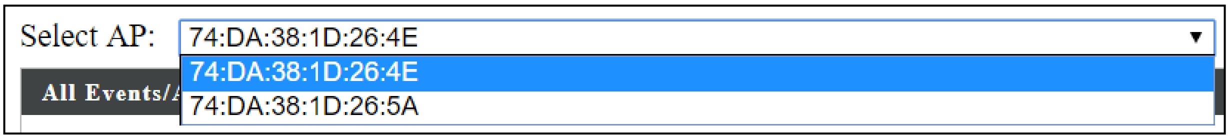
Known Rogue Devices

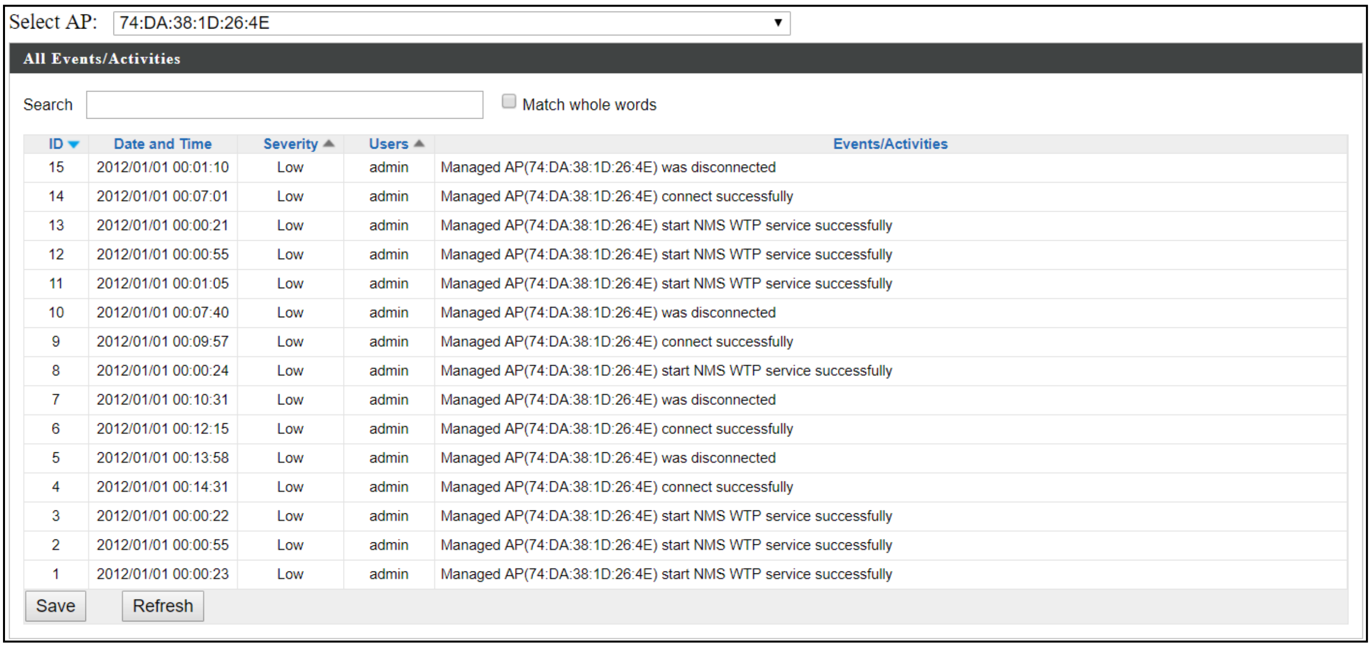
Search □ Match whole words

X-4-6 Information

X-4-6-1 All Events/Activities

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





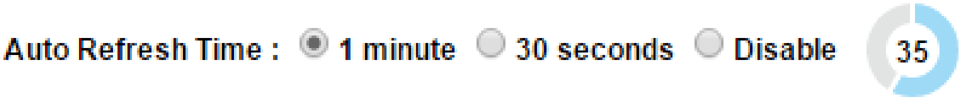
ID ▼	Date and Time	Severity ▲	Users ▲	Events/Activities
15	2012/01/01 00:01:10	Low	admin	Managed AP(74:DA:38:1D:26:4E) was disconnected
14	2012/01/01 00:07:01	Low	admin	Managed AP(74:DA:38:1D:26:4E) connect successfully
13	2012/01/01 00:00:21	Low	admin	Managed AP(74:DA:38:1D:26:4E) start NMS WTP service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

X-4-6-2 AP Monitoring

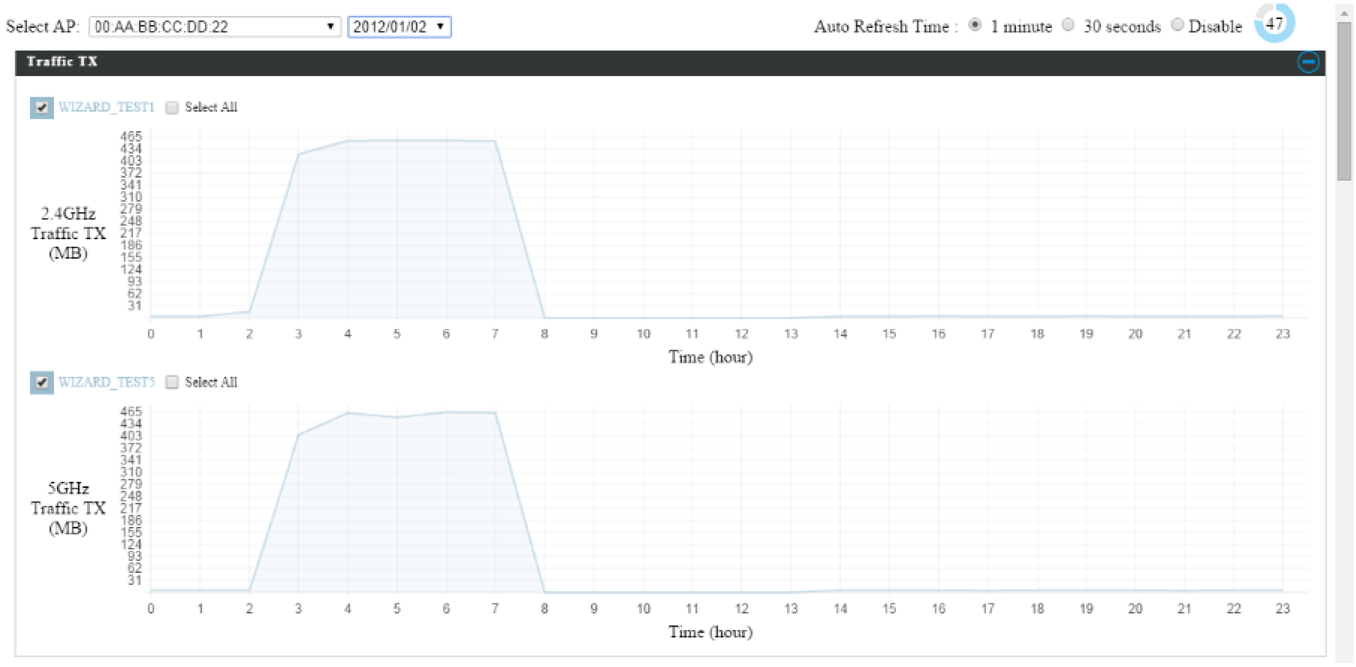
Displays graphical monitoring information about access points in the Array for 2.4GHz & 5GHz: *Traffic Tx (data transmitted in MB), Traffic Rx (data received in MB), No. of Clients, Wireless Channel, Tx Power (wireless radio power), CPU Usage and Memory Usage.*

Use the drop down menus to select an access point and date.

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



Auto Refresh Time : ● 1 minute ○ 30 seconds ○ Disable



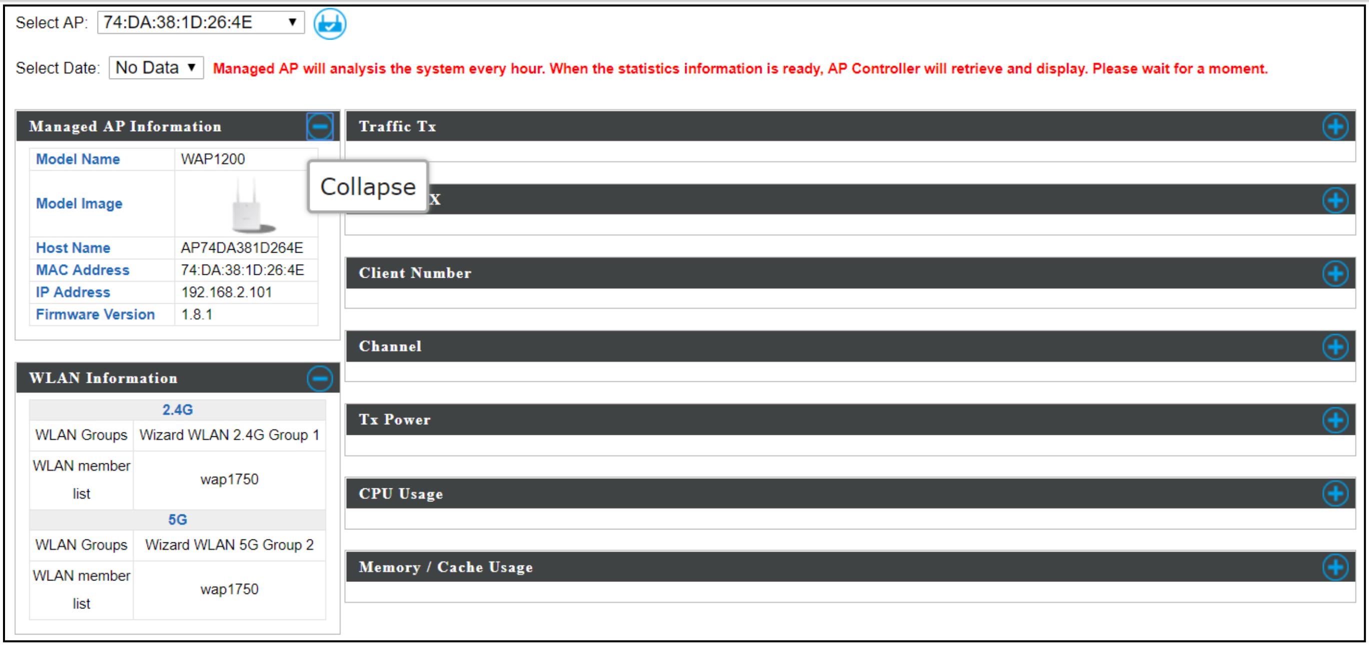
Select AP: 00:AA:BB:CC:DD:22 ▾ 2012/01/02 ▾

Auto Refresh Time : ● 1 minute ○ 30 seconds ○ Disable

Traffic TX

☑ WIZARD_TEST1 □ Select All

☑ WIZARD_TEST5 □ Select All



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

Select Date: No Data Managed AP will analysis the system every hour. When the statistics information is ready, AP Controller will retrieve and display. Please wait for a moment.

Managed AP Information

Model Name	WAP1200
Model Image	
Host Name	AP74DA381D264E
MAC Address	74:DA:38:1D:26:4E
IP Address	192.168.2.101
Firmware Version	1.8.1

WLAN Information

2.4G	
WLAN Groups	Wizard WLAN 2.4G Group 1
WLAN member list	wap1750
5G	
WLAN Groups	Wizard WLAN 5G Group 2
WLAN member list	wap1750

Traffic Tx

X

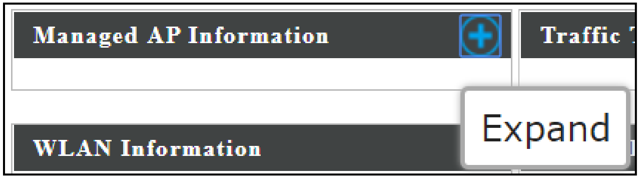
Client Number

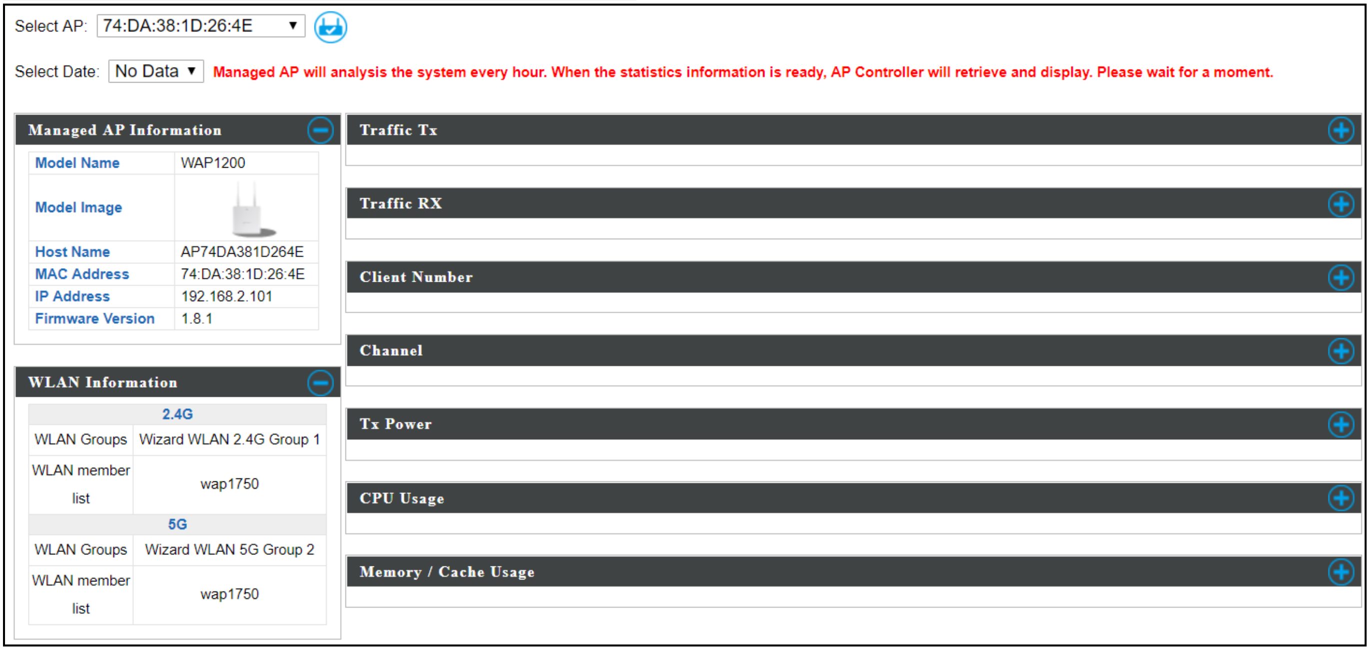
Channel

Tx Power

CPU Usage

Memory / Cache Usage





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

Select Date: No Data Managed AP will analysis the system every hour. When the statistics information is ready, AP Controller will retrieve and display. Please wait for a moment.

Managed AP Information

Model Name	WAP1200
Model Image	
Host Name	AP74DA381D264E
MAC Address	74:DA:38:1D:26:4E
IP Address	192.168.2.101
Firmware Version	1.8.1

WLAN Information

2.4G	
WLAN Groups	Wizard WLAN 2.4G Group 1
WLAN member list	wap1750
5G	
WLAN Groups	Wizard WLAN 5G Group 2
WLAN member list	wap1750

Traffic Tx

Traffic RX

Client Number

Channel

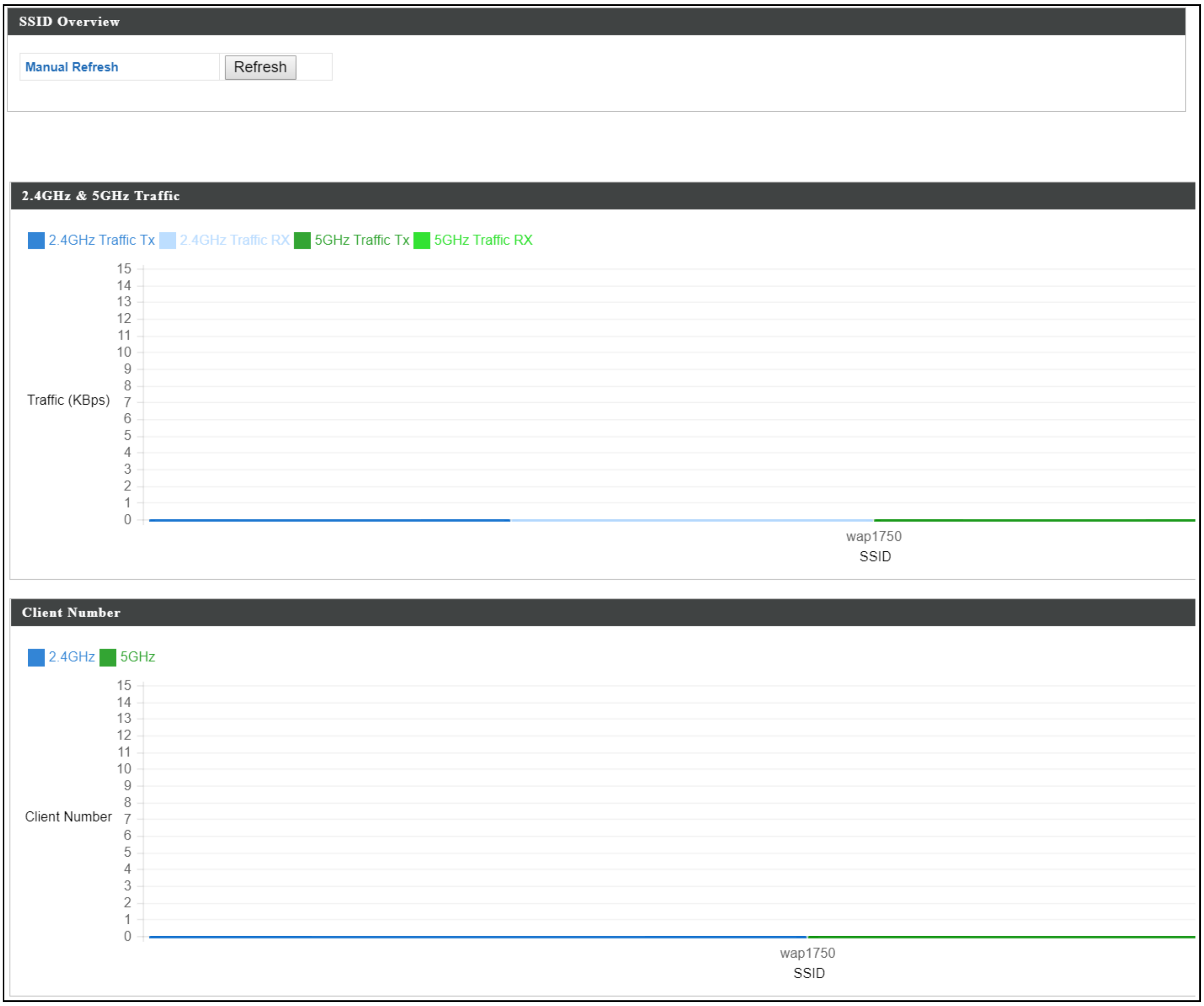
Tx Power

CPU Usage

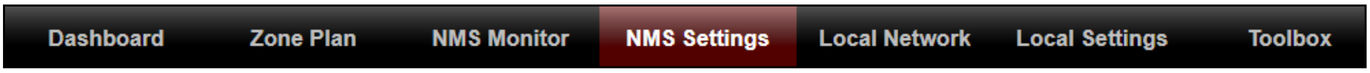
Memory / Cache Usage

X-4-6-3 SSID Overview

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



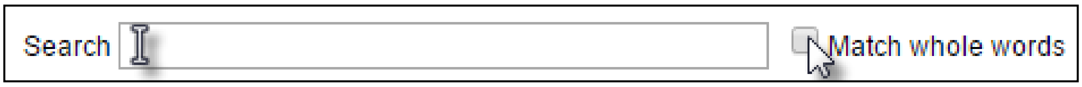
X-5 NMS Settings

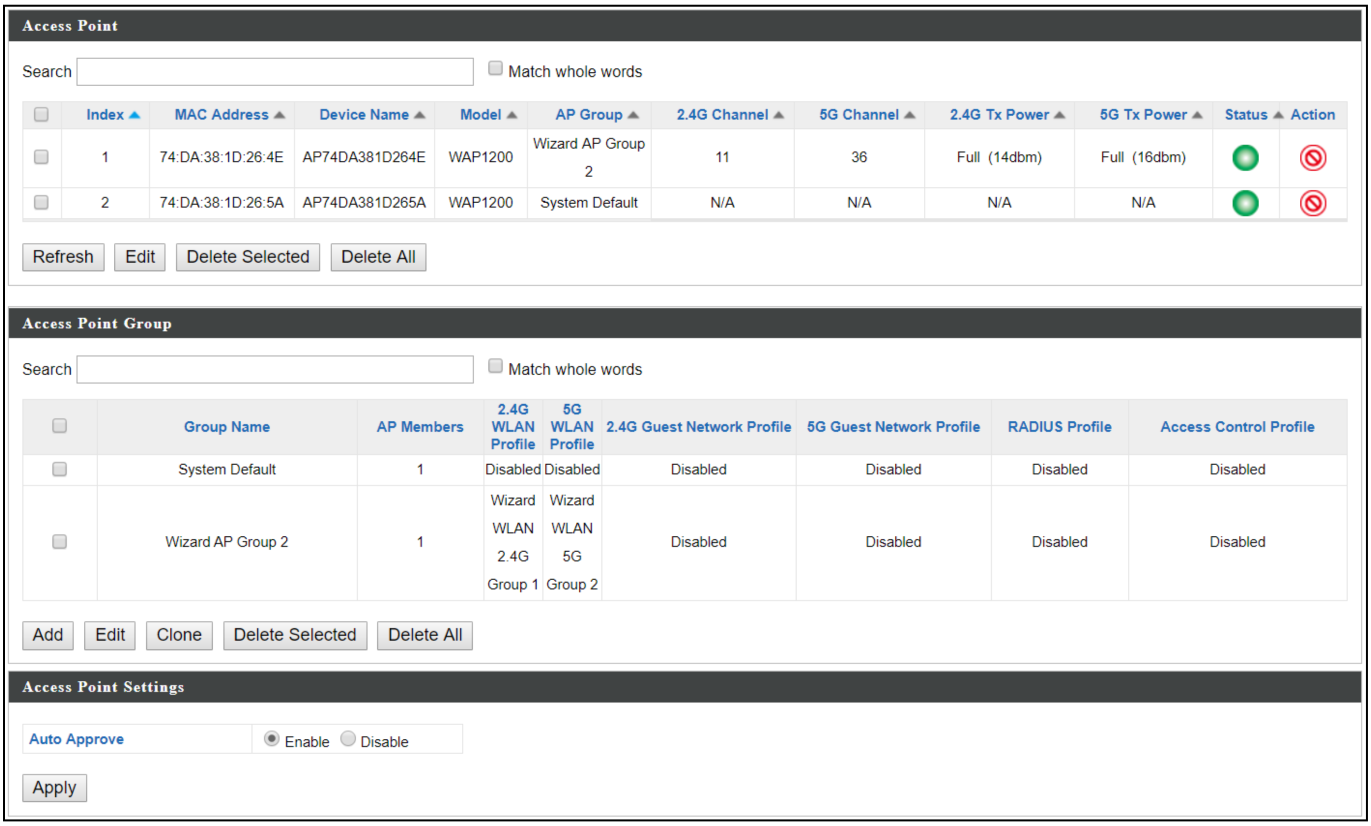


X-5-1 Access Point

Displays information about each access point and access point group in the local network and allows you to edit access points and edit or add access point groups.

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





Access Point

Search □ Match whole words

□	Index ▲	MAC Address ▲	Device Name ▲	Model ▲	AP Group ▲	2.4G Channel ▲	5G Channel ▲	2.4G Tx Power ▲	5G Tx Power ▲	Status ▲	Action
□	1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	Wizard AP Group 2	11	36	Full (14dbm)	Full (16dbm)	●	⊘
□	2	74:DA:38:1D:26:5A	AP74DA381D265A	WAP1200	System Default	N/A	N/A	N/A	N/A	●	⊘

Refresh | Edit | Delete Selected | Delete All

Access Point Group

Search □ Match whole words

□	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
□	System Default	1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
□	Wizard AP Group 2	1	Wizard WLAN 2.4G Group 1	Wizard WLAN 5G Group 2	Disabled	Disabled	Disabled	Disabled

Add | Edit | Clone | Delete Selected | Delete All

Access Point Settings

Auto Approve ● Enable ○ Disable

Apply

The **Status** icon displays *grey* (disconnected), *red* (authentication failed/incompatible NMS version), *orange* (upgrading firmware), *yellow* (connecting), *green* (connected) or *blue* (waiting for approval) for each individual Managed AP. Refer to the *Status Icons in* ***X-2-3 Managed AP*** for full descriptions.

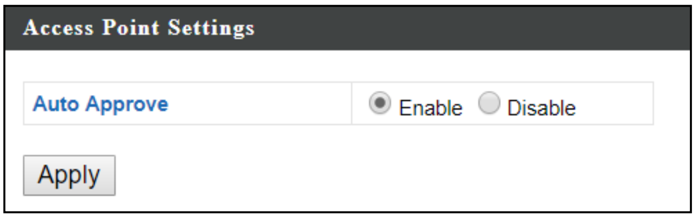
The **“Action”** icons enable you to allow or disallow an access point: 🚫 ✓

Select an access point or access point group using the check-boxes and click “**Edit**” to make configurations, or click “**Add**” to add a new access point group:

☑ Edit

Add

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



Access Point Settings

Auto Approve ● Enable ○ Disable

Apply

Access Point Settings	
Auto Approve	Enable or disable Auto Approve for all Managed APs.

To manually approve a Managed AP, use the *allow* “Action” icon for the specified access point:

X-5-1-1 Edit Access Point

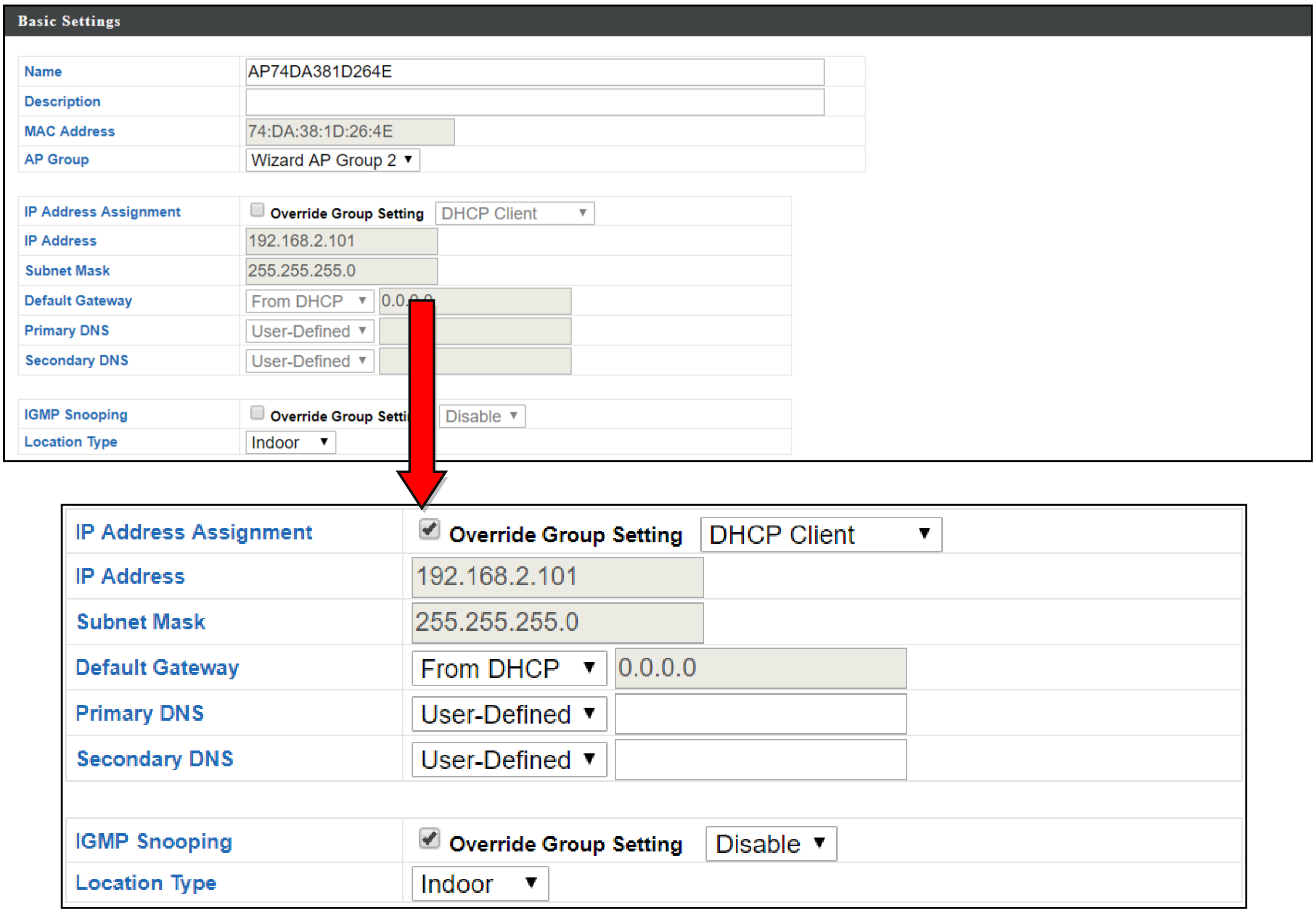
Configure your selected access point on your LAN. You can set the access point as a DHCP client or specify a static IP address for your access point, and assign the access point to an AP group, as well as edit 2.4GHz & 5GHz wireless radio settings. Event log is displayed at the bottom of the page.

You can also use **Profile Settings** to assign the access point to WLAN, Guest Network, RADIUS and Access Control groups independently from Access Point Group settings.

Click “Save” to save the settings. Click “Cancel” to forfeit the changes. Click “Save and Apply” to save and apply the settings.

X-5-1-1-1 Edit Basic Settings

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



Basic Settings

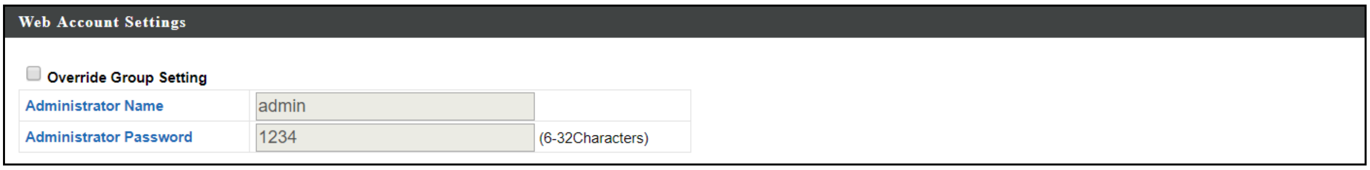
Name	AP74DA381D264E
Description	
MAC Address	74:DA:38:1D:26:4E
AP Group	Wizard AP Group 2
IP Address Assignment	□ Override Group Setting DHCP Client
IP Address	192.168.2.101
Subnet Mask	255.255.255.0
Default Gateway	From DHCP 0.0.0.0
Primary DNS	User-Defined
Secondary DNS	User-Defined
IGMP Snooping	□ Override Group Setting Disable
Location Type	Indoor

IP Address Assignment	☑ Override Group Setting DHCP Client
IP Address	192.168.2.101
Subnet Mask	255.255.255.0
Default Gateway	From DHCP 0.0.0.0
Primary DNS	User-Defined
Secondary DNS	User-Defined
IGMP Snooping	☑ Override Group Setting Disable
Location Type	Indoor

Basic Settings	
Name	Edit the access point name. The default name is AP + MAC address.
Description	Enter a description of the access point for reference e.g. 2nd Floor Office.
MAC Address	Displays MAC address.
AP Group	Use the drop down menu to assign the AP to an AP Group.

	You can edit AP Groups from the **NMS Settings → Access Point** page.
IP Address Assignment	Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server, or select “Static IP” to manually specify a static/fixed IP address for your access point (below). Check the box “Override Group Setting” if the AP is a member of an AP Group and you wish to use a different setting than the AP Group setting.
IP Address	Specify the IP address here. This IP address will be assigned to your 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.
Primary DNS	DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.
Secondary DNS	DHCP users can select “From DHCP” to get secondary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.
IGMP Snooping	Enable / Disable the IGMP Snooping function. IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic.
Location Type	Select the location of the AP (indoor or outdoor).

X-5-1-1-2 Edit Web Account Settings



Web Account Settings

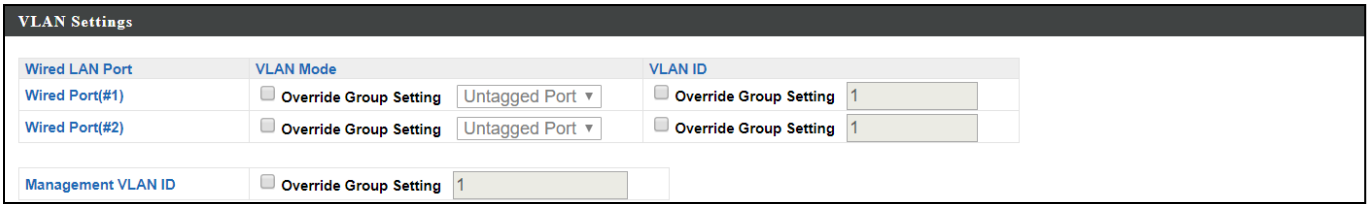
□ Override Group Setting

Administrator Name	admin	
Administrator Password	1234	(6-32Characters)

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

☑ Override Group Setting

X-5-1-1-3 Edit VLAN Settings



VLAN Settings

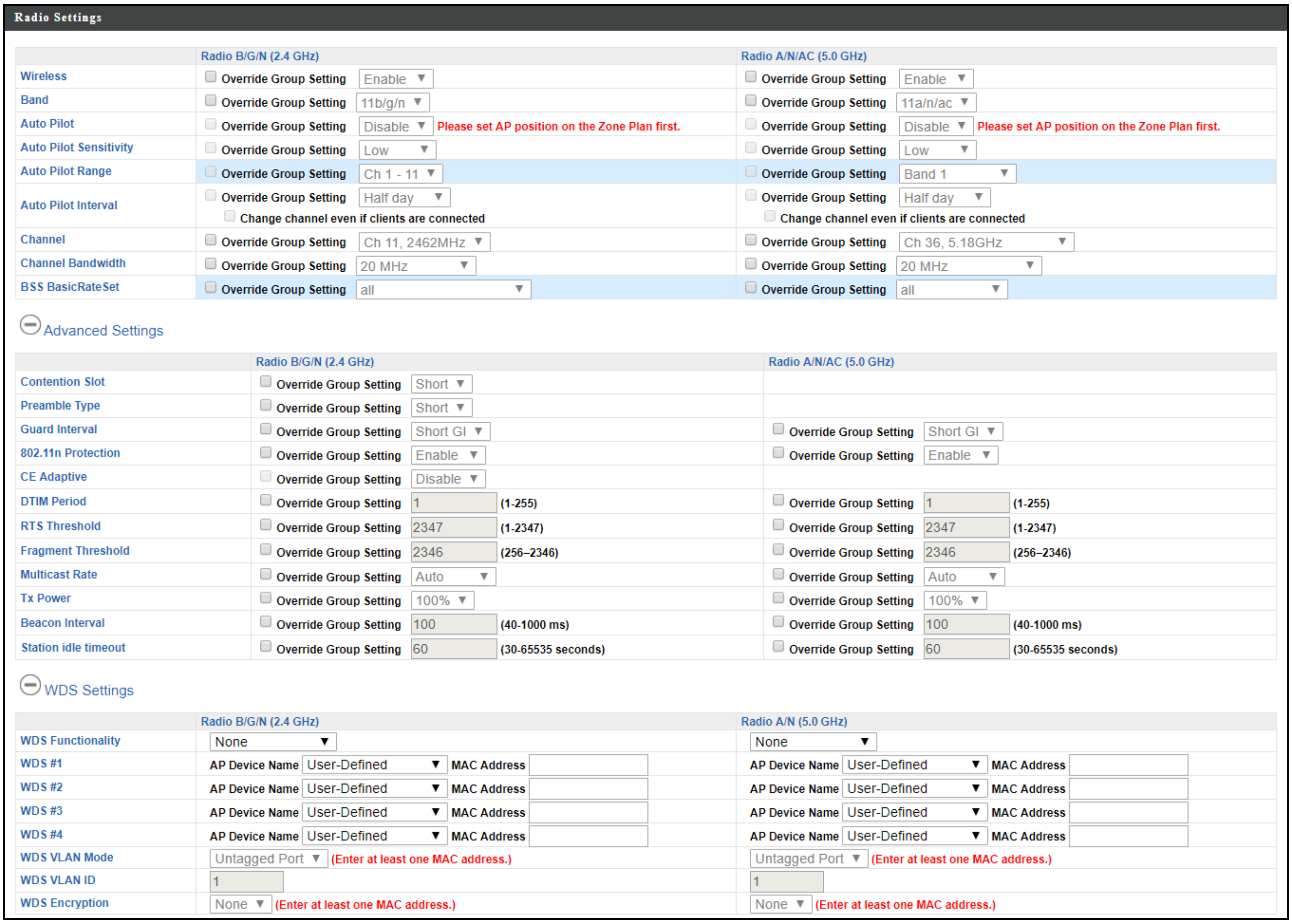
Wired LAN Port	VLAN Mode	VLAN ID
Wired Port(#1)	□ Override Group Setting Untagged Port ▼	□ Override Group Setting 1
Wired Port(#2)	□ Override Group Setting Untagged Port ▼	□ Override Group Setting 1

Management VLAN ID	□ Override Group Setting 1

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

☑ Override Group Setting

X-5-1-1-4 Edit Radio Settings



Radio Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Wireless	□ Override Group Setting Enable ▼	□ Override Group Setting Enable ▼
Band	□ Override Group Setting 11b/g/n ▼	□ Override Group Setting 11a/n/ac ▼
Auto Pilot	□ Override Group Setting Disable ▼ Please set AP position on the Zone Plan first.	□ Override Group Setting Disable ▼ Please set AP position on the Zone Plan first.
Auto Pilot Sensitivity	□ Override Group Setting Low ▼	□ Override Group Setting Low ▼
Auto Pilot Range	□ Override Group Setting Ch 1 - 11 ▼	□ Override Group Setting Band 1 ▼
Auto Pilot Interval	□ Override Group Setting Half day ▼ □ Change channel even if clients are connected	□ Override Group Setting Half day ▼ □ Change channel even if clients are connected
Channel	□ Override Group Setting Ch 11, 2462MHz ▼	□ Override Group Setting Ch 36, 5.18GHz ▼
Channel Bandwidth	□ Override Group Setting 20 MHz ▼	□ Override Group Setting 20 MHz ▼
BSS BasicRateSet	□ Override Group Setting all ▼	□ Override Group Setting all ▼

Advanced Settings

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

WDS Settings

	Radio B/G/N (2.4 GHz)	Radio A/N (5.0 GHz)
WDS Functionality	None ▼	None ▼
WDS #1	AP Device Name User-Defined ▼ MAC Address	AP Device Name User-Defined ▼ MAC Address
WDS #2	AP Device Name User-Defined ▼ MAC Address	AP Device Name User-Defined ▼ MAC Address
WDS #3	AP Device Name User-Defined ▼ MAC Address	AP Device Name User-Defined ▼ MAC Address
WDS #4	AP Device Name User-Defined ▼ MAC Address	AP Device Name User-Defined ▼ MAC Address
WDS VLAN Mode	Untagged Port ▼ (Enter at least one MAC address.)	Untagged Port ▼ (Enter at least one MAC address.)
WDS VLAN ID	1	1
WDS Encryption	None ▼ (Enter at least one MAC address.)	None ▼ (Enter at least one MAC address.)

Radio Settings	
Wireless	Enable or disable the access point’s 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point’s 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot Sensitivity	Select sensitivity of Auto Pilot.
Auto Pilot	Select a range from which the auto channel setting (above)

Range	will choose a channel.
Auto Pilot Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel	When Auto Pilot is disabled, select a channel (1-11) manually.
Channel Bandwidth	Set the channel bandwidth or use Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

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

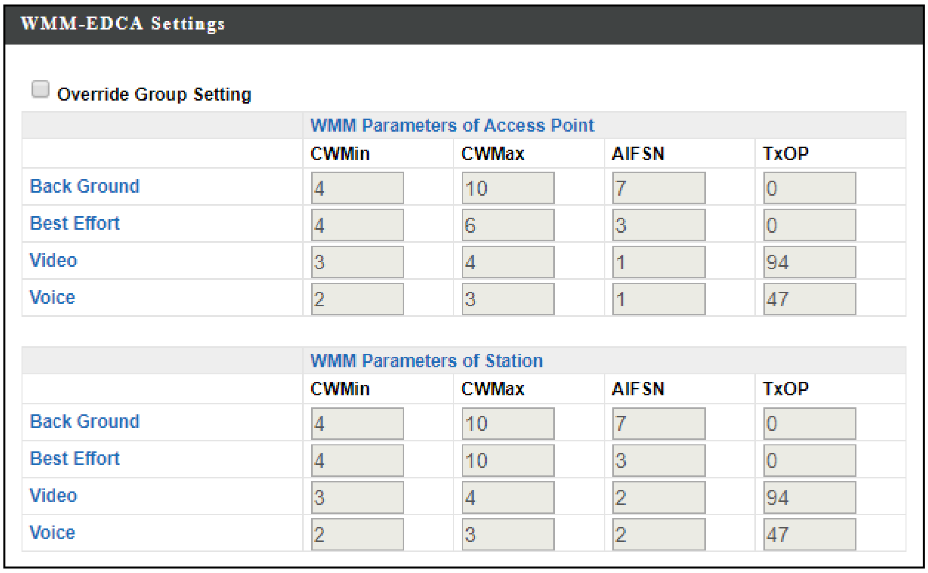
Changing these settings can adversely affect the performance of your access point.

Advanced Settings	
Contention Slot	Select "Short" or "Long" – this value is used for contention windows in WMM (see ***X-6-7 WMM***).
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is "Short Preamble".
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n 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.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.

Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the access point to a wireless client to verify if the station is still alive/active.

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

X-5-1-1-5 Edit WMM-EDCA Settings



WMM-EDCA Settings

□ Override Group Setting

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

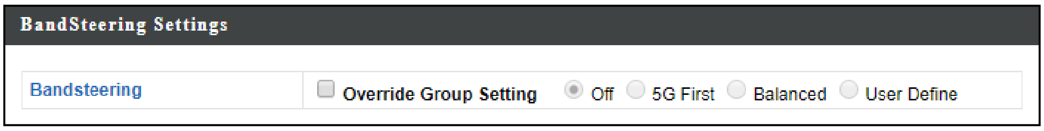
WMM Parameters of Station	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	10	3	0
Video	3	4	2	94
Voice	2	3	2	47

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

☑ Override Group Setting

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

X-5-1-1-6 Edit BandSteering Settings



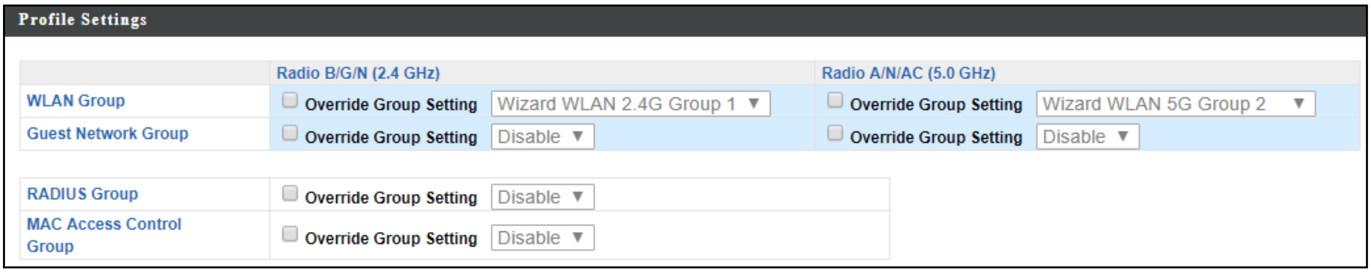
BandSteering Settings

Bandsteering □ Override Group Setting ● Off ○ 5G First ○ Balanced ○ User Define

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

☑ Override Group Setting

X-5-1-1-7 Edit Profile Settings



Profile Settings

	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)	
WLAN Group	□ Override Group Setting	Wizard WLAN 2.4G Group 1 ▼	□ Override Group Setting	Wizard WLAN 5G Group 2 ▼
Guest Network Group	□ Override Group Setting	Disable ▼	□ Override Group Setting	Disable ▼
RADIUS Group	□ Override Group Setting	Disable ▼		
MAC Access Control Group	□ Override Group Setting	Disable ▼		

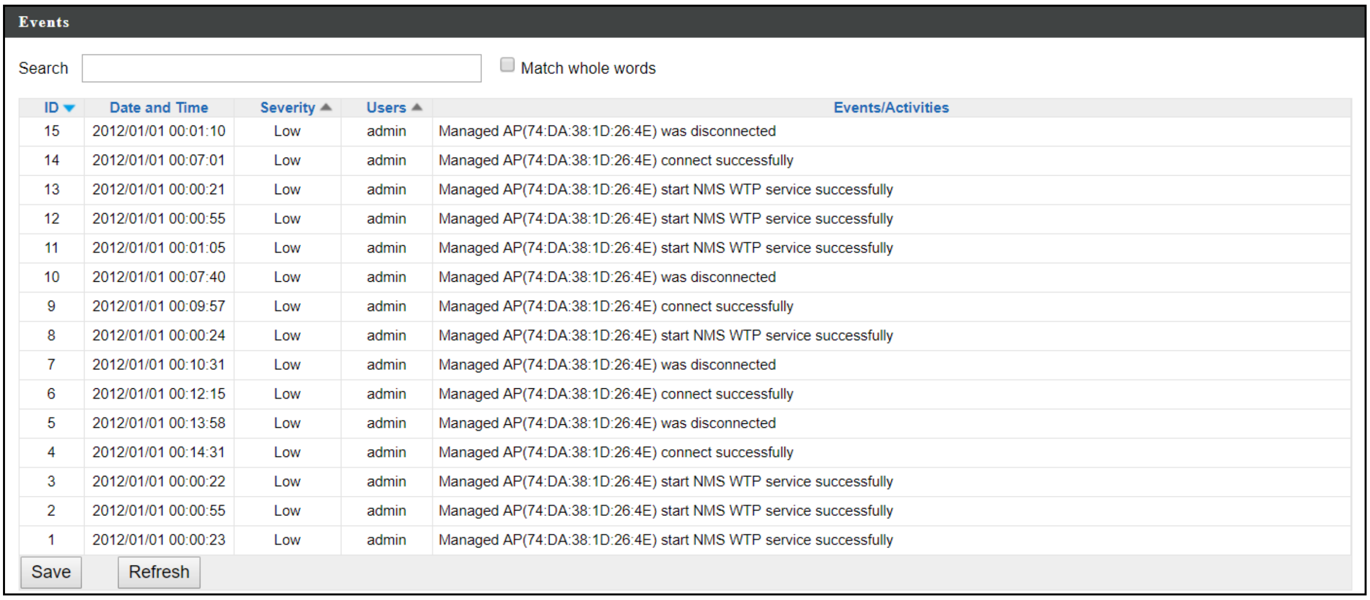
When “**Override Group Setting**” is checked, options/fields will turn white to allow adjustments.

☑ Override Group Setting

Profile Settings	
WLAN Group	Assign the access point’s 2.4GHz or 5GHz SSID(s) to a WLAN Group. You can edit WLAN groups in **NMS Settings → WLAN**.
Guest Network Group	Assign the access point’s 2.4GHz or 5GHz SSID(s) to a Guest Network Group. You can edit Guest Network groups in **NMS Settings → Guest Network**.
RADIUS Group	Assign the access point’s 2.4GHz SSID(s) to a RADIUS group. You can edit RADIUS groups in **NMS Settings → RADIUS**.
MAC Access Control Group	Assign the access point’s 2.4GHz SSID(s) to a RADIUS group. You can edit RADIUS groups in **NMS Settings → Access Control**

X-5-1-1-8 Events

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



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

X-5-1-2 Add/Edit Access Point Group

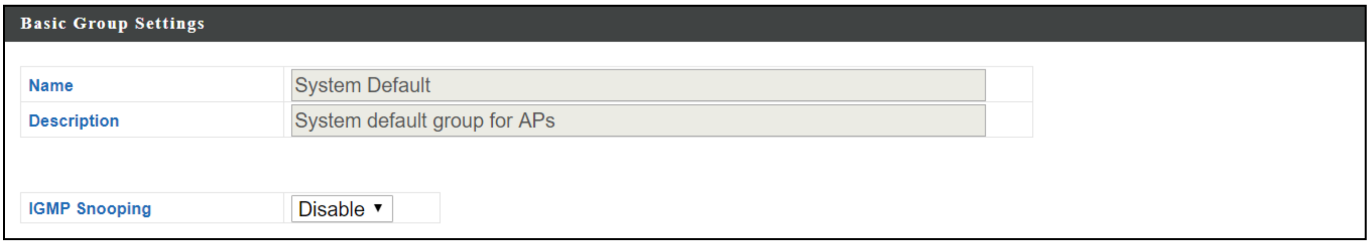
Configure your selected access point group. Access point group settings apply to all access points in the group, unless individually set to override group settings.

You can use **Profile Group Settings** to assign the access point group to WLAN, Guest Network, RADIUS and Access Control groups.

Click “Save” to save the settings. Click “Cancel” to forfeit the changes. Click “Save and Apply” to save and apply the settings.

X-5-1-2-1 Edit Basic Group Settings

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

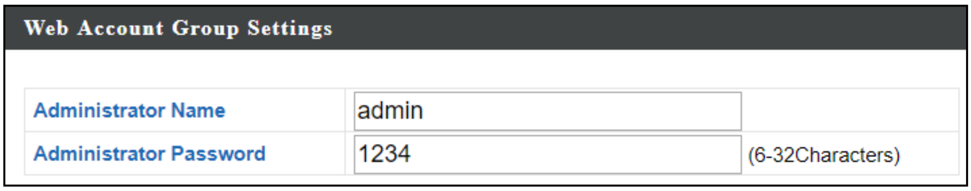


Basic Group Settings

Name	System Default
Description	System default group for APs
IGMP Snooping	Disable ▾

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

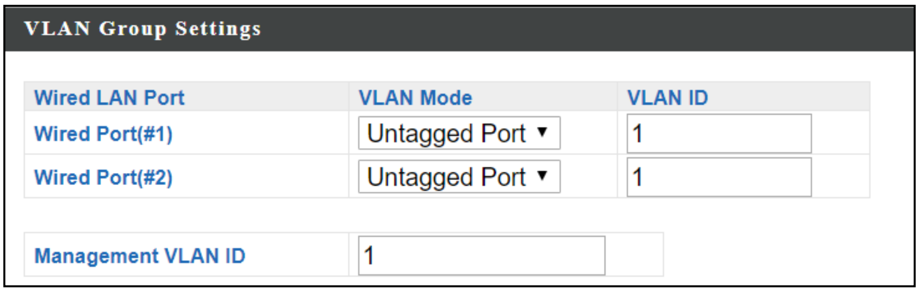
X-5-1-2-2 Edit Web Account Group Settings



Web Account Group Settings

Administrator Name	admin	
Administrator Password	1234	(6-32Characters)

X-5-1-2-3 Edit VLAN Group Settings

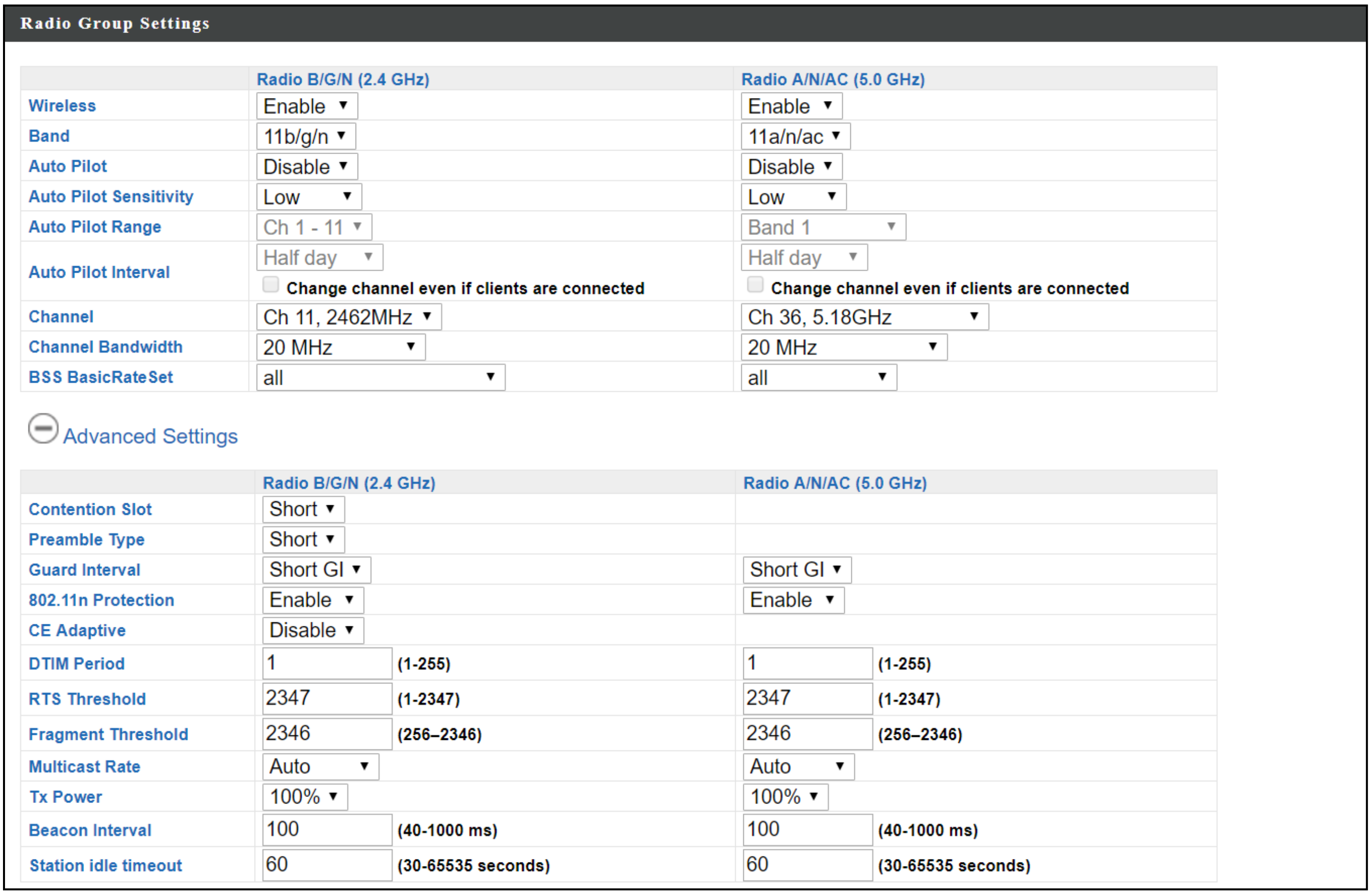


VLAN Group Settings

Wired LAN Port	VLAN Mode	VLAN ID
Wired Port(#1)	Untagged Port ▾	1
Wired Port(#2)	Untagged Port ▾	1

Management VLAN ID	1

X-5-1-2-4 Edit Radio Group Settings



Radio Group Settings

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

Advanced Settings

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

Radio Group Settings	
Wireless	Enable or disable the access point group's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the access point group. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point group's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot Sensitivity	Select sensitivity of Auto Pilot.
Auto Pilot Range	Select a range from which the auto channel setting (above) will choose a channel.

Auto Pilot Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the “Change channel even if clients are connected” box according to your preference.
Channel	When Auto Pilot is disabled, select a channel (1-11) manually.
Channel Bandwidth	Set the channel bandwidth or use Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

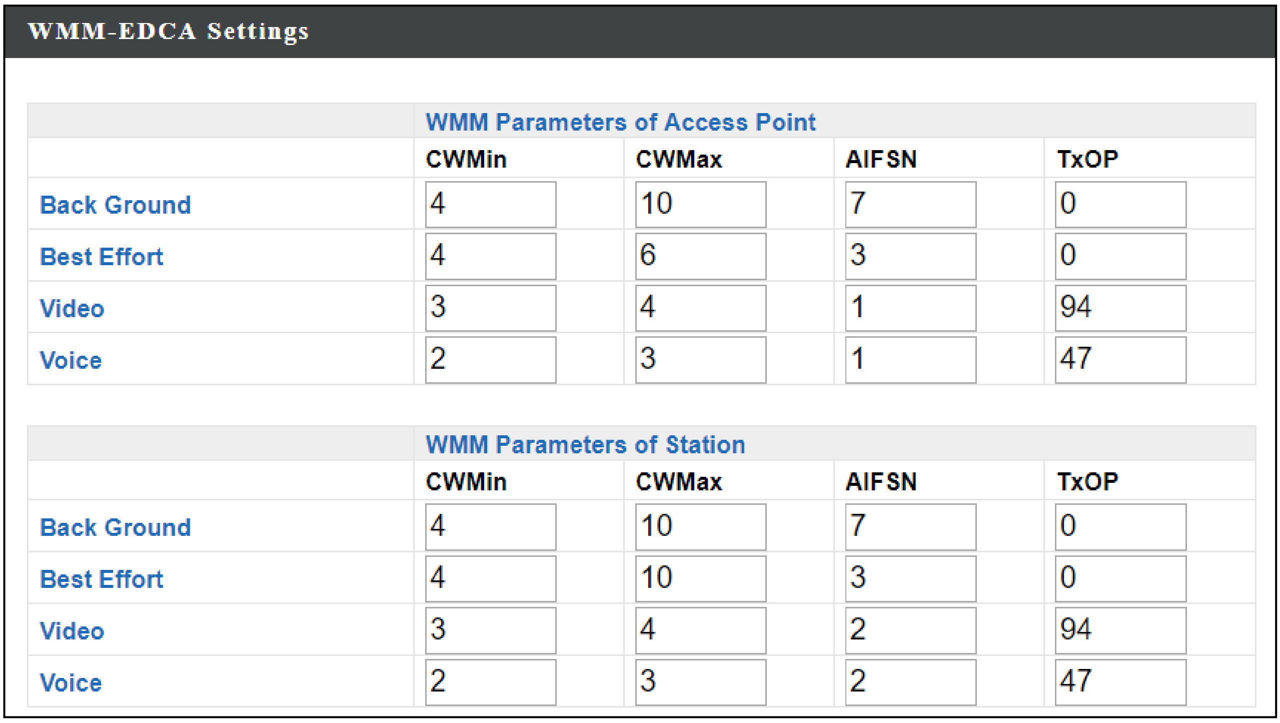
These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

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

Advanced Settings	
Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM (see ***X-6-7 WMM***).
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is “Short Preamble”.
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n 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.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.

Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the "Auto" setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the access point to a wireless client to verify if the station is still alive/active.

X-5-1-2-5 Edit WMM-EDCA Settings

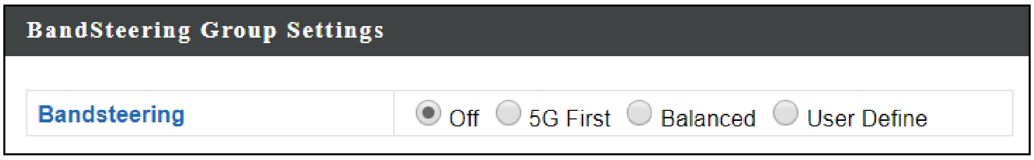


WMM-EDCA Settings

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

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

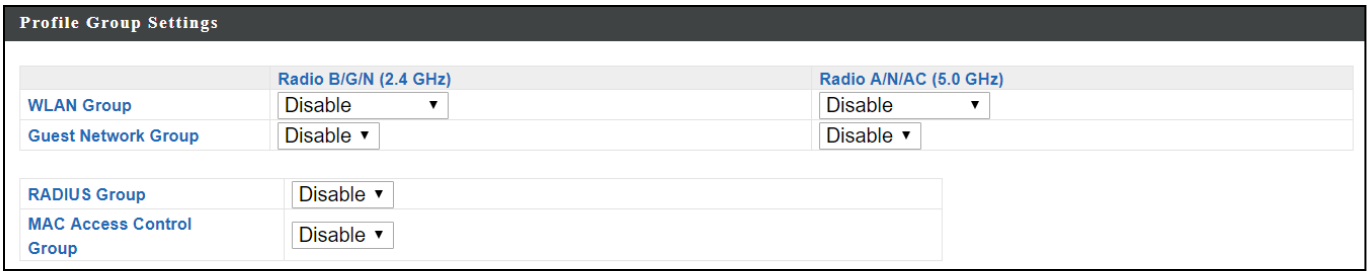
X-5-1-2-6 Edit BandSteering Settings



BandSteering Group Settings

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

X-5-1-2-7 Edit Profile Settings



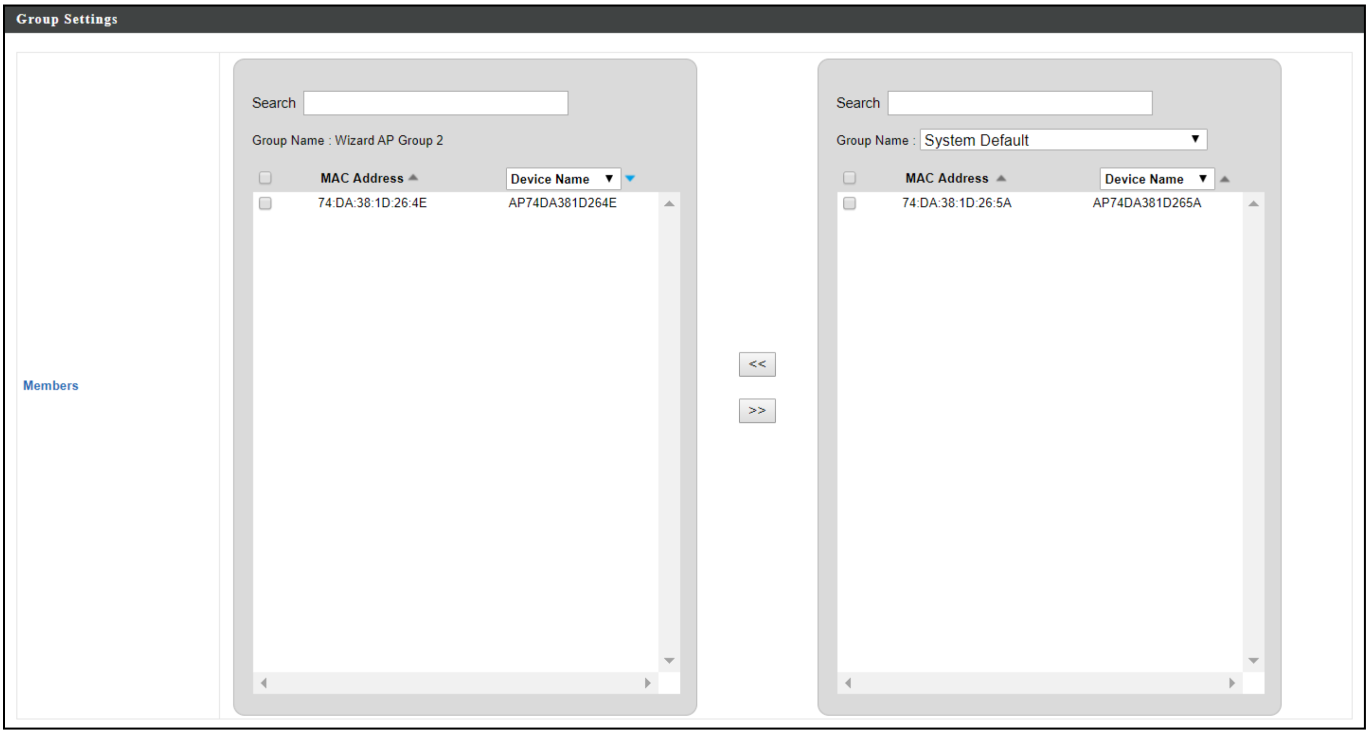
Profile Group Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
WLAN Group	Disable ▾	Disable ▾
Guest Network Group	Disable ▾	Disable ▾

RADIUS Group	Disable ▾
MAC Access Control Group	Disable ▾

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

X-5-1-2-8 Edit Group Settings



Group Settings

Members

Search

Group Name : Wizard AP Group 2

□	MAC Address	Device Name
□	74:DA:38:1D:26:4E	AP74DA381D264E

Search

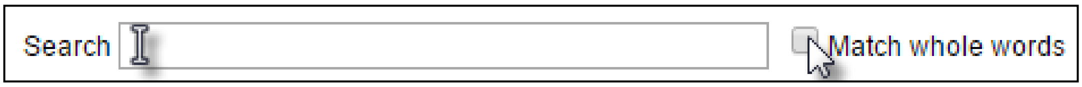
Group Name : System Default

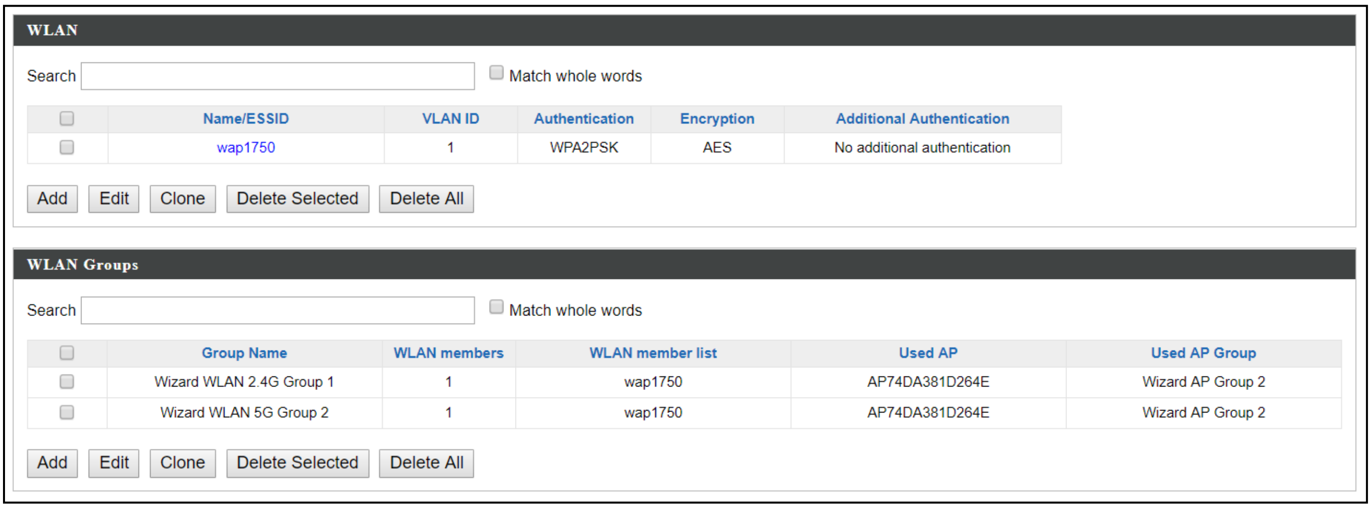
□	MAC Address	Device Name
□	74:DA:38:1D:26:5A	AP74DA381D265A

X-5-2 WLAN

Displays information about each WLAN and WLAN group in the local network and allows you to add or edit WLANs & WLAN Groups. When you add a WLAN Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).

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





WLAN

Search □ Match whole words

□	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
□	wap1750	1	WPA2PSK	AES	No additional authentication

Add | Edit | Clone | Delete Selected | Delete All

WLAN Groups

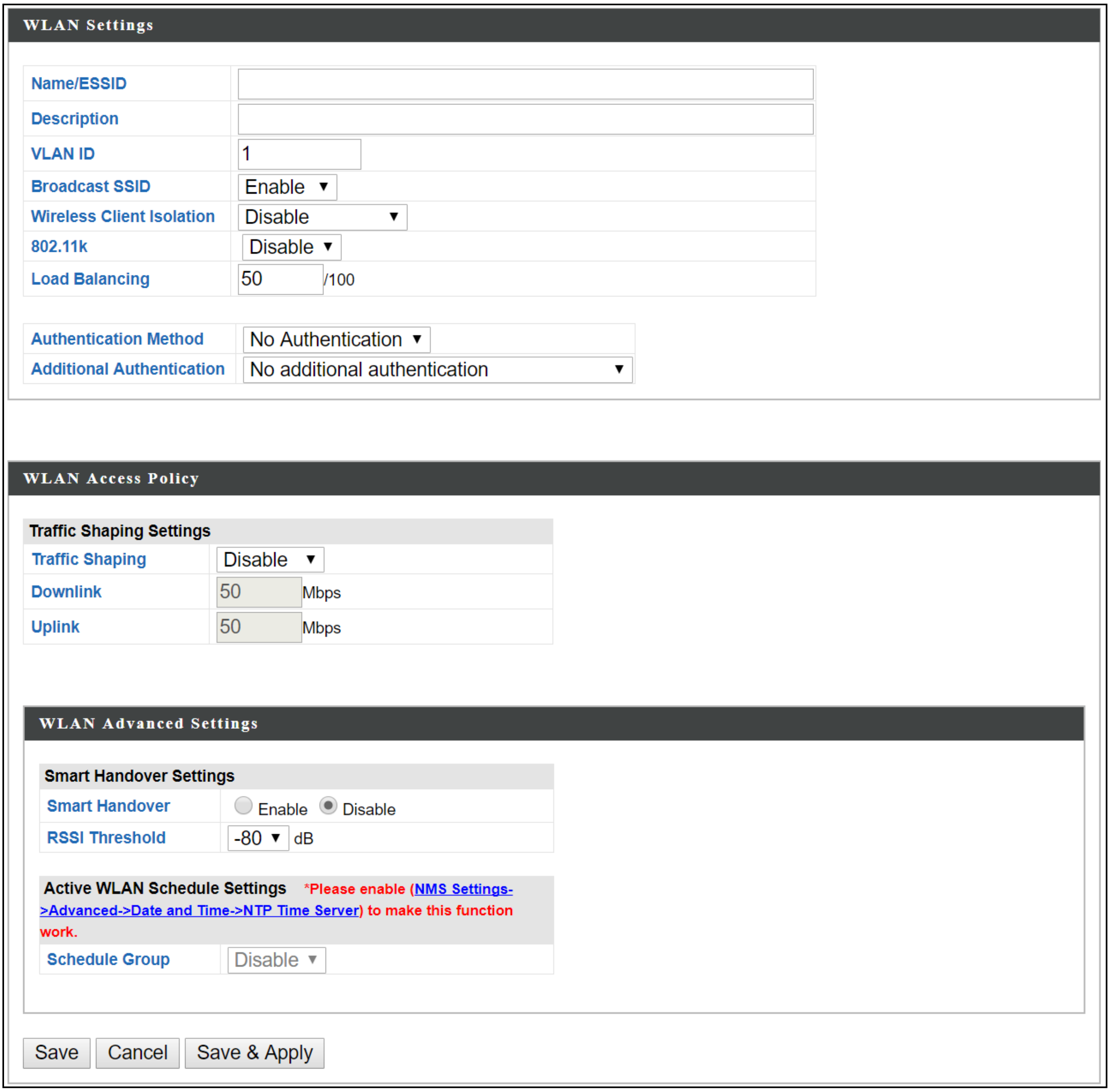
Search □ Match whole words

□	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
□	Wizard WLAN 2.4G Group 1	1	wap1750	AP74DA381D264E	Wizard AP Group 2
□	Wizard WLAN 5G Group 2	1	wap1750	AP74DA381D264E	Wizard AP Group 2

Add | Edit | Clone | Delete Selected | Delete All

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

X-5-2-1 Add/Edit WLAN



Name/ESSID	
Description	
VLAN ID	1
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
802.11k	Disable ▼
Load Balancing	50 /100

Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

Traffic Shaping Settings	
Traffic Shaping	Disable ▼
Downlink	50 Mbps
Uplink	50 Mbps

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

Active WLAN Schedule Settings *Please enable (NMS Settings->Advanced->Date and Time->NTP Time Server) to make this function work.

Schedule Group	Disable ▼

WLAN Settings	
Name/ESSID	Edit the WLAN name (SSID).
Description	Enter a description of the SSID for reference e.g. 2nd Floor Office HR.
VLAN ID	Specify the VLAN ID.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi

	network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the 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.
802.11k	Enable / Disable to define and expose radio and network information (helps facilitate the management and maintenance of a mobile wireless LAN).
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu.
WPA Type	It can select WPA only or WPA2 only or WPA/WPA2 Mixed Mode-PSK
Encryption Type	It can select TKIP/AES Mixed Mode or AES
Key Renewal Interval	It can set renewal internal time
Pre-Shared Key Type	It can set Passphrase or Hex (64 characters)
Pre-Shared Key	It can set 8-64 characters
Additional Authentication	Select an additional authentication method from the drop down menu.

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

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

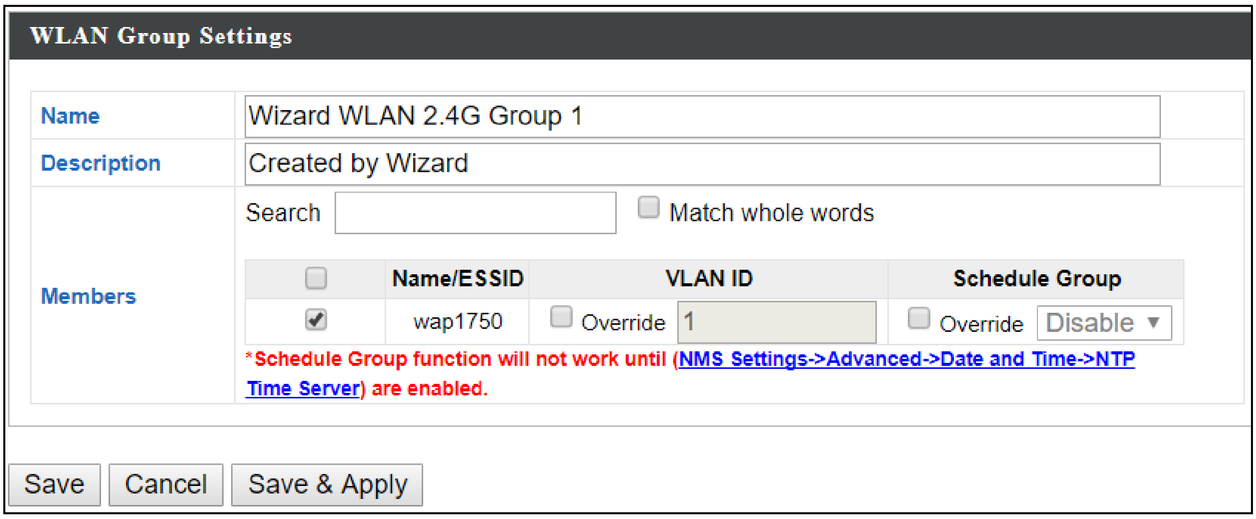
⚠ ***Select hard-to-guess passwords which include combinations of numbers, letters and symbols, and change your password regularly.***

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

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

X-5-2-2 Add/Edit WLAN Group

When you add a WLAN Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).



WLAN Group Settings

Name	Wizard WLAN 2.4G Group 1
Description	Created by Wizard
Members	Search ☐ Match whole words

☐	Name/ESSID	VLAN ID	Schedule Group
☑	wap1750	☐ Override 1	☐ Override Disable ▼

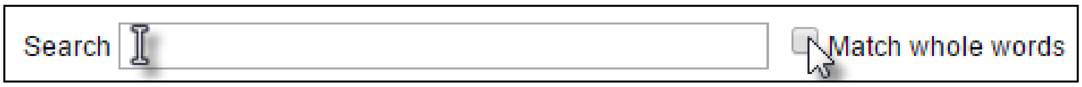
*Schedule Group function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.

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

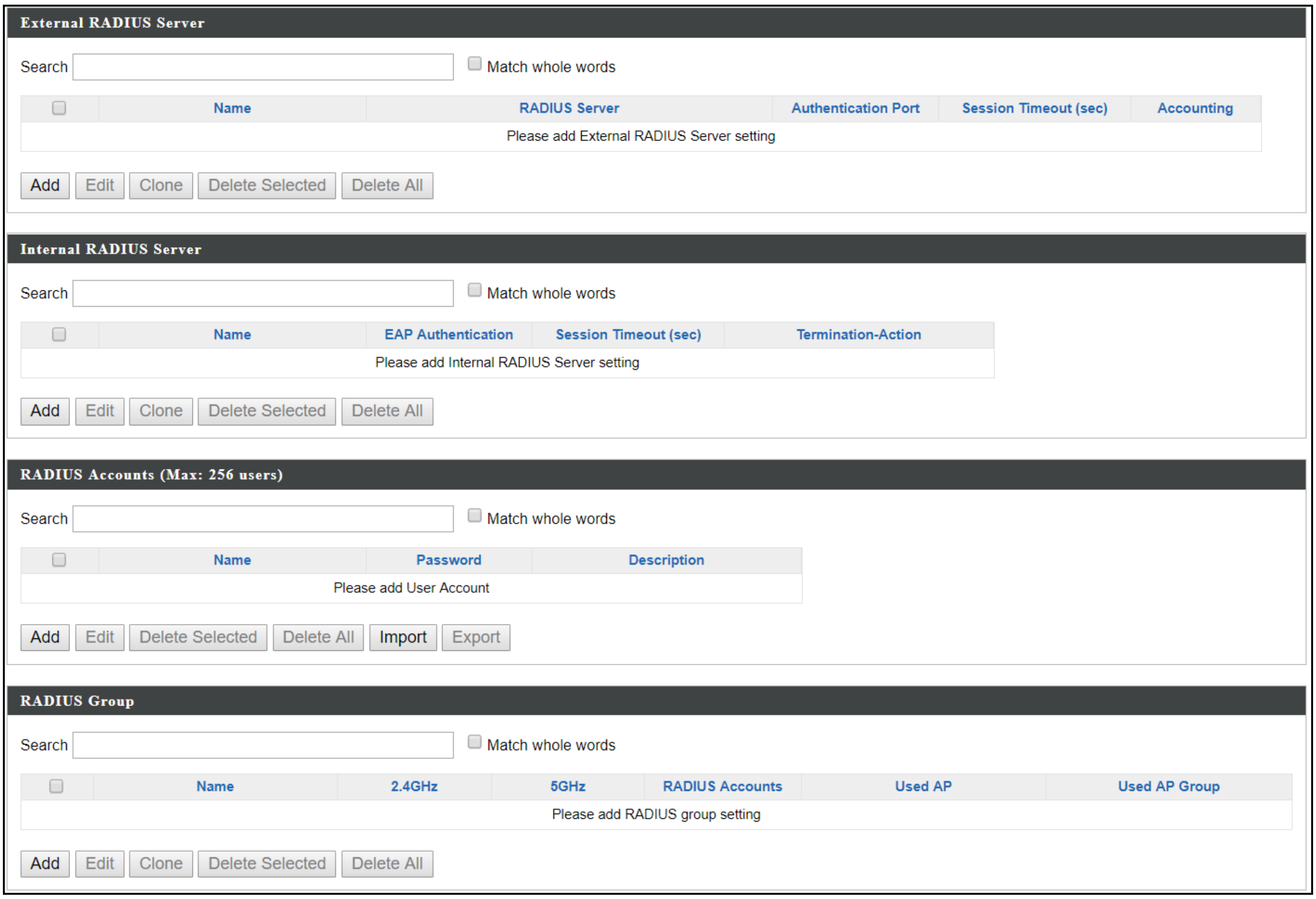
X-5-3 RADIUS

Displays information about External & Internal RADIUS Servers, Accounts and Groups and allows you to add or edit RADIUS Servers, Accounts & Groups. When you add a RADIUS Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).

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



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



External RADIUS Server

Search □ Match whole words

□	Name	RADIUS Server	Authentication Port	Session Timeout (sec)	Accounting
Please add External RADIUS Server setting					

Add | Edit | Clone | Delete Selected | Delete All

Internal RADIUS Server

Search □ Match whole words

□	Name	EAP Authentication	Session Timeout (sec)	Termination-Action
Please add Internal RADIUS Server setting				

Add | Edit | Clone | Delete Selected | Delete All

RADIUS Accounts (Max: 256 users)

Search □ Match whole words

□	Name	Password	Description
Please add User Account			

Add | Edit | Delete Selected | Delete All | Import | Export

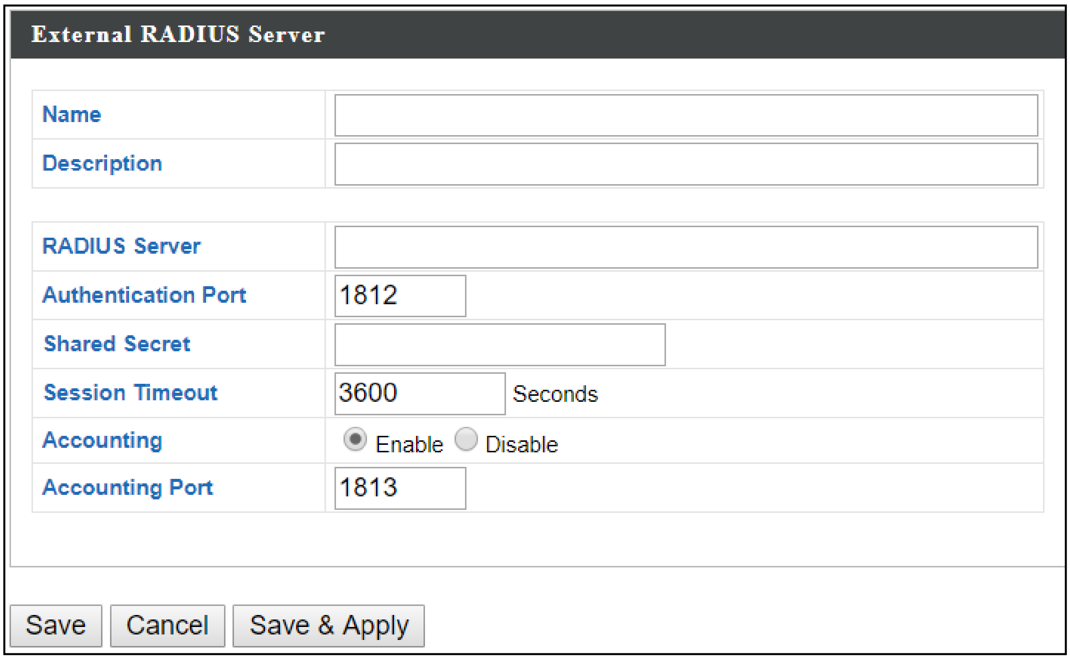
RADIUS Group

Search □ Match whole words

□	Name	2.4GHz	5GHz	RADIUS Accounts	Used AP	Used AP Group
Please add RADIUS group setting						

Add | Edit | Clone | Delete Selected | Delete All

X-5-3-1 Add/Edit External RADIUS Server

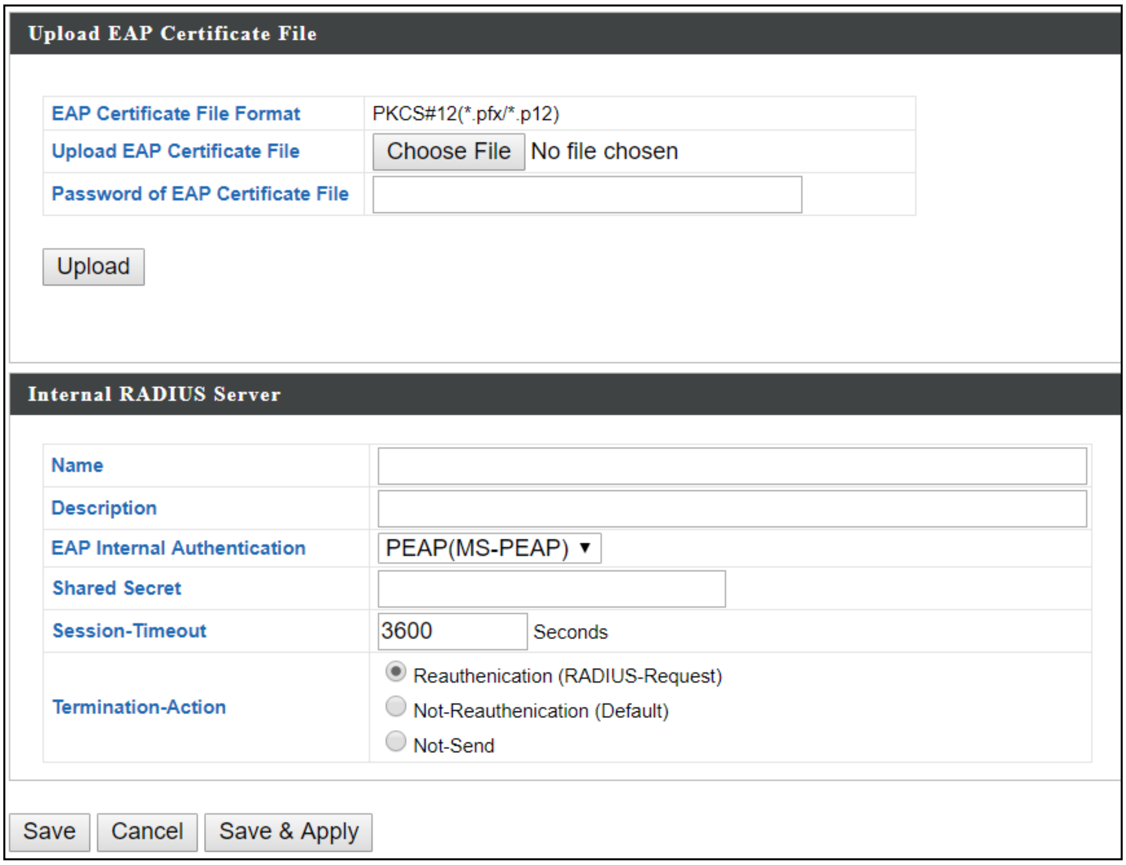


External RADIUS Server

Name	
Description	
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 Seconds
Accounting	● Enable ○ Disable
Accounting Port	1813

Name	Enter a name for the RADIUS Server.
Description	Enter a description of the RADIUS Server for reference.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in ***X-6-2-3*** or ***X-6-3-3***.
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.

X-5-3-2 Add/Edit Internal RADIUS Server



Upload EAP Certificate File

EAP Certificate File Format	PKCS#12(*.pfx/*.p12)
Upload EAP Certificate File	Choose File No file chosen
Password of EAP Certificate File	

Internal RADIUS Server

Name	
Description	
EAP Internal Authentication	PEAP(MS-PEAP) ▼
Shared Secret	
Session-Timeout	3600 Seconds
Termination-Action	● Reauthenication (RADIUS-Request) ○ Not-Reauthenication (Default) ○ Not-Send

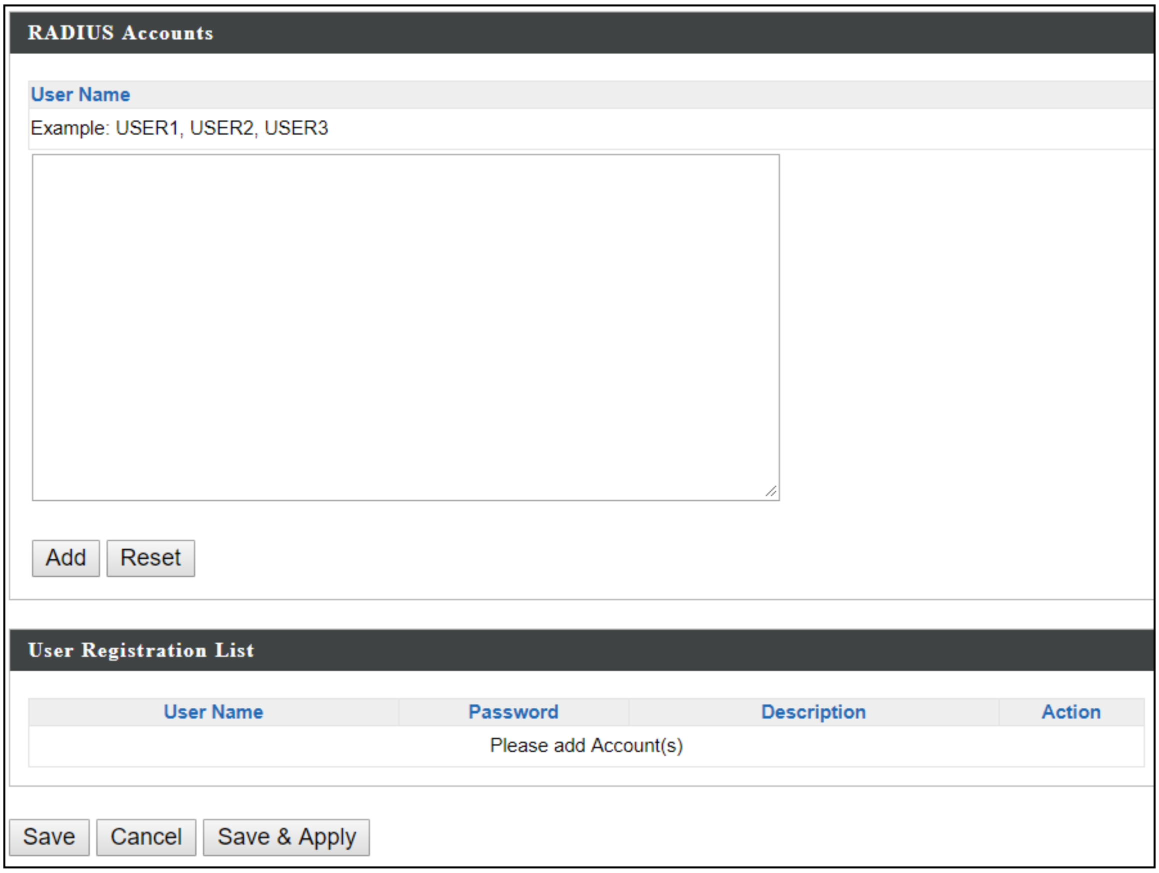
Upload EAP Certificate File	
EAP Certificate File Format	Displays the EAP certificate file format: PKCS#12(*.pfx/*.p12)
EAP Certificate File	Click "Upload" to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will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

Internal RADIUS Server	
Name	Enter a name for the Internal RADIUS Server.
Description	Enter a description of the Internal RADIUS Server for reference.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click "Upload" to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made

	certificate.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
Shared Secret	Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Termination Action	Select a termination-action attribute: "Reauthentication" sends a RADIUS request to the access point, "Not-Reauthentication" sends a default termination-action attribute to the access point, "Not-Send" no termination-action attribute is sent to the access point.

X-5-3-3 Add/Edit/Import/Export RADIUS Accounts

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



RADIUS Accounts

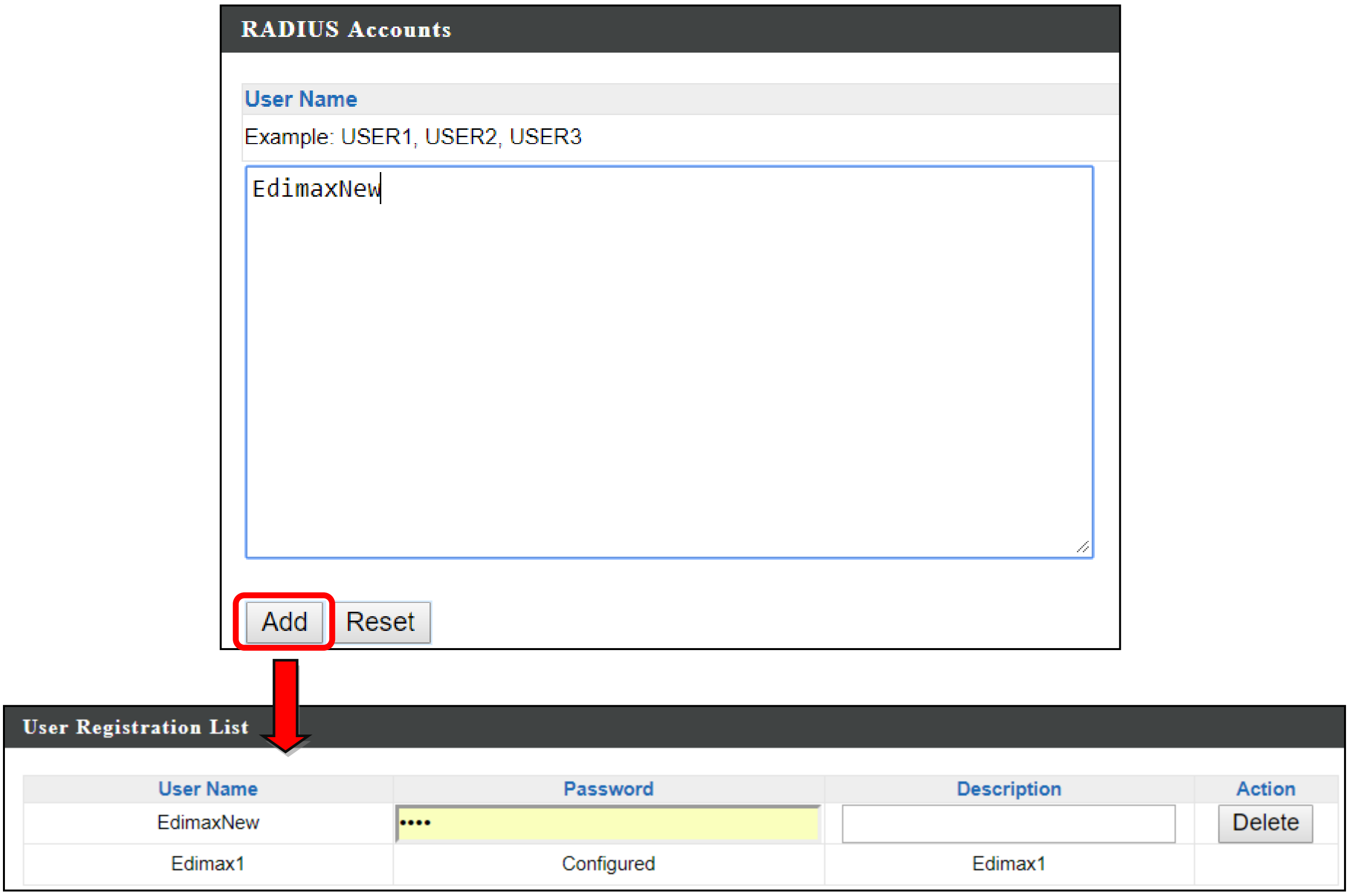
User Name

Example: USER1, USER2, USER3

User Registration List

User Name	Password	Description	Action
Please add Account(s)			

Add



RADIUS Accounts

User Name

Example: USER1, USER2, USER3

EdimaxNew

User Registration List

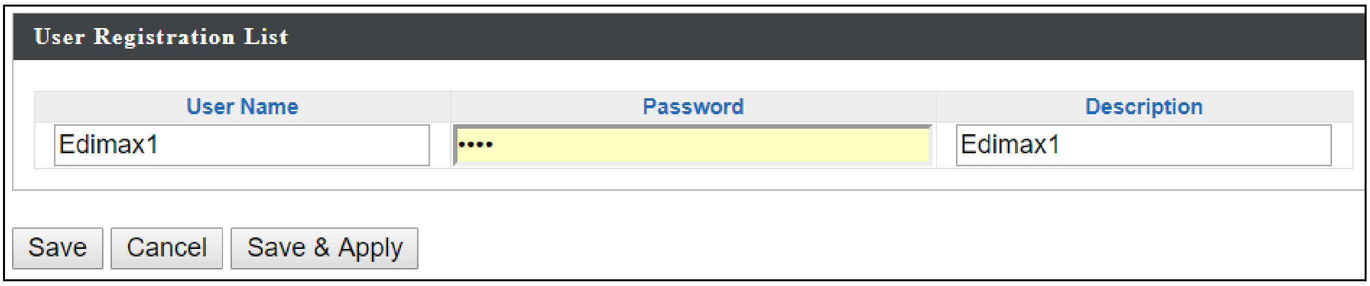
User Name	Password	Description	Action
EdimaxNew	••••		Delete
Edimax1	Configured	Edimax1	

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

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

Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

Edit



User Registration List

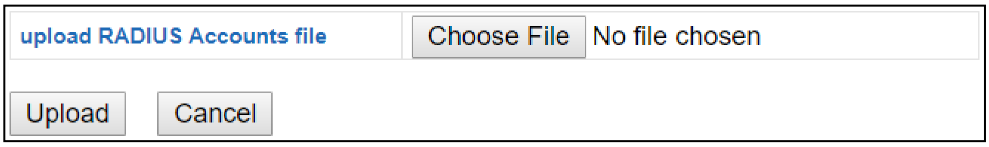
User Name	Password	Description
Edimax1	••••	Edimax1

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

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

Import

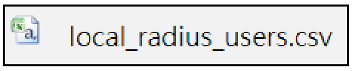
If you wish to import RADIUS accounts, press “Import”. The following page is displayed below. Choose a file from a file and press “Upload” to import RADIUS accounts.



upload RADIUS Accounts file: No file chosen

Export

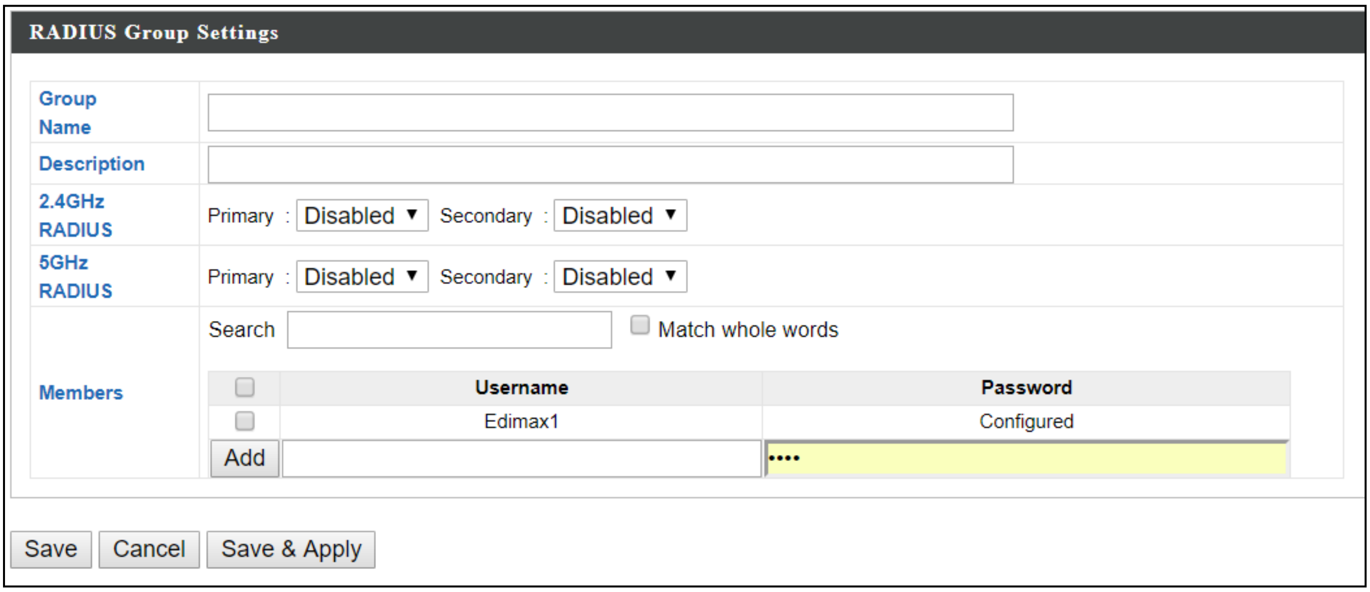
If you wish to export your current list of RADIUS accounts, press “Export”. Your list will be saved in a format similar to the one below:



local_radius_users.csv

X-5-3-4 Add/Edit RADIUS Group

When you add a RADIUS Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).



RADIUS Group Settings

Group Name	
Description	
2.4GHz RADIUS	Primary : Disabled ▾ Secondary : Disabled ▾
5GHz RADIUS	Primary : Disabled ▾ Secondary : Disabled ▾
Members	Search □ Match whole words

□	Username	Password
□	Edimax1	Configured
Add		••••

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

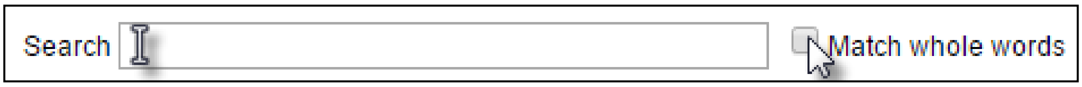
X-5-4 Access Control

MAC Access Control 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 not on the list of permitted MAC addresses attempts to connect to the access point, it will be denied.

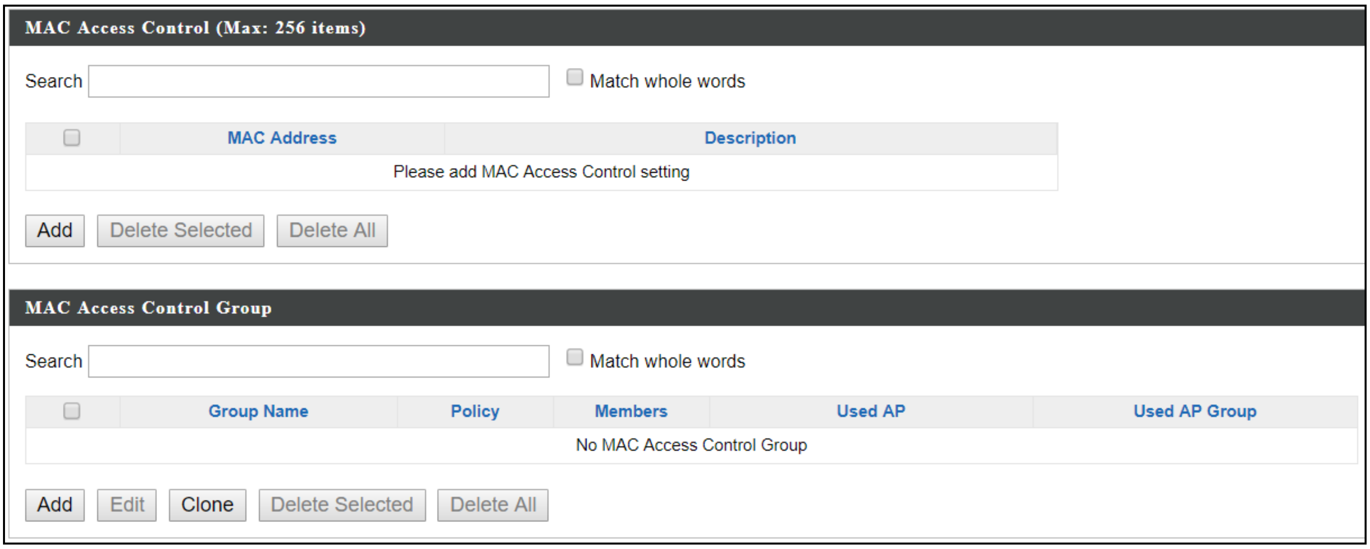
The Access Control panel displays information about MAC Access Control & MAC Access Control Groups and Groups and allows you to add or edit MAC Access Control & MAC Access Control Group settings. When you add an Access Control Group, it will be available for selection in **NMS Settings →** **Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).

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



Search □ Match whole words

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



MAC Access Control (Max: 256 items)

Search □ Match whole words

□	MAC Address	Description
Please add MAC Access Control setting		

Add | Delete Selected | Delete All

MAC Access Control Group

Search □ Match whole words

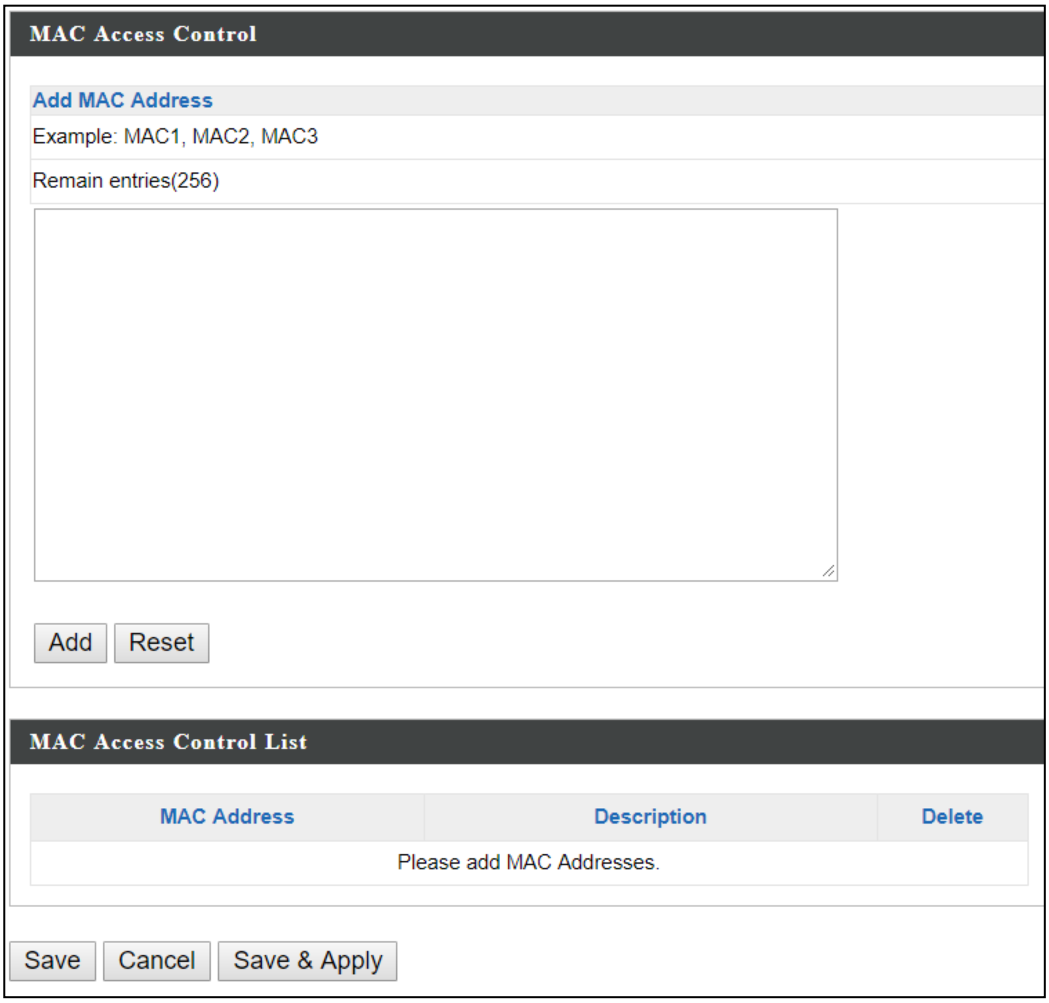
□	Group Name	Policy	Members	Used AP	Used AP Group
No MAC Access Control Group					

Add | Edit | Clone | Delete Selected | Delete All

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

X-5-4-1 Add/Edit MAC Access Control

Click “Add” to enter the page shown below:



MAC Access Control

Add MAC Address

Example: MAC1, MAC2, MAC3

Remain entries(256)

MAC Access Control List

MAC Address	Description	Delete
Please add MAC Addresses.		

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.

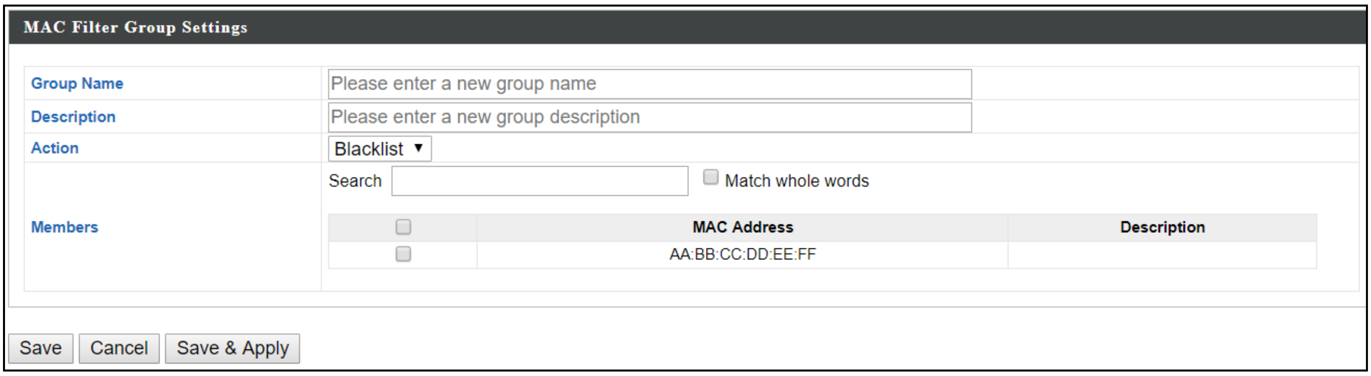
MAC address entries will be listed in the “MAC Address Filtering Table”. Select an entry using the “Select” checkbox.

Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

X-5-4-2 Add/Edit/Clone MAC Access Control Group

When you add an Access Control Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).

Click “Add” to enter the page shown below:



MAC Filter Group Settings

Group Name	Please enter a new group name
Description	Please enter a new group description
Action	Blacklist ▾
Members	Search □ Match whole words

□	MAC Address	Description
□	AA:BB:CC:DD:EE:FF	

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

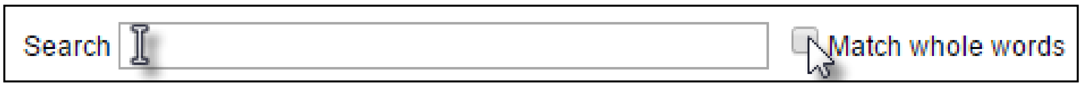
Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

X-5-5 Guest Network

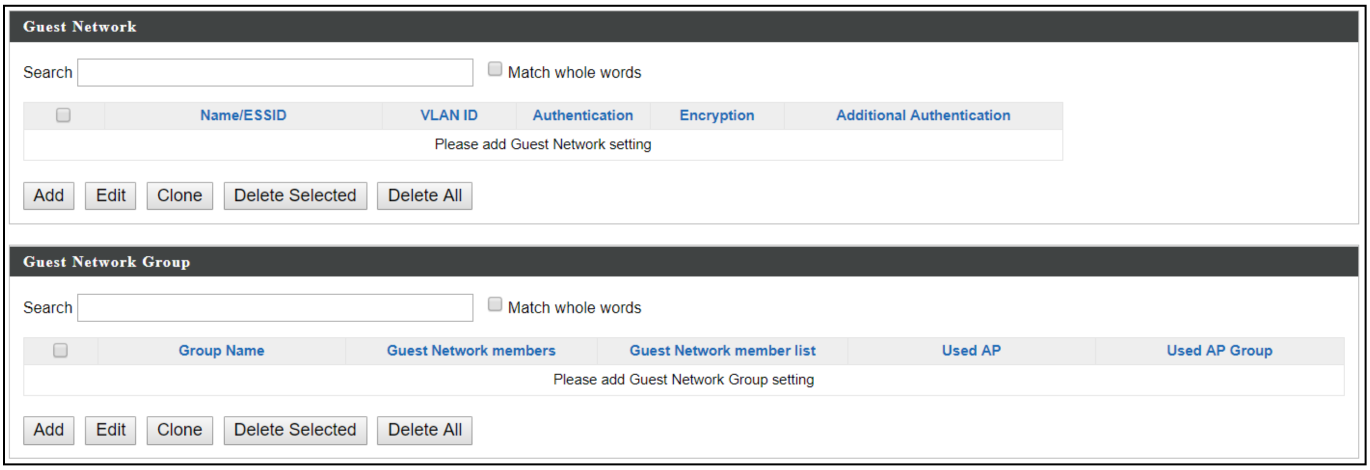
You can setup an additional “Guest” Wi-Fi network so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. The “Guest” screen displays settings for your guest Wi-Fi network.

The Guest Network panel displays information about Guest Networks and Guest Network Groups and allows you to add or edit Guest Network and Guest Network Group settings. When you add a Guest Network Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).

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



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



Guest Network

Search □ Match whole words

□	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
Please add Guest Network setting					

Add | Edit | Clone | Delete Selected | Delete All

Guest Network Group

Search □ Match whole words

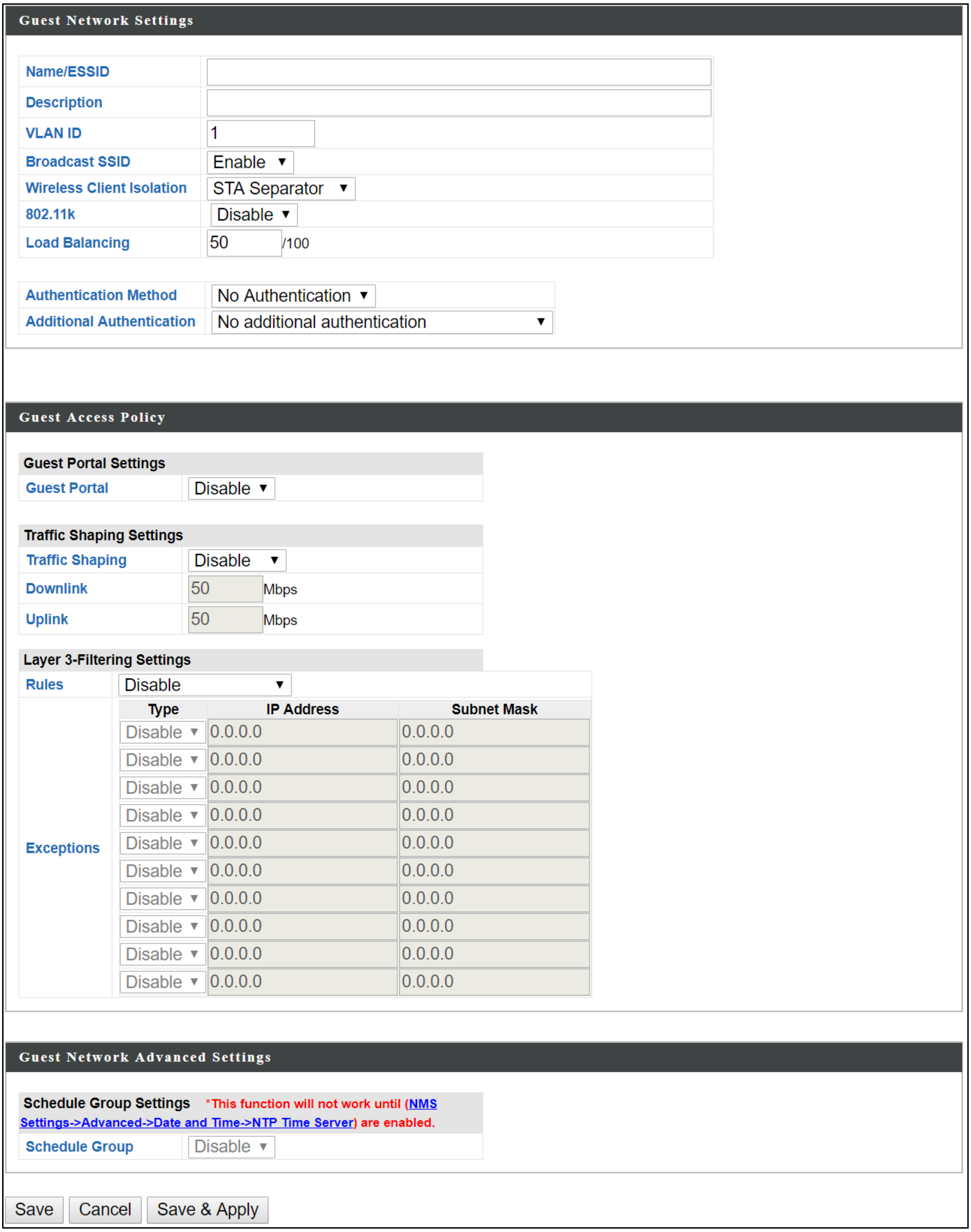
□	Group Name	Guest Network members	Guest Network member list	Used AP	Used AP Group
Please add Guest Network Group setting					

Add | Edit | Clone | Delete Selected | Delete All

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

X-5-5-1 Add/Edit Guest Network

Click “Add” to enter the page shown below:



Guest Network Settings

Name/ESSID	
Description	
VLAN ID	1
Broadcast SSID	Enable ▼
Wireless Client Isolation	STA Separator ▼
802.11k	Disable ▼
Load Balancing	50 /100

Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

Guest Access Policy

Guest Portal Settings

Guest Portal	Disable ▼

Traffic Shaping Settings

Traffic Shaping	Disable ▼
Downlink	50 Mbps
Uplink	50 Mbps

Layer 3-Filtering Settings

Rules	Disable ▼		
	Type	IP Address	Subnet Mask
Exceptions	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0
	Disable ▼	0.0.0.0	0.0.0.0

Guest Network Advanced Settings

Schedule Group Settings *This function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.

Schedule Group	Disable ▼

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

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

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

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

Please refer to ***X-6-2-3*** or ***X-6-3-3*** for more information on authentication and additional authentication types.

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

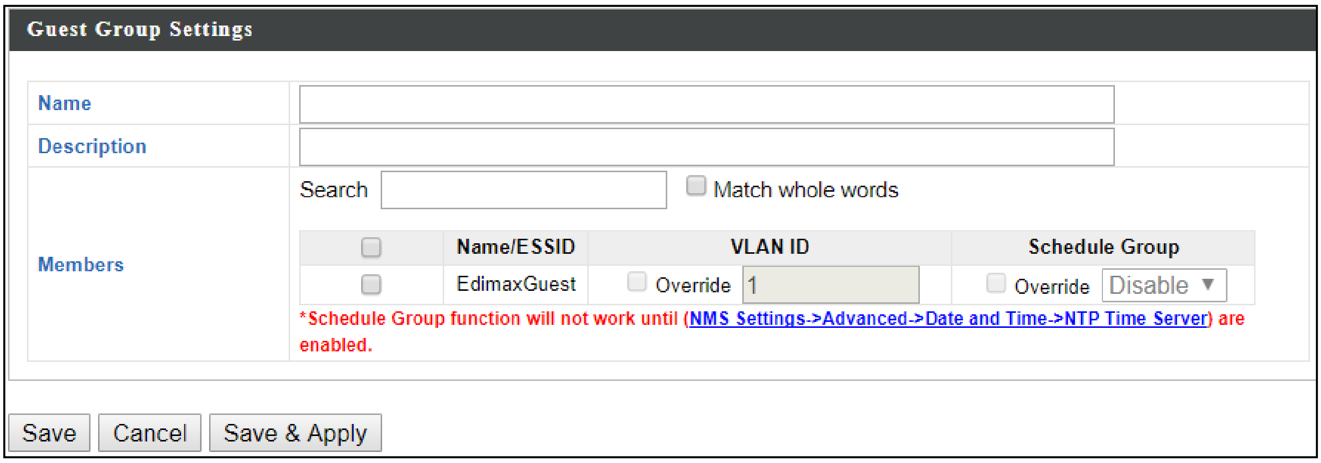
Guest Network Advanced Settings	
Schedule Group	Select a schedule group.

Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

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

X-5-5-2 Add/Edit Guest Network Group

When you add a Guest Network Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings** & access point group **Profile Group Settings** (**X-5-1**).



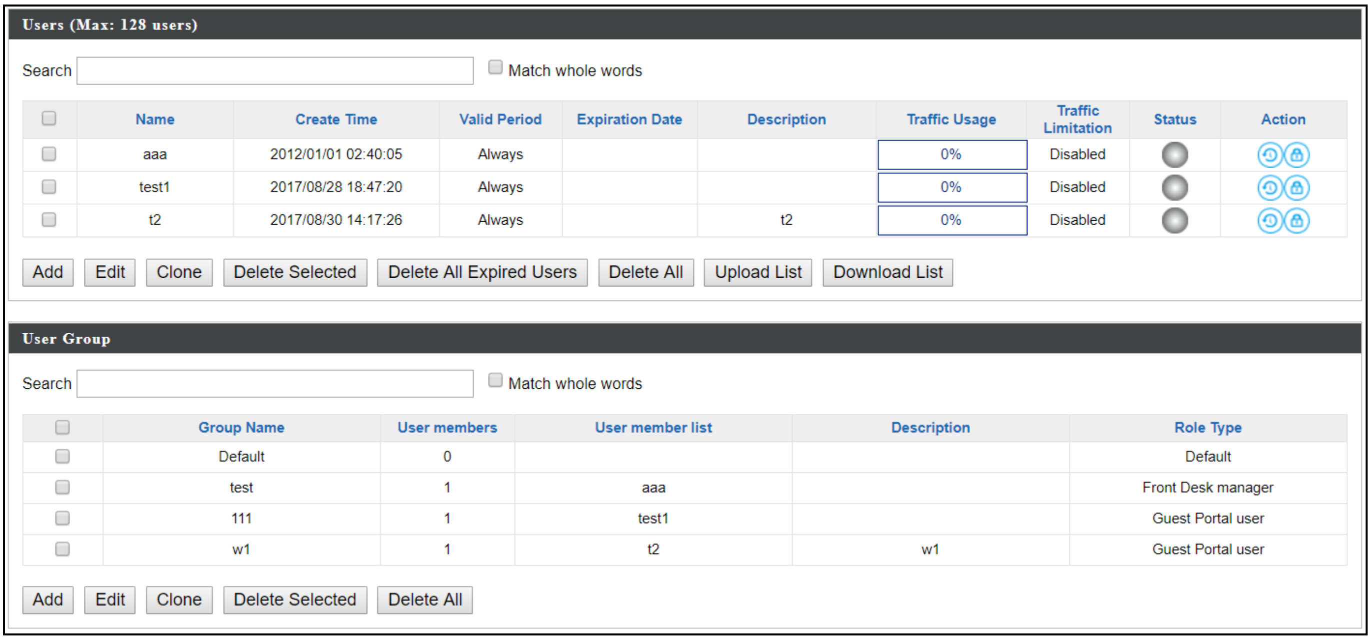
□	Name/ESSID	VLAN ID	Schedule Group
□	EdimaxGuest	□ Override 1	□ Override Disable ▼

*Schedule Group function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.

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

Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

X-5-6 Users



Users (Max: 128 users)

Search ☐ Match whole words

☐	Name	Create Time	Valid Period	Expiration Date	Description	Traffic Usage	Traffic Limitation	Status	Action
☐	aaa	2012/01/01 02:40:05	Always			0%	Disabled	●	
☐	test1	2017/08/28 18:47:20	Always			0%	Disabled	●	
☐	t2	2017/08/30 14:17:26	Always		t2	0%	Disabled	●	

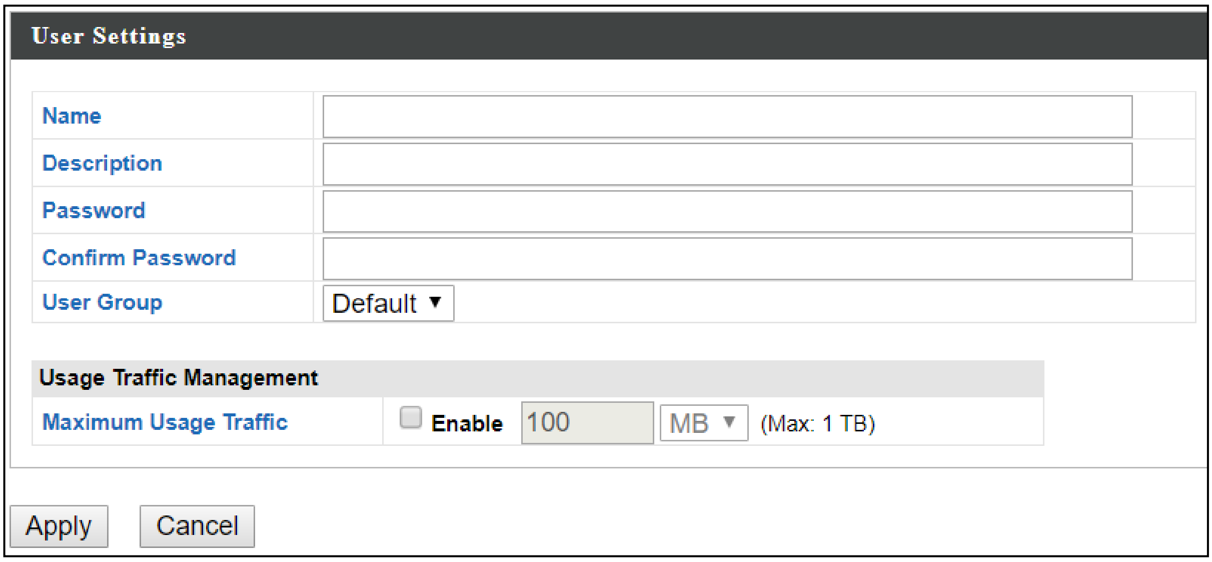
User Group

Search ☐ Match whole words

☐	Group Name	User members	User member list	Description	Role Type
☐	Default	0			Default
☐	test	1	aaa		Front Desk manager
☐	111	1	test1		Guest Portal user
☐	w1	1	t2	w1	Guest Portal user

User Panel

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



User Settings

Name	
Description	
Password	
Confirm Password	
User Group	Default ▼

Usage Traffic Management

Maximum Usage Traffic	☐ Enable 100 MB ▼ (Max: 1 TB)

Press "Save" to save the above actions, or "Cancel" to forfeit the changes. Check the checkbox of the user(s) you wish to delete and press "Delete Selected" to delete (multiple selections possible).

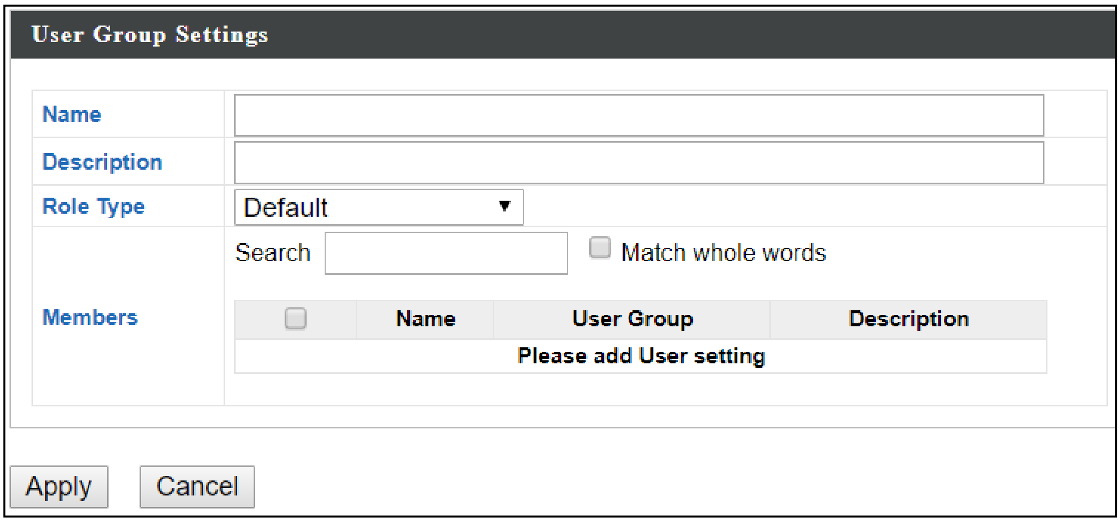
Press "Delete All Expired Users" to delete the expired users.

Press "Delete All" to delete all users.

Use “Upload List” to upload a user list.
Use “Download List” to download existing list for possible future reference.

User Group Panel

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



User Group Settings

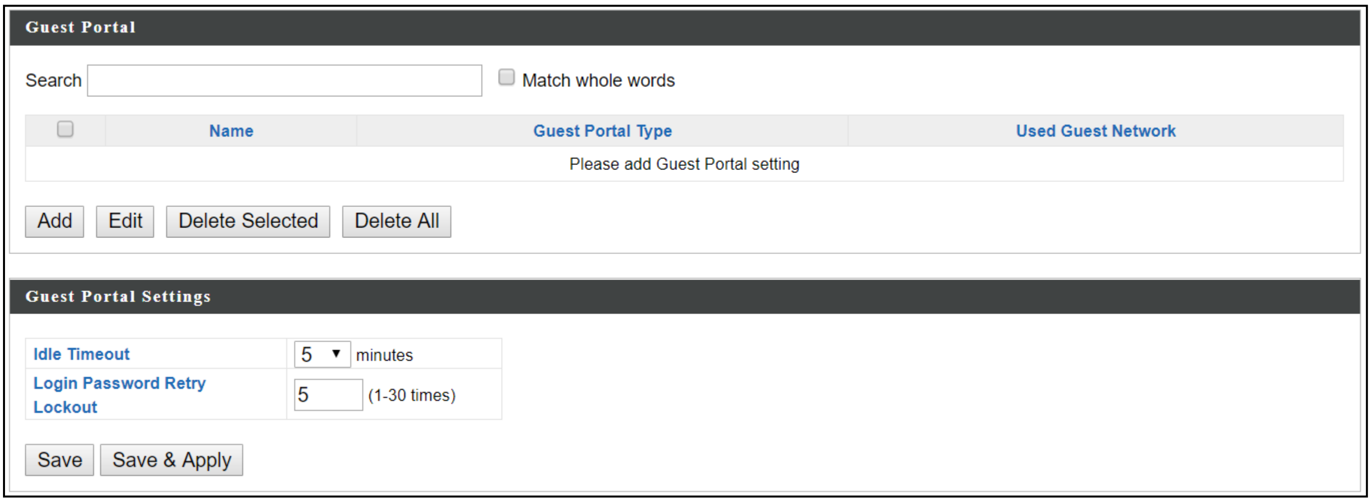
Name	
Description	
Role Type	Default ▾
Members	Search □ Match whole words

□	Name	User Group	Description
Please add User setting			

Press “Save” to save the above actions, or “Cancel” to forfeit the changes.
Check the checkbox of the user group(s) you wish to delete and press “Delete Selected” to delete (multiple selections possible).
Press “Delete All” to delete all user groups.

X-5-7 Guest Portal

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



Guest Portal

Search ________ □ Match whole words

□	Name	Guest Portal Type	Used Guest Network
Please add Guest Portal setting			

Guest Portal Settings

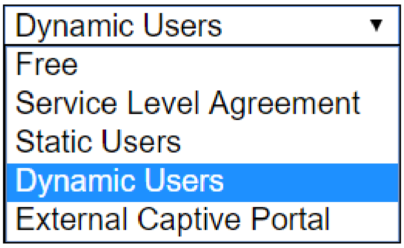
Idle Timeout	5 ▾ minutes
Login Password Retry Lockout	5 (1-30 times)

Check the checkbox of the portal(s) you wish to delete and press "Delete Selected" to delete (multiple selections possible).
Press "Delete All" to delete all portals.

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

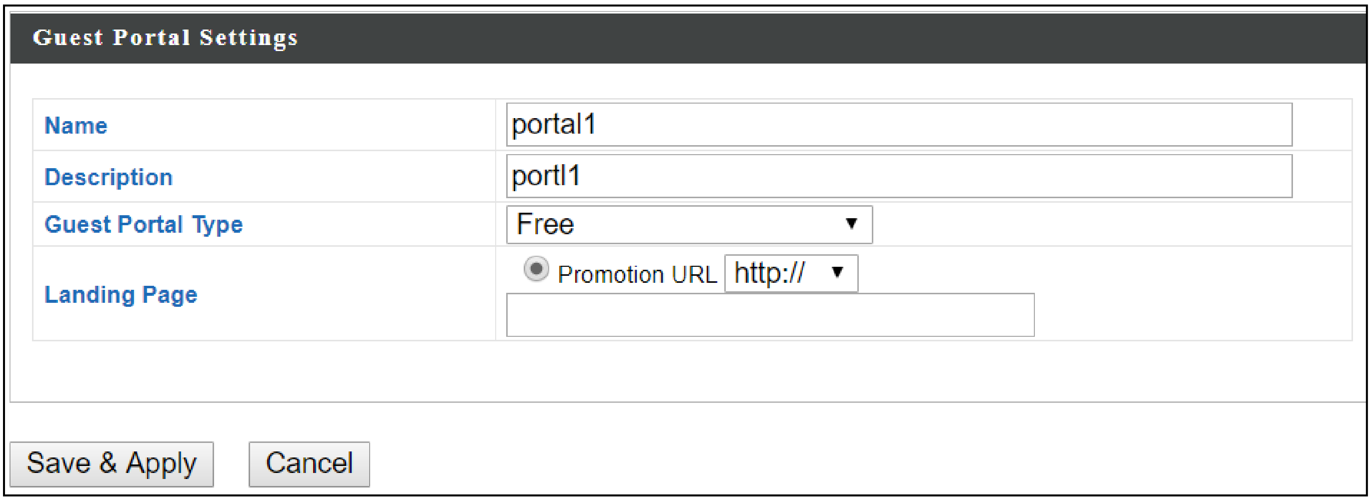
Add / Edit

Enter the fields according to the selected "Guest Portal Type" below:



Press "Save & Apply" to save the above actions, or "Cancel" to forfeit the changes.

X-5-7-1 Free Guest Portal Type

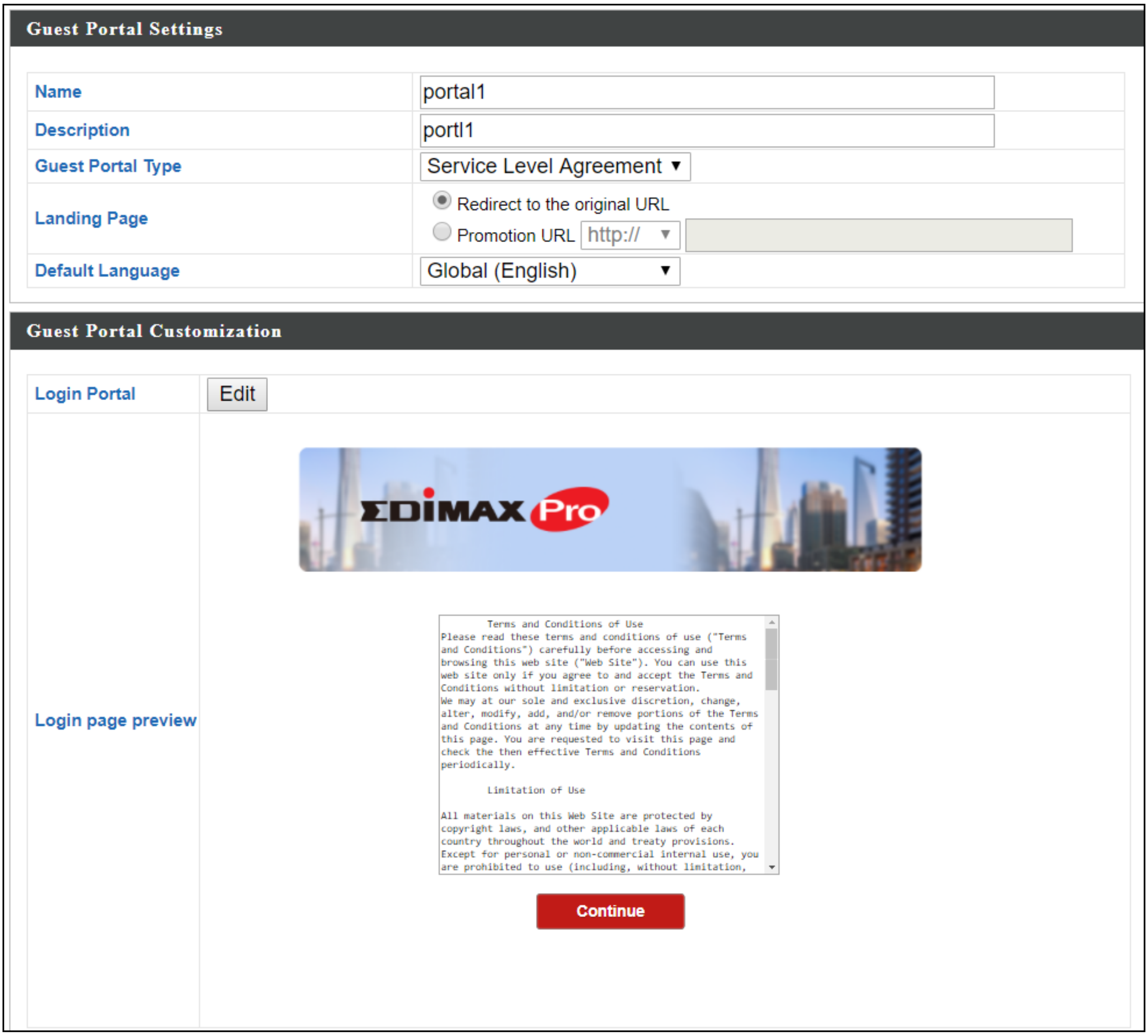


Guest Portal Settings

Name	portal1
Description	portl1
Guest Portal Type	Free ▼
Landing Page	● Promotion URL http:// ▼

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

X-5-7-2 User Level Agreement Guest Portal Type



Guest Portal Settings

Name	portal1
Description	portl1
Guest Portal Type	Service Level Agreement ▾
Landing Page	● Redirect to the original URL ○ Promotion URL http:// ▾
Default Language	Global (English) ▾

Guest Portal Customization

Login Portal: Edit

Login page preview

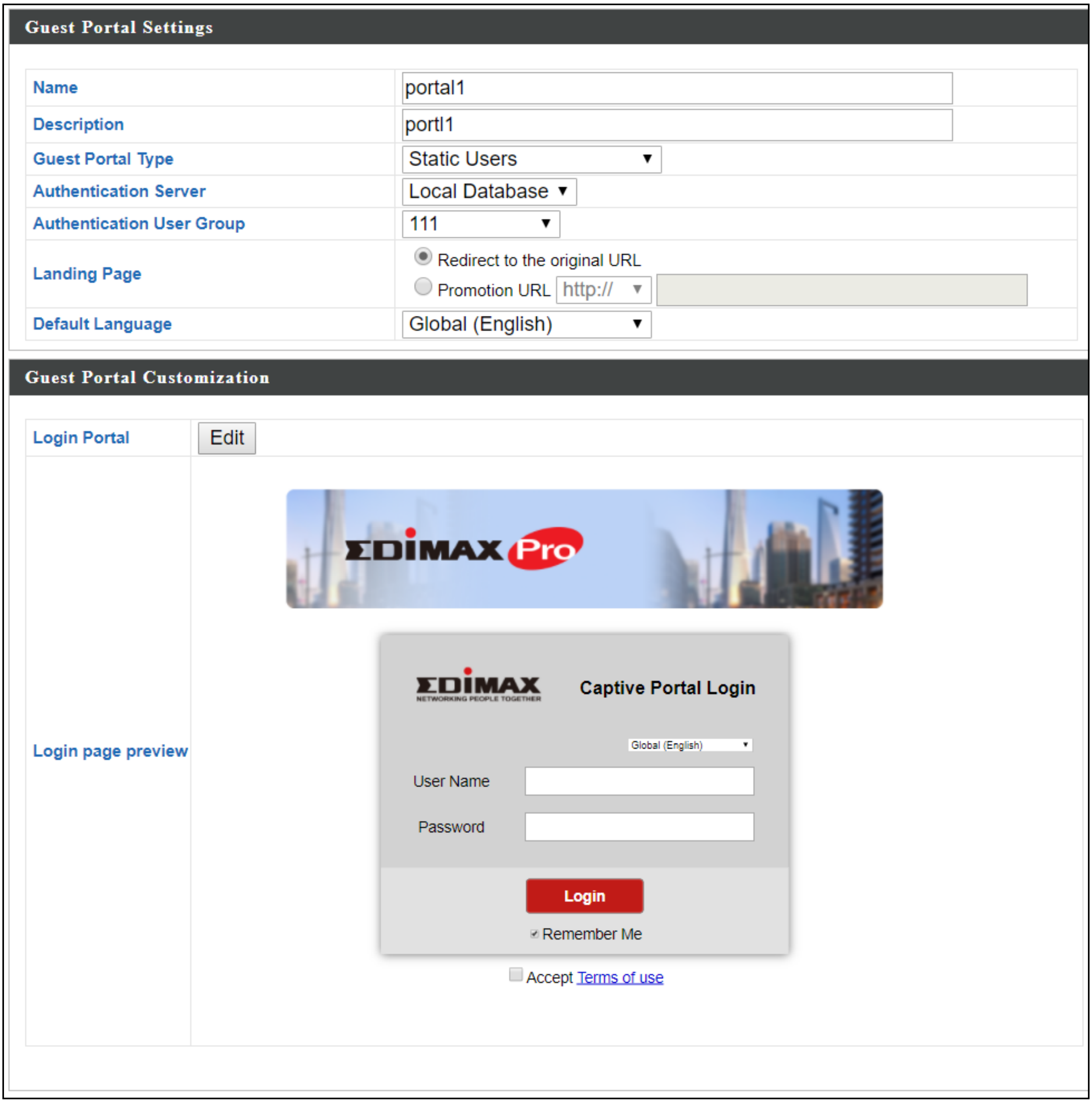
```
        Terms and Conditions of Use
Please read these terms and conditions of use ("Terms
and Conditions") carefully before accessing and
browsing this web site ("Web Site"). You can use this
web site only if you agree to and accept the Terms and
Conditions without limitation or reservation.
We may at our sole and exclusive discretion, change,
alter, modify, add, and/or remove portions of the Terms
and Conditions at any time by updating the contents of
this page. You are requested to visit this page and
check the then effective Terms and Conditions
periodically.

        Limitation of Use

All materials on this Web Site are protected by
copyright laws, and other applicable laws of each
country throughout the world and treaty provisions.
Except for personal or non-commercial internal use, you
are prohibited to use (including, without limitation,
```

Continue

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

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

X-5-7-3 Static Users Guest Portal Type



Guest Portal Settings

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

Guest Portal Customization

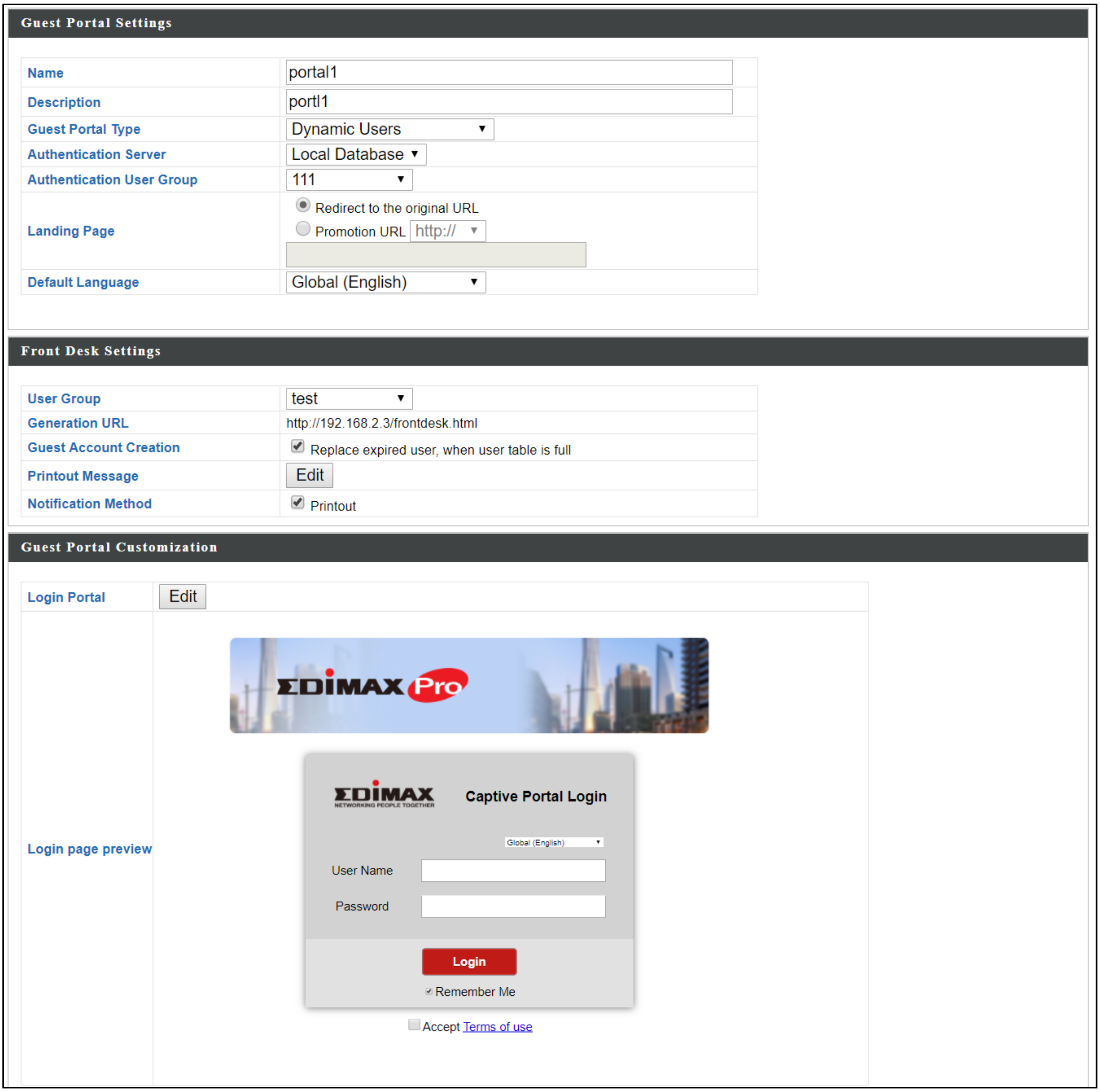
Login Portal	Edit
Login page preview	Captive Portal Login Global (English) ▼ User Name Password Login ☑ Remember Me □ Accept Terms of use

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Authentication Server	Select an authentication server.
Authentication User Group	Select an authentication user group.

Landing Page	Select between “Redirect to the original URL” or “Promotion URL” (enter the promotion URL).
Default Language	Choose a default language.

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

X-5-7-4 Dynamic Users Guest Portal Type



Guest Portal Settings

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

Front Desk Settings

User Group	test ▾
Generation URL	http://192.168.2.3/frontdesk.html
Guest Account Creation	☑ Replace expired user, when user table is full
Printout Message	Edit
Notification Method	☑ Printout

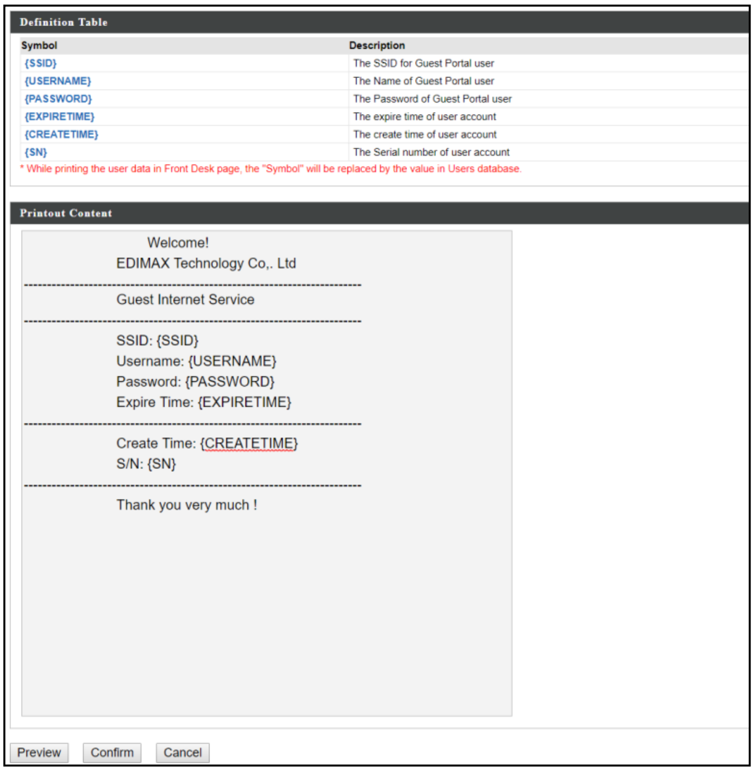
Guest Portal Customization

Login Portal: Edit

Login page preview

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

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



Definition Table

Symbol	Description
{SSID}	The SSID for Guest Portal user
{USERNAME}	The Name of Guest Portal user
{PASSWORD}	The Password of Guest Portal user
{EXPIRETIME}	The expire time of user account
{CREATETIME}	The create time of user account
{SN}	The Serial number of user account

* While printing the user data in Front Desk page, the "Symbol" will be replaced by the value in Users database.

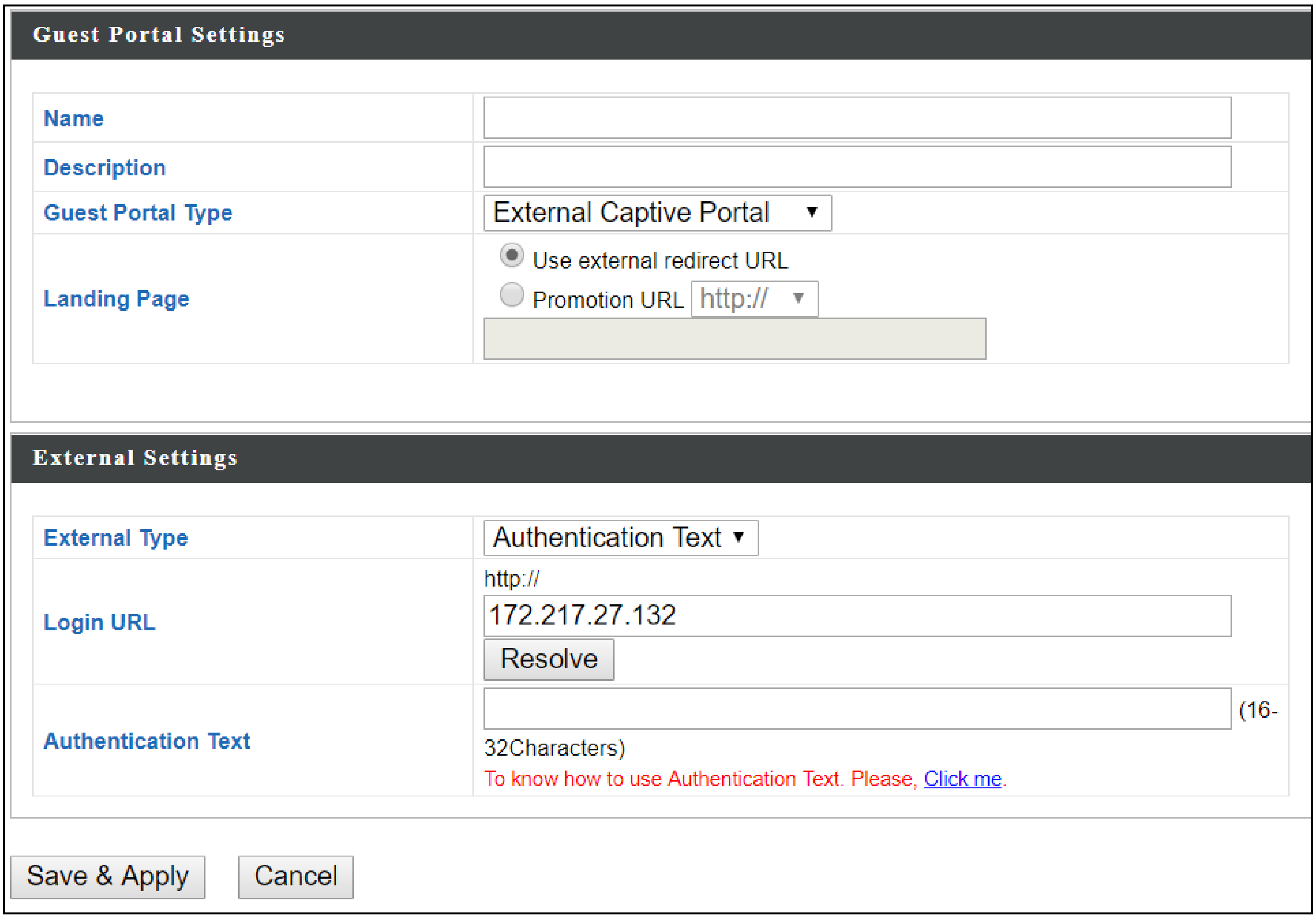
Printout Content

```
          Welcome!
      EDIMAX Technology Co,. Ltd
------------------------------------------------------------------------
      Guest Internet Service
------------------------------------------------------------------------
      SSID: {SSID}
      Username: {USERNAME}
      Password: {PASSWORD}
      Expire Time: {EXPIRETIME}
------------------------------------------------------------------------
      Create Time: {CREATETIME}
      S/N: {SN}
------------------------------------------------------------------------
      Thank you very much !
```

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

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

X-5-7-5 External Captive Portal Guest Portal Type



Guest Portal Settings

Name	
Description	
Guest Portal Type	External Captive Portal ▾
Landing Page	● Use external redirect URL ○ Promotion URL http:// ▾

External Settings

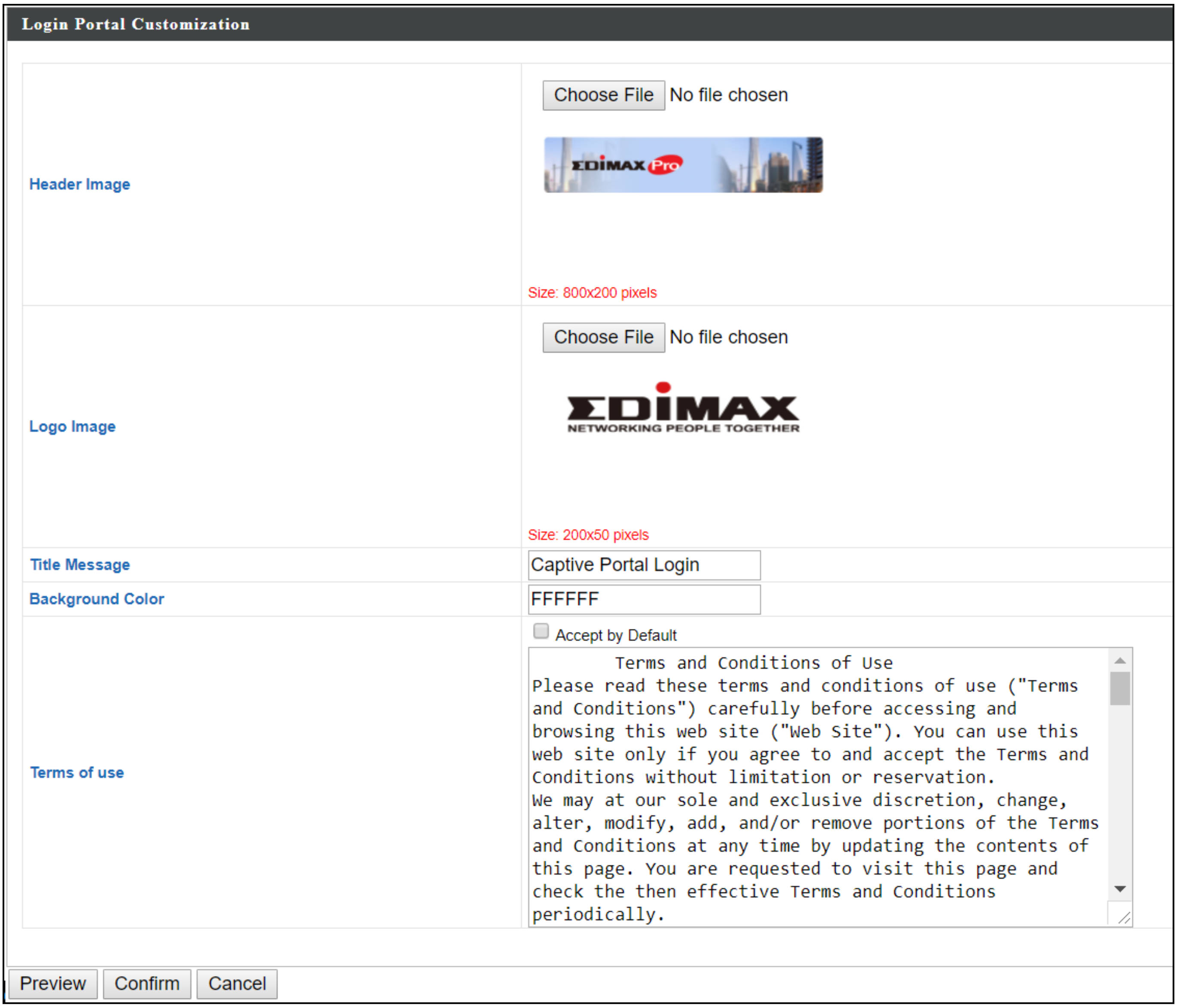
External Type	Authentication Text ▾
Login URL	http:// 172.217.27.132 Resolve
Authentication Text	(16-32Characters) To know how to use Authentication Text. Please, Click me.

Save & Apply   Cancel

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

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

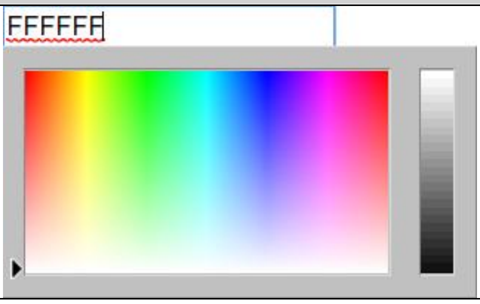
X-5-7-6 Editing “Login Portal”



Login Portal Customization

Header Image	Choose File No file chosen Size: 800x200 pixels
Logo Image	Choose File No file chosen Size: 200x50 pixels
Title Message	Captive Portal Login
Background Color	FFFFFF
Terms of use	□ Accept by Default Terms and Conditions of Use Please read these terms and conditions of use ("Terms and Conditions") carefully before accessing and browsing this web site ("Web Site"). You can use this web site only if you agree to and accept the Terms and Conditions without limitation or reservation. We may at our sole and exclusive discretion, change, alter, modify, add, and/or remove portions of the Terms and Conditions at any time by updating the contents of this page. You are requested to visit this page and check the then effective Terms and Conditions periodically.

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

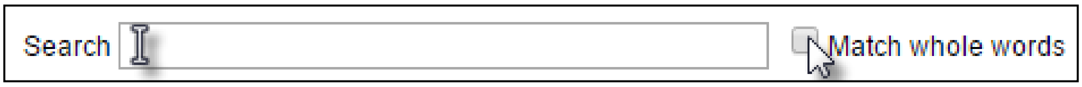
	 FFFFFF
Terms of use	Enter / edit the terms of use message

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

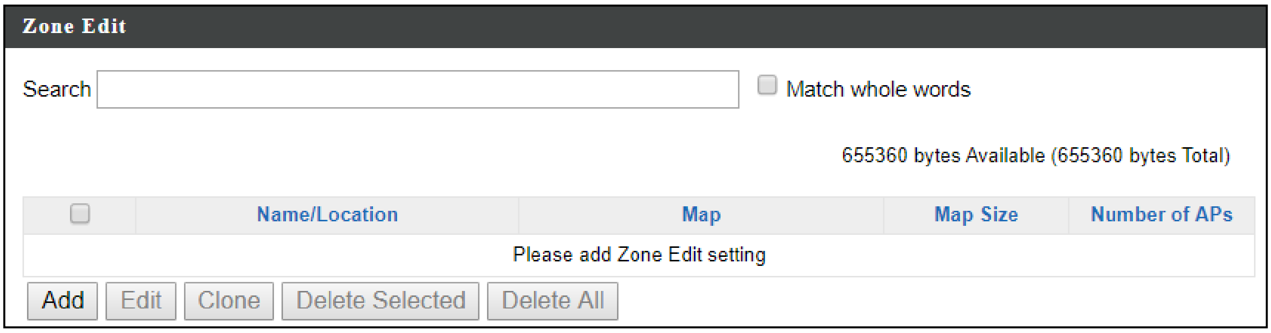
X-5-8 Zone Edit

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

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



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



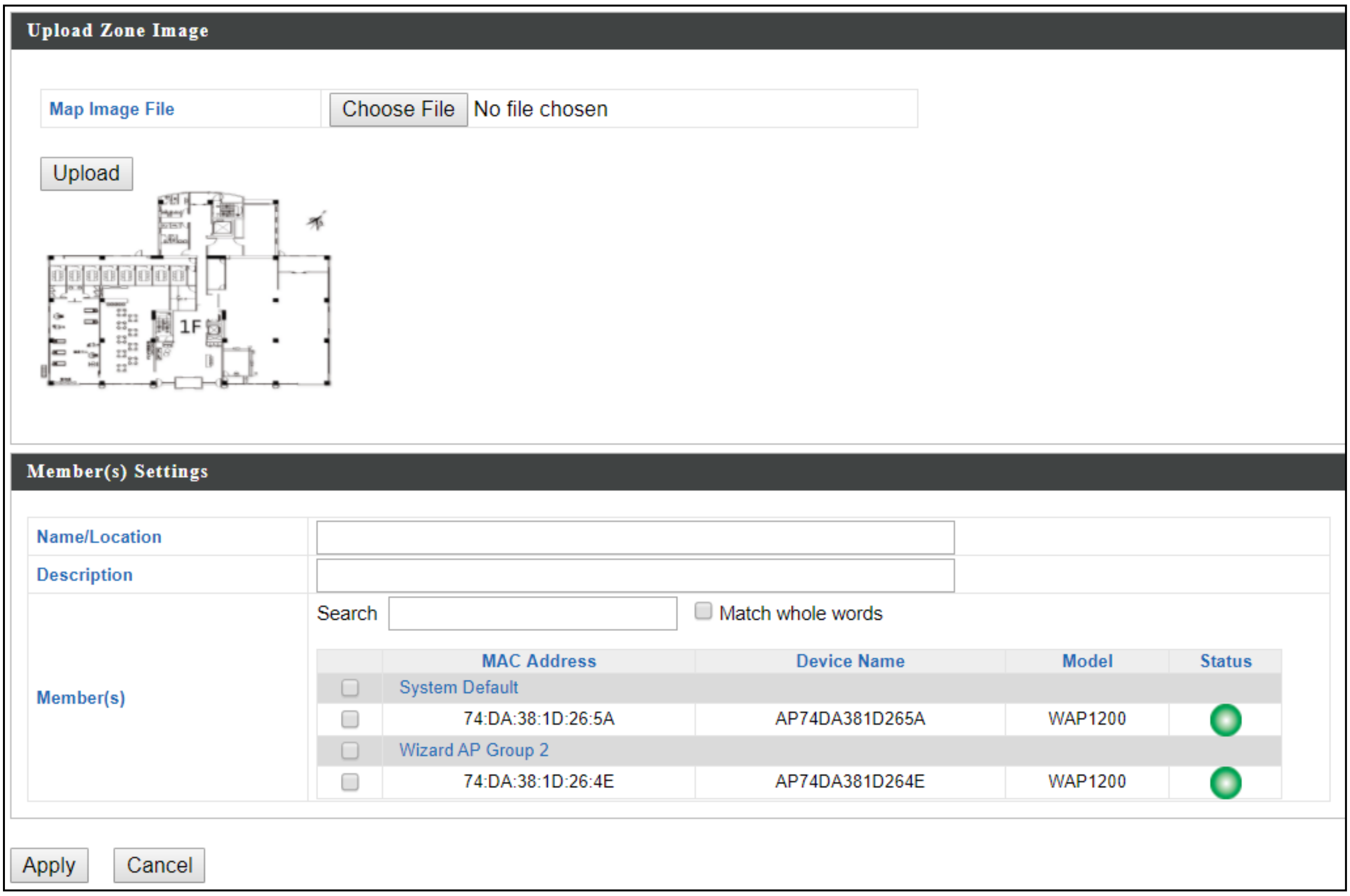
Zone Edit

Search □ Match whole words

655360 bytes Available (655360 bytes Total)

□	Name/Location	Map	Map Size	Number of APs
Please add Zone Edit setting				

Add/Edit Zone



Upload Zone Image

Map Image File	Choose File No file chosen

Upload

Member(s) Settings

Name/Location	
Description	
Member(s)	Search □ Match whole words

	MAC Address	Device Name	Model	Status
□	System Default			
□	74:DA:38:1D:26:5A	AP74DA381D265A	WAP1200	●
□	Wizard AP Group 2			
□	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	●

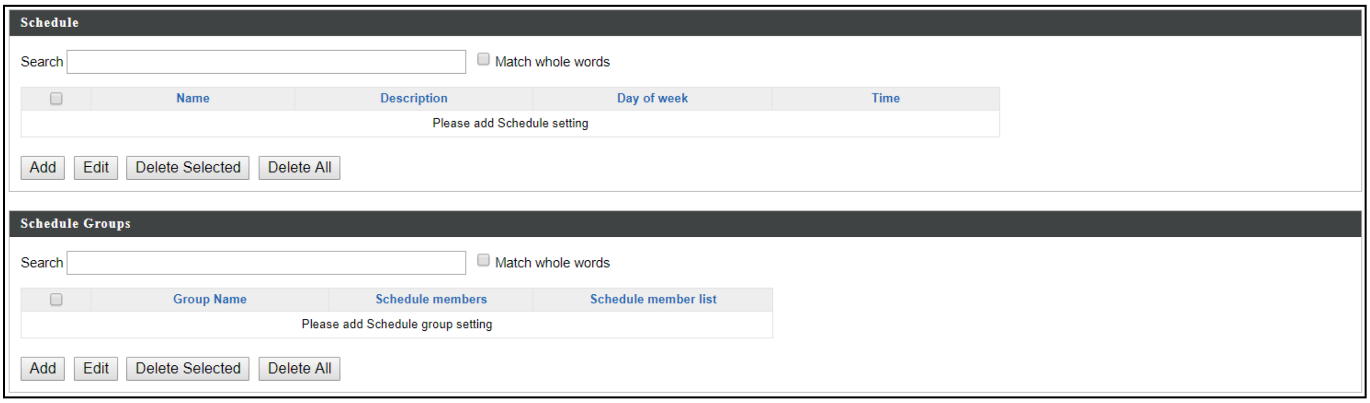
Apply Cancel

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

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

X-5-9 Schedule

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



Schedule

Search ________ □ Match whole words

□	Name	Description	Day of week	Time
Please add Schedule setting				

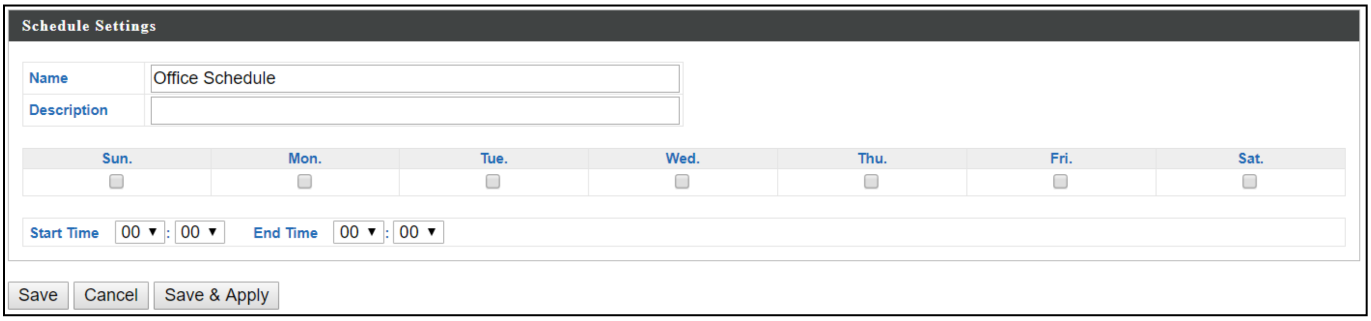
Schedule Groups

Search ________ □ Match whole words

□	Group Name	Schedule members	Schedule member list
Please add Schedule group setting			

Check the checkbox of the schedules(s) you wish to delete and press “Delete Selected” to delete (multiple selections possible).
Press “Delete All” to delete all schedules.

<u>Add / Edit</u>



Schedule Settings

Name	Office Schedule
Description	

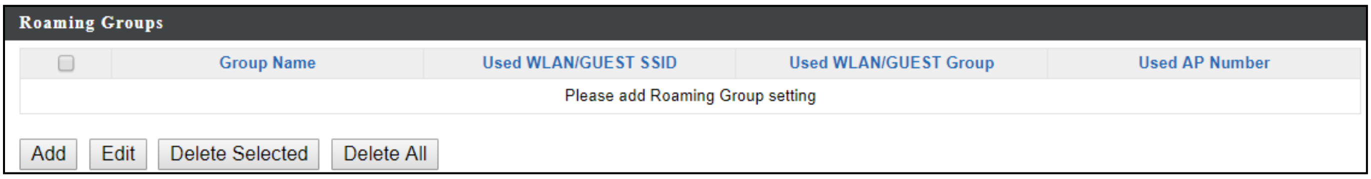
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
□	□	□	□	□	□	□

Start Time 00 : 00 End Time 00 : 00

Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

X-5-10 Smart Roaming

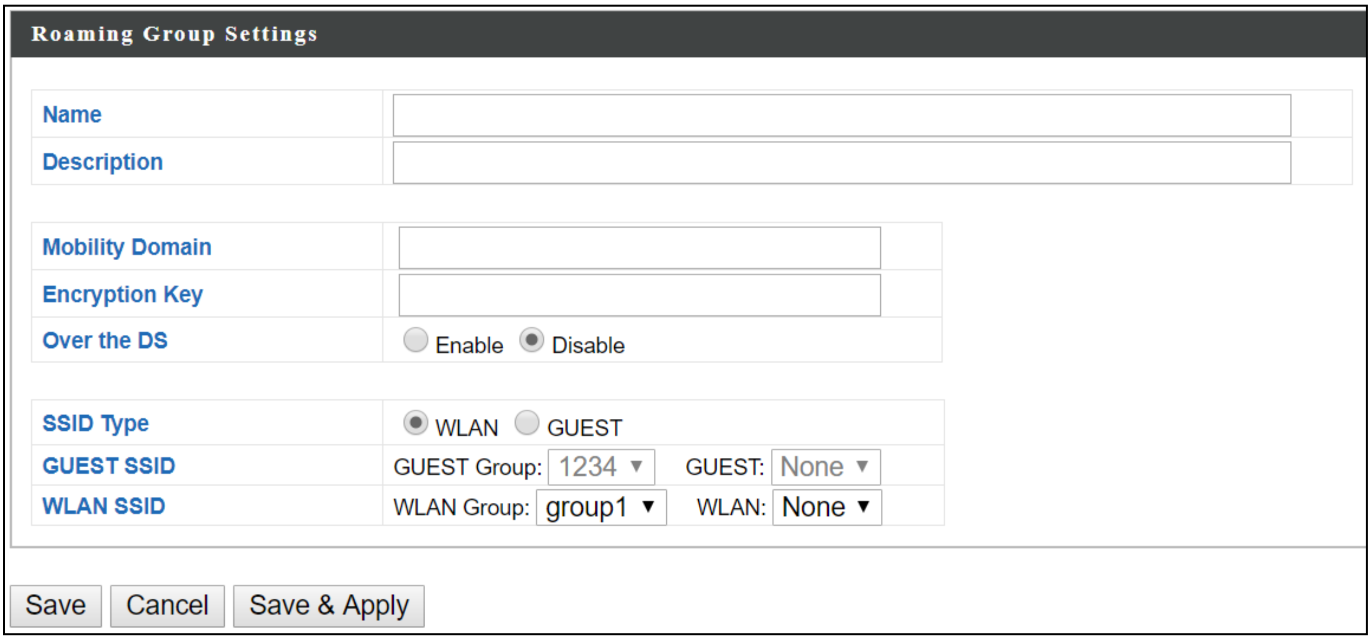
Smart roaming permits continuous connectivity on wireless devices that are moving. The handoffs from one station to another are fast and secure, and are managed seamlessly.



Roaming Groups

□	Group Name	Used WLAN/GUEST SSID	Used WLAN/GUEST Group	Used AP Number
Please add Roaming Group setting				

Add / Edit



Roaming Group Settings

Name	
Description	
Mobility Domain	
Encryption Key	
Over the DS	○ Enable ● Disable
SSID Type	● WLAN ○ GUEST
GUEST SSID	GUEST Group: 1234 ▼ GUEST: None ▼
WLAN SSID	WLAN Group: group1 ▼ WLAN: None ▼

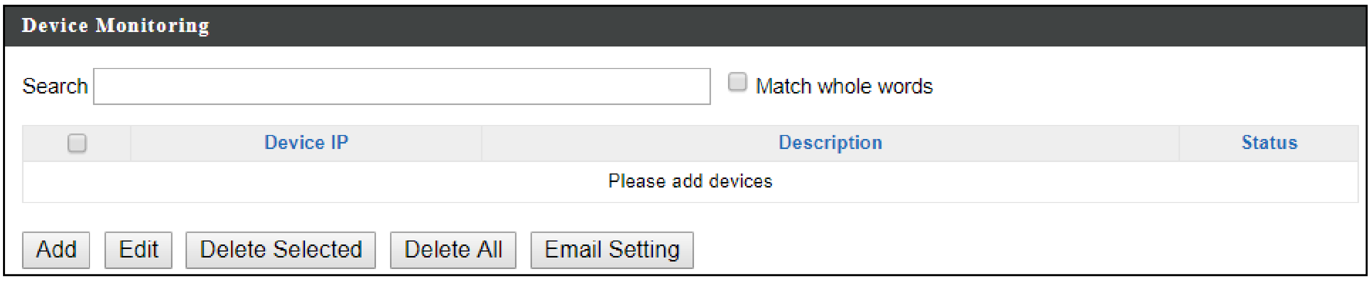
Roaming Group Settings	
Name	Enter / edit the name of roaming group.
Description	Enter / edit a description for reference.
Mobility Domain	Enter / edit a mobility domain.
Encryption Key	Enter / edit an encryption key.
Over the DS	Check to enable / disable this function.
SSID Type	Select the SSID type.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

	WLAN from the drop down menu.

Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

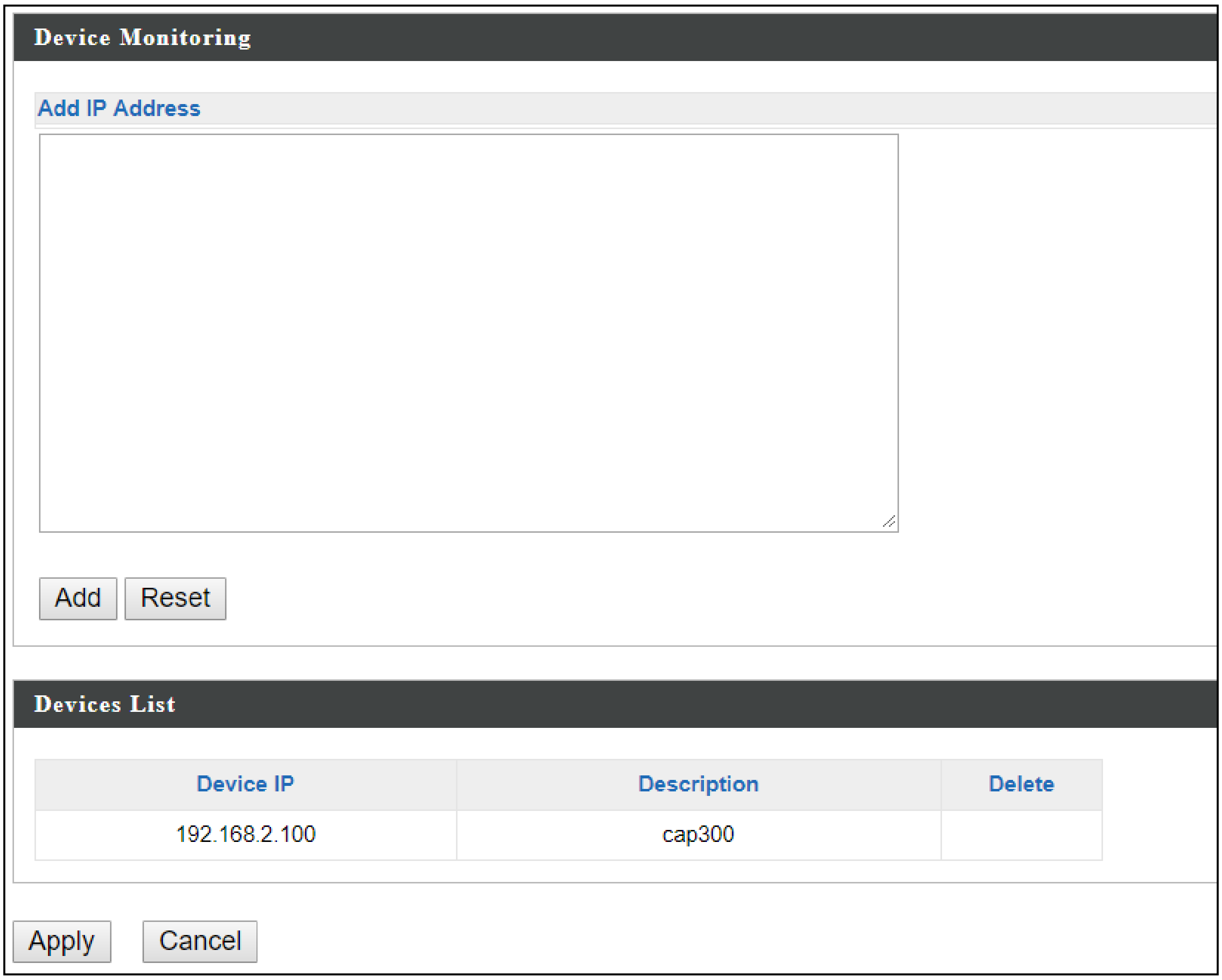
X-5-11 Device Monitoring

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



□	Device IP	Description	Status
Please add devices			

Add / Edit



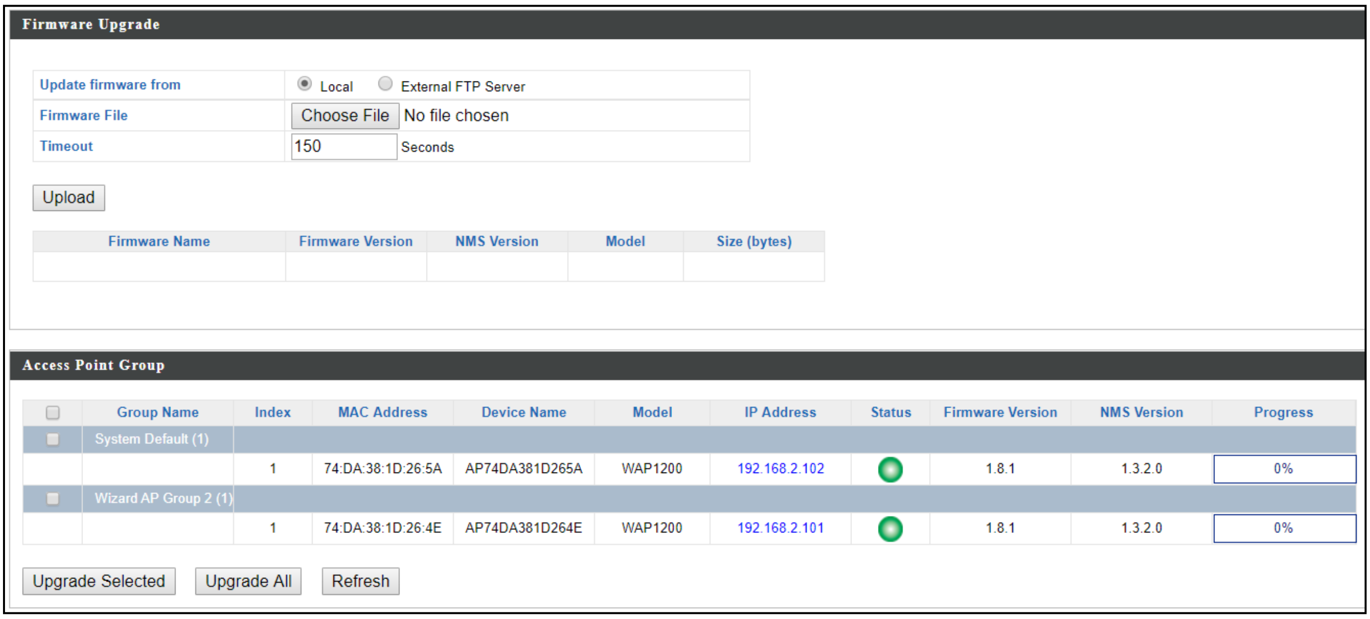
Device IP	Description	Delete
192.168.2.100	cap300	

Enter an IP Address(es) and click "Add" to add the device(s). Click "Reset" to clear the field.
Press "Apply" to apply the above action or "Cancel" to forfeit the addition.

X-5-12 Firmware Upgrade

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

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



Firmware Upgrade

Update firmware from	● Local ○ External FTP Server
Firmware File	Choose File No file chosen
Timeout	150 Seconds

Upload

Firmware Name	Firmware Version	NMS Version	Model	Size (bytes)

Access Point Group

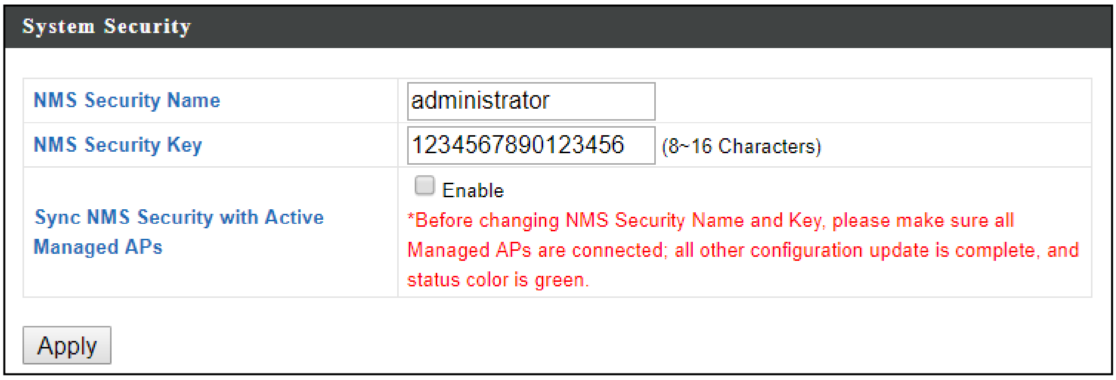
□	Group Name	Index	MAC Address	Device Name	Model	IP Address	Status	Firmware Version	NMS Version	Progress
□	System Default (1)									
		1	74:DA:38:1D:26:5A	AP74DA381D265A	WAP1200	192.168.2.102	●	1.8.1	1.3.2.0	0%
□	Wizard AP Group 2 (1)									
		1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	●	1.8.1	1.3.2.0	0%

Upgrade Selected Upgrade All Refresh

X-5-13 Advanced

X-5-13-1 System Security

Configure the NMS system login name and password.



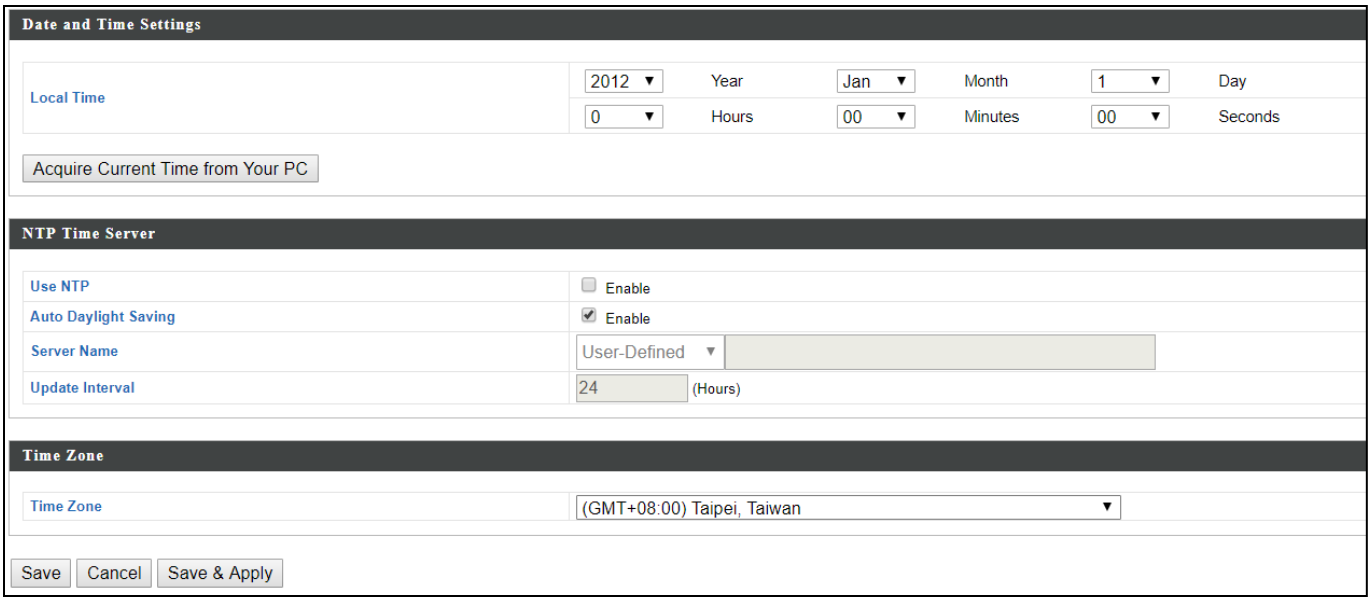
System Security

NMS Security Name	administrator
NMS Security Key	1234567890123456 (8~16 Characters)
Sync NMS Security with Active Managed APs	□ Enable *Before changing NMS Security Name and Key, please make sure all Managed APs are connected; all other configuration update is complete, and status color is green.

Press “Apply” to apply the settings.

X-5-13-2 Date & Time

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



Date and Time Settings

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

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

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

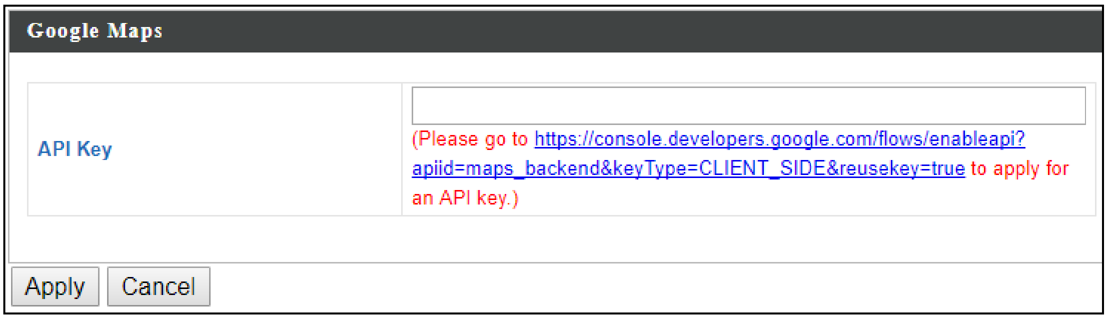
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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

Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

X-5-13-3 Google Maps

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

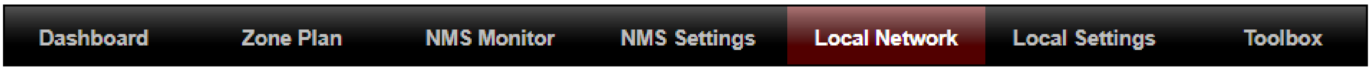


API Key

(Please go to https://console.developers.google.com/flows/enableapi?apiid=maps_backend&keyType=CLIENT_SIDE&reusekey=true to apply for an API key.)

Press "Apply" to apply the setting or "Cancel" to forfeit the change.

X-6 Local Network



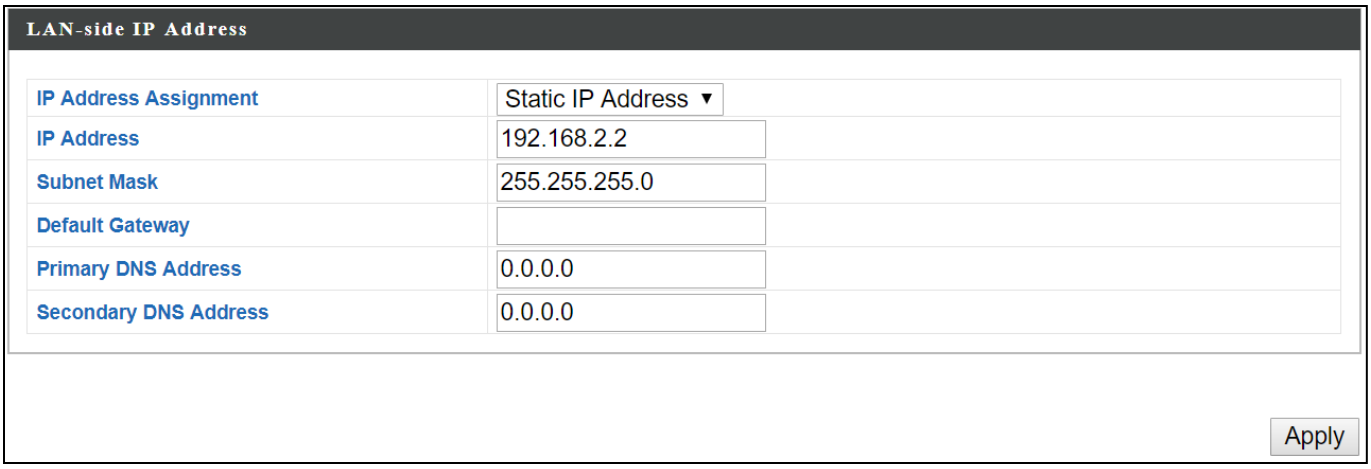
X-6-1 Network Settings

X-6-1-1 LAN-Side IP Address

The “LAN-side IP address” page allows you to configure your AP Controller on your Local Area Network (LAN). You can enable the 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. You can also set your AP Controller as a DHCP server to assign IP addresses to other devices on your LAN.

The access point’s default IP address is 192.168.2.2

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



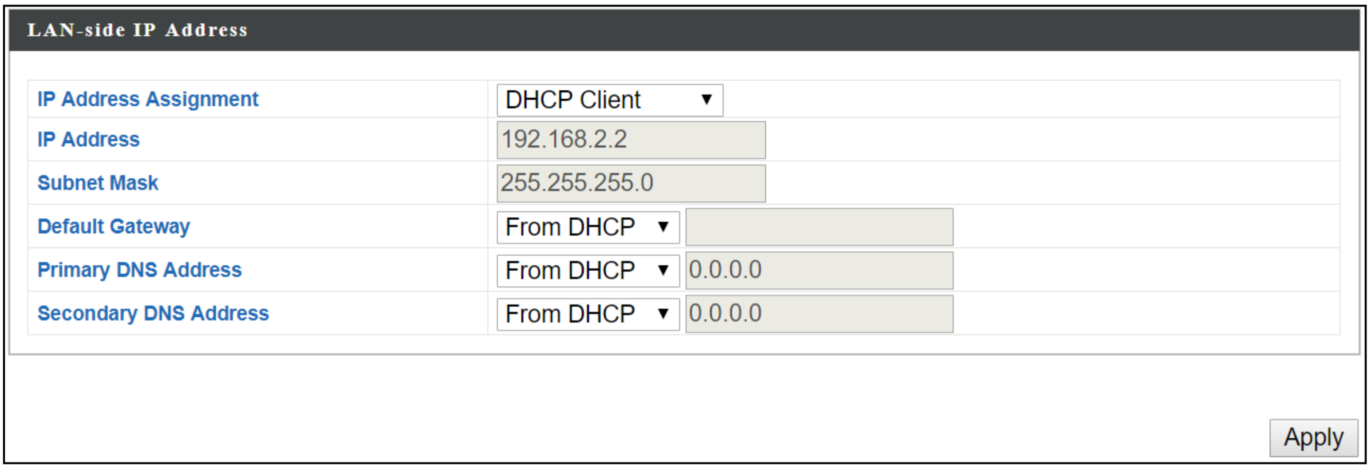
LAN-side IP Address

IP Address Assignment	Static IP Address ▼
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0

LAN-side IP Address	
IP Address Assignment	Select “Static IP” to manually specify a static/fixed IP address for your access point. Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server, or select “DHCP Server” for your access point to

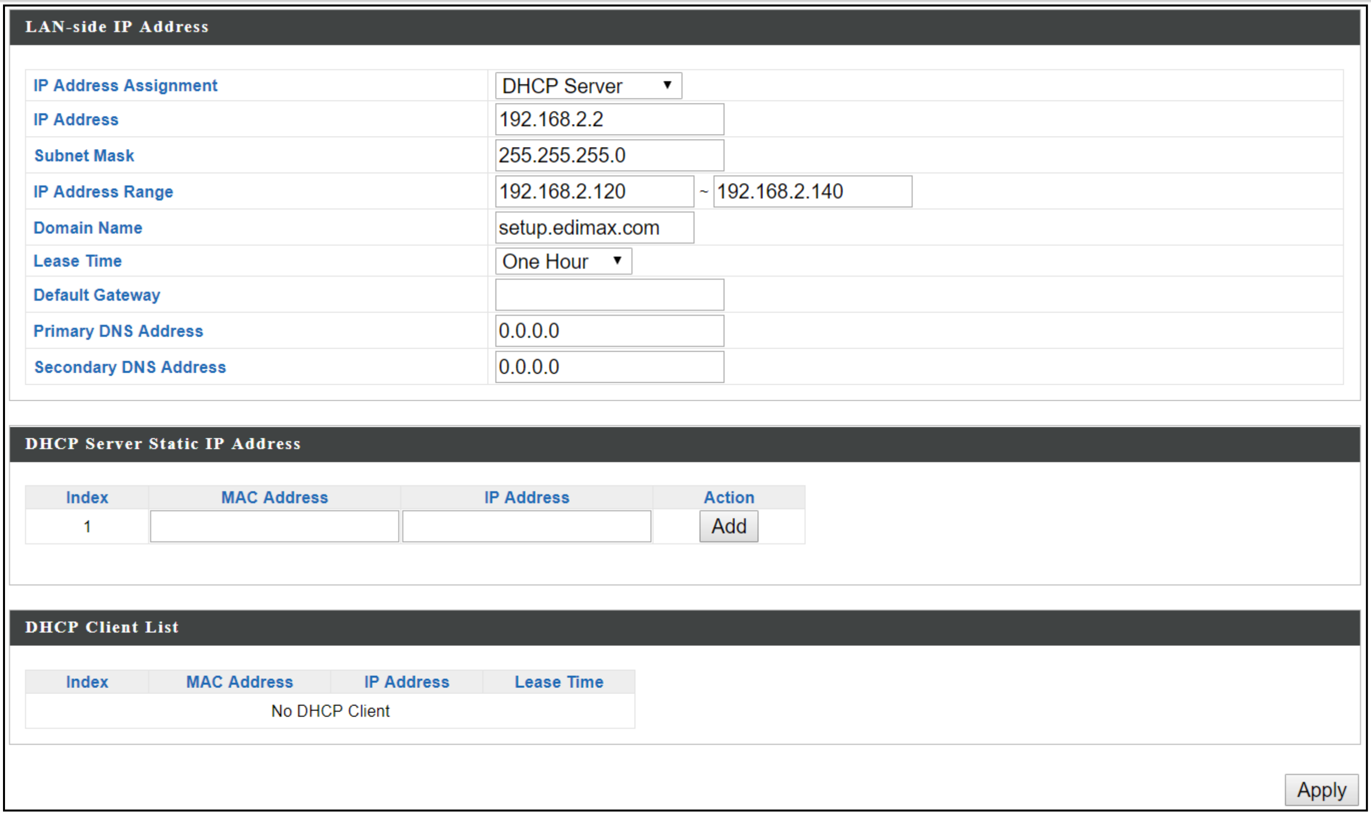
	act as a DHCP server and assign IP addresses on your LAN.

Static IP Address	
IP Address	Specify the IP address here. This IP address will be assigned to your 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.
Primary DNS Address	For static IP users, the default value is blank.
Secondary DNS Address	For static IP users, the default value is blank.


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

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



LAN-side IP Address

IP Address Assignment	DHCP Server ▼
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
IP Address Range	192.168.2.120 ~ 192.168.2.140
Domain Name	setup.edimax.com
Lease Time	One Hour ▼
Default Gateway	
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0

DHCP Server Static IP Address

Index	MAC Address	IP Address	Action
1			Add

DHCP Client List

Index	MAC Address	IP Address	Lease Time
No DHCP Client			

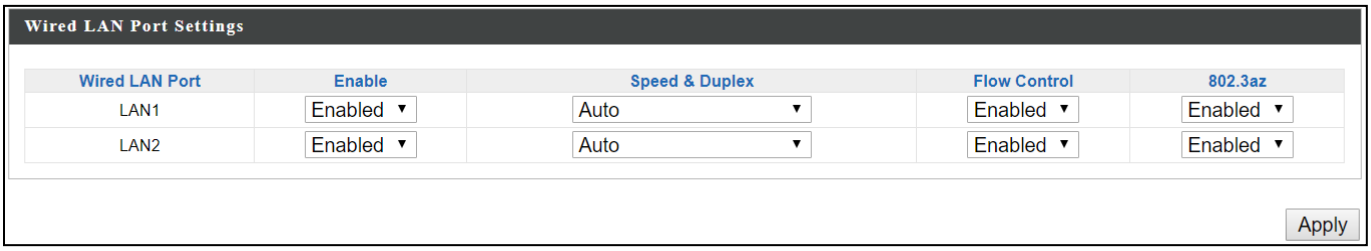
DHCP Server	
IP Address	Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
IP Address Range	Enter the start and end IP address of the IP address range which your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

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

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

X-6-1-2 LAN Port Settings

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



Wired LAN Port Settings

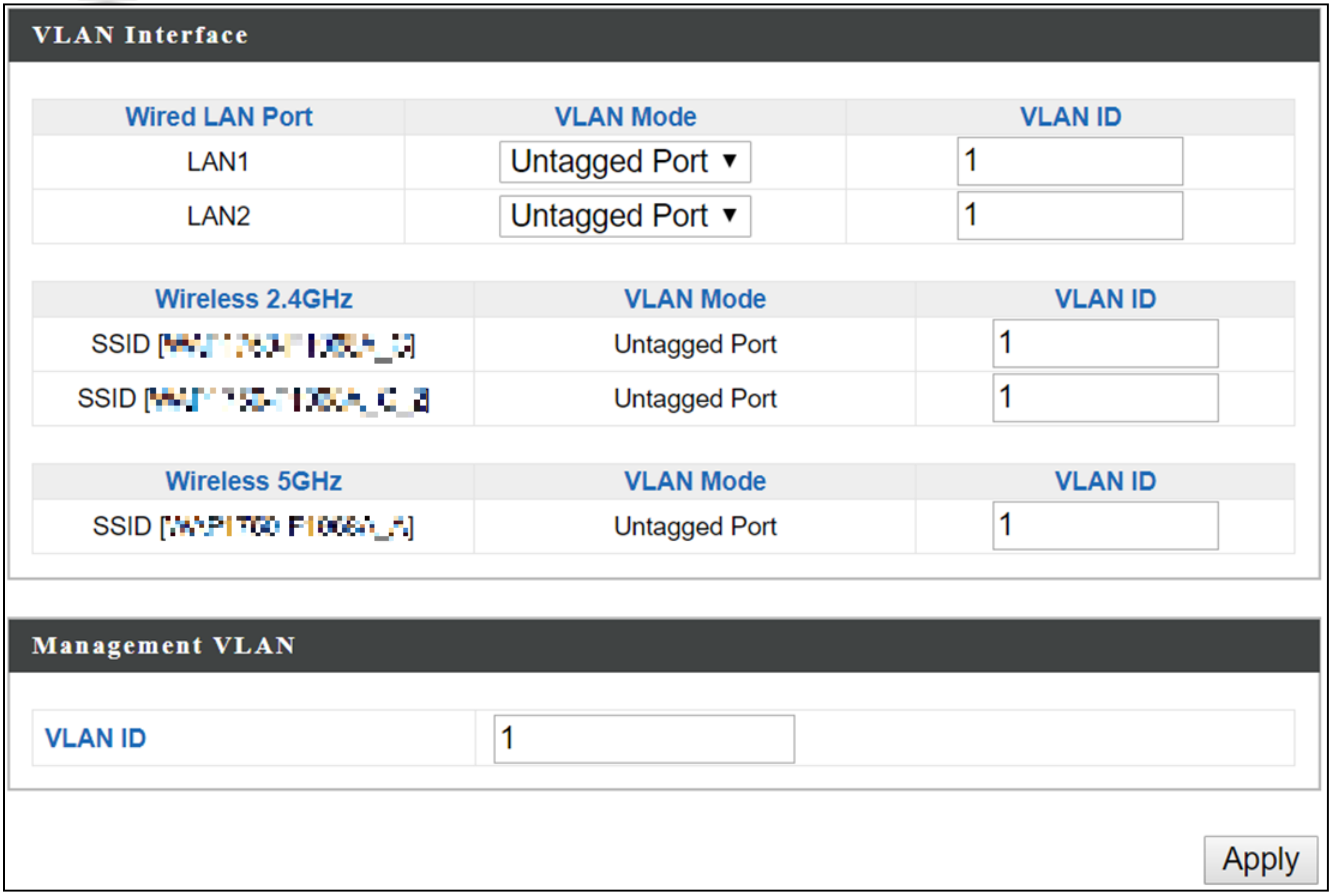
Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
LAN1	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼
LAN2	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼

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.
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.

X-6-1-3 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.

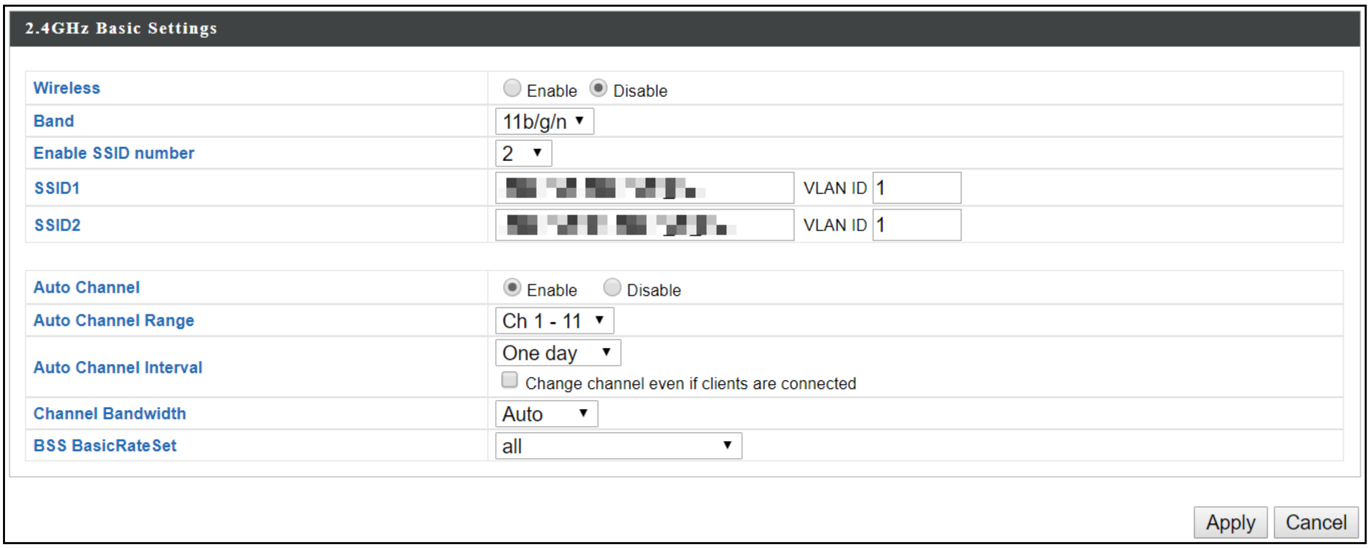
Press "Apply" to confirm the settings.

X-6-2 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.

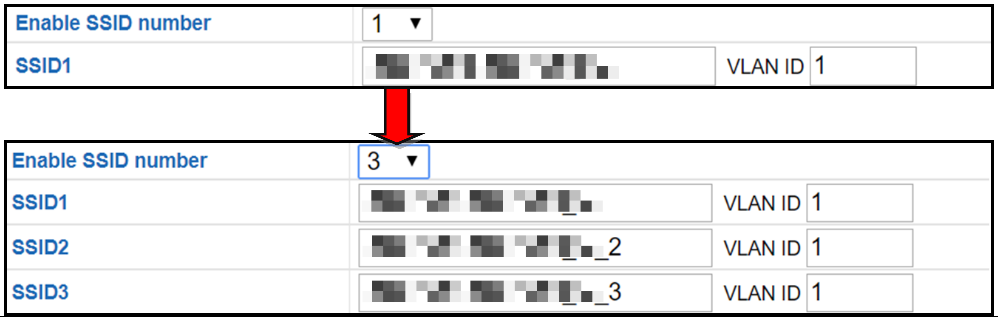
X-6-2-1 Basic

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



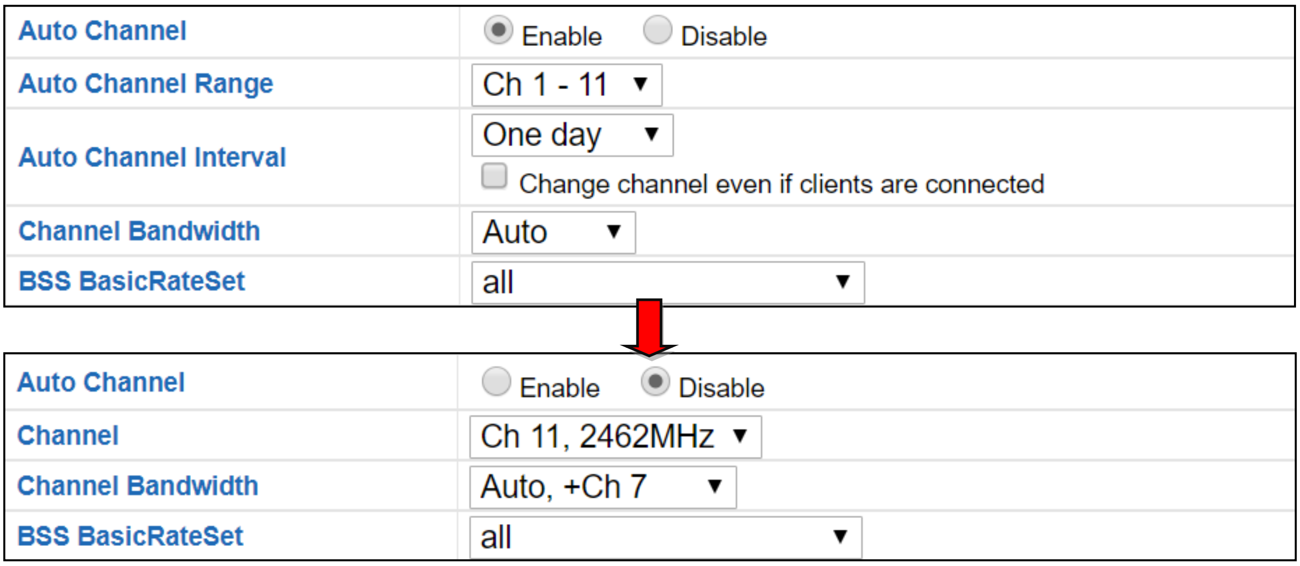
2.4GHz Basic Settings

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).

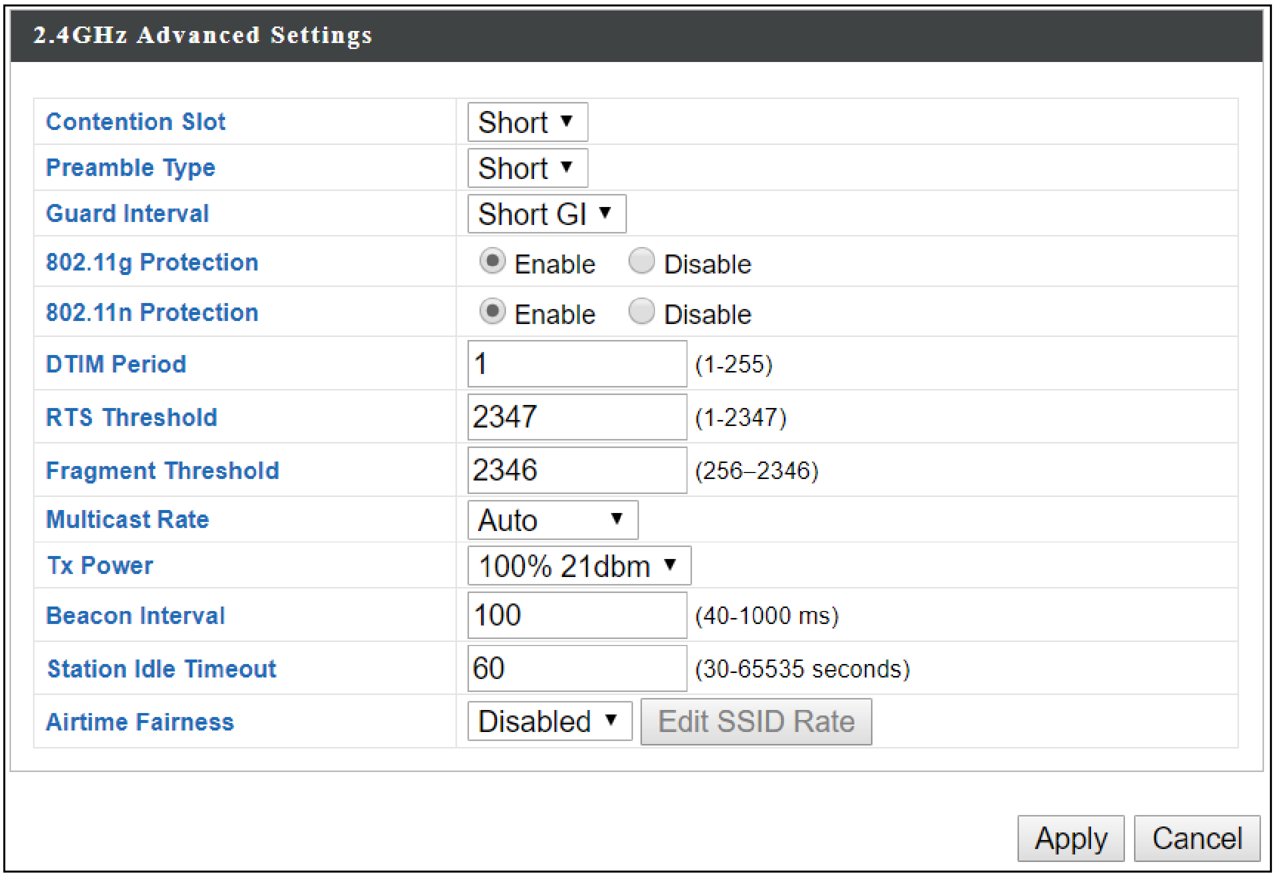
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

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

X-6-2-2 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.

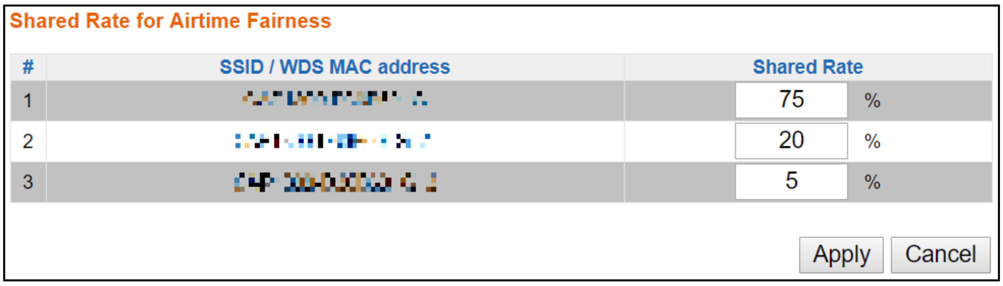
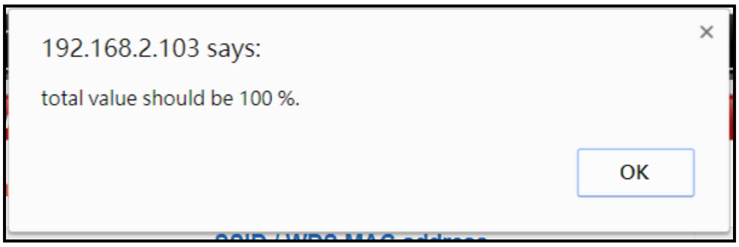


2.4GHz Advanced Settings

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 ***X-6-7 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.

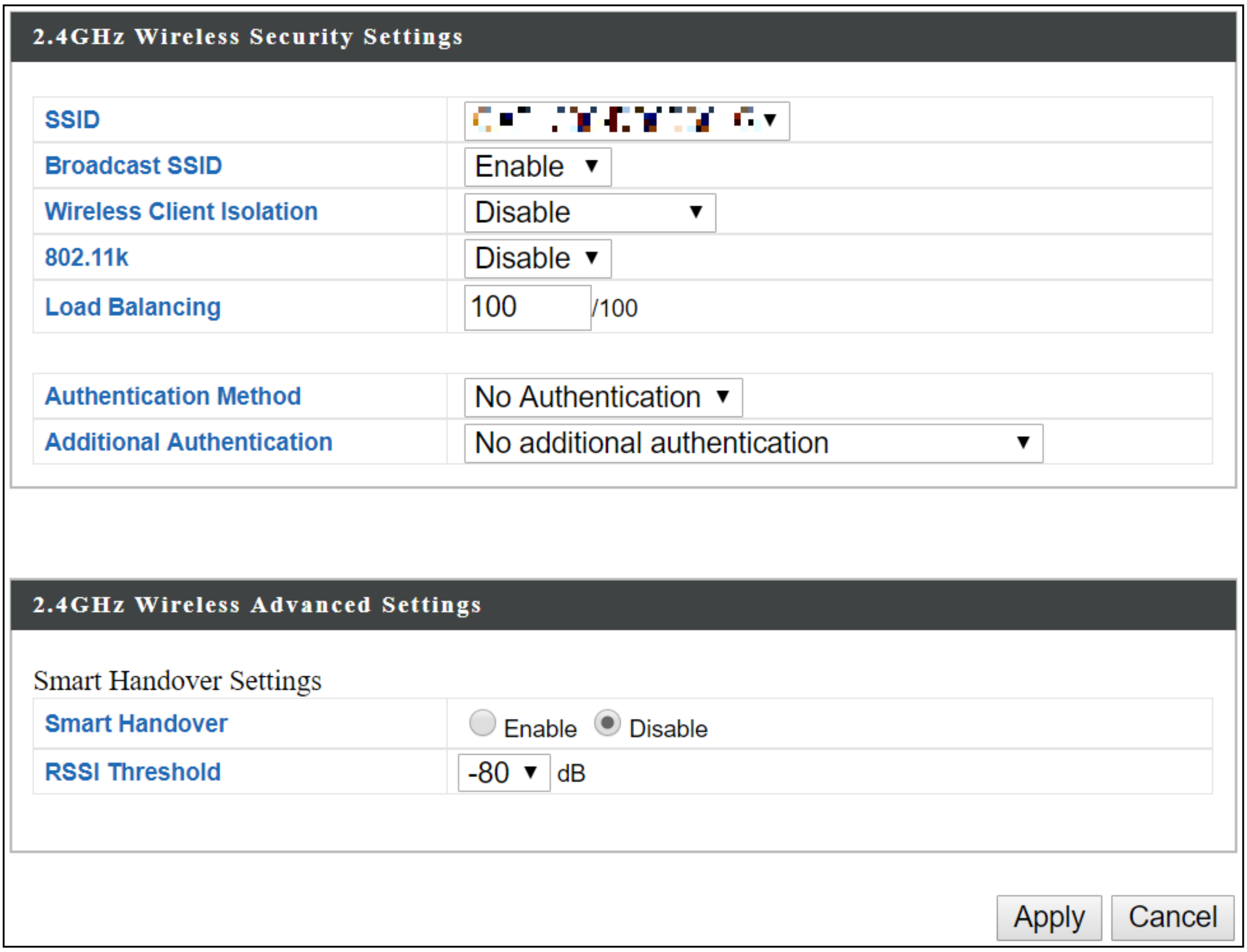
Airtime Fairness	Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate. Set airtime fairness to “Auto”, “Static” or “Disable”. When “Auto” is selected, the share rate is automatically managed. When “Static” is selected, press “Edit SSID Rate” to enter a % for each SSID’s share rate as shown below:  Shared Rate for Airtime Fairness # | SSID / WDS MAC address | Shared Rate 1 | [redacted] | 75 % 2 | [redacted] | 20 % 3 | [redacted] | 5 % The % field has to add up to 100% or the system will display a message:  192.168.2.103 says: 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.

X-6-2-3 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 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.

X-6-2-3-1 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** X-6-4 WPS **for WPS settings.

MAC Address Filter

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

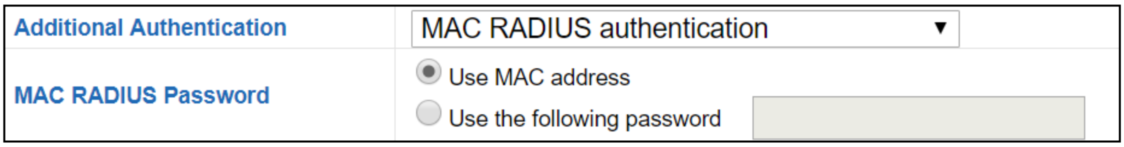
See** X-6-6 MAC Filter **to configure MAC filtering.

MAC-RADIUS Authentication

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

See** X-6-5 RADIUS **to configure RADIUS servers.

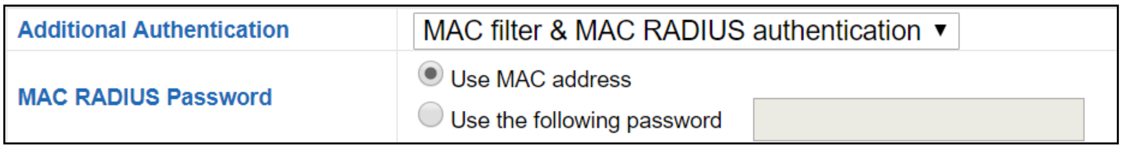
WPS must be disabled to use MAC-RADIUS authentication. See** X-6-4 WPS **for WPS settings.



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.

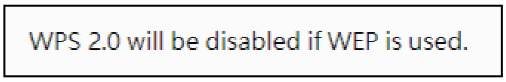


Additional Authentication	MAC filter & MAC RADIUS authentication ▼
MAC RADIUS Password	● Use MAC address ○ Use the following password

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 **X-6-5 RADIUS.**

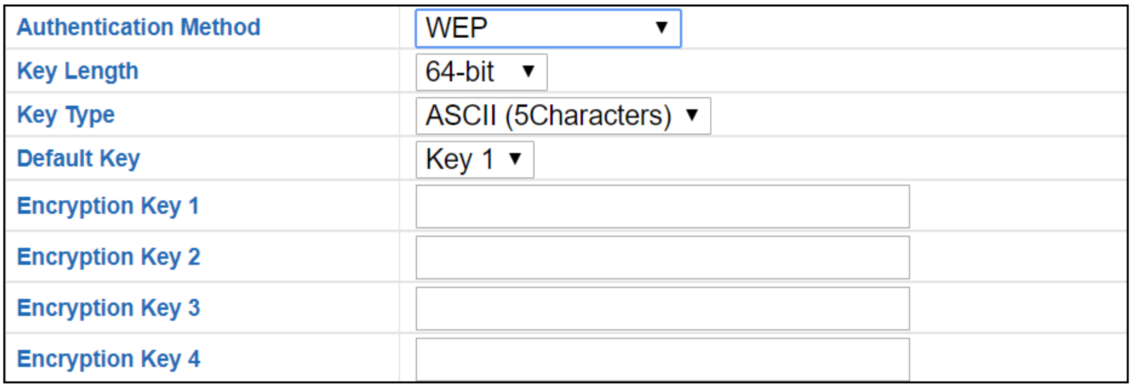
X-6-2-3-2 WEP

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:



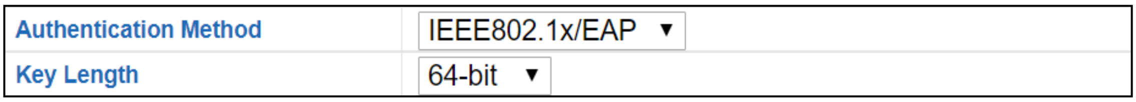
Authentication Method	WEP ▼
Key Length	64-bit ▼
Key Type	ASCII (5Characters) ▼
Default Key	Key 1 ▼
Encryption Key 1	
Encryption Key 2	
Encryption Key 3	
Encryption Key 4	

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.

X-6-2-3-3 IEEE802.1x/EAP

Below is a figure showing the configurable fields:



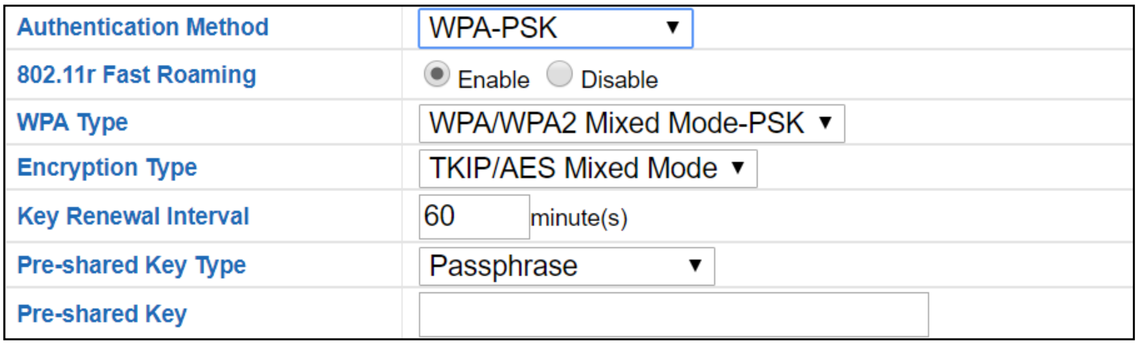
Authentication Method	IEEE802.1x/EAP ▼
Key Length	64-bit ▼

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

X-6-2-3-4 WPA-PSK

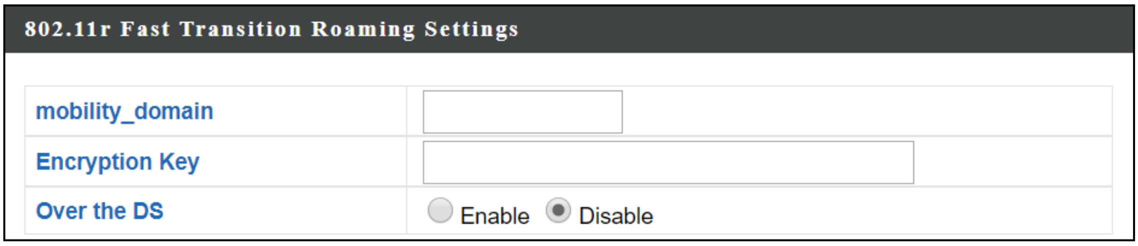
WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

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

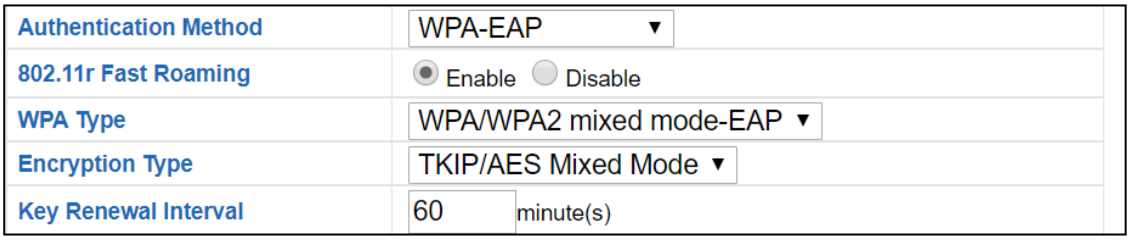
mobility_domain	
Encryption Key	
Over the DS	○ Enable ● Disable

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	Choose from “Passphrase” (8 – 63 alphanumeric characters)

Key Type	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.

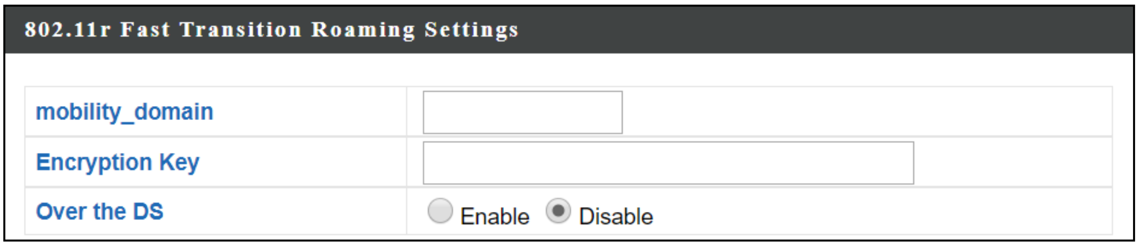
802.11r Fast Transition Roaming Settings	
Mobility_domain	Specify the mobility domain (2.4GHz or 5GHz)
Encryption Key	Specify the encryption key
Over the DS	Enable or disable this function.

X-6-2-3-5 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.

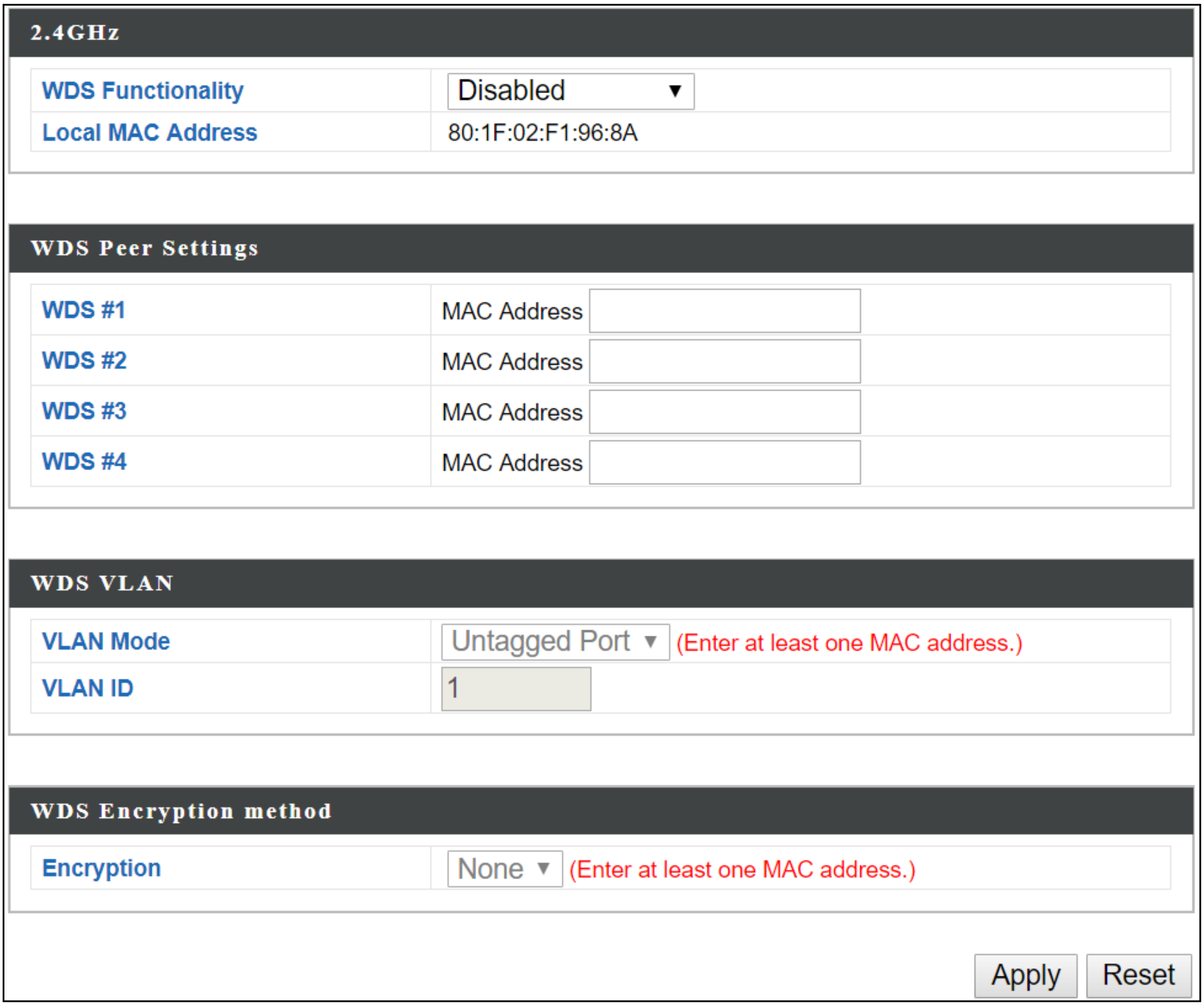
Press “Apply” to apply the configuration, or “Cancel” to forfeit the changes.

X-6-2-4 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.



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.

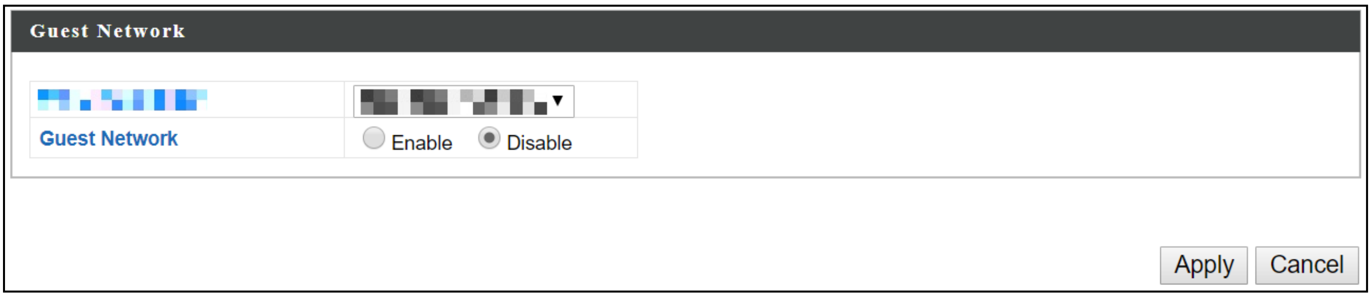
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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.

X-6-2-5 Guest Network

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



Guest Network

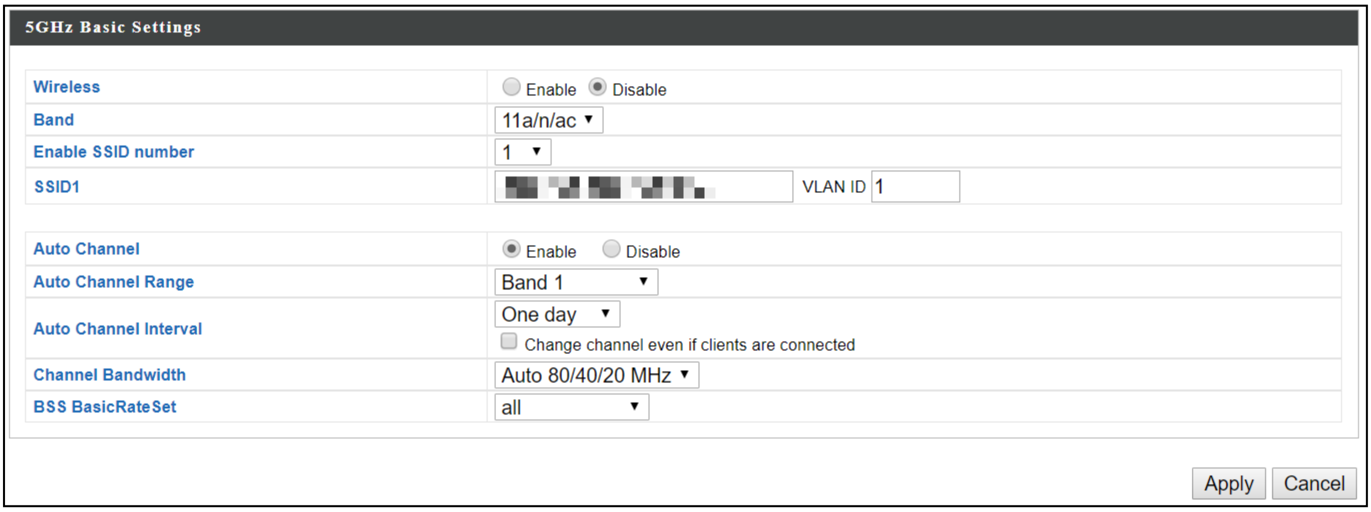
[redacted]	[redacted] ▾
Guest Network	○ Enable ● Disable

X-6-3 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.

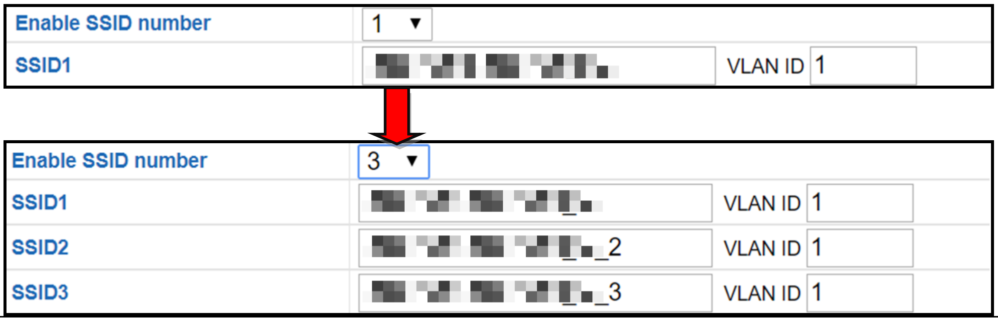
X-6-3-1 Basic

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



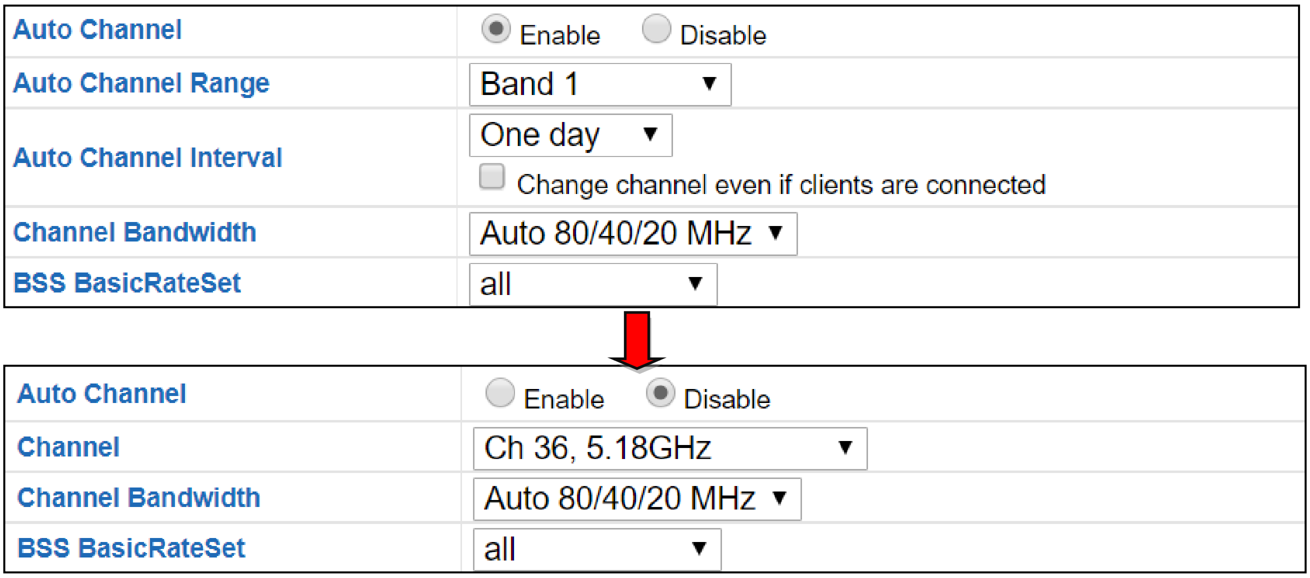
5GHz Basic Settings

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	Select a range to which auto channel selection can choose

Channel Range	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 ▼

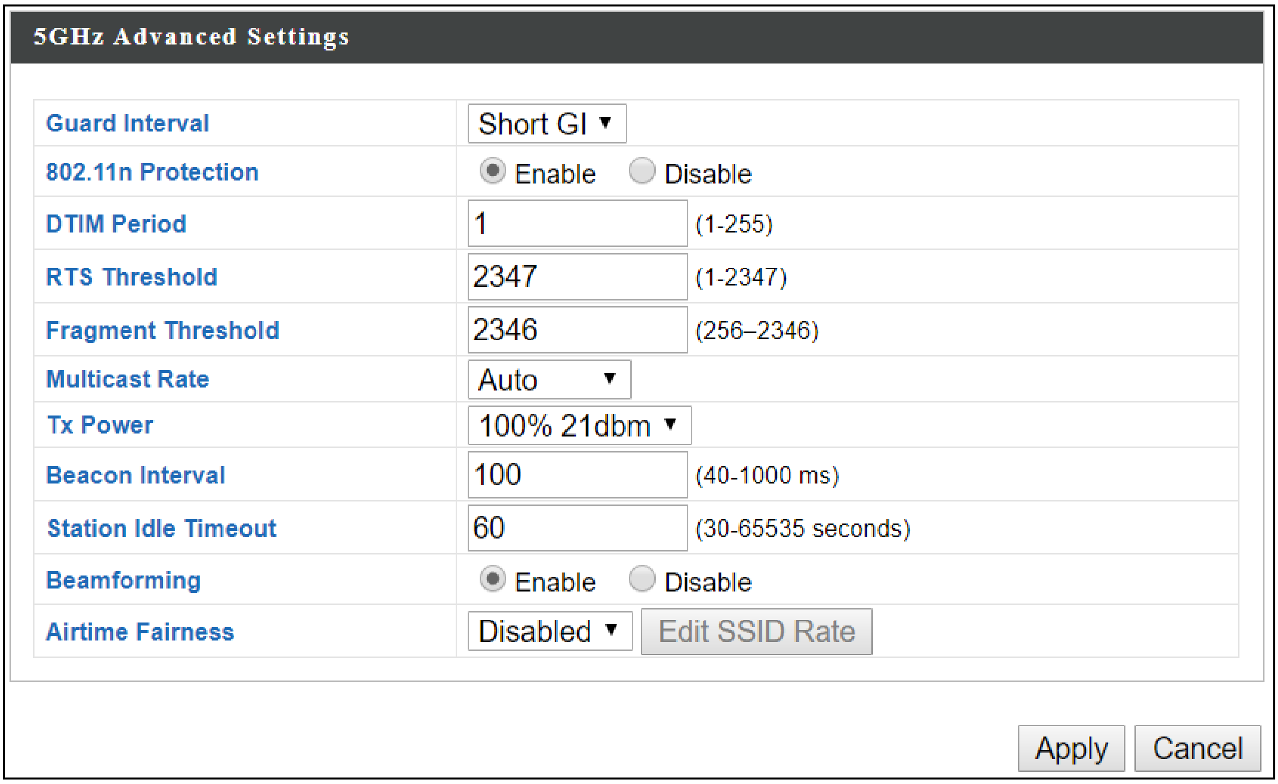
Channel	Select a wireless channel.
Channel Bandwidth	Select the channel bandwidth: 20MHz (lower performance but less interference); or Auto 40/20 MHz; or Auto 80/40/20 MHz (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates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

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

X-6-3-2 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.

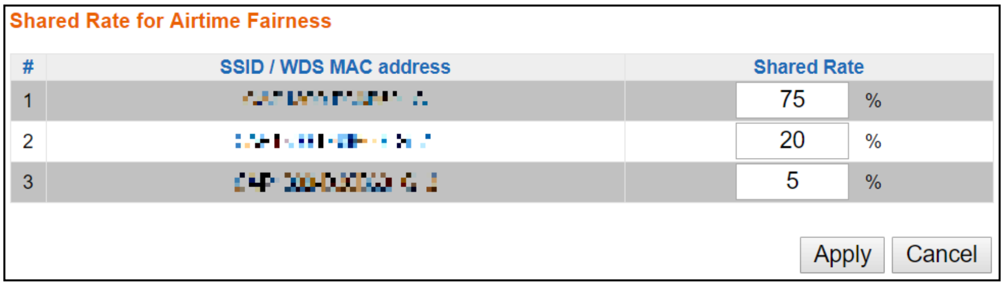


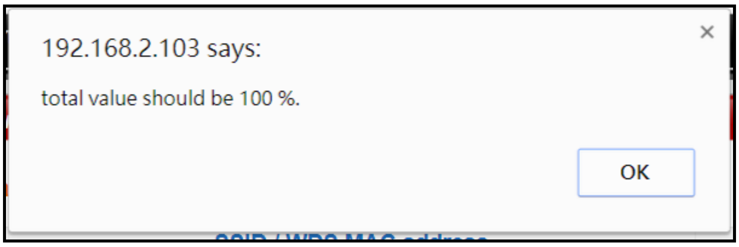
5GHz Advanced Settings

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.

<table>
<tr>
<td><b>Airtime Fairness</b></td>
<td>Airtime Fairness gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate.
Set airtime fairness to “Auto”, “Static” or “Disable”.
When “Auto” is selected, the share rate is automatically managed.
When “Static” is selected, press “Edit SSID Rate” to enter a % for each SSID’s share rate as shown below:

Shared Rate for Airtime Fairness
<table>
<tr><th>#</th><th>SSID / WDS MAC address</th><th>Shared Rate</th></tr>
<tr><td>1</td><td>[redacted]</td><td>75 %</td></tr>
<tr><td>2</td><td>[redacted]</td><td>20 %</td></tr>
<tr><td>3</td><td>[redacted]</td><td>5 %</td></tr>
</table>

The % field has to add up to 100% or the system will display a message:

192.168.2.103 says:
total value should be 100 %.

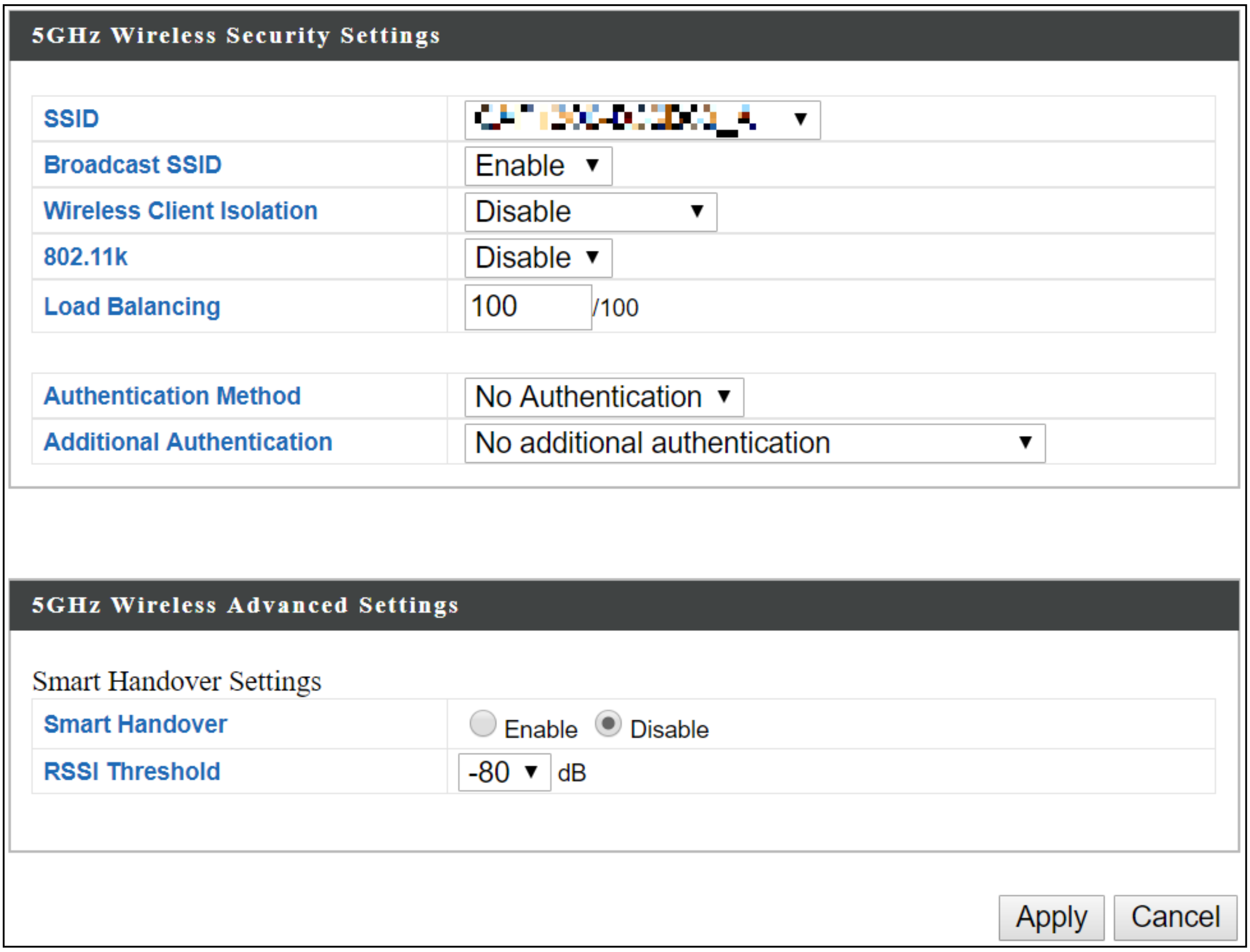
Airtime fairness is disabled if “Disable” is selected.</td>
</tr>
</table>

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

X-6-3-3 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 ***X-6-2-3 Security*** for your method.

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

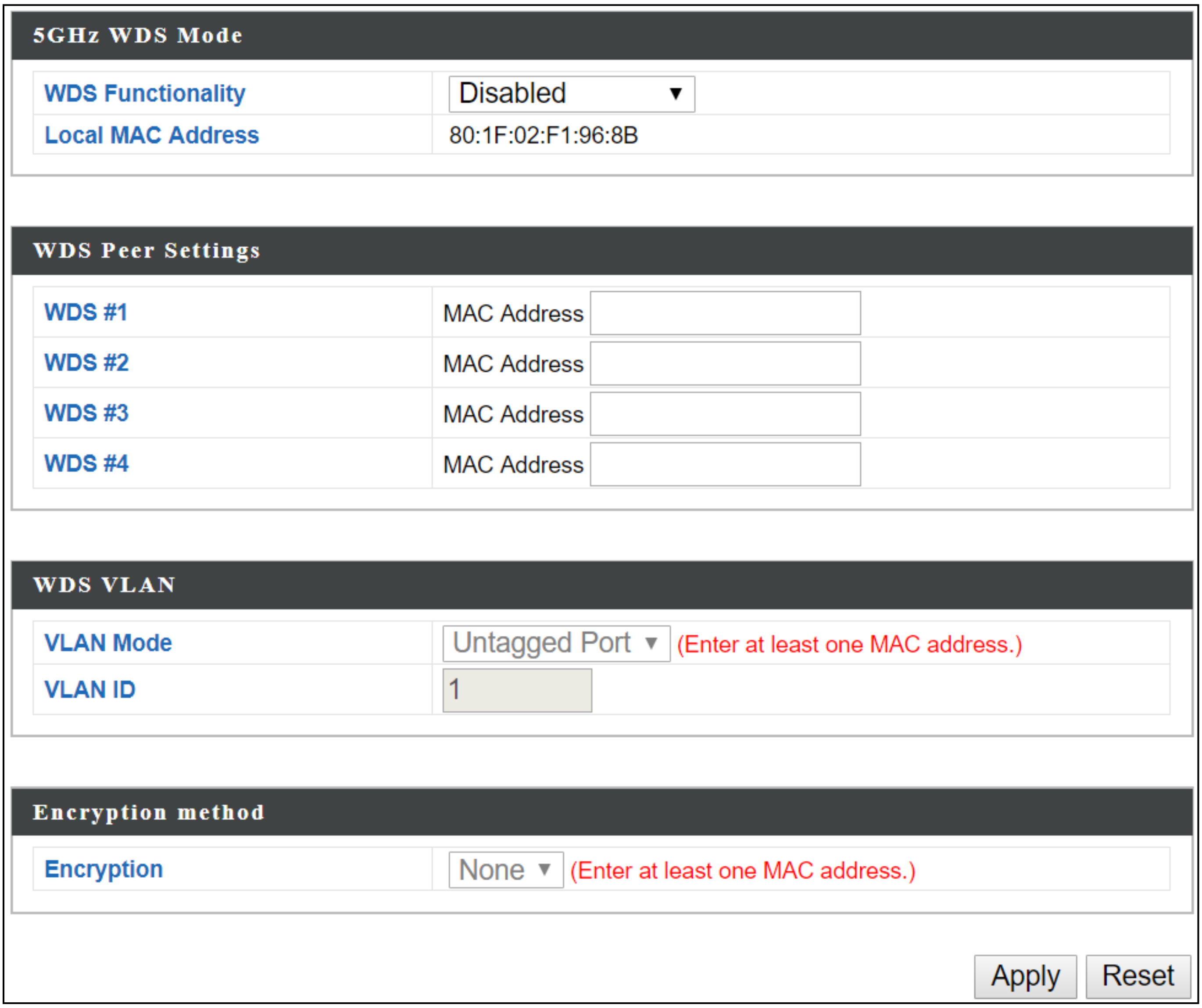
Please refer back to ***X-6-2-3 Security*** for more information on authentication and additional authentication types.

X-6-3-4 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.

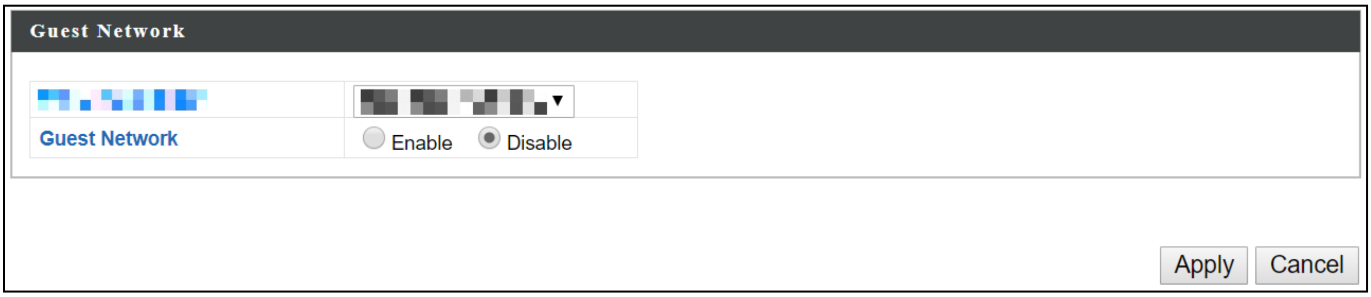
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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.

X-6-3-5 Guest Network

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



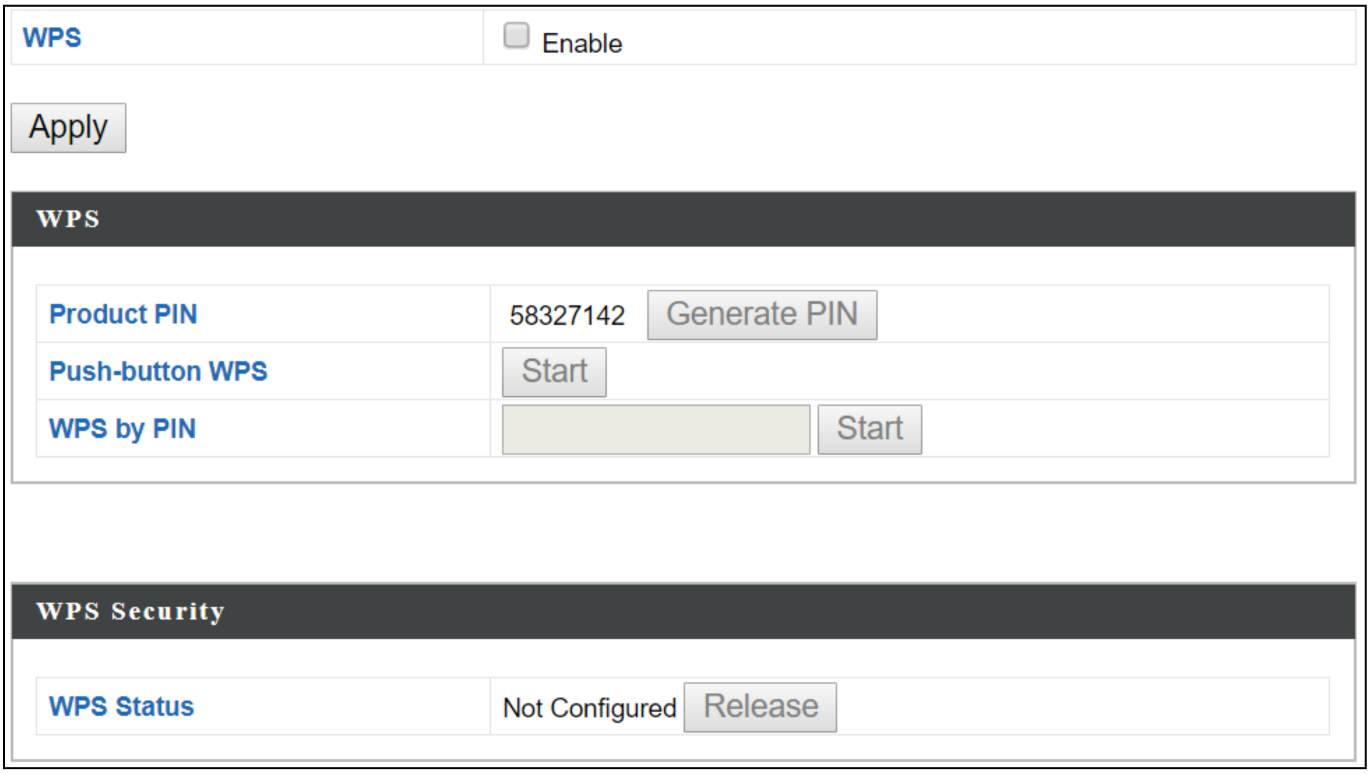
Guest Network

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

X-6-4 WPS

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

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



WPS □ Enable

WPS

Product PIN	58327142 Generate PIN
Push-button WPS	Start
WPS by PIN	Start

WPS Security

WPS Status	Not Configured Release

WPS	Check/uncheck this box to enable/disable WPS functionality. WPS must be disabled when using MAC-RADIUS authentication (see ***X-6-2-3-1 & X-6-5***).

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 access point 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.

X-6-5 RADIUS

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

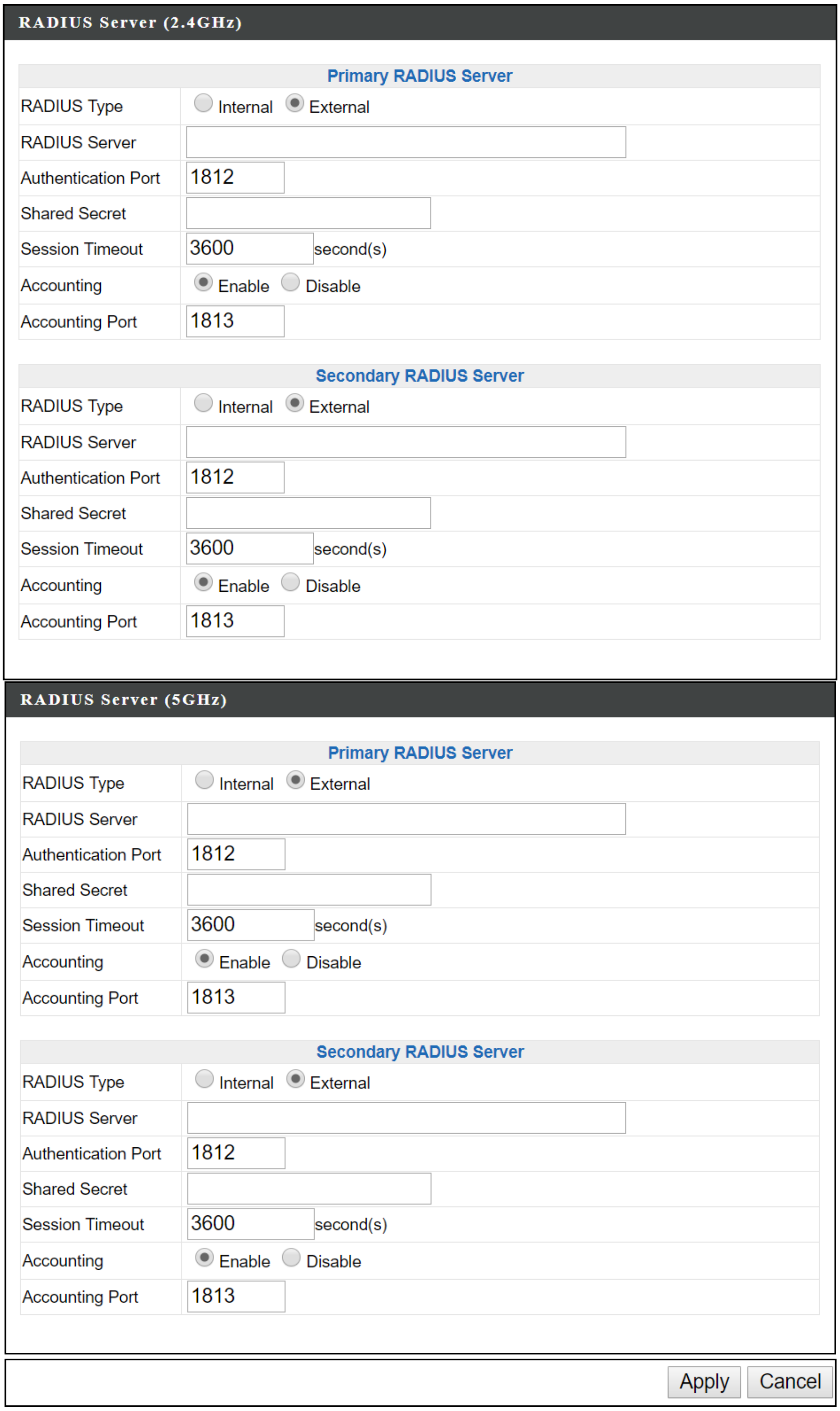
A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The access point 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 X-6-2-3 & X-6-3-3).***

X-6-5-1 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

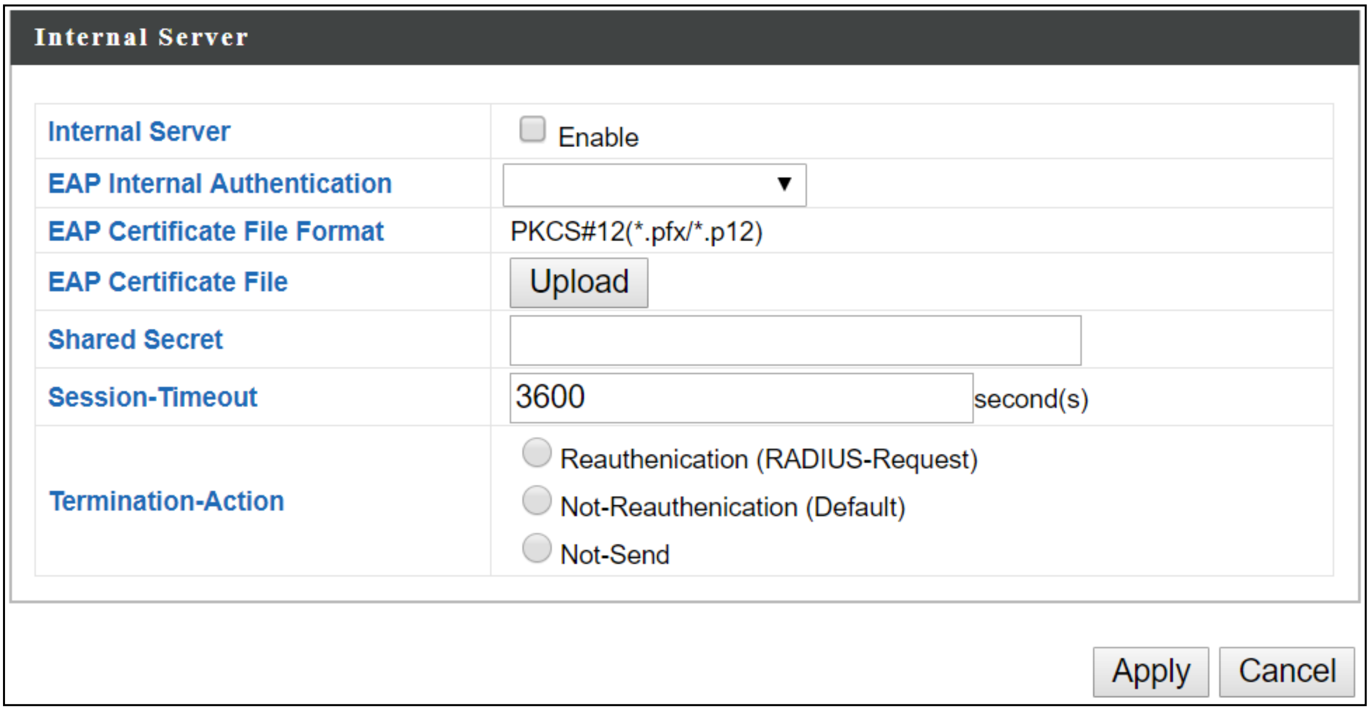
RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in **X-6-2-3** or **X-6-3-3**.
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.

X-6-5-2 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 X-6-2-3 & X-6-3-3).



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

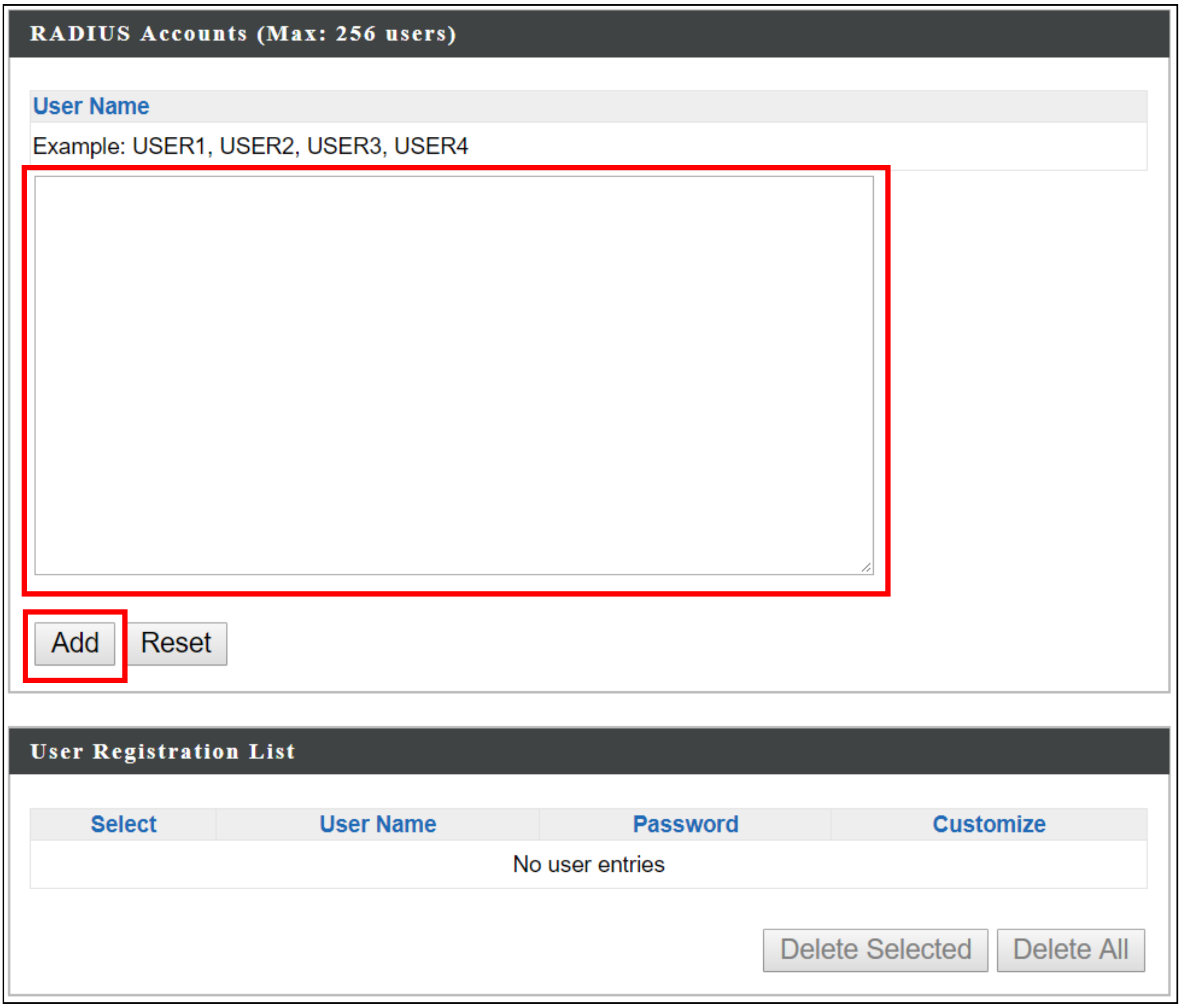
Internal Server	Check/uncheck to enable/disable the access point’s internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click “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 **X-6-2-3** or **X-6-3-3**.
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.

X-6-5-3 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)

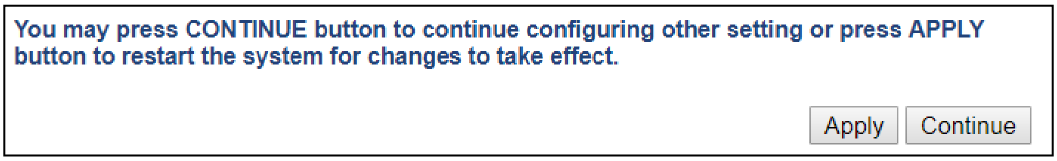
User Name

Example: USER1, USER2, USER3, USER4

User Registration List

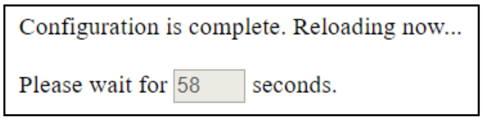
Select	User Name	Password	Customize
No user entries			

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



You may press CONTINUE button to continue configuring other setting or press APPLY button to restart the system for changes to take effect.

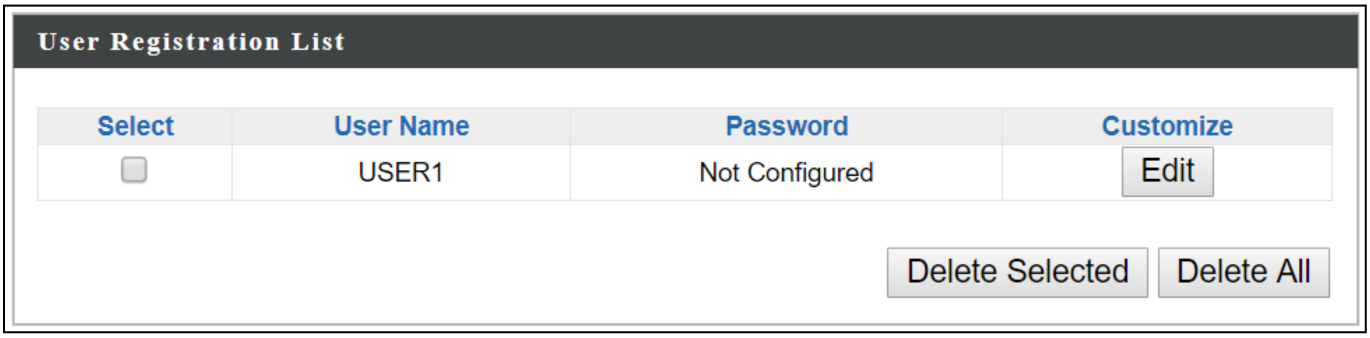
If you choose to apply the settings (by clicking “Apply”), your system will restart the system with a message shown below:



Configuration is complete. Reloading now...

Please wait for 58 seconds.

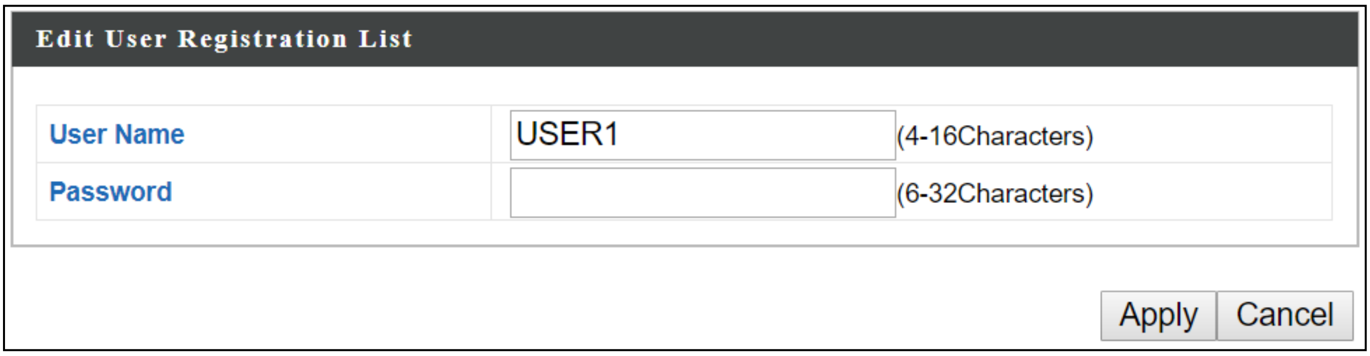
Press "Continue" see the new user registration list.



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.

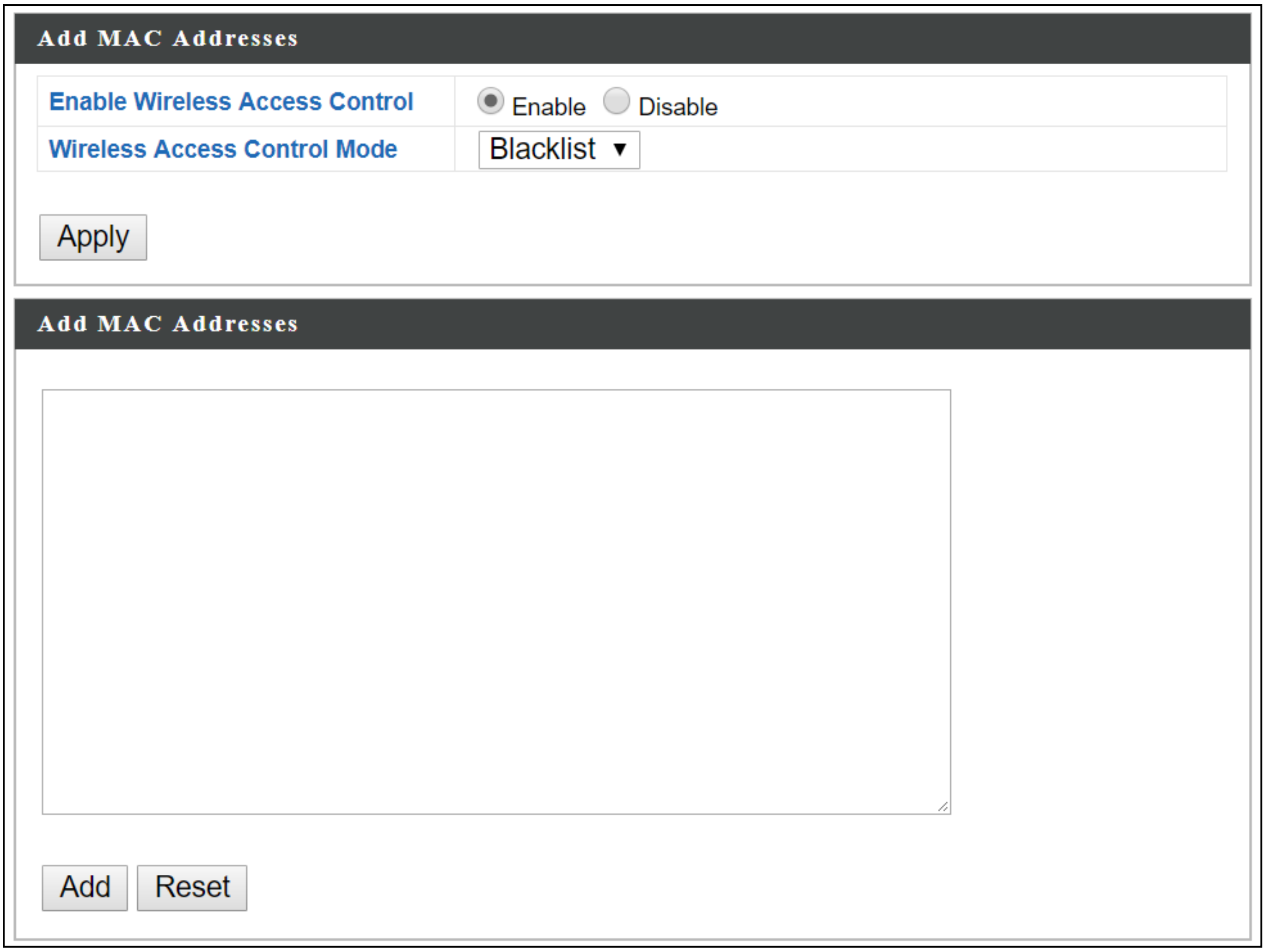
X-6-6 MAC Filter

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 X-6-2-3 Security).***

The MAC address filtering table is displayed below:

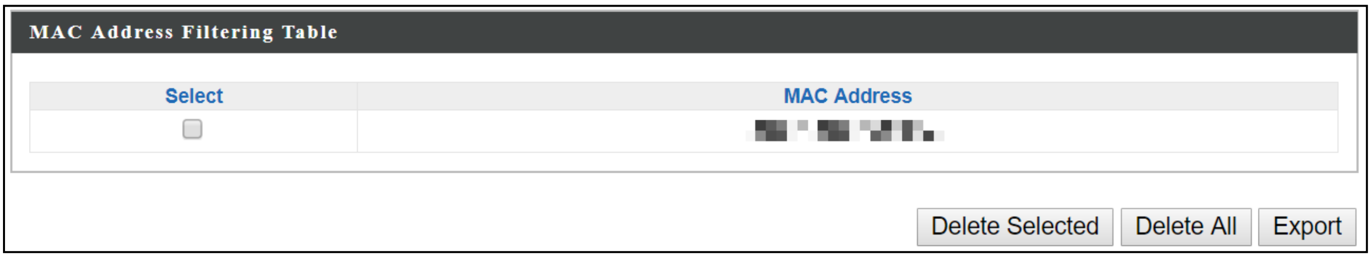


Add MAC Addresses

Enable Wireless Access Control	● Enable ○ Disable
Wireless Access Control Mode	Blacklist ▾

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.



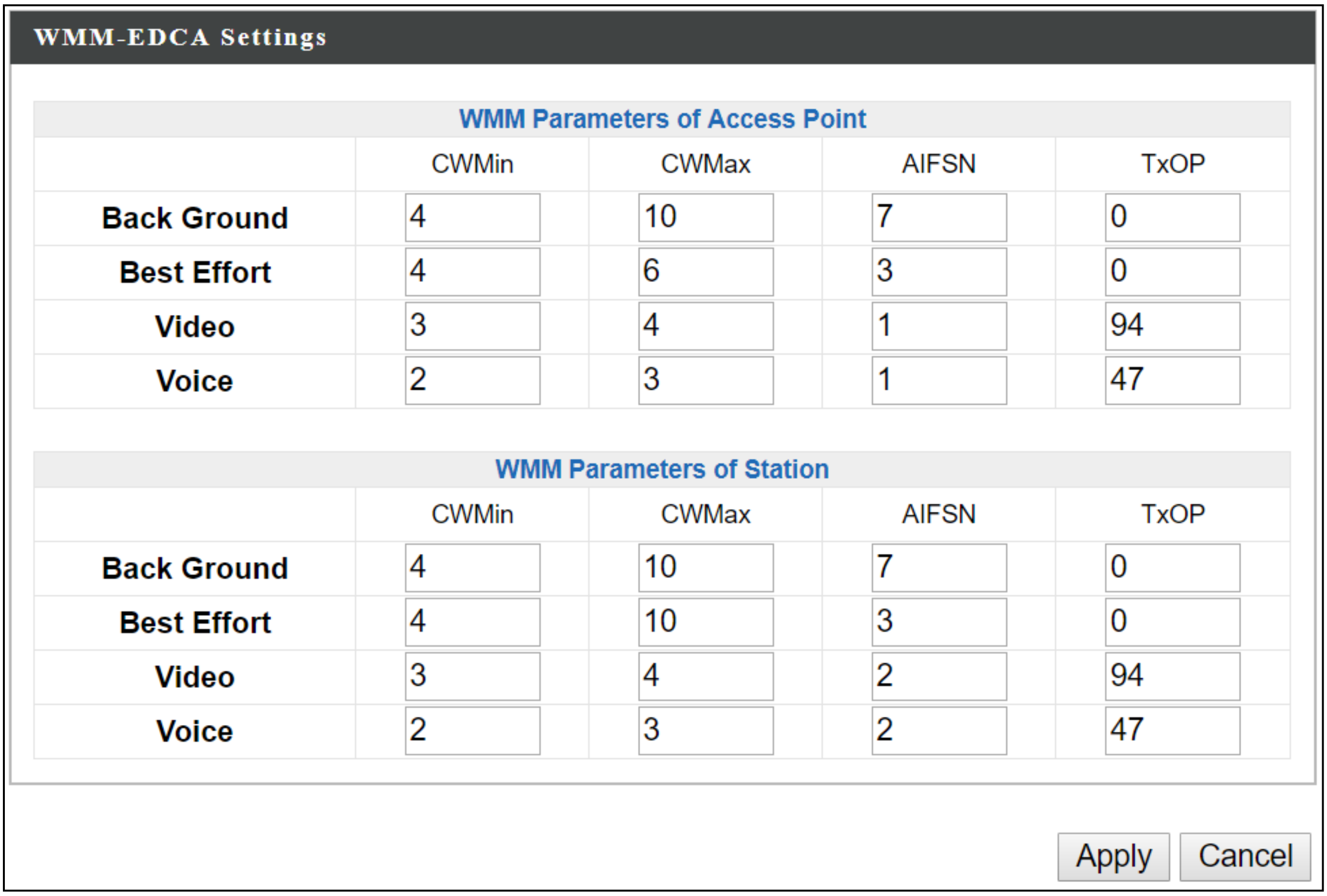
MAC Address Filtering Table

Select	MAC Address
☐	[redacted]

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.

X-6-7 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:

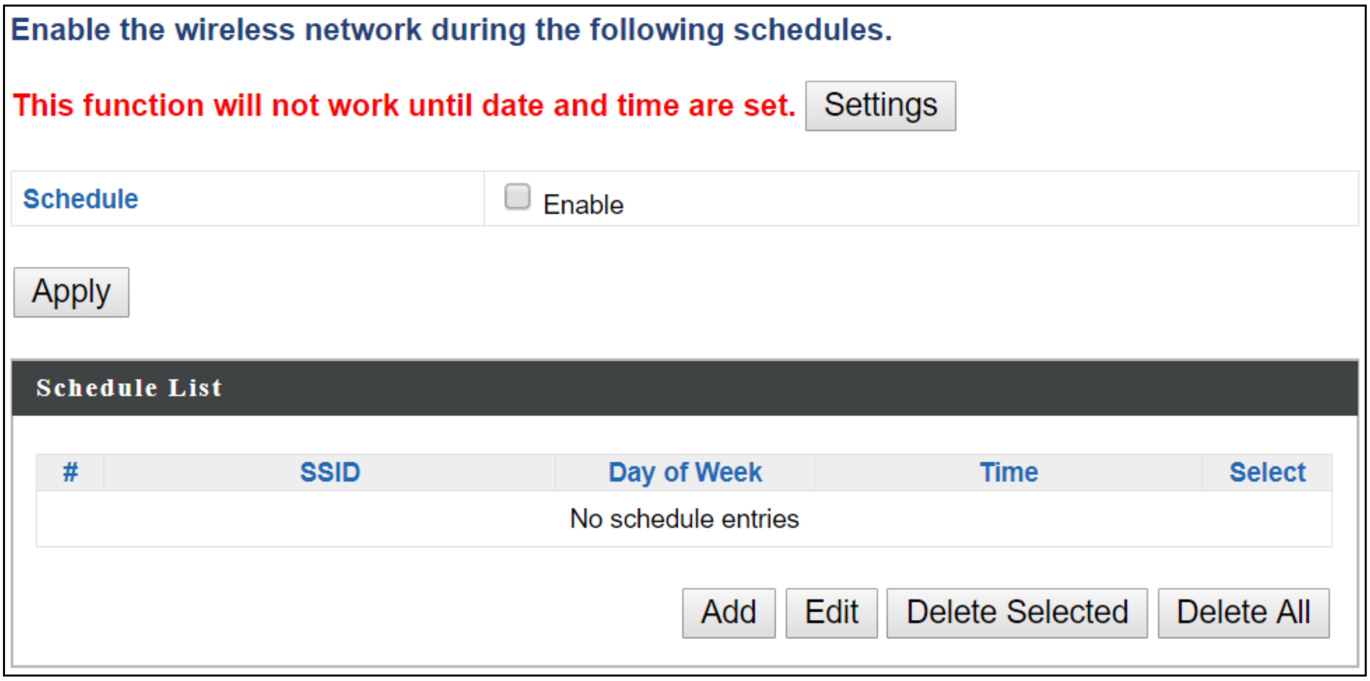
CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value 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.

X-6-8 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.

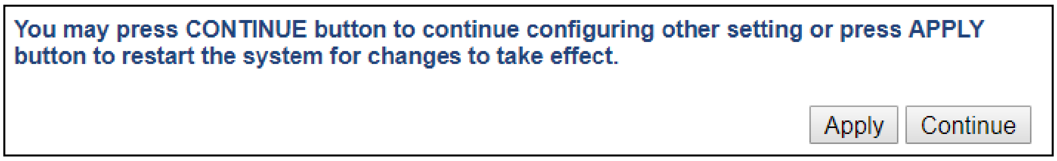
This function will not work until date and time are set.

Schedule □ Enable

Schedule List

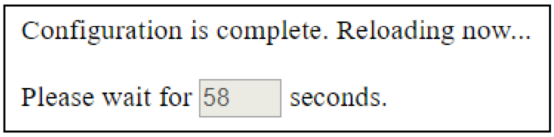
#	SSID	Day of Week	Time	Select
No schedule entries				

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



You may press CONTINUE button to continue configuring other setting or press APPLY button to restart the system for changes to take effect.

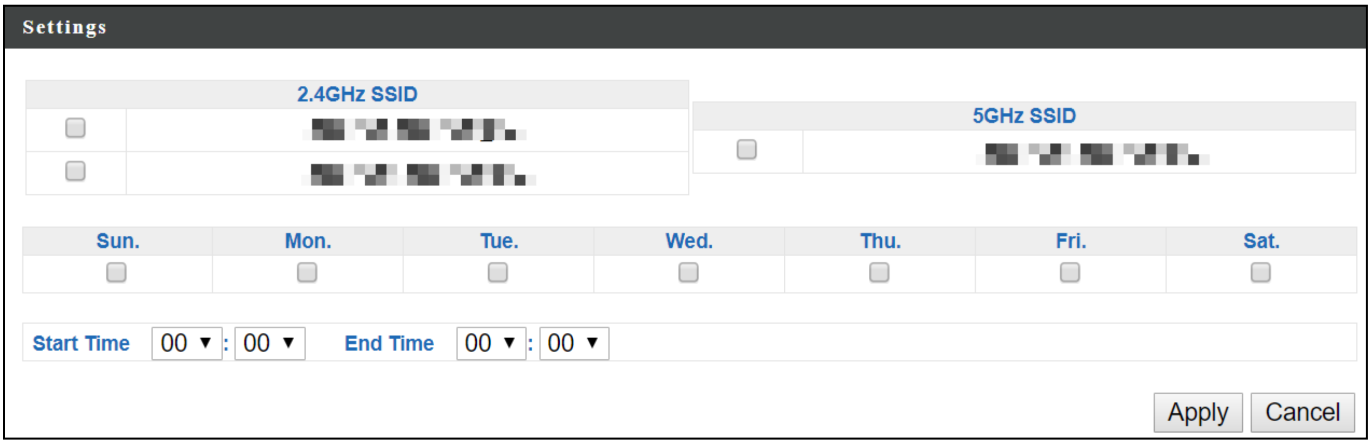
If you choose to apply the settings (by clicking “Apply”), your system will restart the system with a message shown below:



Configuration is complete. Reloading now...

Please wait for 58 seconds.

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

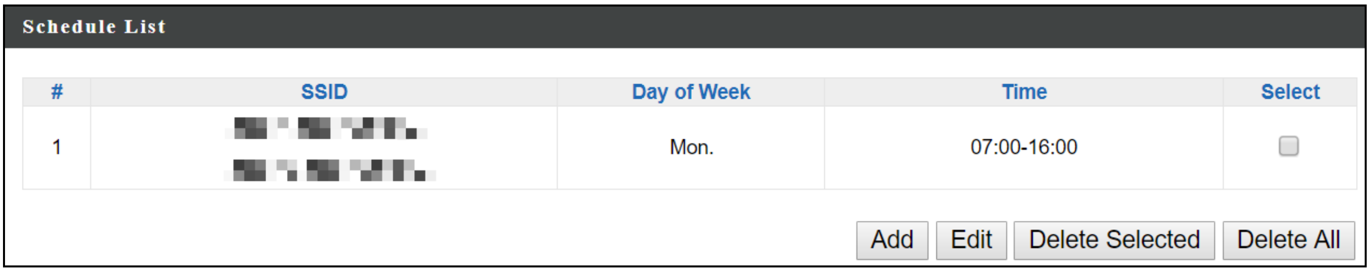
	2.4GHz SSID
□	[redacted]
□	[redacted]

	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] [redacted]	Mon.	07:00-16:00	□

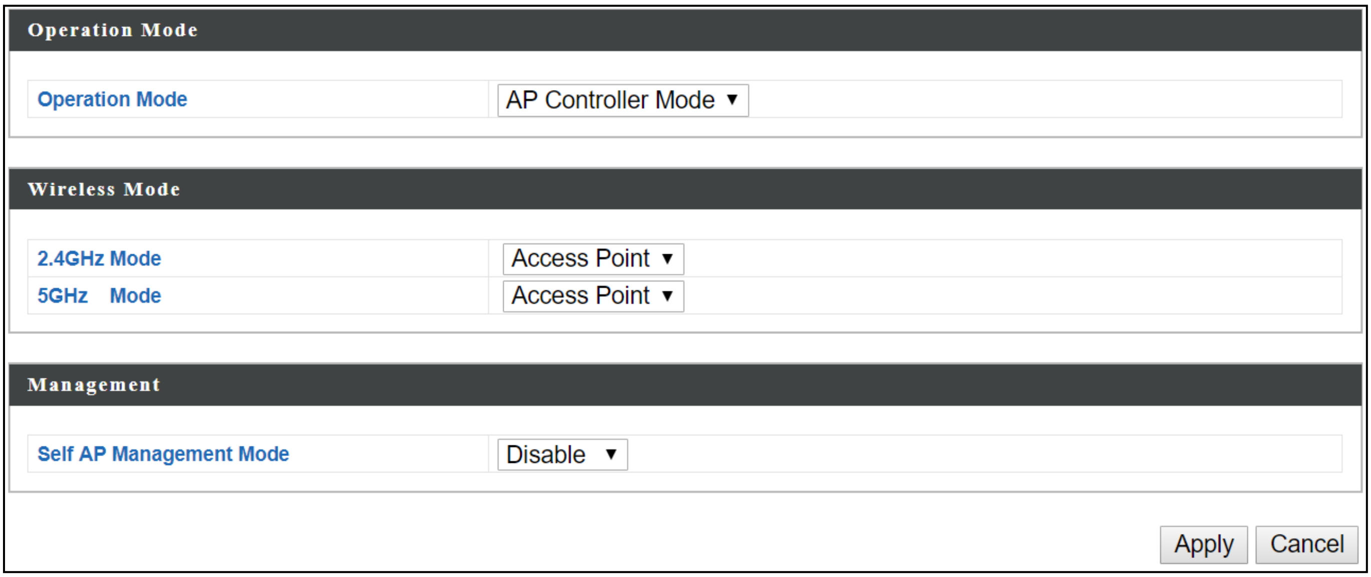
3. Select “Add” to add more schedules; or
Check the box of currently available schedule, select “Edit” to edit, or select “Delete Selected” to delete; or
Select “Delete All” to delete all schedules.

X-7 Local Settings

X-7-1 Operation Mode

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

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



Operation Mode

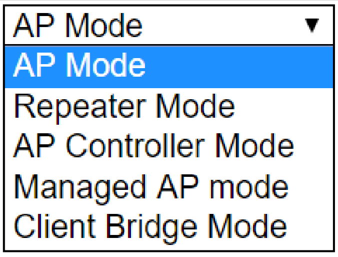
Operation Mode	AP Controller Mode ▼

Wireless Mode

2.4GHz Mode	Access Point ▼
5GHz Mode	Access Point ▼

Management

Self AP Management Mode	Disable ▼



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

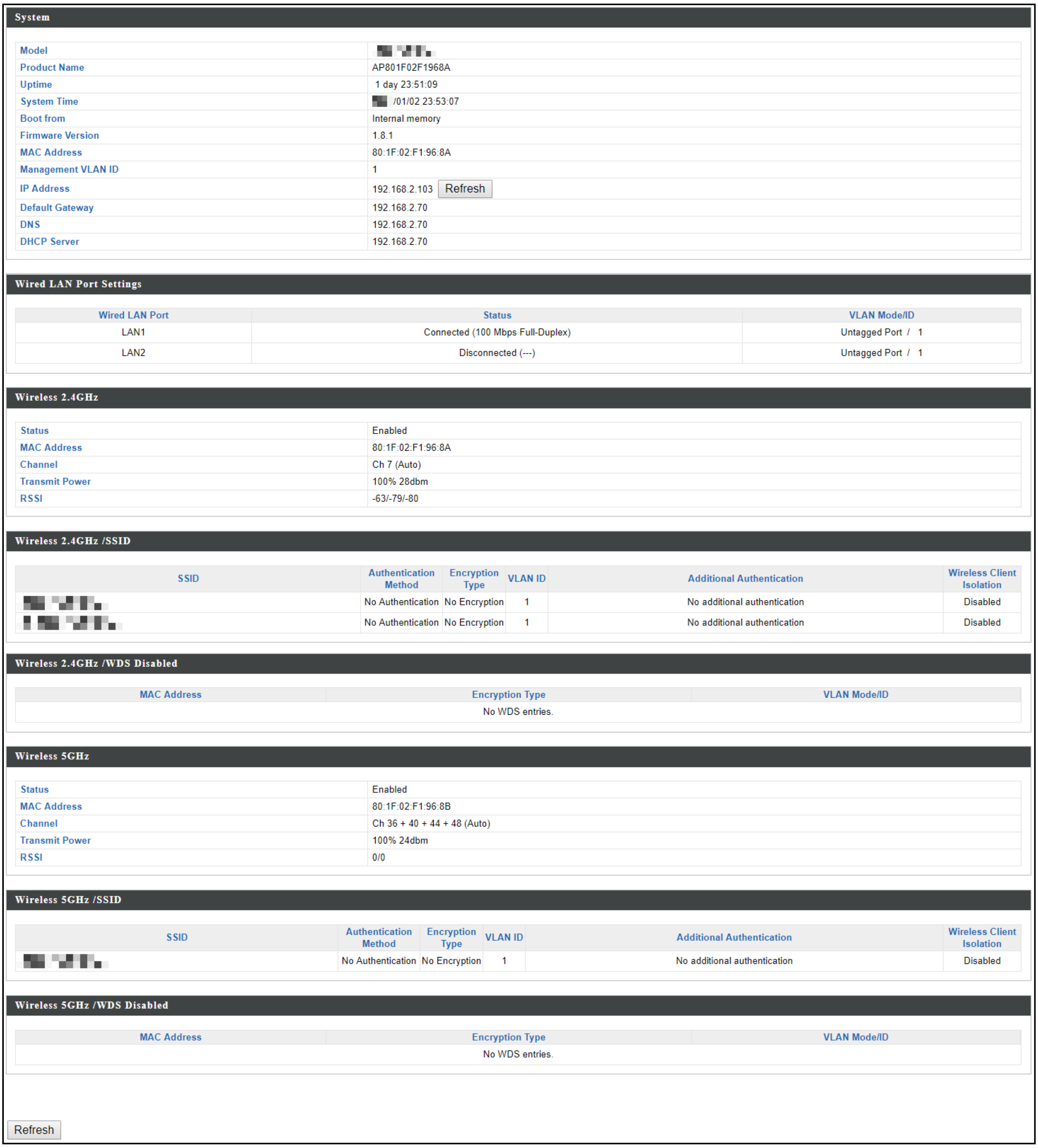
In AP Controller Mode the access point will switch to the Edimax Pro NMS user interface.

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

X-7-2 Network Settings

X-7-2-1 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.	

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 ***X-6-1-3 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.

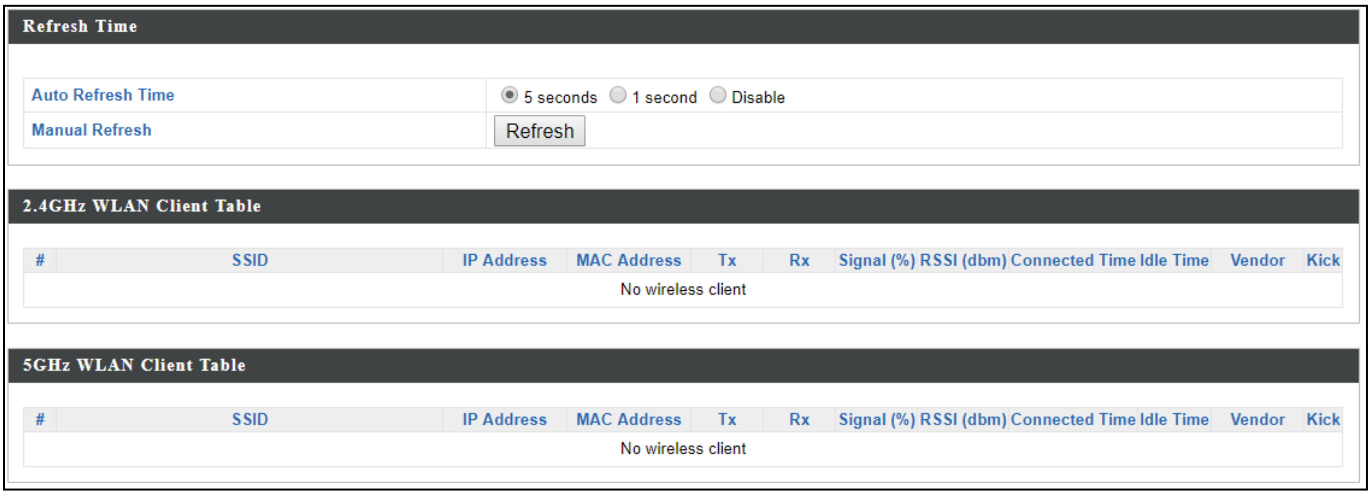
Wireless 2.4GHZ (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID. See ***X-6-1 Network Settings***.
Encryption Type	Displays the encryption type for the specified SSID. See ***X-6-1 Network Settings***.
VLAN ID	Displays the VLAN ID for the specified SSID. See ***X-6-1-3 VLAN***.
Additional Authentication	Displays the additional authentication type for the specified SSID. See ***X-6-1 Network Settings***.
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID. See ***X-6-1-3 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 ***X-6-2-4 WDS***.
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See ***X-6-2-4 WDS***.

Select “Refresh” to refresh all information.

X-7-2-2 Wireless Clients

“Wireless Clients” page displays information about all wireless clients connected to the access point 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

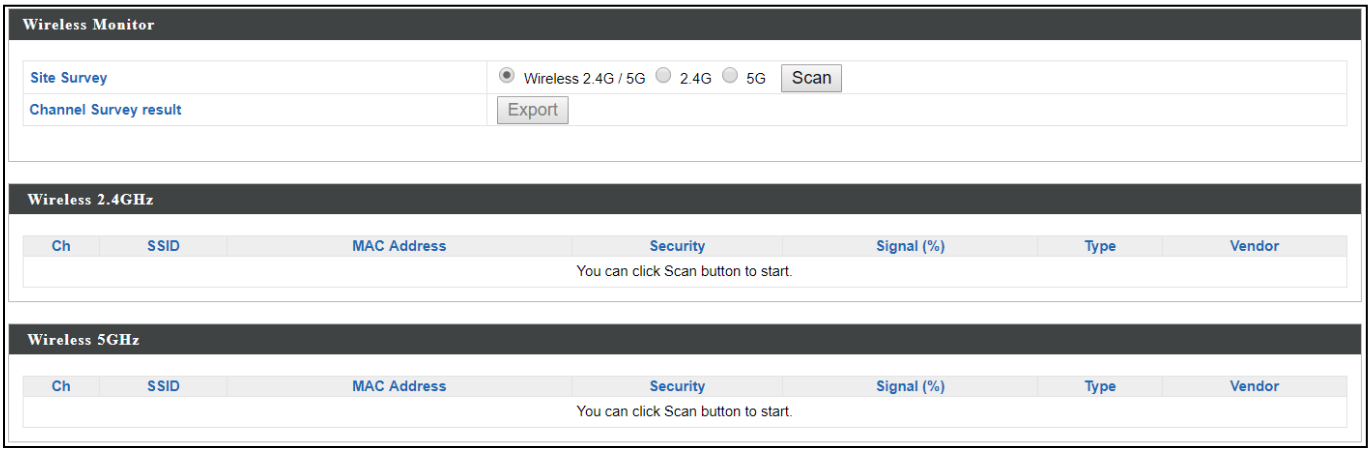
#	SSID	IP Address	MAC Address	Tx	Rx	Signal (%)	RSSI (dbm)	Connected Time	Idle Time	Vendor	Kick
No wireless client											

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.

X-7-2-3 Wireless Monitor

“Wireless Monitor” is a tool built into the access point 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.						

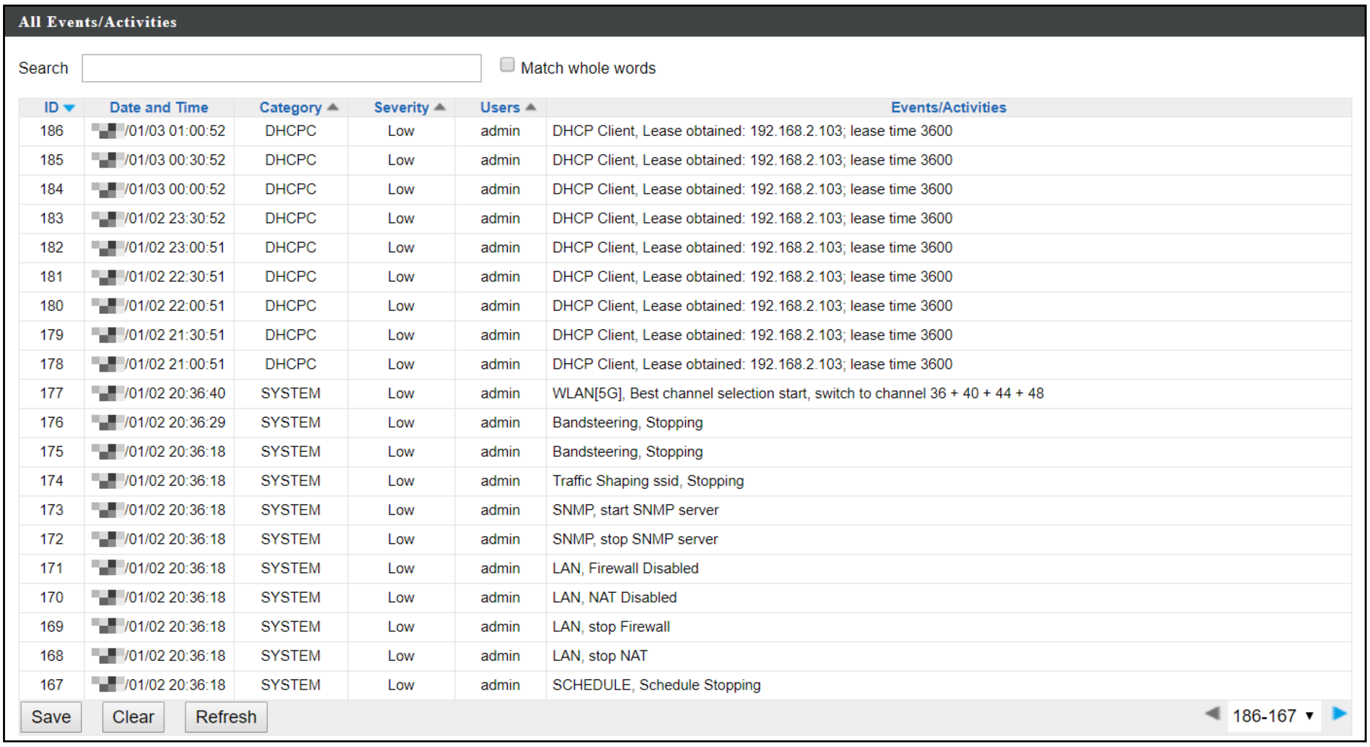
Wireless Monitor	
Site Survey	Select which frequency (or both) to scan, and click “Scan” to begin.
Channel Survey Result	After a scan is complete, click “Export” to save the results to local storage.

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.

X-7-2-4 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

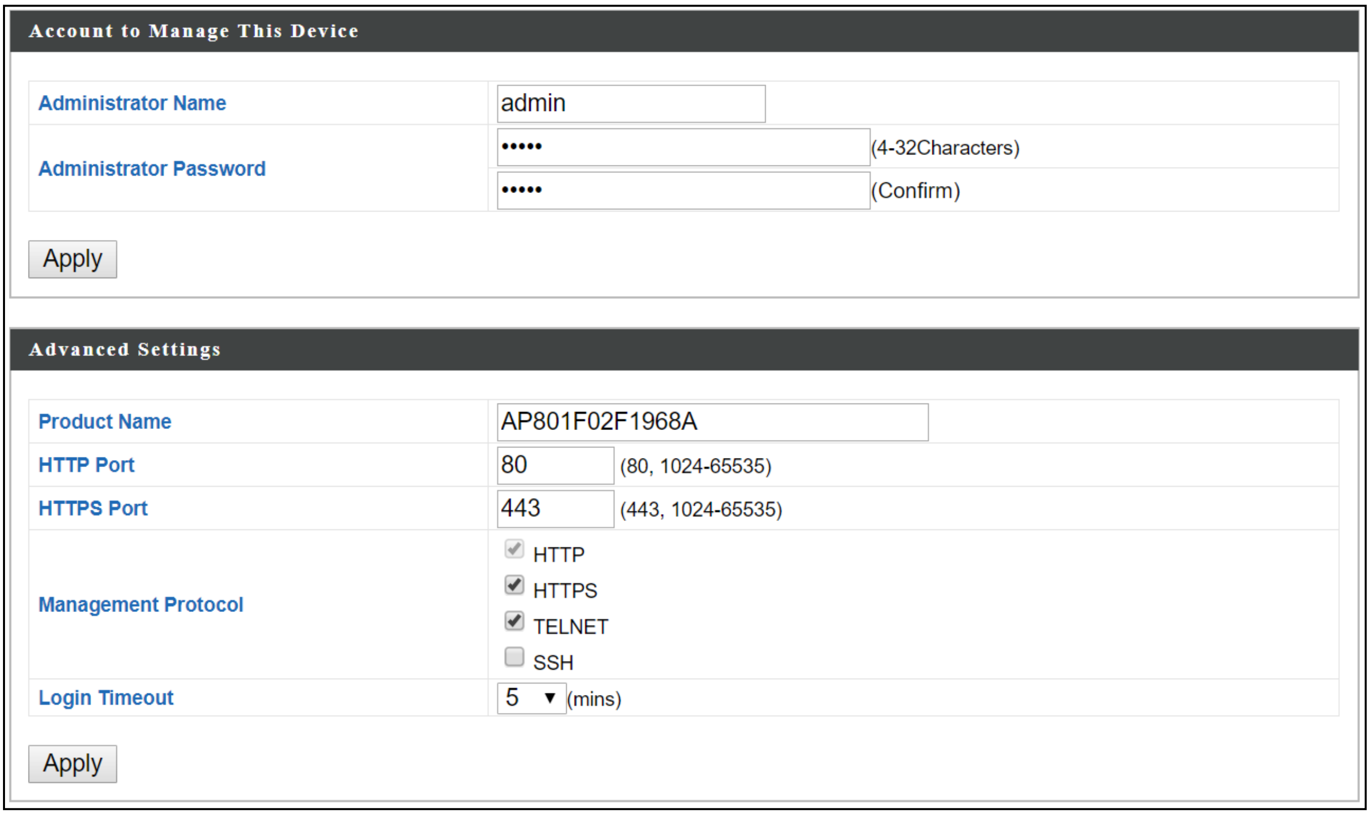
- **WPS**
  M1 - M8 messages
  WPS success
- **Change Settings**
- **System Boot**
  Displays current model name
- **NTP Client**
- **Wired Link**
  LAN Port link status and speed status
- **Proxy ARP**
  Proxy ARP module start & stop
- **Bridge**
  Bridge start & stop.
- **SNMP**
  SNMP server start & 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

X-7-3 Management

X-7-3-1 Admin

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

If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see** I-5 Reset **for how to reset the access point.



Account to Manage This Device

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

Advanced Settings

Product Name	AP801F02F1968A	
HTTP Port	80	(80, 1024-65535)
HTTPS Port	443	(443, 1024-65535)
Management Protocol	☑ HTTP ☑ HTTPS ☑ TELNET ☐ SSH	
Login Timeout	5 ▼	(mins)

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

Press “Apply” to apply the configuration.

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

HTTP

Internet browser HTTP protocol management interface

TELNET

Client terminal with telnet protocol management interface

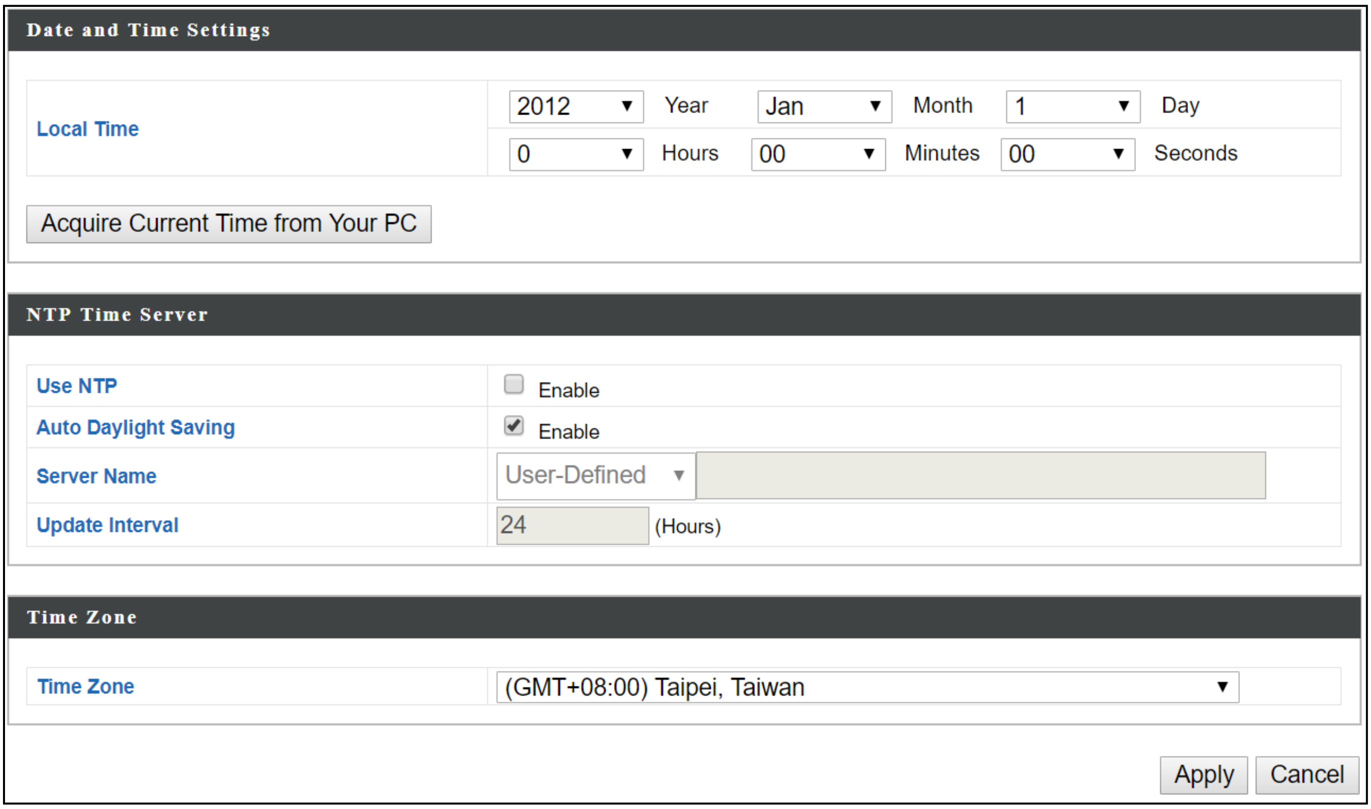
SNMP

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

Press “Apply” to apply the configuration.

X-7-3-2 Date and Time

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



Date and Time Settings

Local Time: 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

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

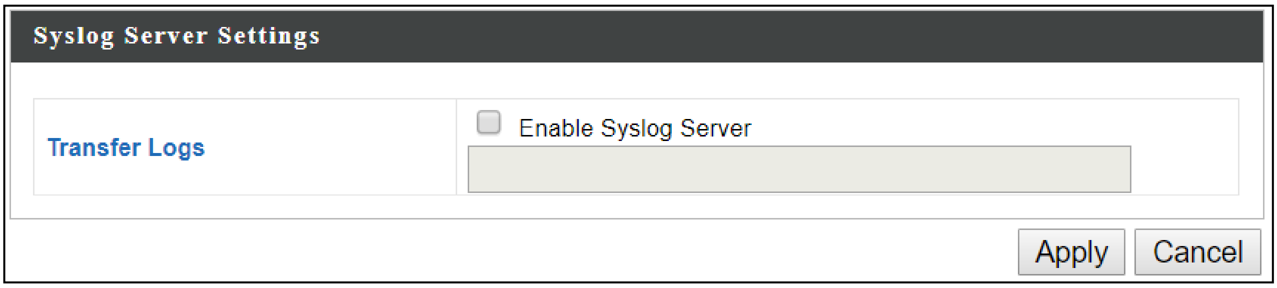
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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

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

X-7-3-3 Syslog Server Settings

The system log can be sent to a server.



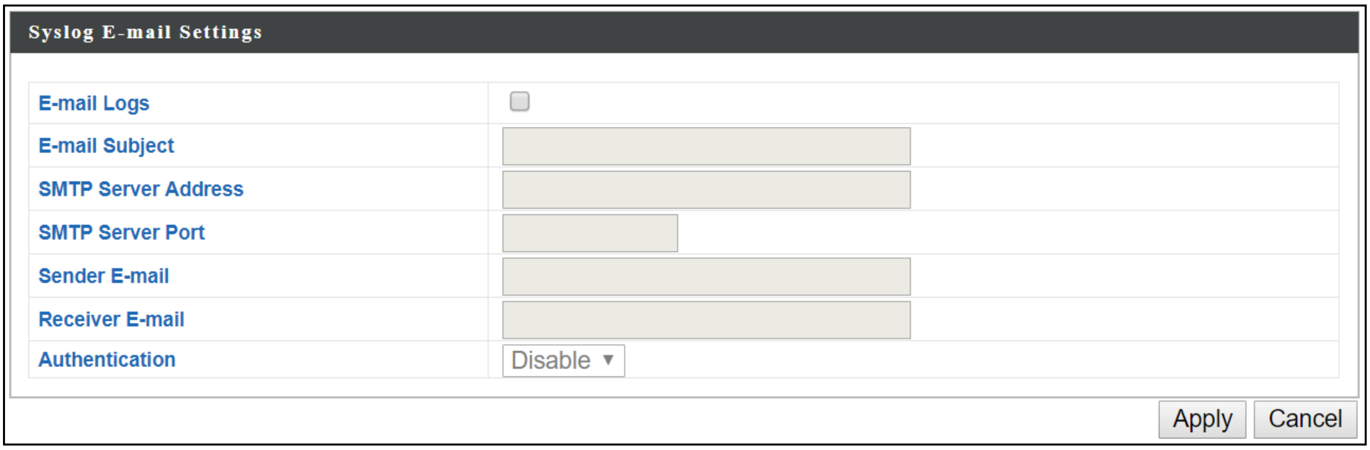
Syslog Server Settings

Transfer Logs	□ Enable Syslog Server

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

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

X-7-3-4 Syslog E-mail Settings



Syslog E-mail Settings

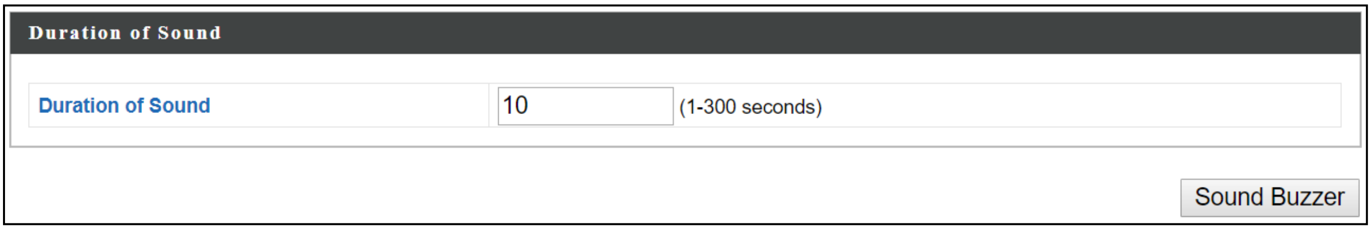
E-mail Logs	□
E-mail Subject	
SMTP Server Address	
SMTP Server Port	
Sender E-mail	
Receiver E-mail	
Authentication	Disable ▼

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

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

X-7-3-5 I’m Here

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



Duration of Sound

Duration of Sound: 10 (1-300 seconds)

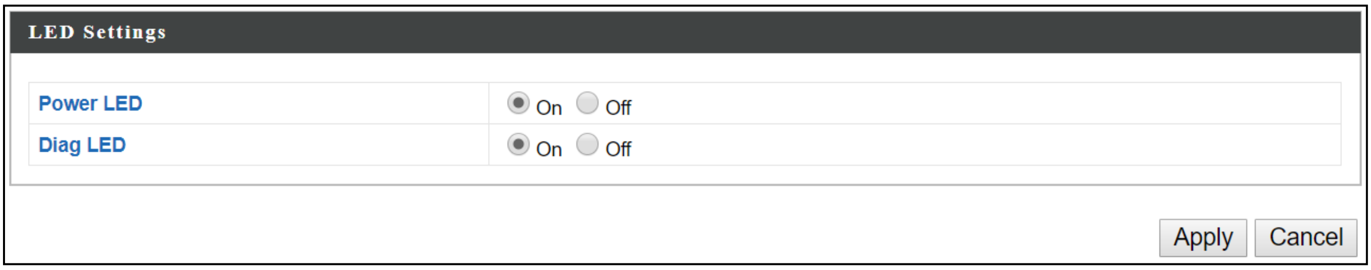
The buzzer is loud!

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

X-7-4 Advanced

X-7-4-1 LED Settings

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



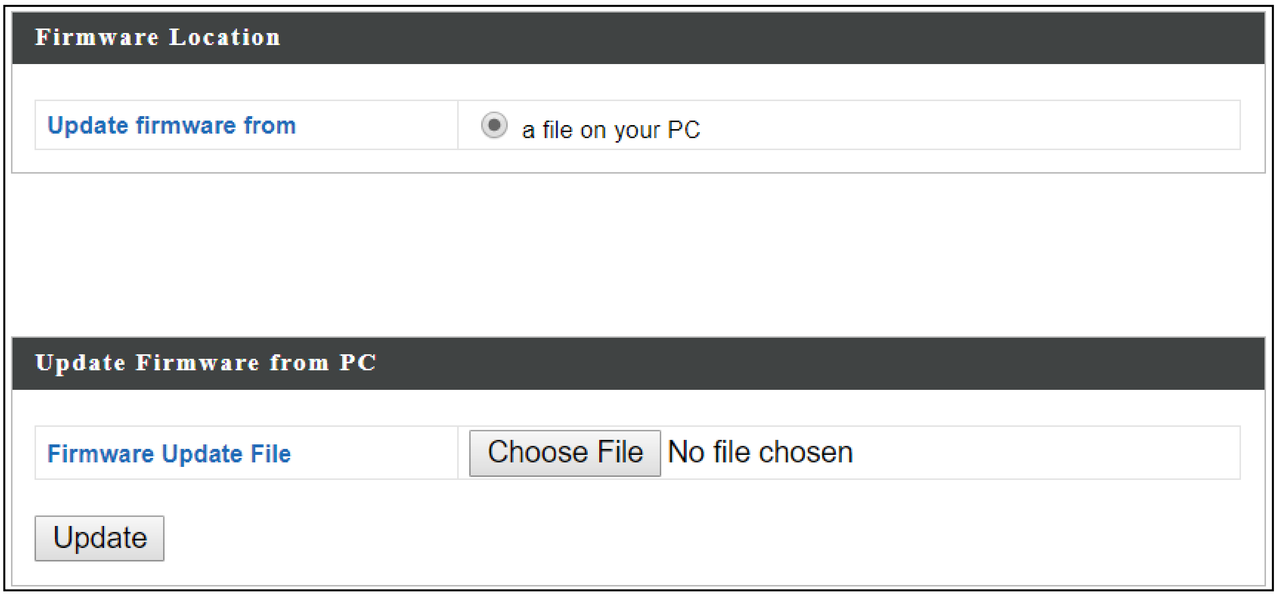
LED Settings

Power LED	● On ○ Off
Diag LED	● On ○ Off

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

X-7-4-2 Update Firmware

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



Firmware Location

Update firmware from: ● a file on your PC

Update Firmware from PC

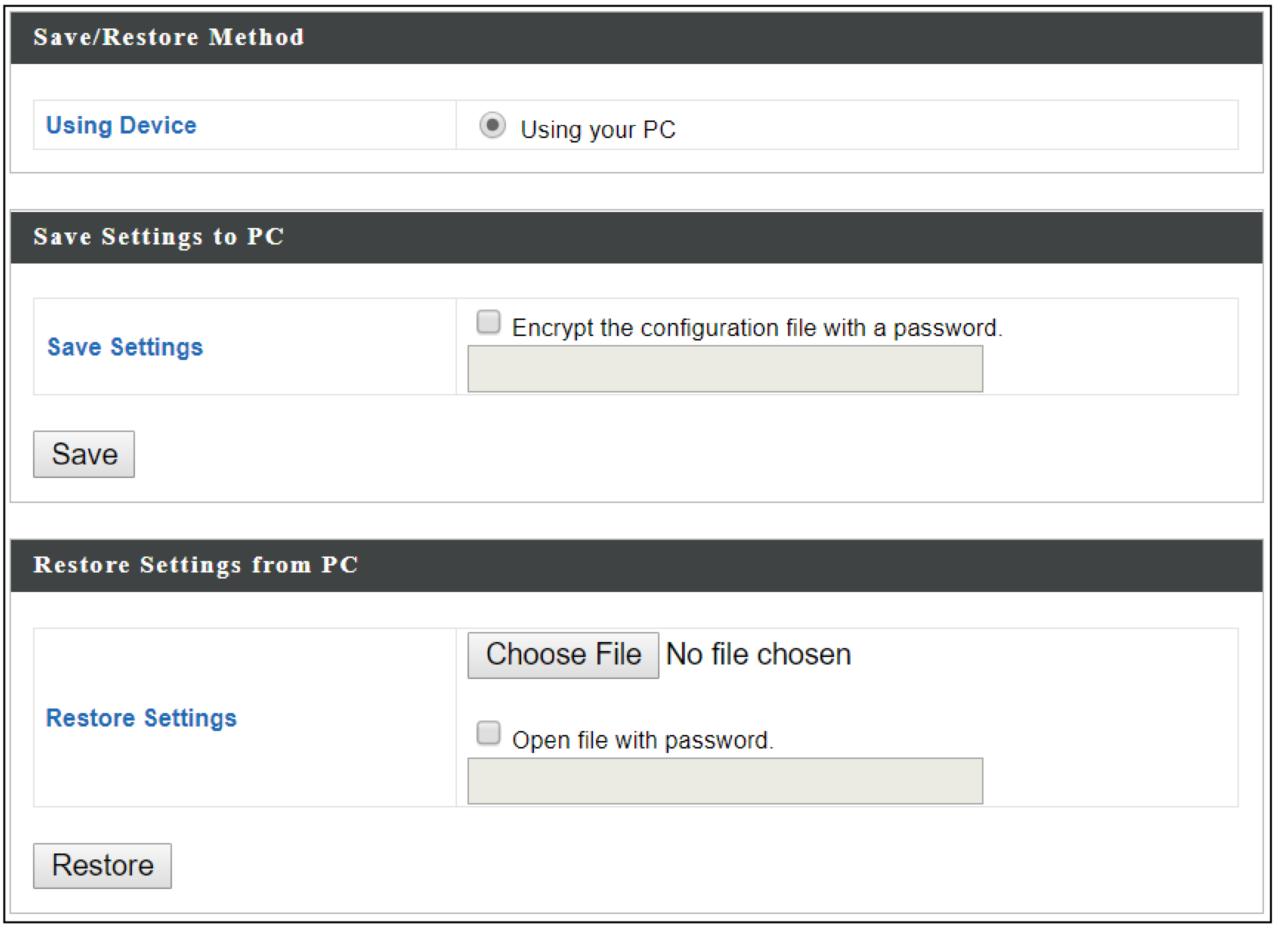
Firmware Update File: Choose File No file chosen

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

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

X-7-4-3 Save/Restore Settings

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



Save/Restore Method

Using Device: ● Using your PC

Save Settings to PC

Save Settings: □ Encrypt the configuration file with a password.

Restore Settings from PC

Restore Settings: Choose File No file chosen

□ Open file with password.

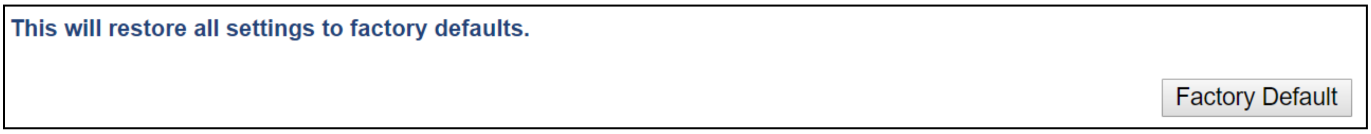
Save Settings to PC	
Save Settings	**Encryption**: If you wish to encrypt the configuration file with a password, check the "Encrypt the configuration file with a password" box and enter a password. Click "Save" to save current settings. A new window will open to allow you to specify a location to save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

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

	Click “Restore” to replace your current settings.

X-7-4-4 Factory Default

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



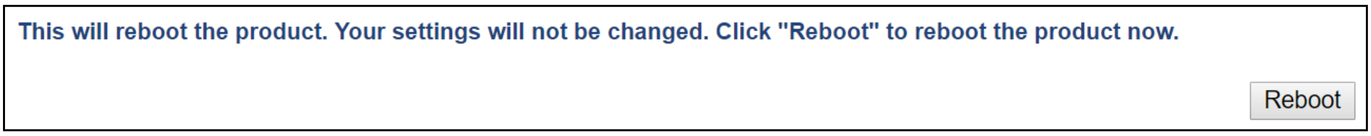
This will restore all settings to factory defaults.

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

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

X-7-4-5 Reboot

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



This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.

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

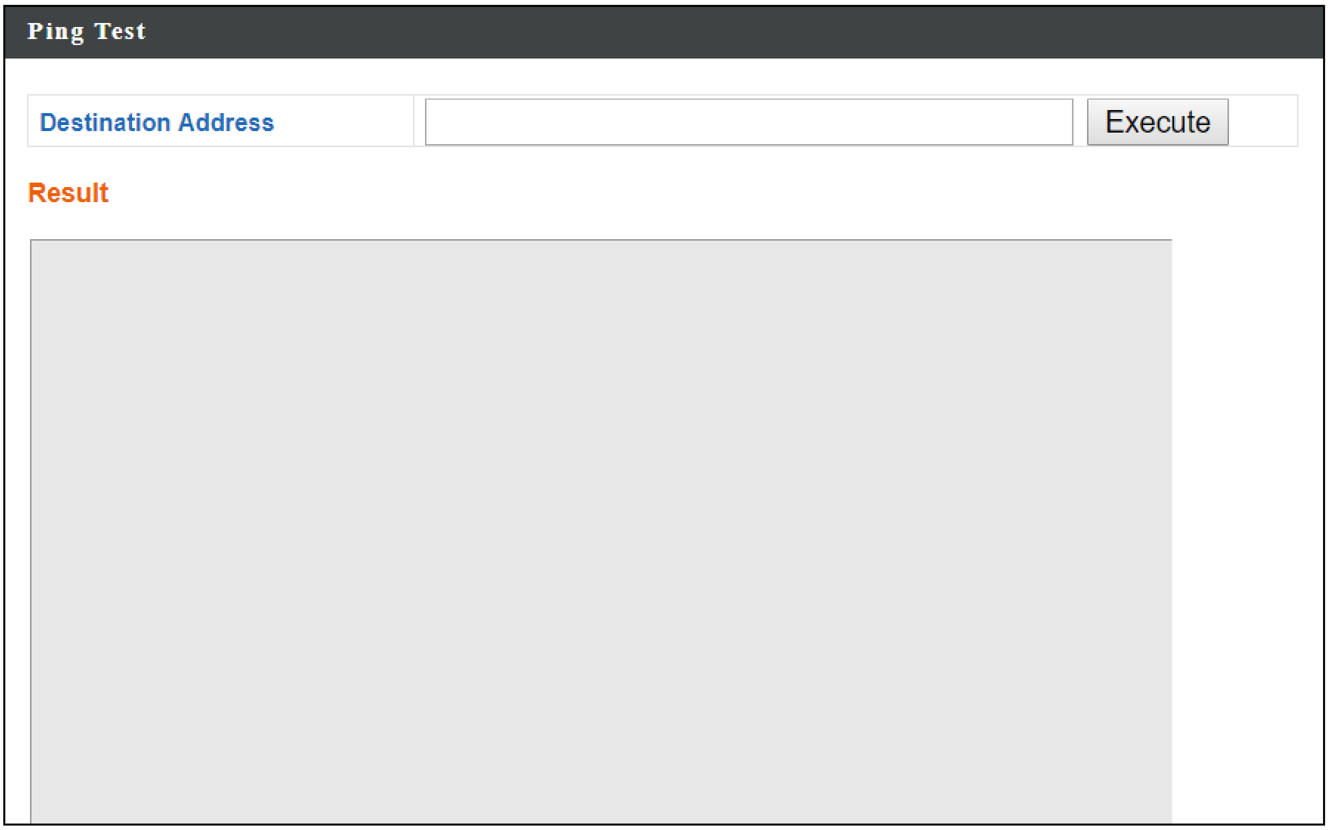
X-8 Toolbox

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

X-8-1 Network Connectivity

X-8-1-1 Ping

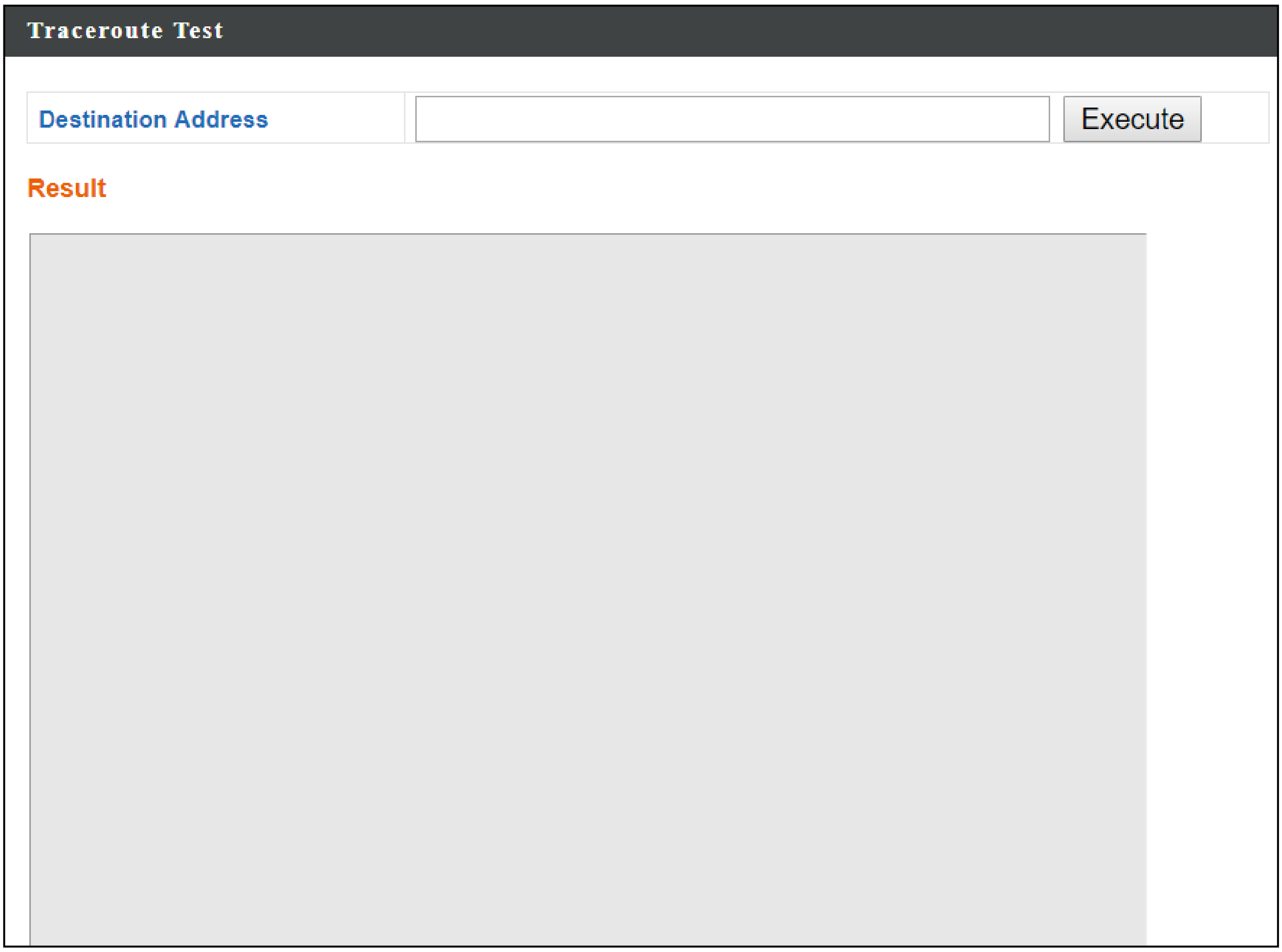
Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.



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

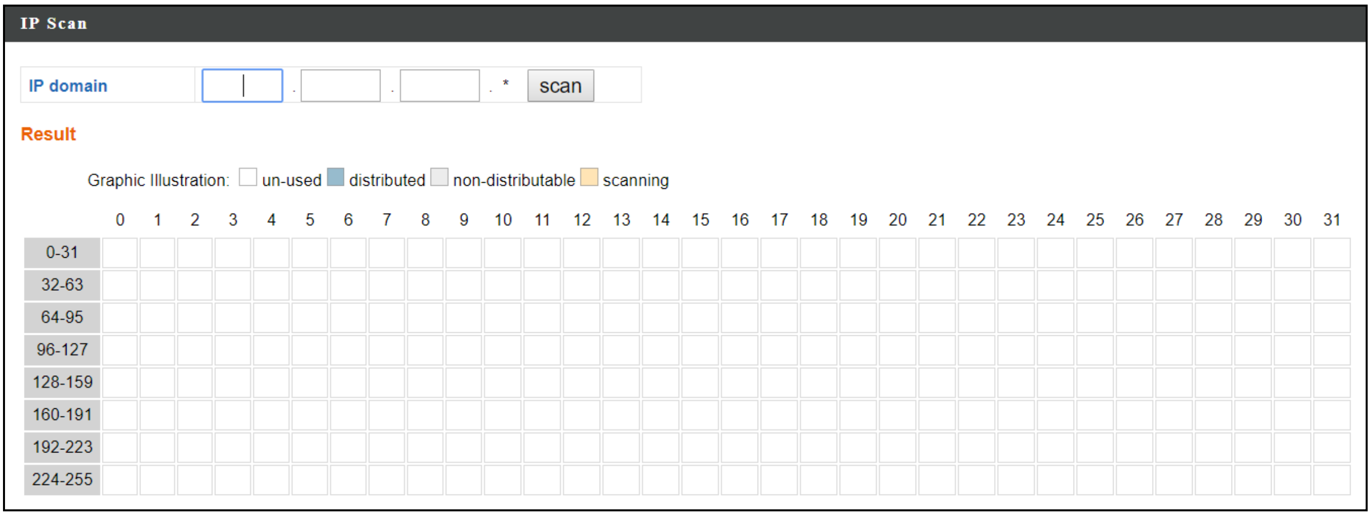
X-8-1-2 Trace Route

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



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

X-8-1-3 IP Scan



IP Scan

IP domain . . . * scan

Result

Graphic Illustration: □ un-used 🟦 distributed ▨ non-distributable 🟨 scanning

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0-31																																
32-63																																
64-95																																
96-127																																
128-159																																
160-191																																
192-223																																
224-255																																

XI Appendix

XI-1 Configuring your IP address

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

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

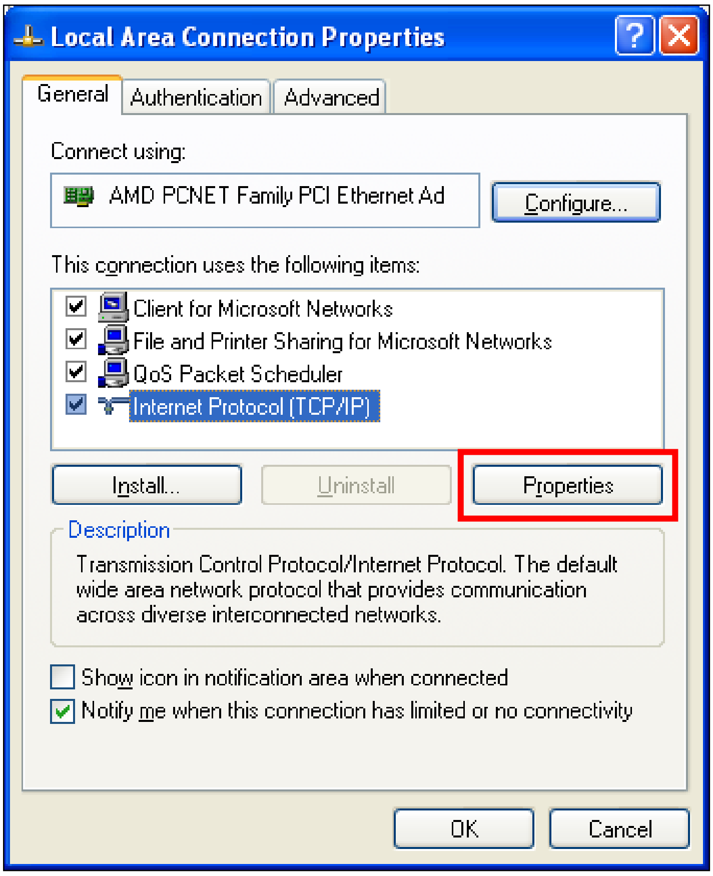
In the following examples we use the IP address **192.168.2.10** though you can use any IP address in the range **192.168.2.x (x = 3 – 254).**

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

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

XI-1-1 Windows XP

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



Connect using:

AMD PCNET Family PCI Ethernet Ad

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

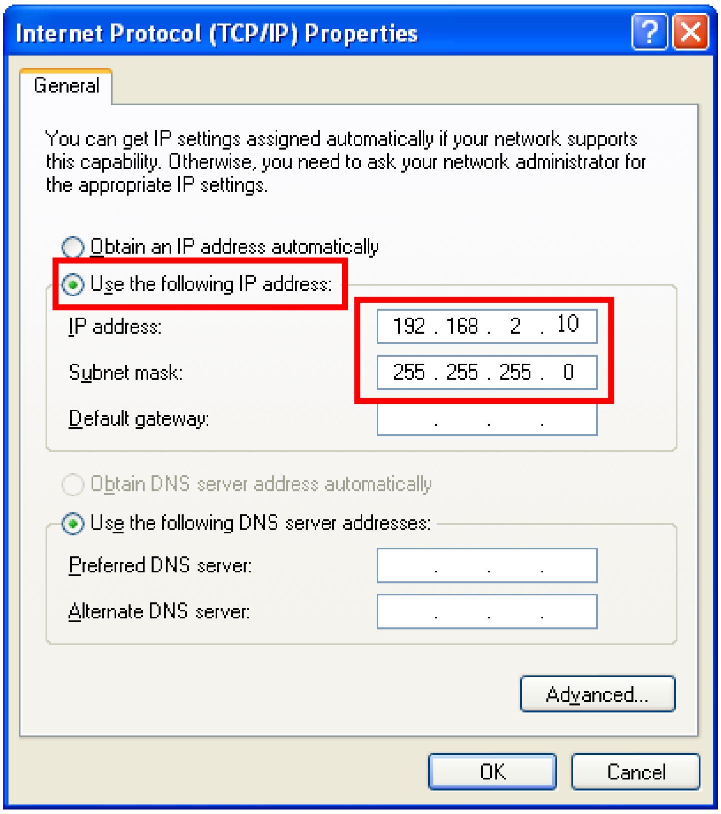
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

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

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click 'OK' when finished.



Internet Protocol (TCP/IP) Properties

General

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: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

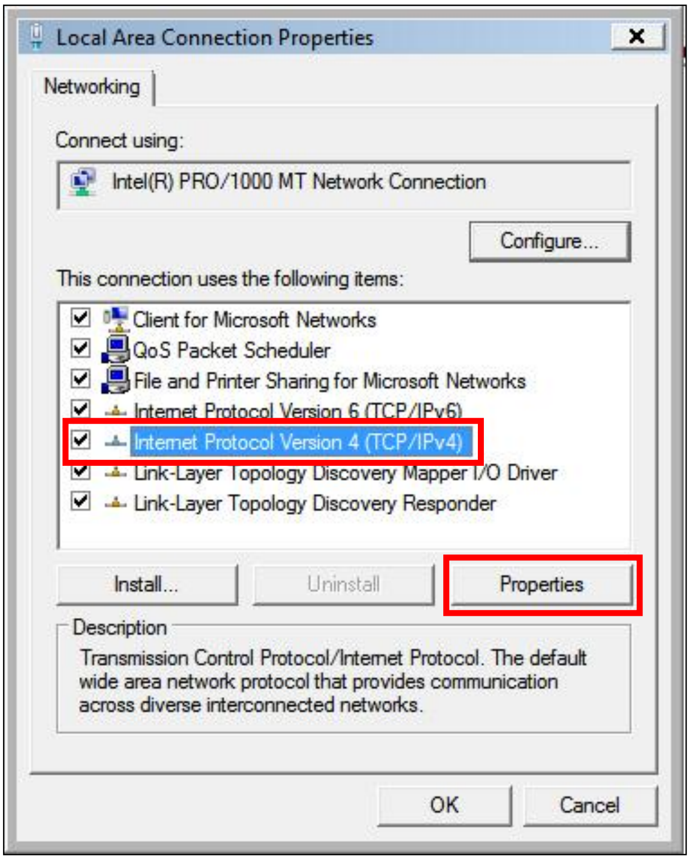
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

XI-1-2 Windows Vista

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



Local Area Connection Properties

Connect using:
Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

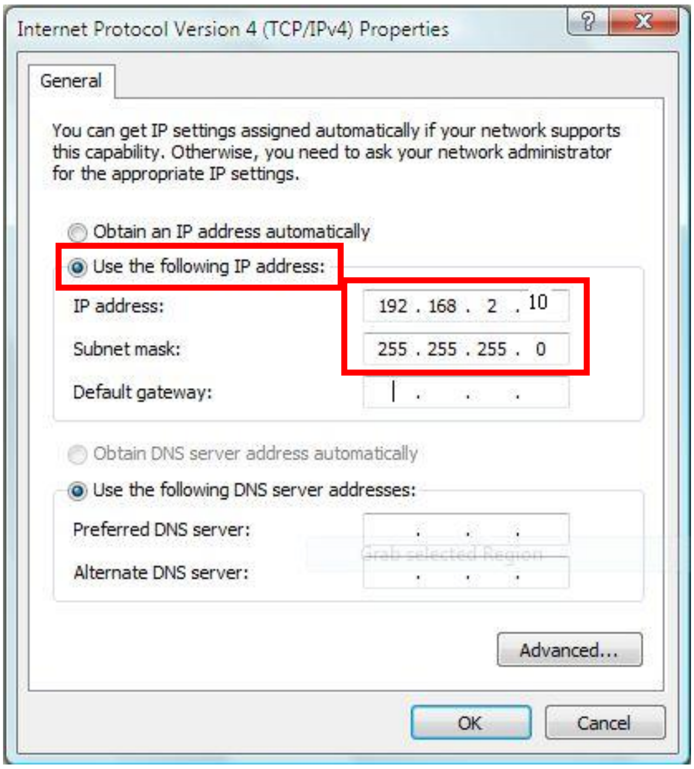
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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:

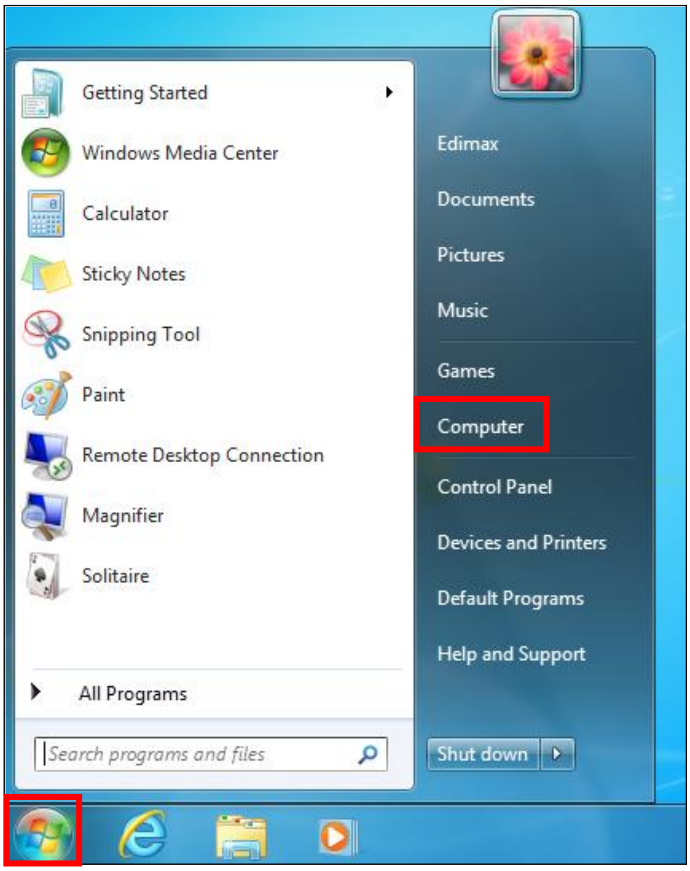
IP address: 192 . 168 . 2 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

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

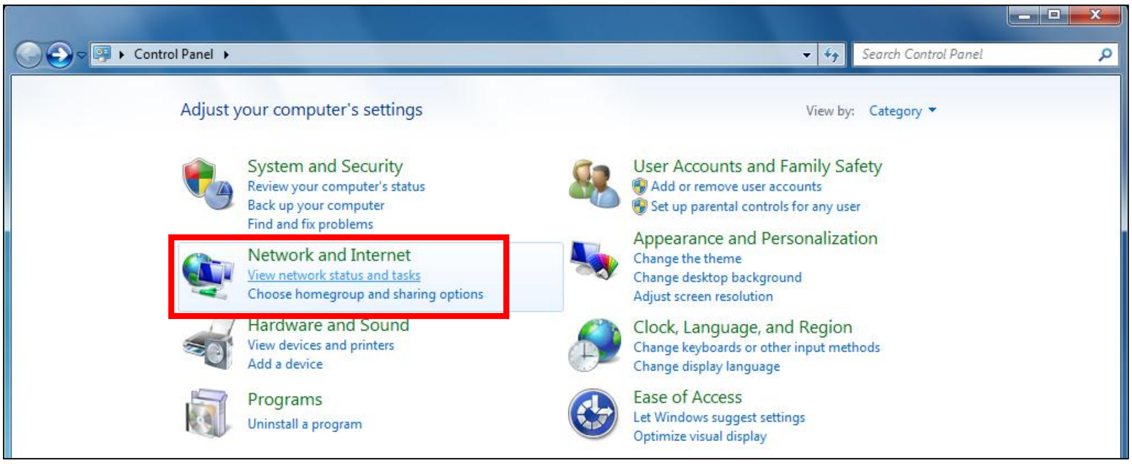
Preferred DNS server: . . .
Alternate DNS server: . . .

XI-1-3 Windows 7

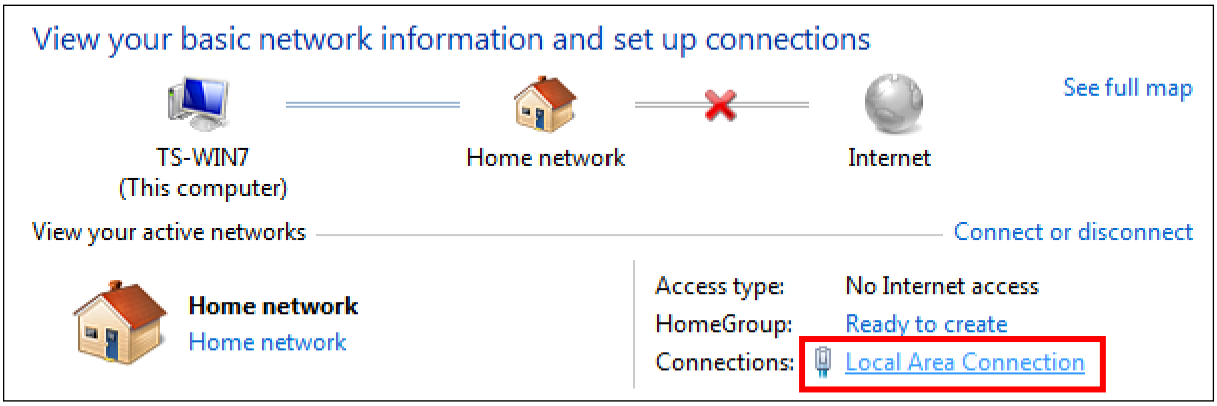
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



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


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3. Click “Local Area Connection”.



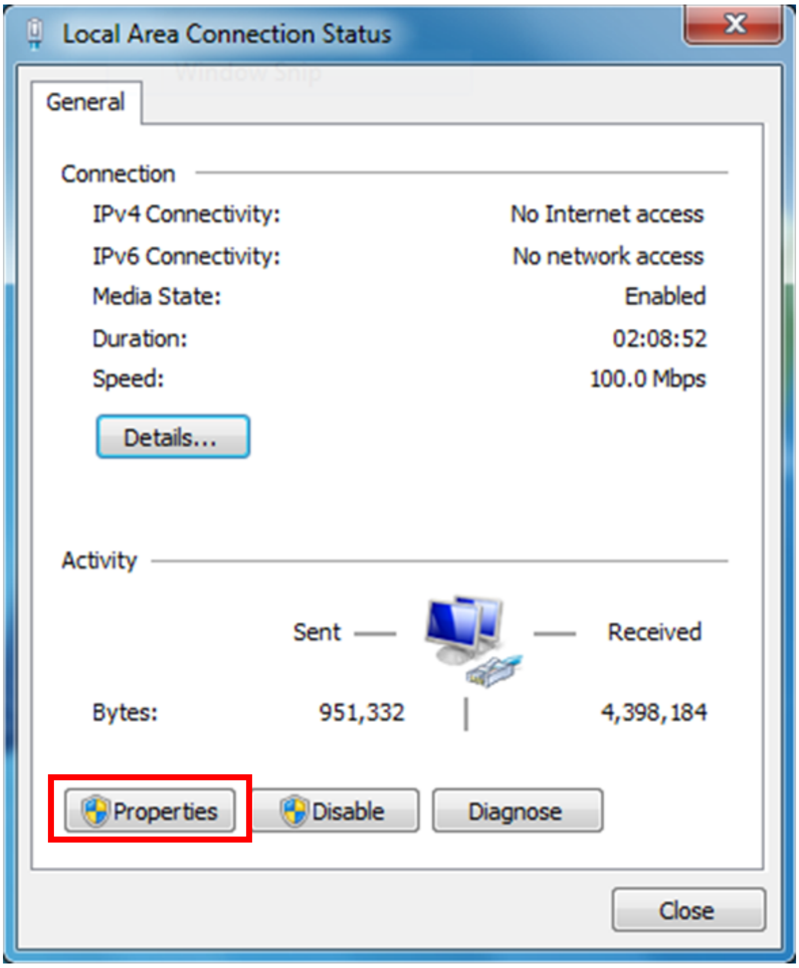
View your basic network information and set up connections

View your active networks

Home network
Home network

Access type: No Internet access
HomeGroup: Ready to create
Connections: Local Area Connection

4. Click “Properties”.



Local Area Connection Status

Connection

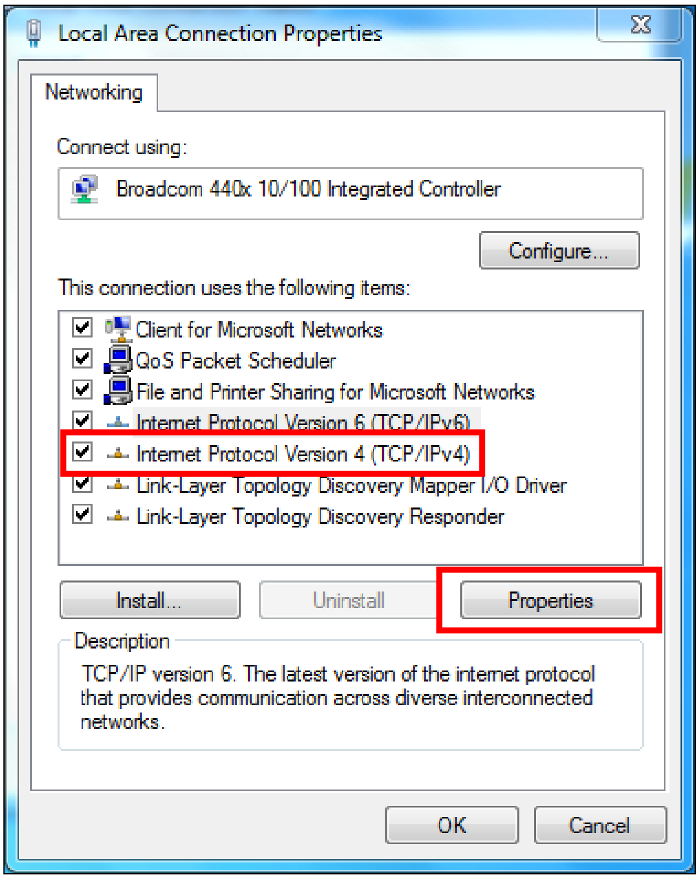
IPv4 Connectivity: No Internet access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 02:08:52
Speed: 100.0 Mbps

Activity

Sent — Received

Bytes: 951,332 | 4,398,184

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



Local Area Connection Properties

Networking

Connect using:

Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

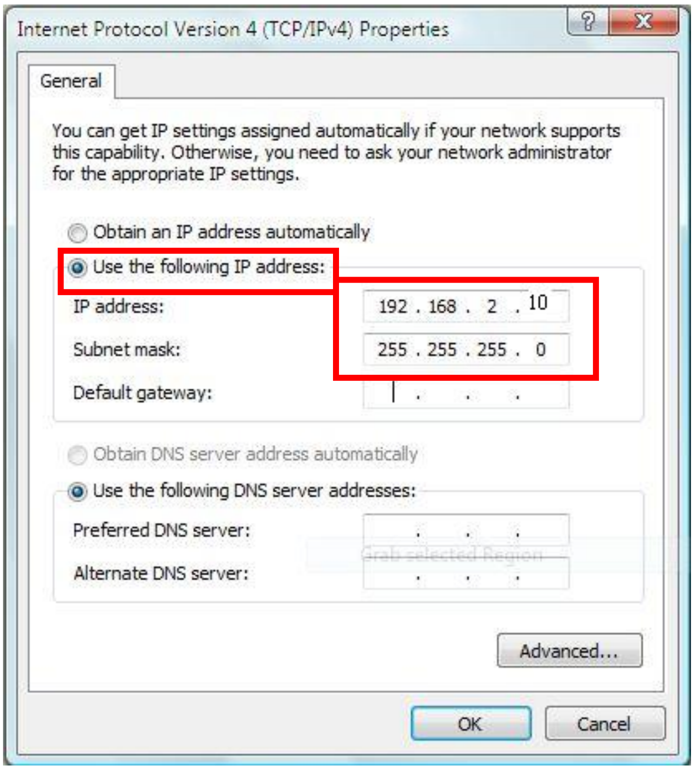
Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

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

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



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: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

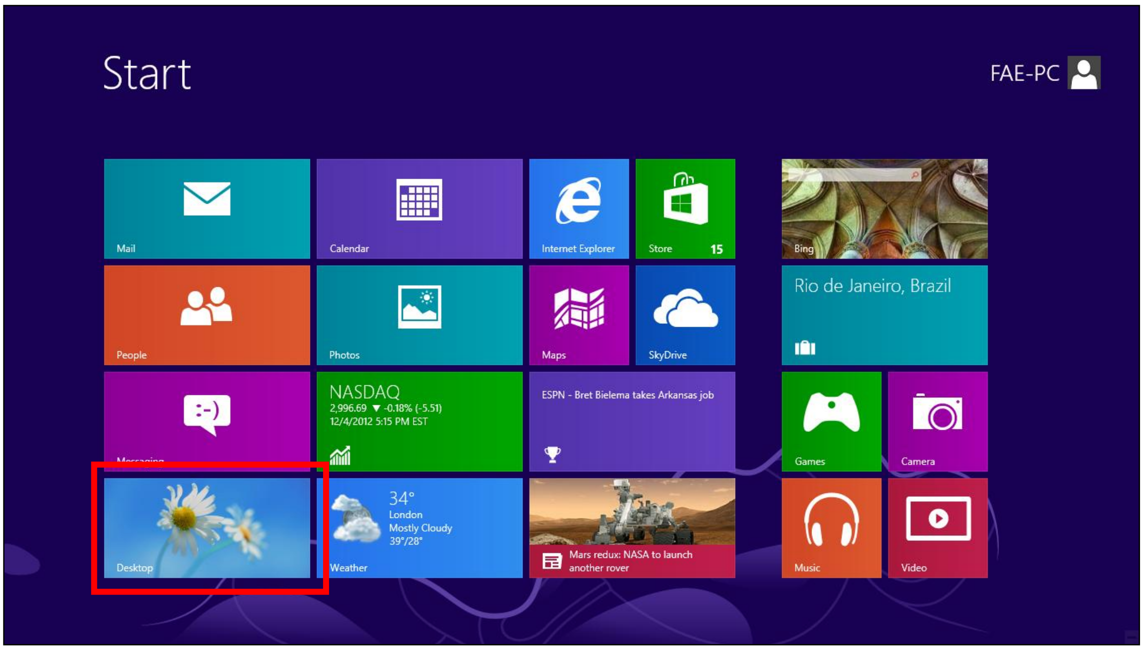
● Use the following DNS server addresses:

Preferred DNS server: . . .

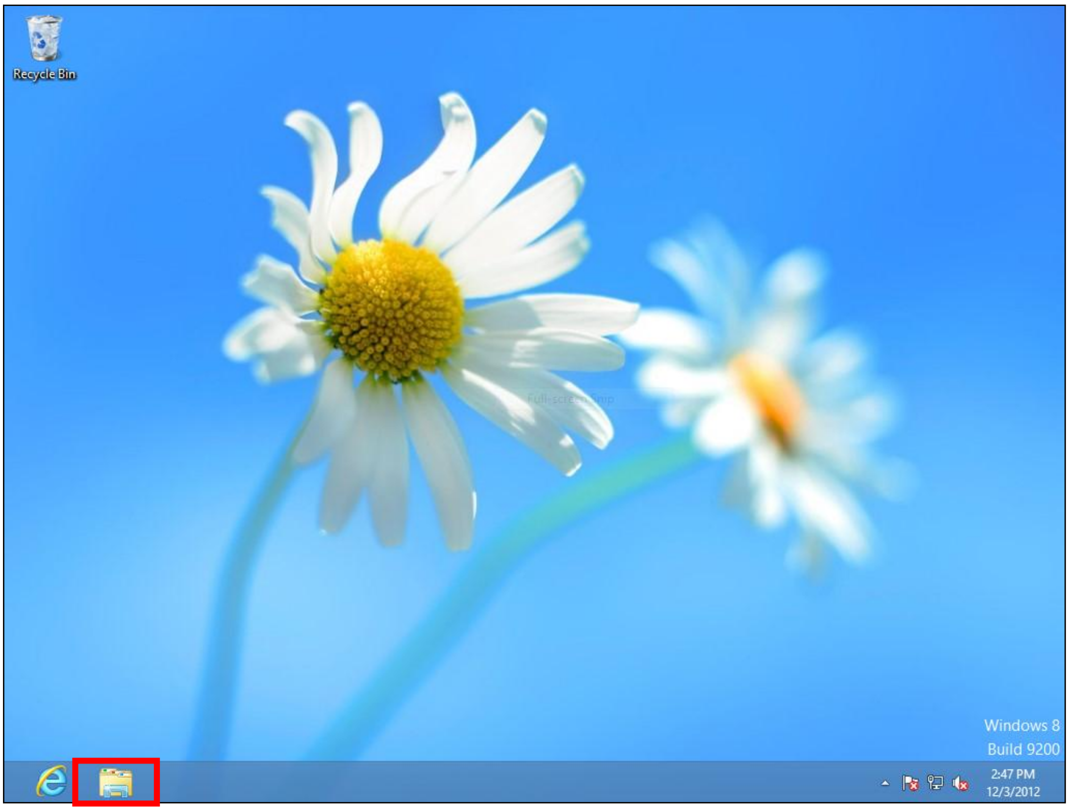
Alternate DNS server: . . .

XI-1-4 Windows 8

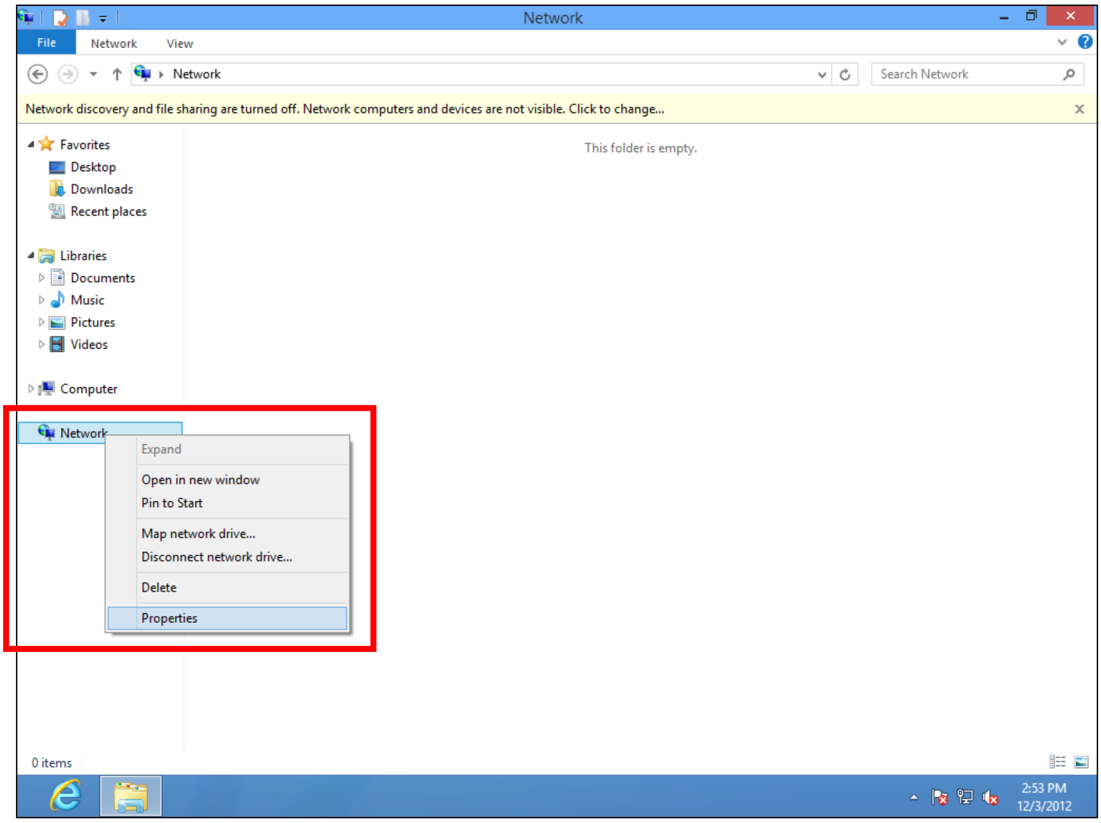
1. From the Windows 8 Start screen, switch to desktop mode by clicking the “Desktop” box.



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



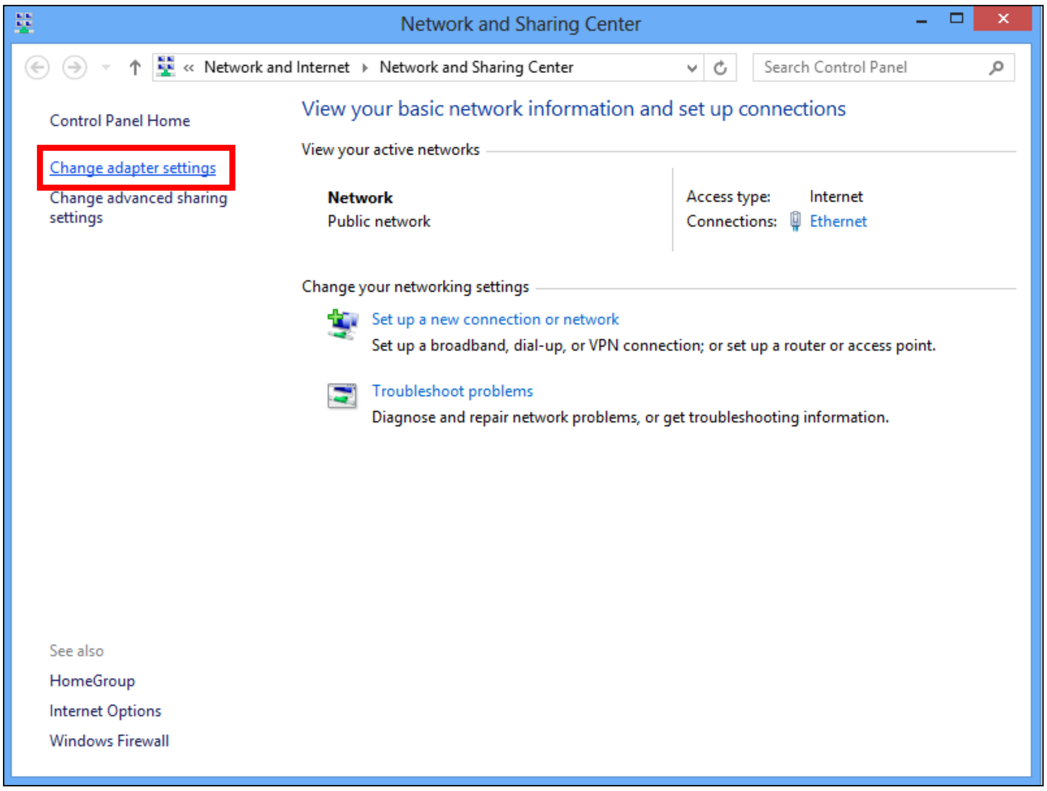
3. Right click "Network" and select "Properties".



Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...

This folder is empty.

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



View your basic network information and set up connections

View your active networks

Network
Public network

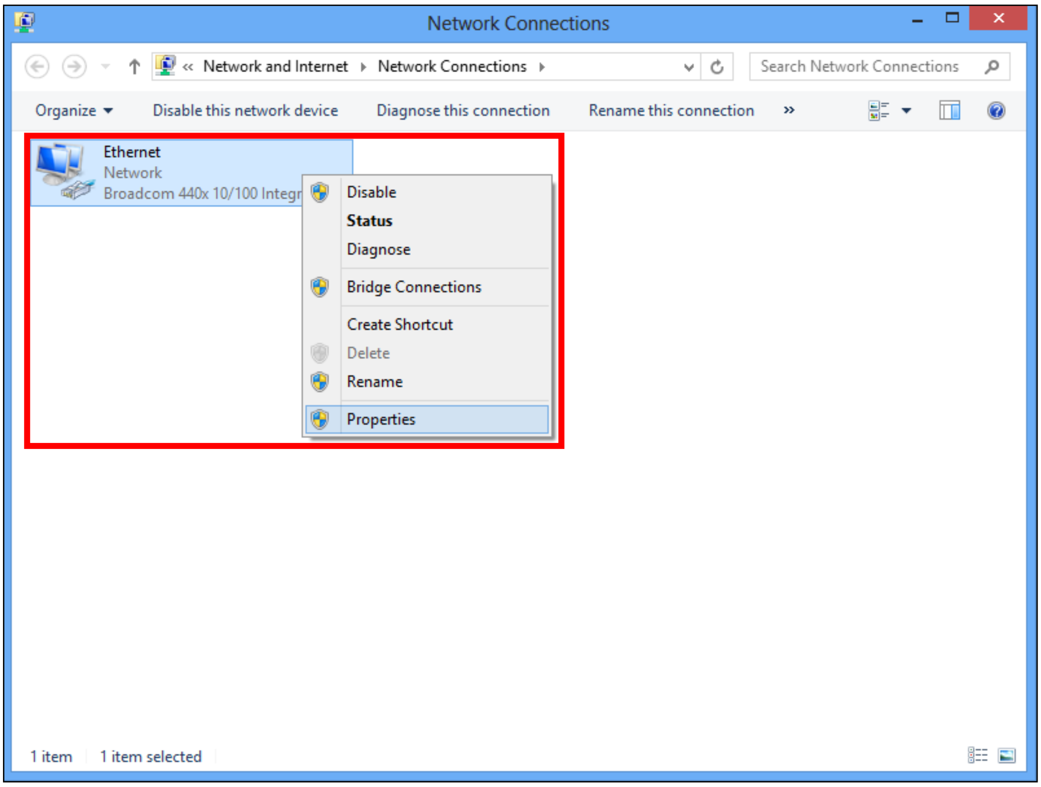
Access type: Internet
Connections: Ethernet

Change your networking settings

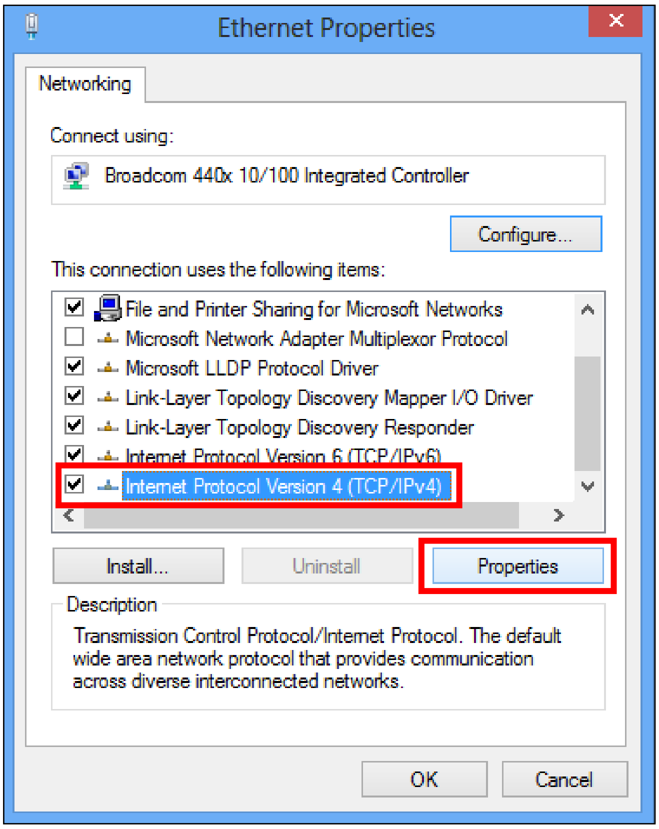
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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



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


Ethernet Properties

Networking

Connect using:

Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

- ☑ File and Printer Sharing for Microsoft Networks
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

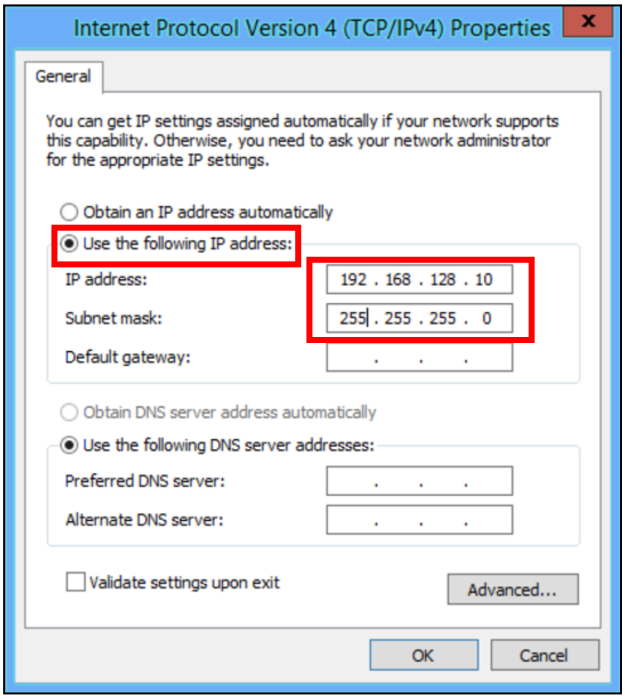
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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: 192 . 168 . 128 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

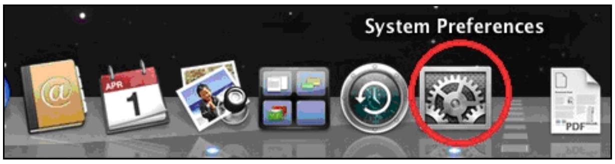
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

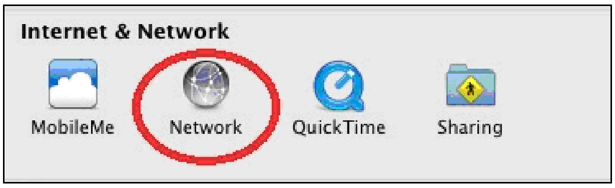
□ Validate settings upon exit

XI-1-5 Mac

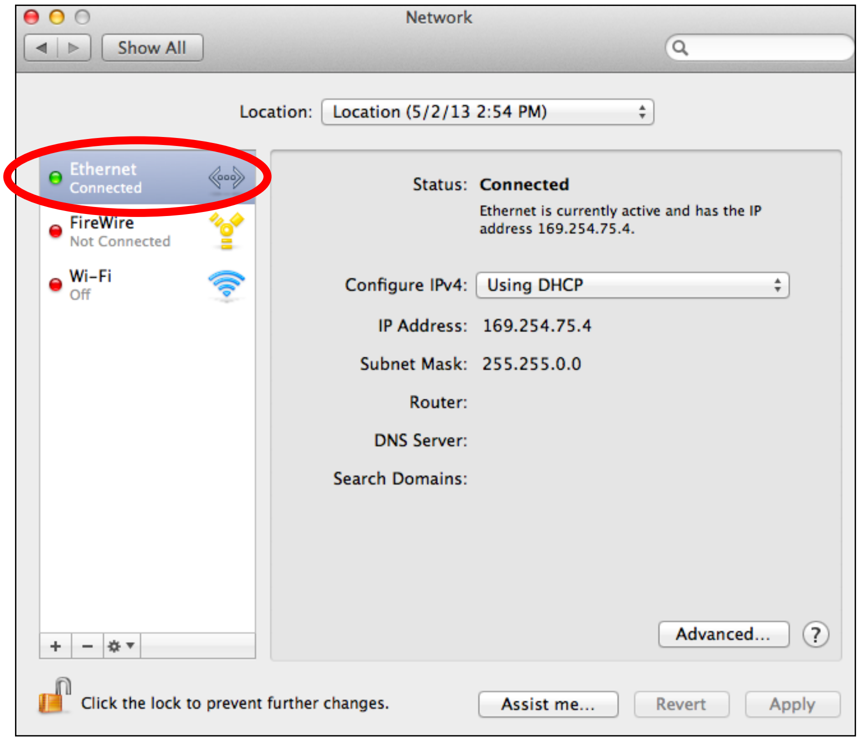
1. Have your Macintosh computer operate as usual, and click on "System Preferences"



2. In System Preferences, click on "Network".



3. Click on "Ethernet" in the left panel.



Location: Location (5/2/13 2:54 PM)

Ethernet Connected

FireWire Not Connected

Wi-Fi Off

Status: Connected

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: Using DHCP

IP Address: 169.254.75.4

Subnet Mask: 255.255.0.0

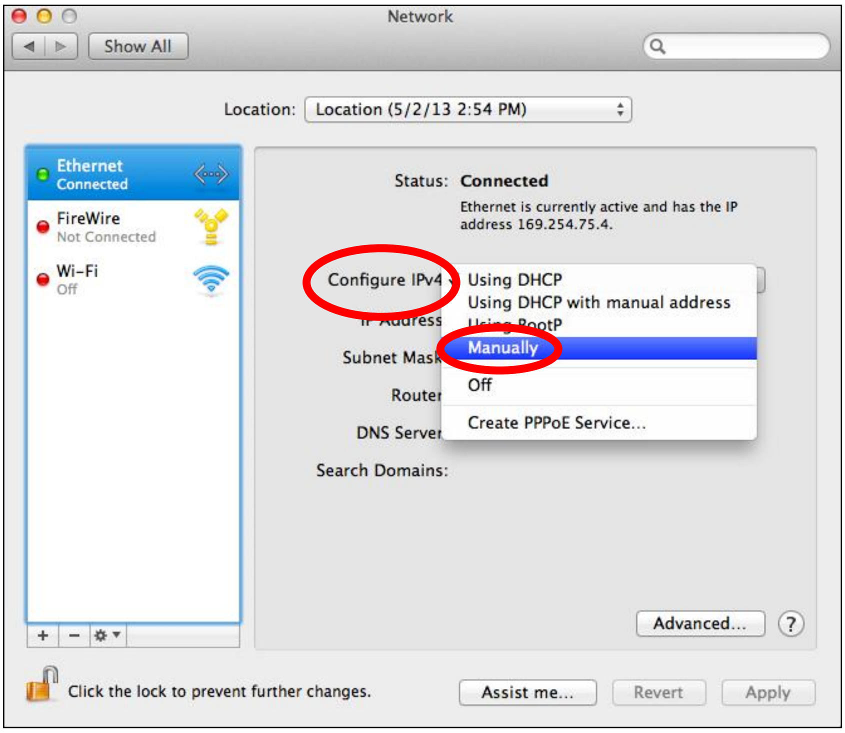
Router:

DNS Server:

Search Domains:

Click the lock to prevent further changes.

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

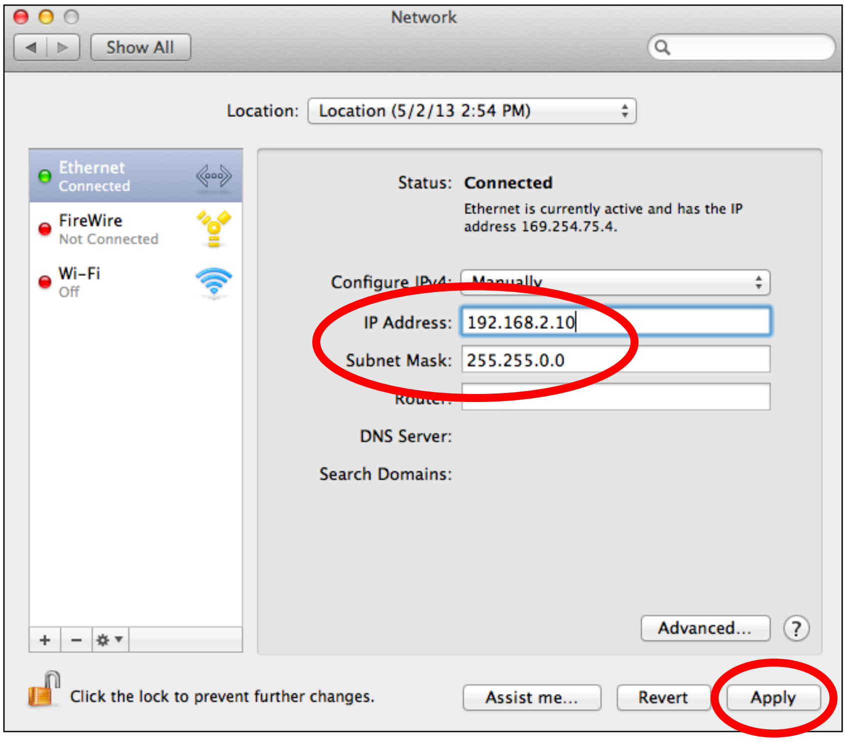


Location: Location (5/2/13 2:54 PM)

Status: **Connected**

Ethernet is currently active and has the IP address 169.254.75.4.

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



Location: Location (5/2/13 2:54 PM)

Status: **Connected**

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: Manually

IP Address: 192.168.2.10

Subnet Mask: 255.255.0.0

XI-2 Command Line Interface

Settings can also be configured using the Command Line Interface using the steps and commands shown below:

Edit Mode

1. Log on this product.

2. Enter the “edit start” command.
```
man$ edit start
```

3. The change of prompt from "man $" to "man [edit] $" indicates that Edit Mode is initiated.
```
man[edit]$
```

In Edit Mode, if more than one command is entered, you can reflect the settings using the following:

```
man[edit]$ wlan 5g band 11a11n brs 24m channel 40 bandwidth 40m+ex_lower_ch

man[edit]$ config timezone 50 man[edit]$ edit end
```

When you run the “edit end” command exit Edit Mode, the setting will be achieved.

XI-2-1 Config

config apname
Name / rename this product.
<Syntax of the command>

```
config apname (apname)
```

- **<Parameter>**
  (apname) – name of the product
- **<Default configuration>**
  AP (MAC address LAN side of this product)
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config apname enterprise-network

config basic_info show status
Show the configuration information setup.
<The syntax of the command>

```
config basic_info show status { admin|buzzer|date&time | led_settings | syslog_server }
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config basic_info show status date&time
  # config basic_info show status led_settings

config buzzer time

Set the sound time.

<The syntax of the command>

```
config buzzer time (time)
```

- **<Parameter>**
  (time) – Buzzer Time. (**1~300 sec**)
- **<Default configuration>**
  10
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config buzzer time 50

config date

Set the internal clock function of this product.

<The syntax of the command>

```
config date (yy) | (yyyy)/(mm)/(dd) [(HH):(MM):(SS) | (HH):(MM) ]
```

- **<Parameter>**

(yy) |(yyyy)	– Enter the two-digit or four-digit year setting.
(mm)	– Enter the two-digit month setting.
(dd)	– Enter the two-digit day setting.
(HH)	– Entered in 24-hour time display setting.
(MM)	– Enter the minute to set.
(SS)	– Enter the second to set.

- **<Default configuration>**
  Jan 1st 2012 00:00:00
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config date 2012/10/10 12:34:56

# config date 12/12/12 15:30

config firmware

Update the firmware of this product.

<The syntax of the command>

```
config firmware target tftp server (tftp-server) file (filename)
```

- **<Parameter>**
  (tftp-server) – Update the firmware from the TFTP server.
  (filename) – Set the name of the firmware file.
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config firmware target tftp server 192.168.2.100 file CAP1300.bin

config init

Return to the initial value all the parameters that are set in this product.

<The syntax of the command>

```
config init [force]
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config init
  # config init force

config led_setting

Set the LED of this product.

<The syntax of the command>

```
config led_setting {led} {on │ off}
```

- **<Parameter>**
  {led} – Enter **power** or **diag** to set either the power or diag LED
- **<Default configuration>**
  On
- **<Command mode>**
  Immediate Mode

- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config led_setting power on
  # config led_setting diag off

config management

Settings for the management interface of this product.

<The syntax of the command>

```
config management {protocol} {disable │ enable}
config management snmp version v1/v2 rcom (rcom) rwcom (rwcom)
config management snmp version v3
config management snmp trap {disable │ enable} trapcom (trapcom) ip (ipaddress)
```

- **<Parameter>**

{**protocol**}	**http**	Set http protocol
	Ssh	Set ssh protocol.
	snmp	Set snmp protocol.
	telnet	Set telnet protocol.
	https	Set https protocol.

  (rcom) Set the community name specified when the SNMP manager sends a "GET Request" for this product. (**6~32** characters)
  (rwcom) Set the community name specified when the SNMP manager to send a "SET Request" for this product. (**6~32** characters)

(v3_name)	Set the name of SNMP v3.
(v3_passwd)	Set the password of SNMP v3.
(trapcom)	Set the trap community name specified.
(ipaddress)	Set the trap community name specified.

- **<Default configuration>**
  enable : http
  enable : https
  enable: telnet
  disable : ssh
  disable : snmp
  rcom : public
  rwcom : private
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config management http disable
  # config management snmp enable
  # config management snmp version v1/v2 rcom edimaxrcom rwcom edimaxrwcom
  # config management snmp version v3 v3_name edimax v3_passwd edimax3047
  # config management snmp trap enable trapcom public ip 192.168.2.100

config ntp client

Set the NTP client function of this product.

<The syntax of the command>

```
config ntp client disable
config ntp client enable server (ntp-server) interval (ntp-interval)
```

- **<Parameter>**
  (ntp-server) Set the host name or IP address of the NTP server.
  (ntp-interval) Set the interval time to query the NTP server. (**1~24**)
- **<Default configuration>**
  Invalid
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config ntp client enable server clock.stdtime.gov.tw interval 24
  # config ntp client disable

config password

Set the password to log in to the setup screen of this product.

<The syntax of the command>

```
config password (username) (oldpassword) (newpassword)
```

- **<Parameter>**
  (username) Specifies the user name.
  (oldpassword) Enter the password that is currently set.
  (newpassword) Enter the password to the new one.
- **<Default configuration>**
  Administrator Name: admin
  Administrator Password: admin
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config password admin 1234 abc789

config reboot

Reboot of this product.

<The syntax of the command>

```
config reboot [force]
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**

Immediate Mode

- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config reboot
  # config reboot force

config restore

Restore the settings from the configuration file of this product.

<The syntax of the command>

config restore target tftp server (tftp-server) file (filename) [pass (password)] [force]

- **<Parameter>**
  tftp Restore configuration from the TFTP server.
  (tftp-server) Set the host name or IP address of the TFTP server.
  (filename) Set the name of the configuration file.
  (password) Set a password to protect the configuration file.
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config restore target tftp server 192.168.3.66 file edimax-cap1300.bin pass 123456

config save

Save the file to the current settings of this product.

<The syntax of the command>

config save target tftp server (tftp-server) file (filename) [pass (password)] [force]

- **<Parameter>**
  tftp Save the settings to TFTP server.
  (tftp-server) Set the host name or IP address of the TFTP server.
  (filename) Set the name of the configuration file.
  (password) Set a password to protect the configuration file.
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config save target tftp server 192.168.11.66 file edimax-cap1300.bin

config syslog clinet

Set the transfer function by the syslog protocol log information.

<The syntax of the command>

```
config syslog client enable server (servername)
config syslog client disable
```

- **<Parameter>**
  (servername) Set the host name or IP address of the syslog server.
- **<Default configuration>**
  Invalid
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  ```
  # config syslog client enable server 192.168.3.202
  # config syslog client disable
  ```

config timezone

Set time zone of the internal clock of this product.

<The syntax of the command>

```
config timezone {zone-name}
```

- **<Parameter>**
  {zone-name} Specify a time zone.
  The values that can be set are as follows:

  0 | (GMT-12:00) Eniwetok, Kwajalein, International Date Line West

  1 | (GMT-11:00) Midway Island, Samoa

  2 | (GMT-10:00) Hawaii

  3 | (GMT-09:00) Alaska

  4 | (GMT-08:00) Pacific Time (US & Canada); Tijuana

  5 | (GMT-07:00) Arizona

  6 | (GMT-07:00) Chihuahua, La Paz, Mazatian

  7 | (GMT-07:00) Mountain Time (US & Canada)

  8 | (GMT-06:00) Central America

  9 | (GMT-06:00) Central Time (US & Canada)

  10 | (GMT-06:00) Guadalajara, Mexico City, Monterrey

  11 | (GMT-06:00) Saskatchewan

  12 | (GMT-05:00) Bogota, Lima, Quito

  13 | (GMT-05:00) Eastern Time (US & Canada)

  14 | (GMT-05:00) Indiana (East)

  15 | (GMT-04:00) Atlantic Time (Canada)

  16 | (GMT-04:00) Caracas, La Paz

  17 | (GMT-04:00) Santiago

  18 | (GMT-03:00) Newfoundland

19 | (GMT-03:00) Brasilia

20 | (GMT-03:00) Buenos Aires, Georgetown

21 | (GMT-03:00) Greenland

22 | (GMT-02:00) Mid-Atlantic

23 | (GMT-01:00) Azores

24 | (GMT-01:00) Cape Verde Is.

25 | (GMT) Casablanca, Monrovia

26 | (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

27 | (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

28 | (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

29 | (GMT+01:00) Brussels, Copenhagen, Madrid, Paris

30 | (GMT+01:00) Sarajevo, Sofija, Warsaw, Zagreb, Skopje, Vilnius

31 | (GMT+01:00) West Central Africa

32 | (GMT+02:00) Athens, Istanbul, Minsk

33 | (GMT+02:00) Bucharest

34 | (GMT+02:00) Cairo

35 | (GMT+02:00) Harare, Pretoria

36 | (GMT+02:00) Helsinki, Riga, Tallinn

37 | (GMT+02:00) Jerusalem

38 | (GMT+03:00) Baghdad

39 | (GMT+03:00) Kuwait, Riyadh

40 | (GMT+03:00) Moscow, St. Petersburg, Volgograd

41 | (GMT+03:00) Nairobi

42 | (GMT+03:30) Tehran

43 | (GMT+04:00) Abu Dhabi, Muscat

44 | (GMT+04:00) Baku, Tbilisi, Yerevan

45 | (GMT+04:30) Kabul

46 | (GMT+05:00) Ekaterinburg

47 | (GMT+05:00) Islamabad, Karachi, Tashkent

48 | (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi

49 | (GMT+05:45) Kathmandu

50 | (GMT+06:00) Almaty, Novosibirsk

51 | (GMT+06:00) Astana, Dhaka

52 | (GMT+06:00) Sri, Jayawardenepura

53 | (GMT+06:30) Rangoon

54 | (GMT+07:00) Bangkok, Hanoi, Jakarta

55 | (GMT+07:00) Krasnoyarsk

56 | (GMT+08:00) Beijing, Hong Kong

57 | (GMT+08:00) Irkutsk, Ulaan Bataar

58 | (GMT+08:00) Kuala Lumpur, Singapore

59 | (GMT+08:00) Perth

60 | (GMT+08:00) Taipei, Taiwan
61 | (GMT+09:00) Osaka, Sapporo, Tokyo
62 | (GMT+09:00) Seoul
63 | (GMT+09:00) Yakutsk
64 | (GMT+09:00) Adelaide
65 | (GMT+09:30) Darwin
66 | (GMT+10:00) Brisbane
67 | (GMT+10:00) Canberra, Melbourne, Sydney
68 | (GMT+10:00) Guam, Port Moresby
69 | (GMT+10:00) Hobart
70 | (GMT+10:00) Vladivostok
71 | (GMT+11:00) Magadan, Solamon, New Caledonia
72 | (GMT+12:00) Auckland, Wllington
73 | (GMT+12:00) Fiji, Kamchatka, Marshall Is.

- **<Default configuration>**
  (GMT+09:00)Osaka, Sapporo,Tokyo
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config timezone 60

config username

Set the user name and password that is used to authenticate users of this product.

<The syntax of the command>

```
config username admin (username) (oldpassword) (newpassword)
```

- **<Parameter>**
  (username) Specifies the user name or administrator name.
  (oldpassword) Enter the password that is currently set.
  (newpassword) Enter the password to the new one.
- **<Default configuration>**
  Administrator Name: admin
  Administrator Password: admin
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # config username admin administrator 1234 1234

XI-2-2 LAN

lan ether port {pd／pse} 8023az

Enable or disable 802.3az for wired ports.

<The syntax of the command>

```
lan ether port {pd｜pse} 8023az {state}
```

- **<Parameter>**
  pd Set one of wired ports.
  pse Set two of wired ports.
  {state} **disable** Disable the ether port of 802.3az.
  enable Enable the ether port of 802.3az.
- **<Default configuration>**
  All valid
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ether port pse 8023az disable

lan ether port {pd／pse} link

Enable or disable the wired port.

<The syntax of the command>

```
lan ether port {pd｜pse} link {disable｜enable}
```

- **<Parameter>**
  pd Set one of wired ports.
  pse Set two of wired ports.
- **<Default configuration>**
  All valid
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ether port pse link disable

lan ether port {pd／pse} speed

Set the wired ports of PHY.

<The syntax of the command>

```
lan ether port {pd｜pse} speed speed auto flowctl {state}
lan ether port {pd｜pse} speed speed {speed} duplex {duplex} flowctl {state}
lan ether port {pd｜pse} speed speed 1000 duplex full flowctl {state}
```

- **<Parameter>**

  pd Set the one of wired ports.
  pse Set the two of wired ports.
  {speed} **10** Set to 10Mbps.
  100 Set to 100Mbps.
  {duplex} **full** Set to full duplex
  half Set to half duplex.
  {state} **disable** Disable the flow control.
  enable Enable the flow control.
- **<Default configuration>**

  speed:auto, flowctl:enable
  (The same configuration on all ports)
- **<Command mode>**

  Immediate Mode, Edit Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # lan ether port pd speed speed auto flowctl enable
  # lan ether port pse speed speed 100 duplex full flowctl disable
  # lan ether port pse speed speed 1000 duplex full flowctl enable

lan ether port {pd / pse} vlan mode

Set the wired ports of VLAN.

<The syntax of the command>

```
lan ether port {pd │ pse} vlan mode {tagged │ untagged} vlan (vlanid)
```

- **<Parameter>**

  pd Set the one of wired ports.
  pse Set the two of wired ports.
  (vlanid) Set the VLAN ID. (**1~4094**)
- **<Default configuration>**

  Vlanid : 1, untagged
  (The same configuration on all ports)
- **<Command mode>**

  Immediate Mode, Edit Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # lan ether port pd vlan mode untagged vlan 404
  # lan ether port pse vlan mode tagged vlan 403

lan ether show status

Show the status of the VLAN wired ports.

<The syntax of the command>

```
lan ether show status
```

- **<Parameter>**

  NA

- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ether show status

lan ip defaultgw

Set the default route, or manual setting of the default gateway that has the management subnet. (If you want to remove the default gateway address set, you enter the clear.)

<The syntax of the command>

```
lan ip defaultgw {clear │ (gateway)}
```

- **<Parameter>**
  (gateway) Enter the default gateway address.
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ip defaultgw clear
  # lan ip defaultgw 192.168.0.250

lan ip dhcp

Set the static ip to dhcp.

<The syntax of the command>

```
lan ip dhcp
```

- **<Parameter>**
  NA
- **<Default configuration>**
  DHCP
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ip dhcp

lan ip dns

Set the address of the DNS server for the subnet management.

<The syntax of the command>

```
lan ip dns {primary | secondary} { (dnsserver) | clear }
```

- **<Parameter>**
  (dnsserver) Enter the IP address of the DNS server.
- **<Default configuration>**
  DHCP
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ip dns primary 10.10.1.127
  # lan ip dns secondary clear

lan ip static

Set the DHCP to static IP.

<The syntax of the command>

```
lan ip static (ipaddress) subnet_mask (maskip)
```

- **<Parameter>**
  (ipaddress) Set the ip address of the lan.
  (maskip) Set the subnet-mask of the lan.
- **<Default configuration>**
  DHCP
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ip static 192.168.10.100 subnet_mask 255.255.255.0

lan ip show status

Show the status of IP settings.

<The syntax of the command>

```
lan ip show status
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ip show status

lan ip vlan

Set the VLAN ID of this product.

<The syntax of the command>

```
lan ip vlan (vlanid)
```

- **<Parameter>**
  (vlanid) Set the VLAN ID. (**1-4094**)
- **<Default configuration>**
  1
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # lan ip vlan 1

XI-2-3 Show

show status config admin

Show the username and advanced settings.

<The syntax of the command>

```
show status config admin
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status config admin

show status config buzzer

Show the sound time status.

<The syntax of the command>

```
show status config buzzer
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**

CAP1300

- **<Examples>**
  # show status config buzzer

### *show status config date&time*

Show the date and time.

<The syntax of the command>

```
show status config date&time.
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status config date&time

### *show status config led_settings*

Show the LED settings.

<The syntax of the command>

```
show status config led_settings
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status config led_settings

### *show status config syslog_server*

Show the status of syslog server.

<The syntax of the command>

```
show status config syslog_server
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode

- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status config syslog_server

show status maclist

Show the maclist information.

<The syntax of the command>

```
show status maclist
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status maclist

show status lan ether

Show the VLAN information.

<The syntax of the command>

```
show status lan ether
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status lan ether

show status lan ip

Show the IP information.

<The syntax of the command>

```
show status lan ip
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode

- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status lan ip

show status radius

Show the radius information.

<The syntax of the command>

show status radius

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status radius

show status system_info

Show the system information.

<The syntax of the command>

show status system_info

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status system_info

show status log

Show the system log information.

<The syntax of the command>

show status log

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**

Immediate Mode, Edit Mode, Reference Mode

- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status system_info

show status wlan {2.4g | 5g} advanced

Show the wireless advanced information.

<The syntax of the command>

```
show status wlan {2.4g | 5g} advanced
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan 2.4g advanced

show status wlan {2.4g / 5g} basic

Show the wireless information.

<The syntax of the command>

```
show status wlan {2.4g | 5g} basic
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan 2.4g basic

show status wlan {2.4g | 5g} clients

Show the status of wireless clients information.

<The syntax of the command>

```
show status wlan {2.4g | 5g} clients
```

- **<Parameter>**
  NA
- **<Default configuration>**

NA

- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan 2.4g clients

show status wlan {2.4g | 5g} security

Show the wireless security information.

<The syntax of the command>

```
show status wlan {2.4g | 5g} security
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan 2.4g security

show status wlan {2.4g | 5g} wds

Show the wireless wds information.

<The syntax of the command>

```
show status wlan {2.4g | 5g} wds
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan 2.4g wds

show status wlan monitor

Show the status of wireless monitor.

<The syntax of the command>

```
show status wlan monitor
```

- **<Parameter>**
  NA

- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan monitor

show status wlan wmm

Show the status of wireless QoS configuration.

<The syntax of the command>

```
show status wlan wmm
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan wmm

show status wlan wps

Show the status of wireless security WPS.

<The syntax of the command>

```
show status wlan wps
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # show status wlan wps

XI-2-4 Wlan

wlan {2.4g | 5g} 80211n_protect

Set the 802.11n protection.

<The syntax of the command>

```
wlan 5g 80211n_protect {state}
wlan 2.4g {protect} {state}
```

- **<Parameter>**

{protect}	**80211n_protect**	Set the 802.11n protection.
	80211g_protect	Set the 802.11g protection.
{state}	**disable**	Disable the 802.11n or 802.11g protection.
	enable	Enable the 802.11n or 802.11g protection.

- **<Default configuration>**
  Enable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 5g 80211n_protect enable
# wlan 2.4g 80211g_protect disable
```

wlan {2.4g | 5g} basic_info show status

Show the wireless information.

<The syntax of the command>

```
wlan {media} basic_info show status { advanced | basic | clients | security | wds }
```

- **<Parameter>**

{media}	**2.4g**	Show the wireless 802.11g information.
	5g	Show the wireless 802.11a information.

- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 2.4g basic_info show status advanced
# wlan 5g basic_info show status security
```

wlan {2.4g | 5g} beacon dtim

Configure the transmission interval of the DTIM.

<The syntax of the command>

```
wlan {media} beacon dtim (num)
```

- **<Parameter>**

{media}	**2.4g**	Set the interval between transmission of 802.11g.
	5g	Set the interval between transmission of 802.11a.
(num)	Set the transmission interval. (**1~255**)	

- **<Default configuration>**
  1
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g beacon dtim 100

wlan {2.4g | 5g} beacon interval

Configure the transmission interval of the beacon.

<The syntax of the command>

```
wlan {media} beacon interval (num)
```

- **<Parameter>**

{media}	**2.4g**	Configure the interval between transmission of 802.11g.
	5g	Configure the interval between transmission of 802.11a.
(num)	Set the transmission interval. (**20~1000** ms)	

- **<Default configuration>**
  100
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g beacon interval 200

wlan {2.4g | 5g} channel change_ch_if_STA_connected

Set the change channel function of this product. (The station is connected status.)

<The syntax of the command>

```
wlan {media} channel change_ch_if_STA_connect {disable | enable}
```

- **<Parameter>**

{media}	**2.4g**	Set the function enable or disable on 802.11g.
	5g	Set the function enable or disable on 802.11a.

- **<Default configuration>**
  Disable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 2.4g channel change_ch_if_STA_connect enable

### ***wlan {2.4g | 5g} channel checktime***

Set the channel check time.

<The syntax of the command>

```
wlan {media} channel checktime {period}
```

- **<Parameter>**

{media}	**2.4g**	Set the channel check time on 802.11g.
	5g	Set the channel check time on 802.11a.
{period}	**half_hr**	Set the half hour time to check channel.
	one_hr	Set the one hour time to check channel.
	two_hr	Set the two hours time to check channel.
	half_day	Set the half day time to check channel.
	one_day	Set the one day time to check channel.
	two_day	Set the two days time to check channel.

- **<Default configuration>**
  half hour
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g channel checktime one_hr

### ***wlan {2.4g | 5g} {disable | enable}***

Set the radio to enable or disable the wlan.

<The syntax of the command>

```
wlan {media} {state}
```

- **<Parameter>**

{media}	**2.4g**	Enable or disable the wlan of the 802.11g.
	5g	Enable or disable the wlan of the 802.11a.
{state}	**disable**	Disable the wlan.
	enable	Enable the wlan.

- **<Default configuration>**
  2.4g: disable

  5g: disable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g enable
  # wlan 2.4g enable

wlan {2.4g | 5g} fragmentthreshold

Set the fragment threshold.

<The syntax of the command>

```
wlan {media} fragmentthreshold (num)
```

- **<Parameter>**

{media}	**2.4g**	Enable or disable the wlan of the 802.11g.
	5g	Enable or disable the wlan of the 802.11a.
(num)	Set the threshold for the frame size of frame transmission to perform fragmentation. (**256~2346**)	

- **<Default configuration>**
  2.4g: 2346
  5g: 2346
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 5g fragmentthreshold 2345
# wlan 2.4g fragmentthreshold 2344
```

wlan {2.4g | 5g} keepalive

Set the keepalive interval terminal.

<The syntax of the command>

```
wlan {media} keepalive (num)
```

- **<Parameter>**

{media}	**2.4g**	Set the keepalive interval function of 802.11g terminal.
	5g	Set the keepalive interval function of 802.11a terminal.
(num)	Set the interval between sending keepalive. (**0~65535** seconds)	

- **<Default configuration>**
  60
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 5g keepalive 120
```

wlan {2.4g | 5g} gi

Set the guard interval.

<The syntax of the command>

```
wlan {media} gi {mode}
```

- **<Parameter>**

{media}	**2.4g**	Set the guard interval of 802.11g.
	5g	Set the guard interval of 802.11a.

{mode}	**short**	Set the guard interval to short.
	long	Set the guard interval to long.

- **<Default configuration>**
  short
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 2.4g gi long

wlan {2.4g | 5g} mrate

Configure the multicast or broadcast rate.

<The syntax of the command>

```
wlan {media} mrate {rate}
```

- **<Parameter>**

{media}	**2.4g**	Set the multicast / broadcast rate of 802.11g
	5g	Set the multicast / broadcast rate of 802.11a
{rate}	Set one of the following rates.	

  (1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, auto)
- **<Default configuration>**
  auto
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g mrate auto

wlan {2.4g | 5g} rtsthreshold

Set the RTS Threshold.

<The syntax of the command>

```
wlan {media} rtsthreshold (num)
```

- **<Parameter>**

{media}	**2.4g**	Set the RTS threshold of 802.11g
	5g	Set the RTS threshold of 802.11a
(num)	Set the threshold on the frame size you begin sending RTS / CTS. (**1~2347**)	

- **<Default configuration>**
  2347
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300

- **<Examples>**
  # wlan 5g rtsthreshold 1800

wlan {2.4g | 5g} ssid addsecurity

Configure additional authentication SSID.

<The syntax of the command>

<No additional authentication> **wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode none**
<Limited by the MAC address list> **wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode macfilter**
<MAC-RADIUS authentication> **wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode macradius { authmac | authpass (authpass) }**
<MAC address list + MAC-RADIUS authentication> **wlan {media} ssid addsecurity { ssidname (ssid) | ssidnum (ssidnum) } mode macradius+macfilter { authmac | authpass (authpass) }**

- **<Parameter>**

{media}	**2.4g**	Set the addsecurity of the SSID on 802.11g.
	5g	Set the addsecurity of the SSID on 802.11a.
(ssid)	Specify the SSID to be set.	
(ssidnum)	Specify the number of the SSID to be set.	
authmac	The MAC address as the password authentication MAC RADIUS.	
authpass	Set the password in the password authentication MAC RADIUS.	
(authpass)	Enter a shared secret.	

- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g ssid addsecurity ssidname edimax5g01-168801 mode none
  # wlan 2.4g ssid addsecurity ssidnum 1 mode macfilter
  # wlan 5g ssid addsecurity ssidname edimax5g01-168801 mode macradius authmac
  # wlan 2.4g ssid addsecurity ssidnum 2 mode macradius+macfilter authpass 12345678

wlan {2.4g | 5g} ssid create

Create the number of the SSID.

<The syntax of the command>

wlan {media} ssid create (num)

- **<Parameter>**

{media}	**2.4g**	Create the multi-SSID on 802.11g.

	5g	Create the multi-SSID on 802.11a.
(num)	Create the number of the SSID.(**1~5**)	

- **<Default configuration>**
  5g ssid number: 1
  2.4g ssid number: 1
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 2.4g ssid create 5

wlan {2.4g | 5g} ssid {disable | enable}

Enable or disable the SSID.

<The syntax of the command>

```
wlan {media} ssid {disable | enable} { ssidname (ssid) | ssidnum (ssidnum)}
```

- **<Parameter>**

{media}	**2.4g**	To enable or disable the SSID on 802.11g.
	5g	To enable or disable the SSID on 802.11a.
(ssid)	Specify the SSID to be set.	
(ssidnum)	Specify the number of the SSID to be set.	

- **<Default configuration>**
  Enable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 2.4g ssid disable ssidnum 2
  # wlan 5g ssid enable ssidname edimax5g01-168801

wlan {2.4g | 5g} ssid loadbalance

Set the loadbalance of the SSID.

<The syntax of the command>

```
wlan {media} ssid loadbalance { ssidname (ssid) | ssidnum (ssidnum)} limit (num)
```

- **<Parameter>**

{media}	**2.4g**	Set the loadbalance of the SSID on 802.11g.
	5g	Set the loadbalance of the SSID on 802.11a.
(ssid)	Specify the SSID to be set.	
(ssidnum)	Specify the number of the SSID to be set.	
(num)	Set the number of the loadbalance	

- **<Default configuration>**
  50

- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 2.4g ssid loadbalance ssidnum 2 limit 20
# wlan 5g ssid loadbalance ssidname edimax5g01-168801 limit 30
```

wlan {2.4g | 5g} ssid privacy

Set the privacy separator feature.

<The syntax of the command>

```
wlan {media} ssid privacy { ssidname (ssid) | ssidnum (ssidnum) } { station | ssid |
disable }
```

- **<Parameter>**

{media}	**2.4g**	Set the privacy separator feature on 802.11g.
	5g	Set the privacy separator feature on 802.11a.
(ssid)	Specify the SSID to be set.	
(ssidnum)	Specify the number of the SSID to be set.	
station	To prohibit communication between all wireless cordless handset in the device. (Between devices)	
ssid	Prohibit communication between different networks SSID.	
disable	Do not use the privacy separator feature.	

- **<Default configuration>**
  Disable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 2.4g ssid privacy ssidname edimax2g01-168800 station
# wlan 5g ssid privacy ssidnum 2 ssid
```

wlan {2.4g | 5g} ssid rename

Change the name of the SSID.

<The syntax of the command>

```
wlan {media} ssid rename {ssidname (ssid) | ssidnum (ssidnum)} (newssid)
```

- **<Parameter>**

{media}	**2.4g**	Change the name of the SSID on 802.11g.
	5g	Change the name of the SSID on 802.11a.
(ssid)	Specify the SSID to be changed.	
(ssidnum)	Specify the number of the SSID to change.	
(newssid)	Specify the SSID to set a new.	

- **<Default configuration>**

- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 2.4g ssid rename ssidname CAP1300-D6D5A0_G air_station_2.4g_2
  # wlan 5g ssid rename ssidnum 2 air_station_5g_2

wlan {2.4g | 5g} ssid security

Set the security of the SSID.

<The syntax of the command>

<No authenticate> **wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode no_auth**
<WEP authentication> **wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode wep length { 64 | 128 } keytype {ascii | hex} defaultkey (num_1-4) key (wepkey)**
<EAP authentication> **wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode eap length { 64 | 128 }**
<WPA-PSK authentication> **wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode { wpapsk|wpa2psk|wpa2mixedpsk } type {cipher} period (num) keytype {passpharse | hex} key (psk)**
<WPA-EAP EAP authentication> **wlan {media} ssid security {ssidname (ssid) | ssidnum (ssidnum)} mode { wpaeap|wpa2eap|wpa2mixedeap } type {cipher} period (num)**

- **<Parameter>**

{media}	**2.4g**	Set the security of the SSID on 802.11g.
	5g	Set the security of the SSID on 802.11a.
(ssid)	Specify the SSID to be set.	
(ssidnum)	Specify the number of the SSID to be set.	
(num_1-4)	Specify the encryption key number to be default key.(**1~4**)	
(wepkey)	Enter the WEP encryption key.	
	ascii	(key length of 64-bit for ascii are 5 characters) (key length of 128-bit for ascii are 13 characters)
	hex	(key length of 64-bit for hex are 10 characters) (key length of 128-bit for hex are 26 characters)
{cipher}	Specify one of the following encryption method.	
	aes	When security mode choose wpaeap/wpa2eap/wpamixedwap or wpapsk/pa2psk/wpamixedpsk, specify the AES encryption method.

tkip When security mode choose wpaeap or wpapsk, specify the TKIP encryption method.

mixed When security mode choose wpaeap/ wpamixedeap or wpapsk/wpamixedpsk, specify the TKIP and AES encryption method.

(num) Specify the period to key renewal. (**0~9999** minutes)

(psk) Enter the pre-shared key.
passphrase (Enter 8 characters)
hex (Enter 64 characters)

- **<Default configuration>**
  No authenticate
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 2.4g ssid security ssidname CAP1300-D6D5A0_G mode wep length 64 keytype ascii defaultkey 2 key 12345
# wlan 5g ssid security ssidname CAP1300-D6D5A0_G mode no_auth
# wlan 5g ssid security ssidnum 1 mode wpa2psk type aes period 60 keytype passphrase key 12345678
# wlan 2.4g ssid security ssidnum 2 mode wpaeap type mixed period 100
```

wlan {2.4g | 5g} ssid vlan

Set the VLAN ID.

<The syntax of the command>

```
wlan {media} ssid vlan {ssidname (ssid) | ssidnum (ssidnum)} vlanid (vlanid)
```

- **<Parameter>**

{media} **2.4g** Set the VLAN ID on 802.11g.
5g Set the VLAN ID on 802.11a.

(ssid) Specify the SSID to be set.

(ssidnum) Specify the number of the SSID to be set.

(vlanid) Set the VLAN ID. (**1~4094**)

- **<Default configuration>**
  1
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 2.4g ssid vlan ssidname edimax2g03-168800 vlanid 4000
# wlan 5g ssid vlan ssidnum 2 vlanid 2000
```

### *wlan {2.4g | 5g} txpower*

Configure the wireless transmit power.

<The syntax of the command>

```
wlan {media} txpower {power}
```

- **<Parameter>**

{**media**}	**2.4g**	Set the 802.11g radio transmit power.
	5g	Set the 802.11a radio transmit power.
{power}	In the range of 10-100%, and set the transmission power in 10%, 25%, 50%, 75%, 90%, 100%. (**10, 25, 50, 75, 90, 100**)	

- **<Default configuration>**
  100
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 2.4g txpower 50

### *wlan {2.4g | 5g} wds delete*

Remove the connection destination of the WDS.

<The syntax of the command>

```
wlan {media} wds delete all
wlan {media} wds delete num (peernum)
wlan {media} wds delete address (peeraddress)
```

- **<Parameter>**

{media}	**2.4g**	Delete a destination on 802.11g WDS.
	5g	Delete a destination on 802.11a WDS.
(peernum)	Specify the peer number of the MAC address to be deleted.	
(peeraddress)	Specify the MAC address to be deleted from the peer.	

- **<Default configuration>**
  NA
- **<Default configuration>**
  100
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  wlan 5g wds delete all
  wlan 2.4g wds delete address 12:22:33:44:55:66
  wlan 5g wds delete num 1

wlan {2.4g | 5g} wds mode

Set the wds mode.

<The syntax of the command>

```
wlan {media} wds mode {mode)}
```

- **<Parameter>**

{media}	**2.4g**	Set the WDS function on 802.11g.
	5g	Set the WDS function on 802.11a.
{mode}	**disable**	Disable the WDS
dedicated_wds		Set the WDS with WDS.
wds_with_ap	Set the WDS with AP.	

- **<Default configuration>**
  disable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g wds mode disable
  # wlan 2.4g wds mode wds_with_ap

wlan {2.4g | 5g} wds num

Add a connection destination of the WDS.

<The syntax of the command>

```
wlan {media} wds num (1-4) add (peeraddress) vlan_mode untagged vlan (vlanid)
{none|aes} key (psk)
wlan {media} wds num (1-4) add (peeraddress) vlan_mode tagged {none|aes} key (psk)
```

- **<Parameter>**

{media}	**2.4g**	Add a destination on 802.11g WDS.
	5g	Add a destination on 802.11a WDS.
(vlanid)	Set the VLAN ID. (**1~4094**)	
(peeraddress)	Set the MAC address of the destination.	
(psk)	encryption key of WDS.	

- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan 5g wds num 1 add 22:22:33:44:55:66 vlan_mode untagged vlan 1 none
  # wlan 2.4g wds num 2 add 12:22:33:44:55:66 vlan_mode tagged aes key 12345678

wlan 2.4g band

Set the operating mode of the radio and BasicRateSet on 802.11g, and configure the wireless channel.

<The syntax of the command>

```
wlan 2.4g band 11b brs { 2m | all } channel {ch} bandwidth 20m
wlan 2.4g band 11b brs { 2m | all } channel {auto-ch} bandwidth 20m
wlan 2.4g band { 11g | 11b11g} brs {brs} channel {ch} bandwidth 20m
wlan 2.4g band { 11g | 11b11g} brs {brs} channel {auto-ch} bandwidth 20m
wlan 2.4g band { 11g11n|11b11g11n} brs {brs} channel {ch} bandwidth {width}
wlan 2.4g band { 11g11n|11b11g11n} brs {brs} channel {auto-ch} bandwidth {autowidth}
```

- **<Parameter>**

{brs} Select from the following basic rate set

2m	Set to 1/2 Mbps
11m	Set to 1/2/5.5/11 Mbps
24m	Set to 1/2/5.5/6/11/12/24Mbps
All	Set all rate supported by current band

{ch} Set the wireless channel of 802.11g

Available channel number: **1-13**

{autoch} Set the wireless auto channel of 802.11g

Available channel number: **auto_1-11ch**, **auto_1-13ch**

{width} Set the wireless bandwidth of 802.11g

20m	Set to 20MHz normal mode
40m+ex_upper_ch	Set to 40MHz normal mode plus extra upper channel Available values: **1-9**
40m+ex_lower_ch	Set to 40MHz normal mode plus extra lower channel Available values: **5-13**
auto+ex_upper_ch	Set to auto mode plus extra upper channel Available values: **1-9**
auto+ex_lower_ch	Set to auto mode plus extra lower channel Available values: **5-13**

{autowidth}

20m	Set to 20MHz normal mode
40m	Set to 40MHz normal mode
auto	Set to auto mode

- **<Default configuration>**

Mode: 11b11g11n
BasicRateSet: 11m
Channel: auto_1-11ch
Bandwidth: 20m

- **<Command mode>**

Immediate Mode, Edit Mode

- **<Compatible Products>**

CAP1300

- **<Examples>**

```
# wlan 2.4g band 11b brs 2m channel 6 bandwidth 20m
# wlan 2.4g band 11b11g brs 24m channel 13 bandwidth 20m
# wlan 2.4g band 11b11g brs 11m channel auto_1-11ch bandwidth 20m
# wlan 2.4g band 11b11g11n brs all channel 10 bandwidth 40m+ex_lower_ch
```

wlan 2.4g conslot

Set the contention slot of 802.11g .

<The syntax of the command>

```
wlan 2.4g conslot {mode}
```

- **<Parameter>**

{mode}	**short**	Set the contention slot to short.
	long	Set the contention slot to long.

- **<Default configuration>**
  short
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 2.4g conslot long
```

wlan 2.4g preamble

Set the preamble of 802.11g

<The syntax of the command>

```
wlan 2.4g preamble {mode}
```

- **<Parameter>**

{mode}	**short**	Set the preamble to short.
	long	Set the preamble to long.

- **<Default configuration>**
  short
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# wlan 2.4g preamble long
```

wlan 5g band

Set the operating mode of the radio and BasicRateSet on 802.11a, and configure the wireless channel.

<The syntax of the command>

```
wlan 5g band 11a brs {brs} channel {ch} bandwidth 20m
wlan 5g band 11a brs {brs} channel {auto-ch} bandwidth 20m
wlan 5g band { 11a11n | 11a11n11ac } brs {brs} channel {ch} bandwidth {width}
wlan 5g band { 11a11n | 11a11n11ac } brs {brs} channel {auto-ch} bandwidth
```

```
{autowidth}
```

- **<Parameter>**

  {brs} Select from the following basic rate set

  24m Set to 6/12/24 Mbps

  All Set all rate supported by current band

  {ch} Set the wireless channel of 802.11a

  Available channel number: **36, 40, 44, 48, 52**, **56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140**

  {autoch} Set the wireless auto channel of 802.11a

  Available channel number: **w52, w52+w53, w52+w53+w56**

  {width} Set the wireless bandwidth of 802.11a

  20m Set to 20MHz normal mode

  40m+ex_upper_ch Set to 40MHz normal mode plus extra upper channel

  Available values: **36, 44, 52, 60, 100, 108, 116, 124, 132**

  40m+ex_lower_ch Set to 40MHz normal mode plus extra lower channel

  Available values: **40, 48, 56, 64, 104, 112, 120, 128, 136**

  80m Set to 80/40/20 MHz normal mode

  {autowidth} Set the wireless auto bandwidth of 802.11a

  20m Set to 20MHz normal mode

  40m Set to 40/20MHz normal mode

  80m Set to 80/40/20MHz normal mode
- **<Default configuration>**

  Mode: 5g11n

  BasicRateSet: 24m

  Channel: w52(auto)

  Bandwidth: 40m
- **<Command mode>**

  Immediate Mode, Edit Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

```
# wlan 5g band 11a brs all channel 40 bandwidth 20m
# wlan 5g band 11a brs all channel w52+w53 bandwidth 20m
# wlan 5g band 11a11n brs 24m channel 36 bandwidth 40m+ex_upper_ch
# wlan 5g band 11a11n brs 24m channel 140 bandwidth 20m
# wlan 5g band 11a11n brs 24m channel w52+w53+w56 bandwidth 40m
# wlan 5g band 11a11n11ac brs 24m channel 44 bandwidth 80m
```

wlan maclist add

Add the registration of MAC address restriction list.

<The syntax of the command>

```
wlan maclist add (macaddress)
```

- **<Parameter>**

  (macaddress) Enter the MAC address to be registered in the list.
- **<Default configuration>**

  NA
- **<Command mode>**

  Immediate Mode, Edit Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # wlan maclist add 12:22:33:44:55:66

wlan maclist delete

Remove the registration of MAC address restriction list.

<The syntax of the command>

```
wlan maclist delete { all | address (macaddress) | num (list-number) } [force]
```

- **<Parameter>**

  (macaddress) Specify the MAC address to be deleted from the list.

  (list-number) Specify the list number of the MAC address to be deleted.
- **<Default configuration>**

  NA
- **<Command mode>**

  Immediate Mode, Edit Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # wlan maclist delete all force

  # wlan maclist delete address 12:22:33:44:55:66 force

  # wlan maclist delete num 1 force

wlan maclist show status

Show the registration of MAC address restriction list.

<The syntax of the command>

```
wlan maclist show status
```

- **<Parameter>**

  NA
- **<Default configuration>**

  NA
- **<Command mode>**

  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # wlan maclist show status

wlan wmm {ap | sta}

Set the WMM parameters.

<The syntax of the command>

```
wlan wmm {ap | sta} {parameter} bk (value) be (value) vi (value) vo (value)
```

- **<Parameter>**

  (parameter) aifsn, cwmax, cwmain, txop

  (value) Set the parameter values. (according to the rules set input **1 < cwmin < 32767, 1 < cwmax <32767, 1 < aifsn < 15, 0 < txop <65535**)
- **<Default configuration>**

	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
		STA		
	CWMin	CWMax	AIFSN	TxOP
Back Ground	15	1023	7	0
Best Effort	15	1023	3	0
Video	7	15	2	94
Voice	3	7	2	47

- **<Command mode>**

  Immediate Mode, Edit Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # wlan wmm ap aifsn bk 10 be 10 vi 10 vo 10

  # wlan wmm sta txop bk 65535 be 65535 vi 65535 vo 65535

wlan wmm show status

Show the QoS configuration information.

<The syntax of the command>

```
wlan wmm show status
```

- **<Parameter>**

  NA
- **<Default configuration>**

  NA
- **<Command mode>**

  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # wlan wmm show status

### *wlan wmm qos*

Enable or disable the wmm qos.

<The syntax of the command>

```
wlan wmm qos {disable | enable}
```

- **<Parameter>**
  NA
- **<Default configuration>**
  disable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan wmm qos enable

### *wlan wps create pincode*

Generate the WPS PIN code.

<The syntax of the command>

```
wlan wps create pincode
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan wps create pincode

### *wlan wps {disable | enable}*

Enable or disable the WPS.

<The syntax of the command>

```
wlan wps {state}
```

- **<Parameter>**

{state}	**disable**	Disable WPS.
	enable	Enable WPS.

- **<Default configuration>**
  enable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan wps disable

wlan wps release

Release the WPS.

<The syntax of the command>

```
wlan wps release
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan wps release

wlan wps show status

Show the status of wlan security WPS.

<The syntax of the command>

```
wlan wps show status
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan wps show status

wlan wps start enrollee pincode

Enter the PIN code to start WPS.

<The syntax of the command>

```
wlan wps start encrollee pincode (pincode)
```

- **<Parameter>**
  (pincode) Enter the pincode (**0~99999999**).
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # wlan wps start enrollee pincode 14766084

wlan wps start push_button

Start the WPS by push the button.

<The syntax of the command>

```
wlan wps start push_button
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  ```
  # wlan wps start push_button
  ```

XI-2-5 Radius

radius {2.4g | 5g} {primary | secondary} enable server

Configure the enable built-in RADIUS server.

<The syntax of the command>

```
radius <media> {primary | secondary} enable server (host) secret (secret) authport
(port)
```

- **<Parameter>**

<media>	**2.4g**	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.
(host)	Specifies the IP address or domain name of the host.	
(secret)	Set the SharedSecret.	
(port)	Set the UDP port of the server used in RADIUS authentication protocol. (**1~65535**)	

- **<Default configuration>**
  primary port: 1812
  secondary port: 1812
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  ```
  # radius 2.4g primary enable server 192.168.2.123 secret 12345678 authport 1813
  ```

radius {2.4g | 5g} {primary | secondary} session_time

Set the RADIUS time to server communication will allow wireless devices.

<The syntax of the command>

```
radius <media> [primary | secondary] session_time (num)
```

- **<Parameter>**

<media>	**2.4g**	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.
(num)	Set the time of the session-time (**0~86400 sec**)	

- **<Default configuration>**
  primary session-timeout: 3600
  secondary session-timeout: 3600
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # radius 5g secondary session_time 4800

radius {2.4g | 5g} {primary | secondary} accounting

Enable or disable the RADIUS Accounting.
<The syntax of the command>

```
radius <media> {primary | secondary} accounting (state)
```

- **<Parameter>**

<media>	**2.4g**	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.
(state)	**enable**	Enable the RADIUS Accounting.
	disable	Disable the RADIUS Accounting.

- **<Default configuration>**
  enable
- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # radius 5g secondary accounting disable
  # radius 5g primary accounting disable

radius {2.4g | 5g} {primary | secondary} accounting_port

Set the UDP port of the server used in RADIUS Accounting protocol.
<The syntax of the command>

```
radius <media> {primary | secondary} accounting_port (port)
```

- **<Parameter>**

<media>	**2.4g**	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.
(port)	Set the UDP port.(**0~65535**)	

- **<Default configuration>**
  primary: 1813

secondary: 1813

- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# radius 5g secondary accounting_port 1814
# radius 2.4g primary accounting_port 1815
```

radius {2.4g | 5g} {primary | secondary} accounting_interval

Set the Accounting interval.

<The syntax of the command>

```
radius <media> {primary | secondary} accounting_interval (interval)
```

- **<Parameter>**

<media>	**2.4g**	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.
(interval)	Set the accounting interval (60 ~ 86400)	

- **<Default configuration>**

- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# radius 5g secondary accounting_interval 60
# radius 2.4g primary accounting_interval 86400
```

radius {2.4g | 5g} {primary | secondary} type [internal | external]

Set the radius type.

<The syntax of the command>

```
radius <media> {primary | secondary} type [internal|external]
```

- **<Parameter>**

<media>	**2.4g**	Set the radius server of 802.11g.
	5g	Set the radius server of 802.11a.

- **<Default configuration>**

- **<Command mode>**
  Immediate Mode, Edit Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**

```
# radius 5g primary type external
# radius 2.4g primary type internal
```

radius admin add

Add the radius user accounts.

<The syntax of the command>

```
radius admin add (username) (password)
```

- **<Parameter>**

  (username) username of the radius account

  (password) password of the radius account
- **<Default configuration>**

  NA
- **<Command mode>**

  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # radius admin add edimax 1234

radius admin delete

delete the radius user accounts.

<The syntax of the command>

```
radius admin delete all
radius admin delete num (list_number)
```

- **<Parameter>**

  (list_number) number of the username list
- **<Default configuration>**

  NA
- **<Command mode>**

  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**

  CAP1300
- **<Examples>**

  # radius admin delete all

  # radius admin delete num 2

radius internal {disable | enable}

enable or disable the internal radius.

<The syntax of the command>

```
radius internal enable
```

- **<Parameter>**

  NA
- **<Default configuration>**

  Disable
- **<Command mode>**

  Immediate Mode, Edit Mode, Reference Mode

- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # radius internal disable
  # radius internal enable

radius internal session_timeout

Set the internal RADIUS time to server communication will allow wireless devices.

<The syntax of the command>

```
radius internal session_timeout (sec)
```

- **<Parameter>**
  (sec) Set the time of the session-timeout (**0~86400 sec**)
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # radius internal session_timeout 86400

radius internal shared_key

Set the shared key of internal RADIUS server.

<The syntax of the command>

```
radius internal shared_key (key)
```

- **<Parameter>**
  (key) Set the shared key
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # radius internal shared_key 1234

radius internal termination_action [not_reauth | not_send | reauth]

Set the termination action to internal RADIUS server.

<The syntax of the command>

```
radius internal termination_action [not_reauth | not_send | reauth]
```

- **<Parameter>**
  NA
- **<Default configuration>**
  Not-Reauthenication

- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # radius internal termination_action not_reauth

radius show status

Show the radius information.

<The syntax of the command>

```
radius show status
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode, Edit Mode, Reference Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # radius show status

XI-2-6 Exit

exit

Quit the CLI.

<The syntax of the command>

```
exit
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # exit

XI-2-7 Quit

quit

Quit the CLI.

<The syntax of the command>

```
quit
```

- **<Parameter>**
  NA
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # quit

XI-2-8 Command

Command

Upload the cli command from tftp server

<The syntax of the command>

```
Command tftp_server (tftp-server) file (filename)
```

- **<Parameter>**

  (tftp-server) Update the Command from the TFTP server.

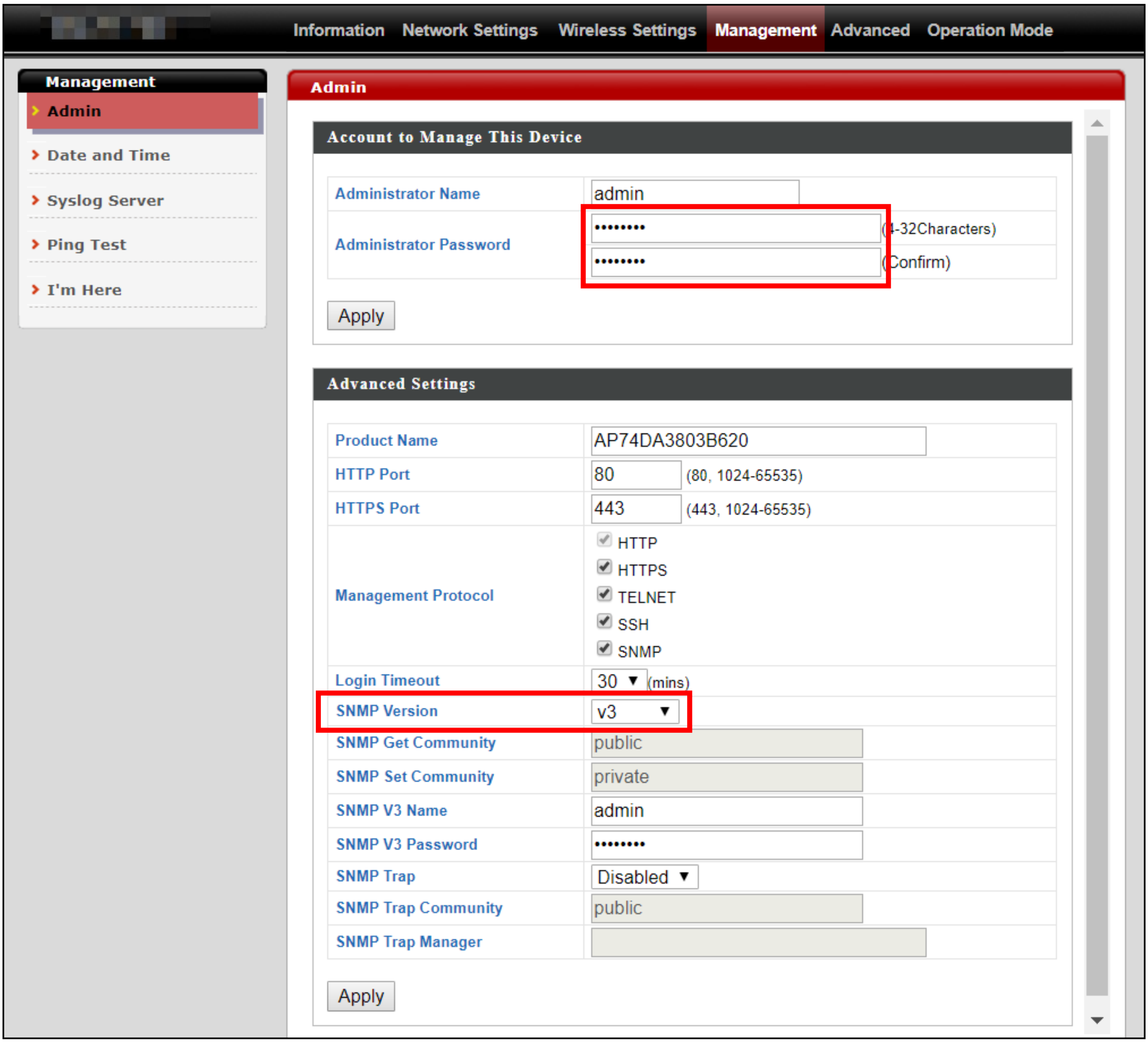
  (filename) Set the name of the Command file.
- **<Default configuration>**
  NA
- **<Command mode>**
  Immediate Mode
- **<Compatible Products>**
  CAP1300
- **<Examples>**
  # Command tftp_server 192.168.2.100 file command.ext

XI-3 Setting AP via ManageEngine MibBrowser with SNMPv3 - Example

XI-3-1 Setting in Web

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

2. SNMP Version: V3



Account to Manage This Device

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

Apply

Advanced Settings

Product Name	AP74DA3803B620
HTTP Port	80 (80, 1024-65535)
HTTPS Port	443 (443, 1024-65535)
Management Protocol	☑ HTTP ☑ HTTPS ☑ TELNET ☑ SSH ☑ SNMP
Login Timeout	30 ▼ (mins)
SNMP Version	v3 ▼
SNMP Get Community	public
SNMP Set Community	private
SNMP V3 Name	admin
SNMP V3 Password	••••••••
SNMP Trap	Disabled ▼
SNMP Trap Community	public
SNMP Trap Manager	

Apply

XI-3-2 Setting Rule

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

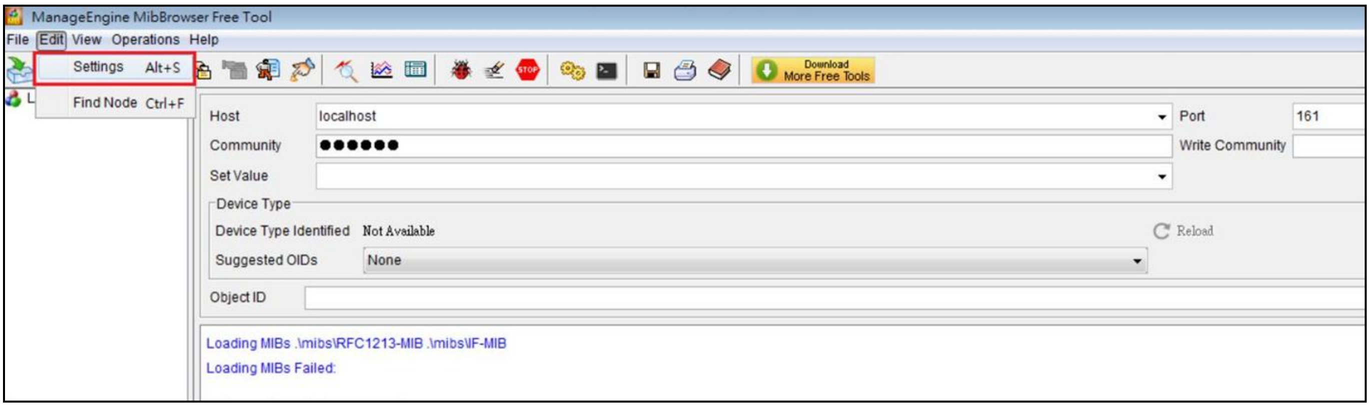
Example: Basic Wireless Settings	Settings
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.3.3 i 2	Auto Channel Disable
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.2.3 i 3	11b/g/n: band
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.4.3 i 7	7: channel
snmpset STRING 192.168.2.2 1.3.6.1.4.1.3822.2000.1.6.3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

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

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

XI-3-3 Setting in ManageEngine MibBrowser

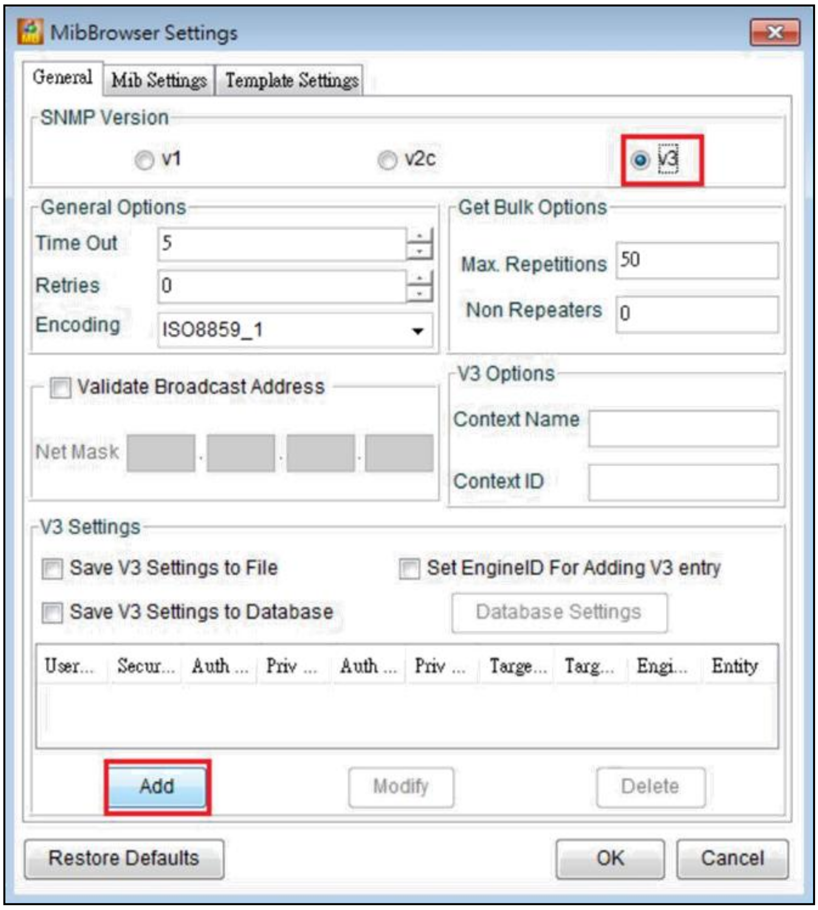
1. Set the version of SNMP



Host: localhost
Port: 161
Community: ●●●●●●
Write Community:
Set Value:
Device Type
Device Type Identified: Not Available
Suggested OIDs: None
Object ID:

Loading MIBs .\mibs\RFC1213-MIB .\mibs\IF-MIB
Loading MIBs Failed:

Figure 1 Step 1:Edit → Settings



MibBrowser Settings

SNMP Version: ○ v1 ○ v2c ● v3

General Options

Time Out: 5

Retries: 0

Encoding: ISO8859_1

Get Bulk Options

Max. Repetitions: 50

Non Repeaters: 0

□ Validate Broadcast Address

Net Mask

V3 Options

Context Name

Context ID

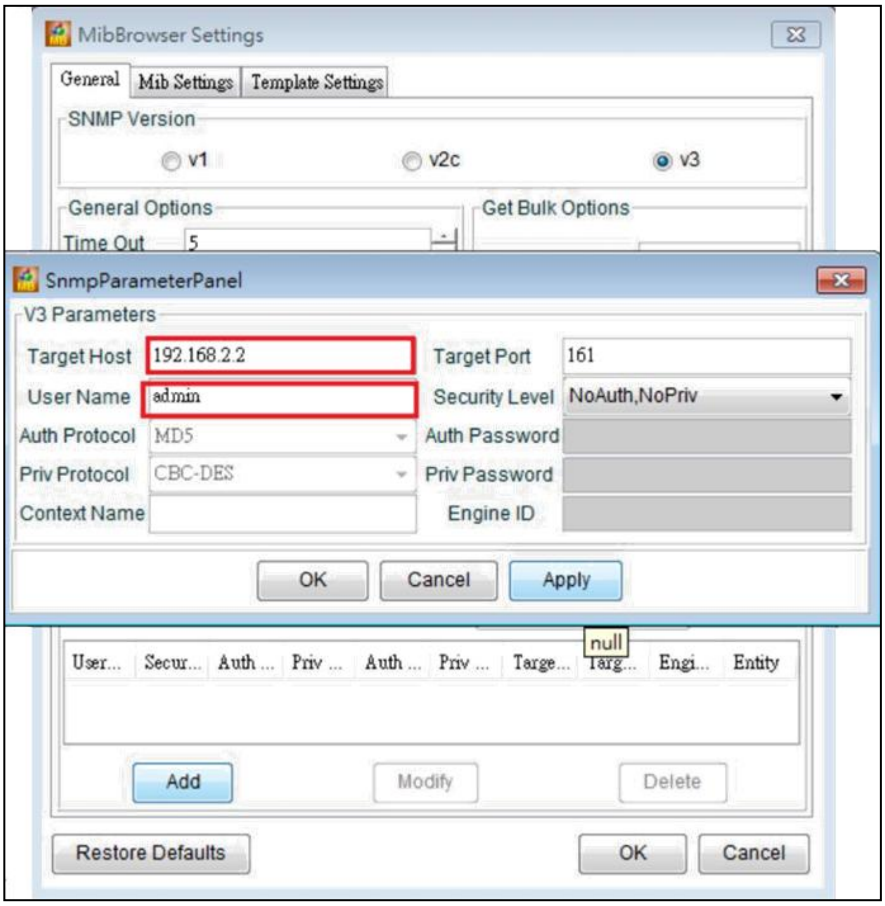
V3 Settings

□ Save V3 Settings to File

□ Set EngineID For Adding V3 entry

□ Save V3 Settings to Database

Figure 2 Step 2: Check v3 and click Add



SnmpParameterPanel

V3 Parameters

Target Host: 192.168.2.2

Target Port: 161

User Name: admin

Security Level: NoAuth,NoPriv

Auth Protocol: MD5

Auth Password

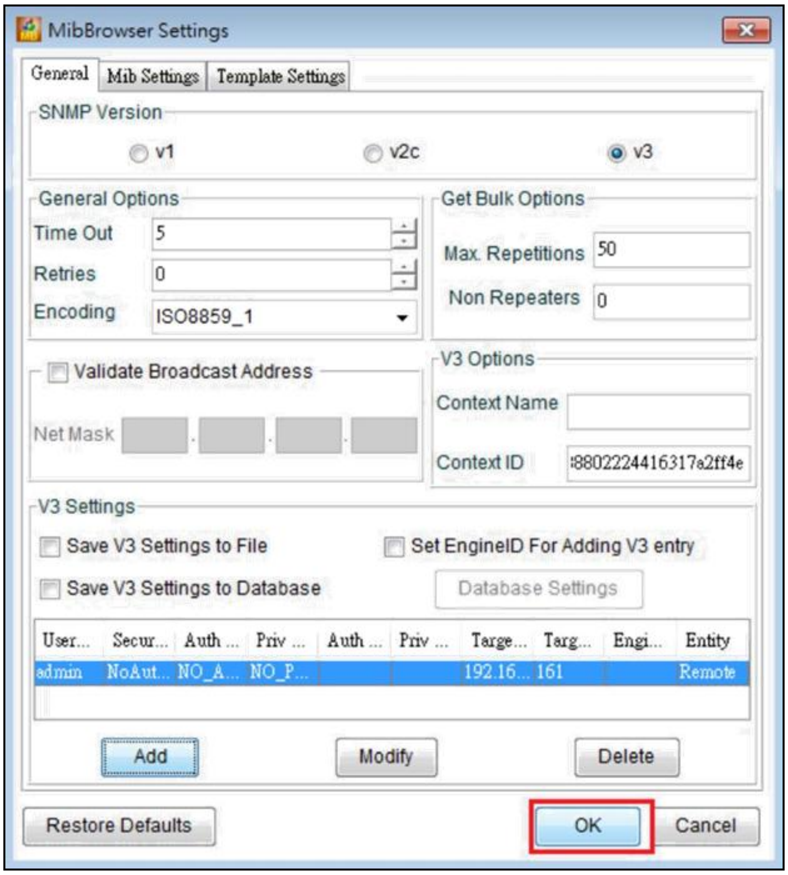
Priv Protocol: CBC-DES

Priv Password

Context Name

Engine ID

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



SNMP Version: ○ v1 ○ v2c ● v3

General Options

Time Out: 5

Retries: 0

Encoding: ISO8859_1

Get Bulk Options

Max. Repetitions: 50

Non Repeaters: 0

V3 Options

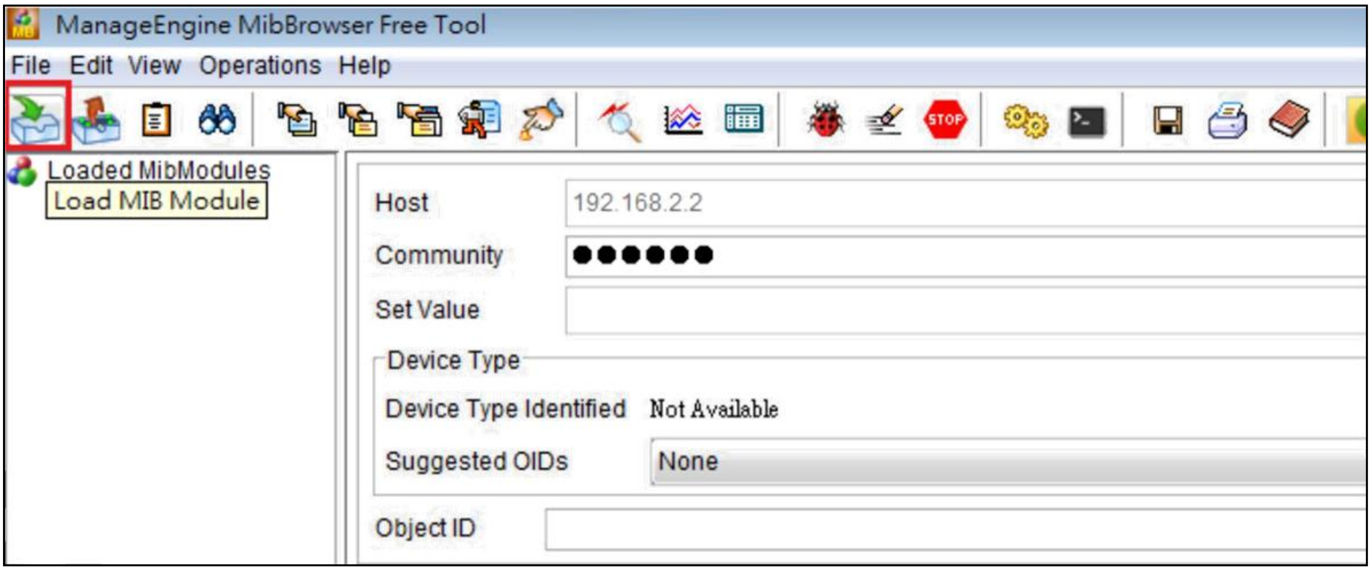
Context Name:

Context ID: :8802224416317a2ff4e

User...	Secur...	Auth ...	Priv ...	Auth ...	Priv ...	Targe...	Targ...	Engi...	Entity
admin	NoAut...	NO_A...	NO_P...			192.16...	161		Remote

Figure 4 Step 4: Click OK

2. Load MIB Module



Host: 192.168.2.2

Community: ●●●●●●●

Set Value:

Device Type

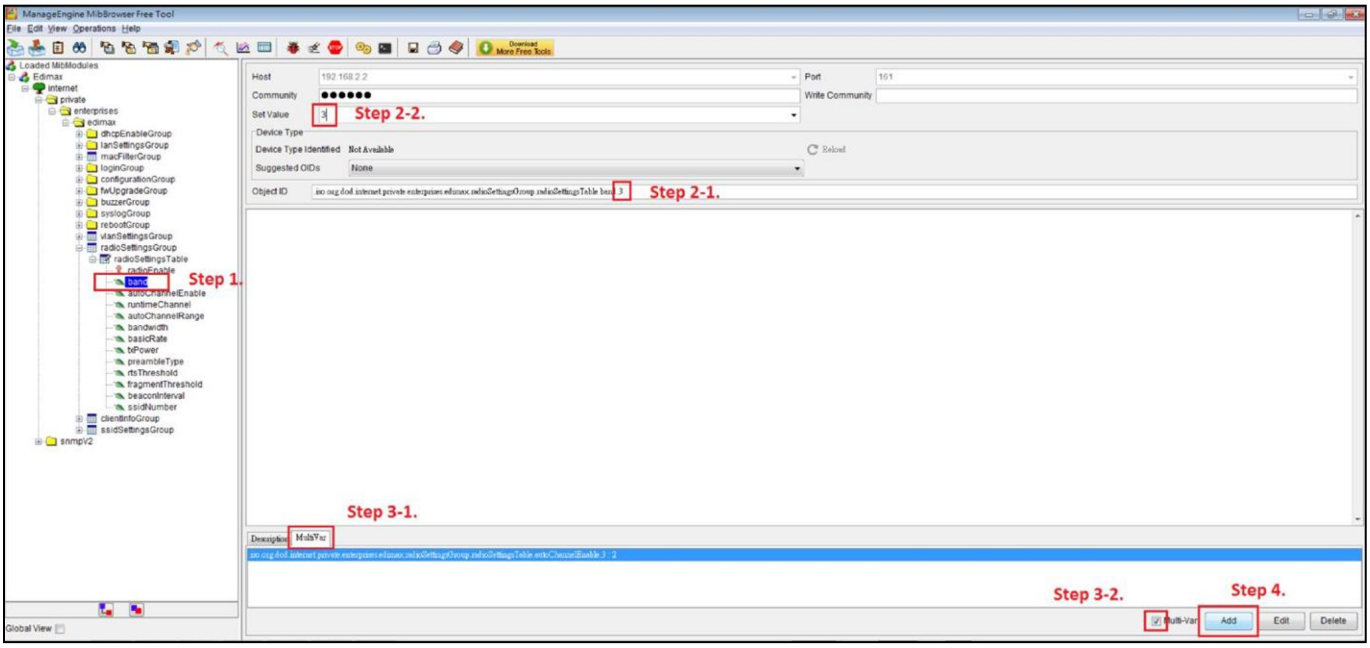
Device Type Identified: Not Available

Suggested OIDs: None

Object ID:

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

3. Add variables



Host: 192.168.2.2
Port: 161
Community: ●●●●●●●
Write Community:
Set Value: 3
Device Type Identified: Not Available
Suggested OIDs: None
Object ID: iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.band.3

iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.autoChannelEnable.3 : 2

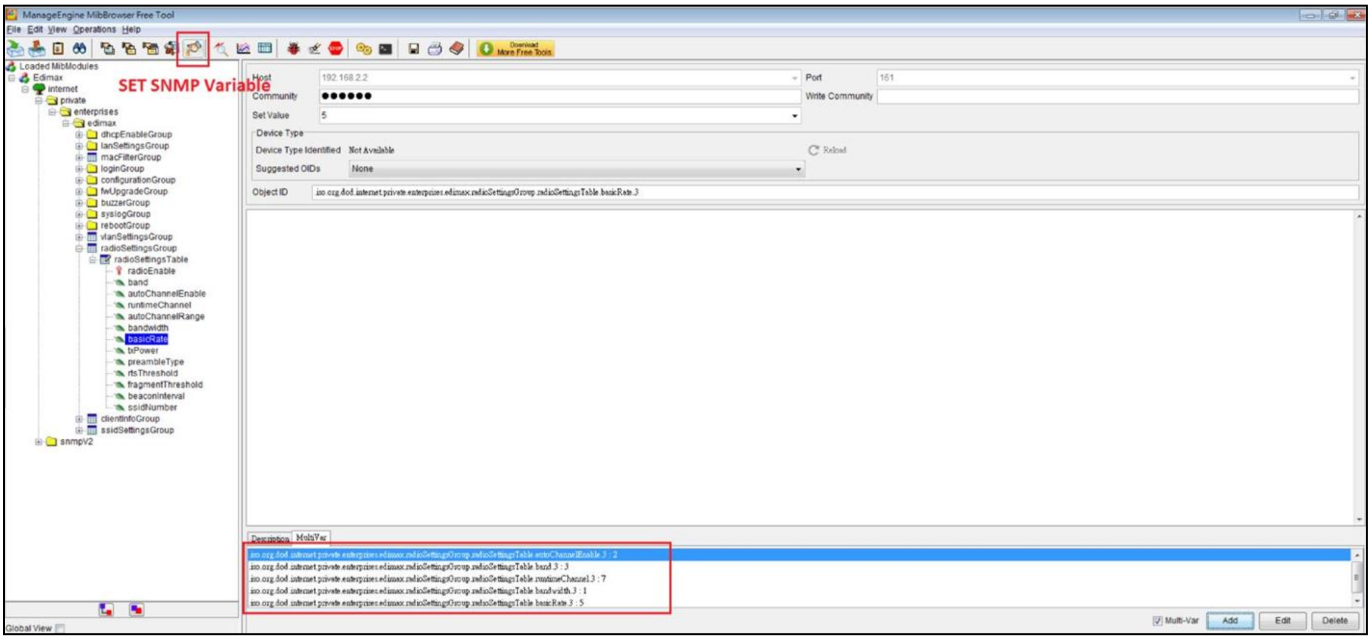
☑ Multi-Var

Step 1.
Step 2-1.
Step 2-2.
Step 3-1.
Step 3-2.
Step 4.

Figure 6 Example of setting the variable

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

4. Set SNMP variables



Host: 192.168.2.2
Port: 161
Community: ●●●●●●
Write Community:
Set Value: 5
Device Type
Device Type Identified: Not Available
Suggested OIDs: None
Object ID: iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.basicRate.3

```
iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.autoChannelEnable.3 : 2
iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.band.3 : 3
iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.runtimeChannel.3 : 7
iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.bandwidth.3 : 1
iso.org.dod.internet.private.enterprises.edimax.radioSettingsGroup.radioSettingsTable.basicRate.3 : 5
```

☑ Multi-Var

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

XII Best Practice

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

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

Follow the example below to:

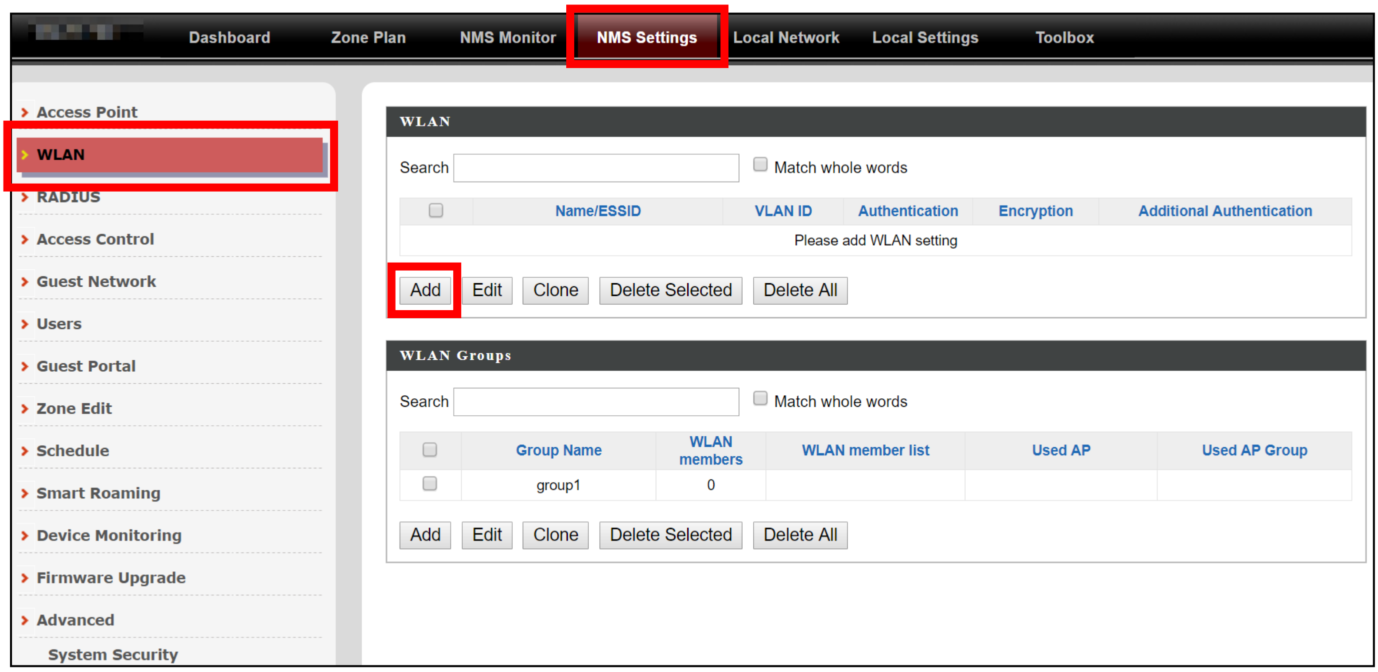
A. Create a WLAN group.

B. Create an access point group.

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

XII-1-1 Create WLAN Group

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



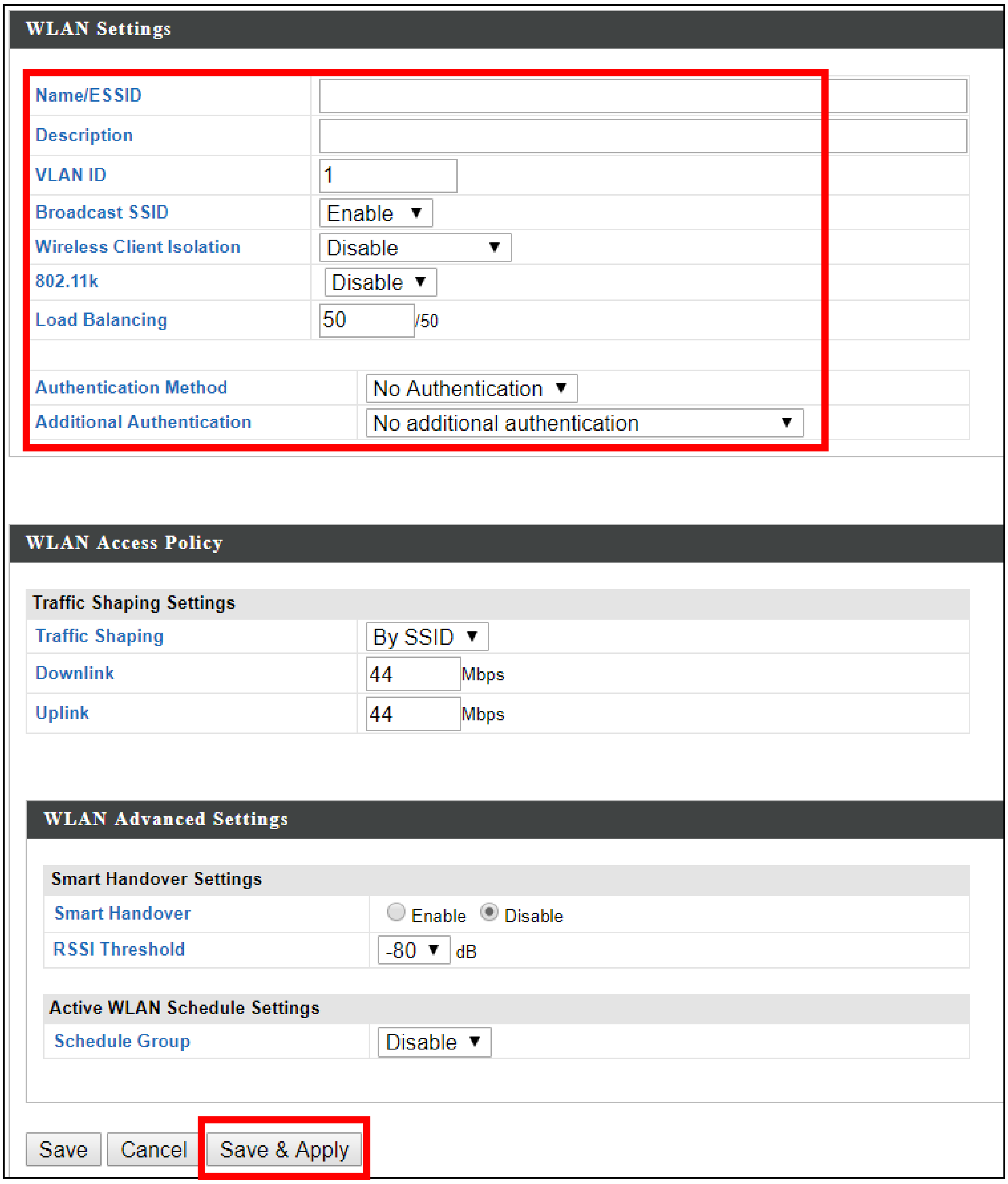
Search ☐ Match whole words

☐	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
	Please add WLAN setting				

Search ☐ Match whole words

☐	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
☐	group1	0			

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



WLAN Settings

Name/ESSID	
Description	
VLAN ID	1
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
802.11k	Disable ▼
Load Balancing	50 /50
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

WLAN Access Policy

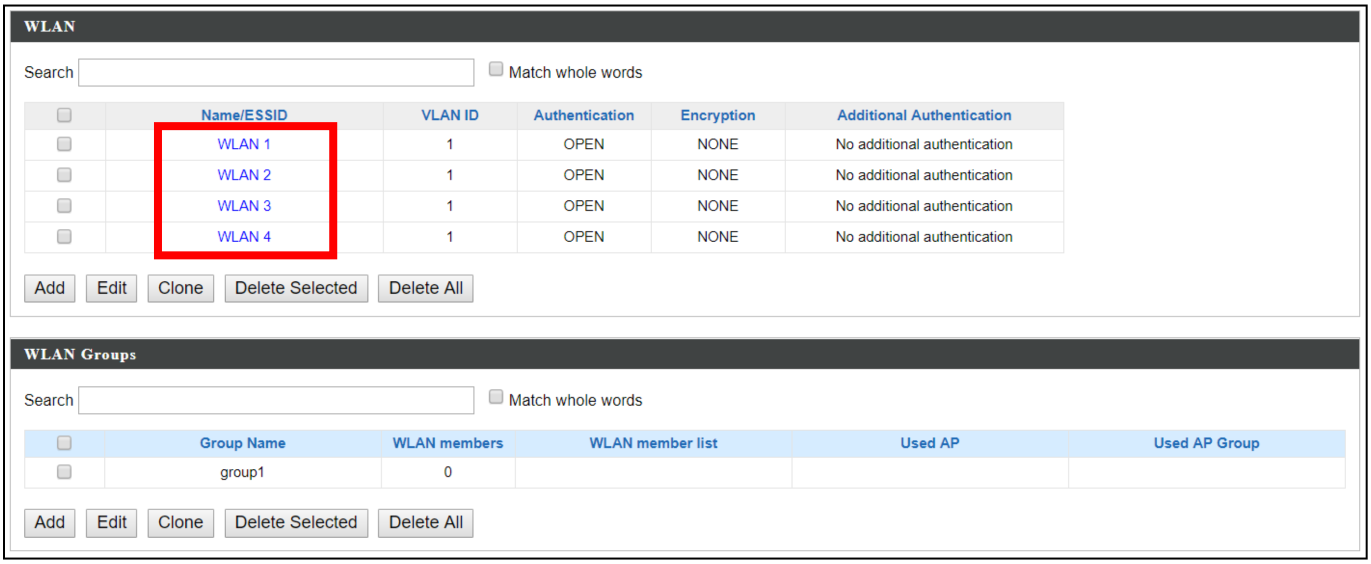
Traffic Shaping Settings	
Traffic Shaping	By SSID ▼
Downlink	44 Mbps
Uplink	44 Mbps

WLAN Advanced Settings

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

Active WLAN Schedule Settings	
Schedule Group	Disable ▼

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



WLAN

Search ☐ Match whole words

☐	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
☐	WLAN 1	1	OPEN	NONE	No additional authentication
☐	WLAN 2	1	OPEN	NONE	No additional authentication
☐	WLAN 3	1	OPEN	NONE	No additional authentication
☐	WLAN 4	1	OPEN	NONE	No additional authentication

Add | Edit | Clone | Delete Selected | Delete All

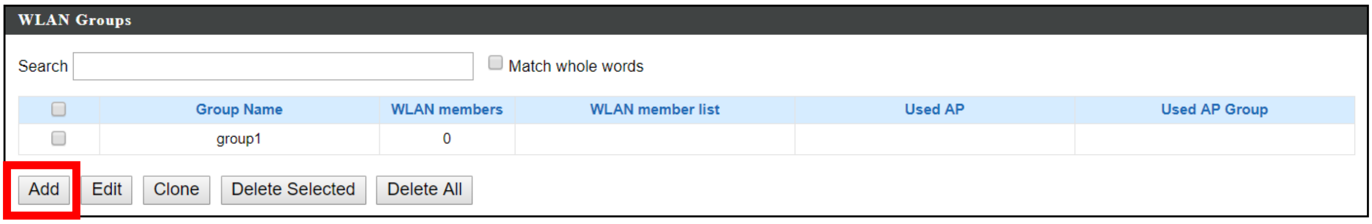
WLAN Groups

Search ☐ Match whole words

☐	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
☐	group1	0			

Add | Edit | Clone | Delete Selected | Delete All

4. Click **“Add”** in the **WLAN Groups** panel:



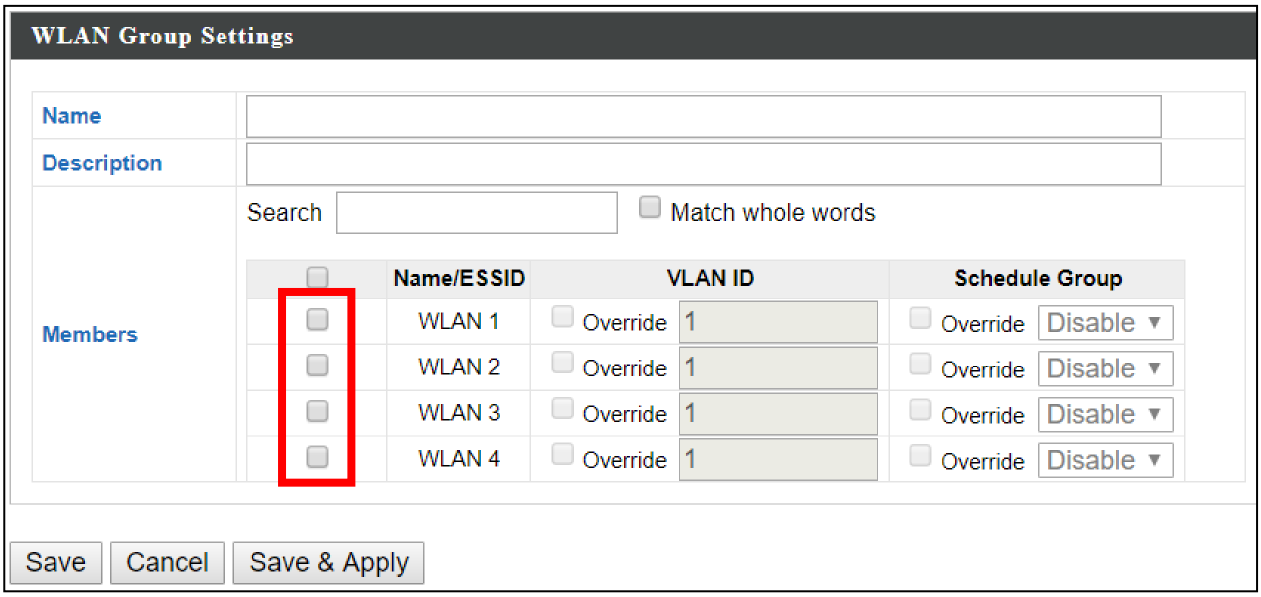
WLAN Groups

Search ☐ Match whole words

☐	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
☐	group1	0			

Add | Edit | Clone | Delete Selected | Delete All

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



WLAN Group Settings

Name

Description

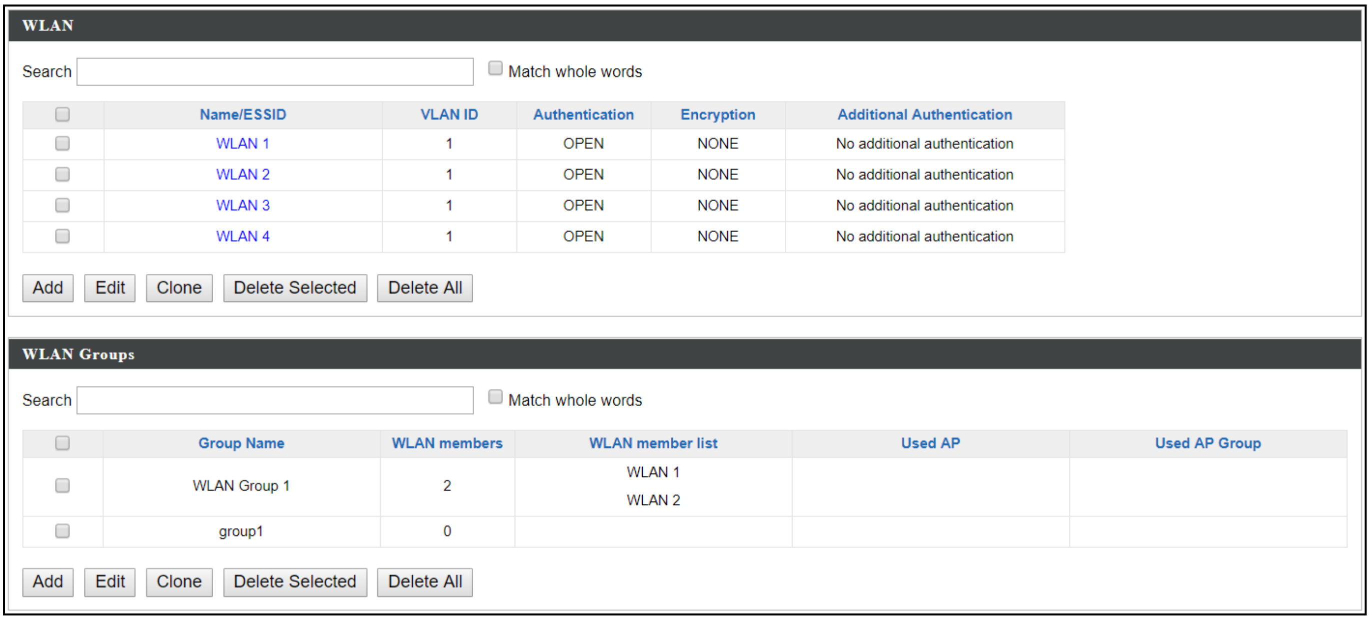
Members

Search ☐ Match whole words

☐	Name/ESSID	VLAN ID		Schedule Group	
☐	WLAN 1	☐ Override	1	☐ Override	Disable ▼
☐	WLAN 2	☐ Override	1	☐ Override	Disable ▼
☐	WLAN 3	☐ Override	1	☐ Override	Disable ▼
☐	WLAN 4	☐ Override	1	☐ Override	Disable ▼

Save | Cancel | Save & Apply

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

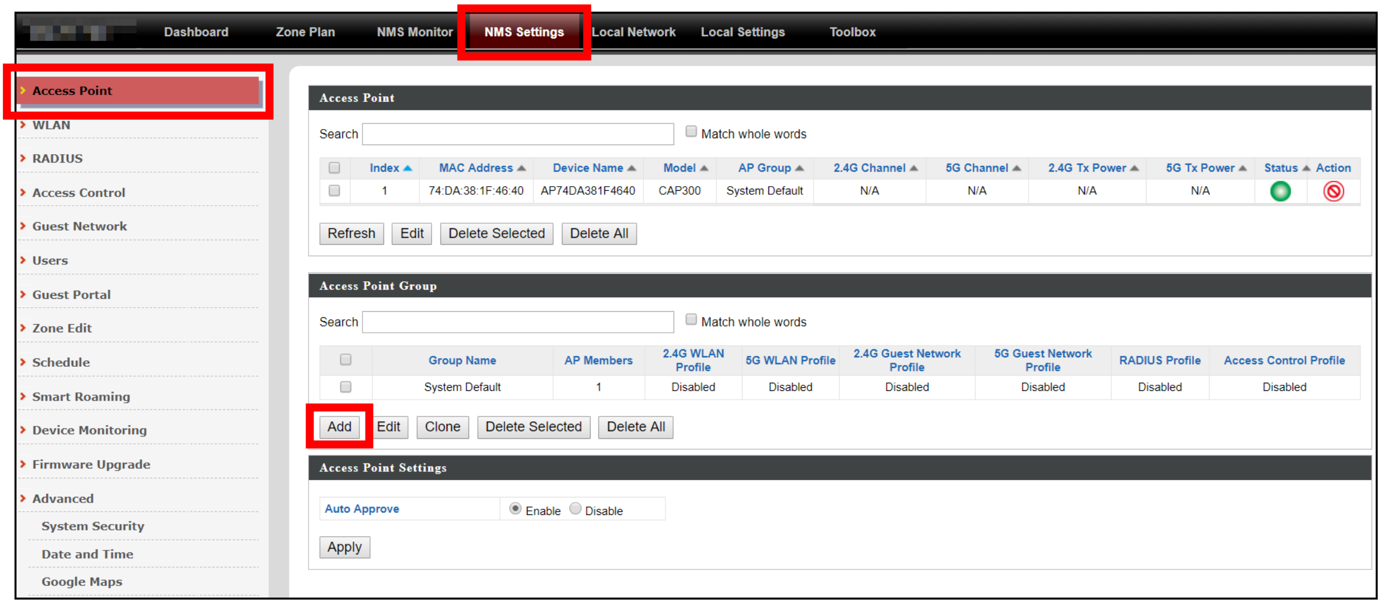


□	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
□	WLAN 1	1	OPEN	NONE	No additional authentication
□	WLAN 2	1	OPEN	NONE	No additional authentication
□	WLAN 3	1	OPEN	NONE	No additional authentication
□	WLAN 4	1	OPEN	NONE	No additional authentication

□	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
□	WLAN Group 1	2	WLAN 1 WLAN 2		
□	group1	0			

XII-1-2 Create Access Point Group

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

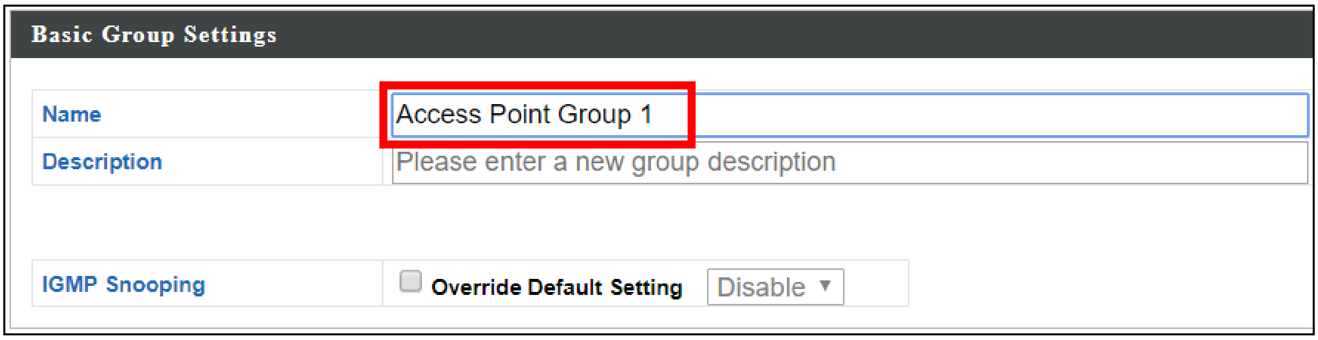


□	Index ▲	MAC Address ▲	Device Name ▲	Model ▲	AP Group ▲	2.4G Channel ▲	5G Channel ▲	2.4G Tx Power ▲	5G Tx Power ▲	Status ▲	Action
□	1	74:DA:38:1F:46:40	AP74DA381F4640	CAP300	System Default	N/A	N/A	N/A	N/A	●	⊘

□	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
□	System Default	1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

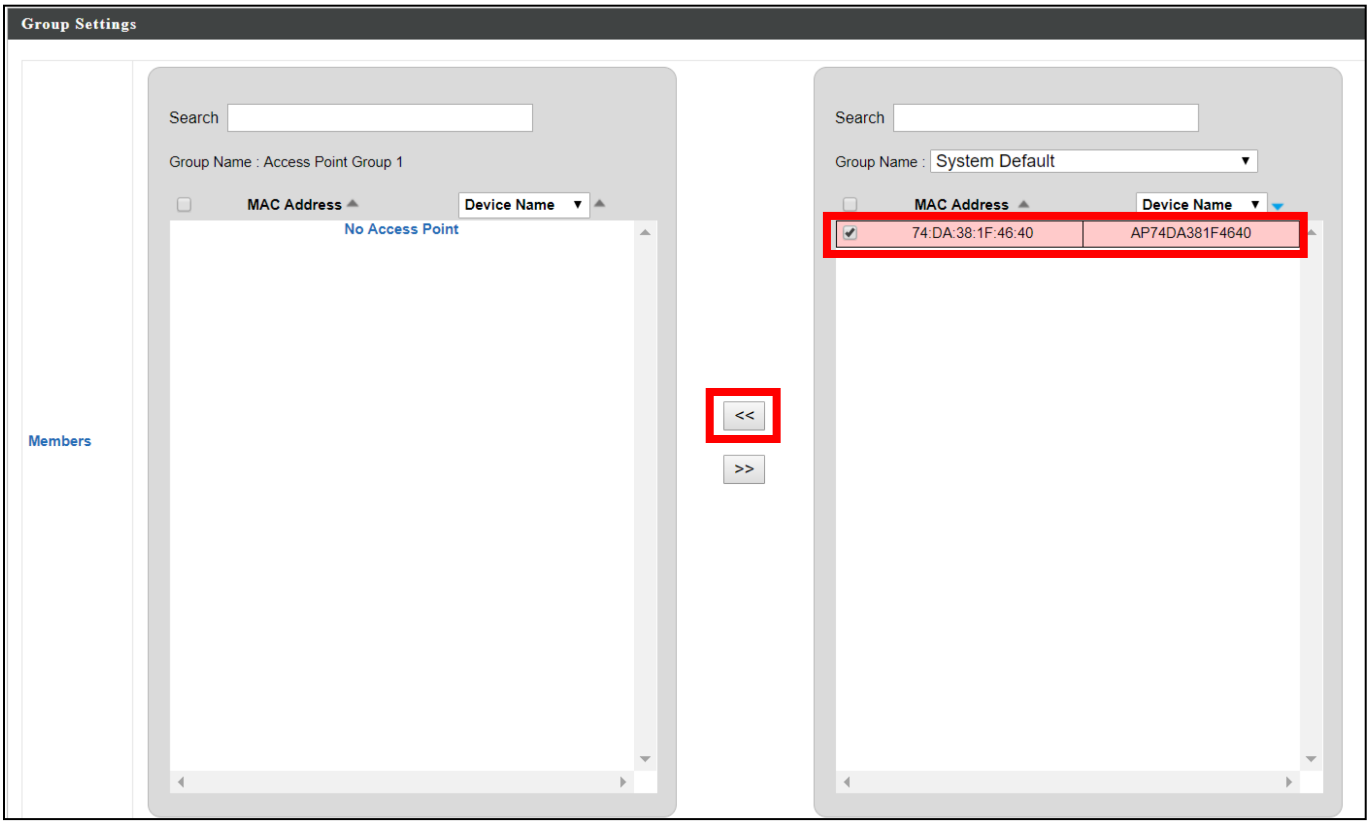
Auto Approve ● Enable ○ Disable

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



Basic Group Settings

Name	Access Point Group 1
Description	Please enter a new group description
IGMP Snooping	□ Override Default Setting Disable ▾



Group Settings

Members

Search

Group Name : Access Point Group 1

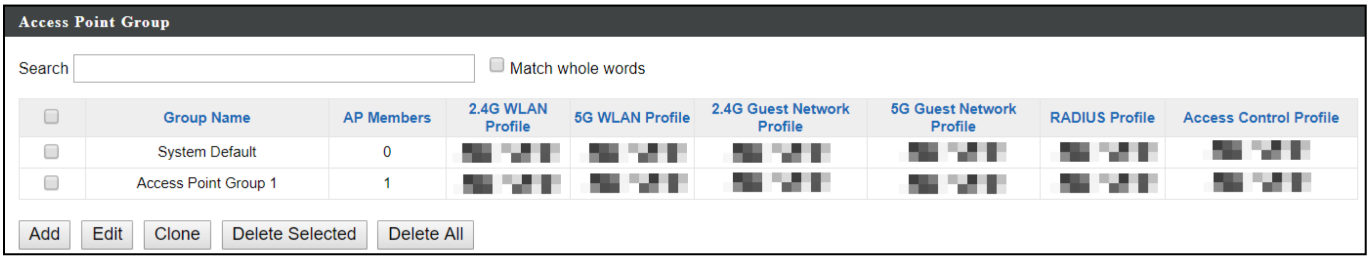
□	MAC Address ▲	Device Name ▾
	No Access Point	

Search

Group Name : System Default ▾

□	MAC Address ▲	Device Name ▾
☑	74:DA:38:1F:46:40	AP74DA381F4640

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



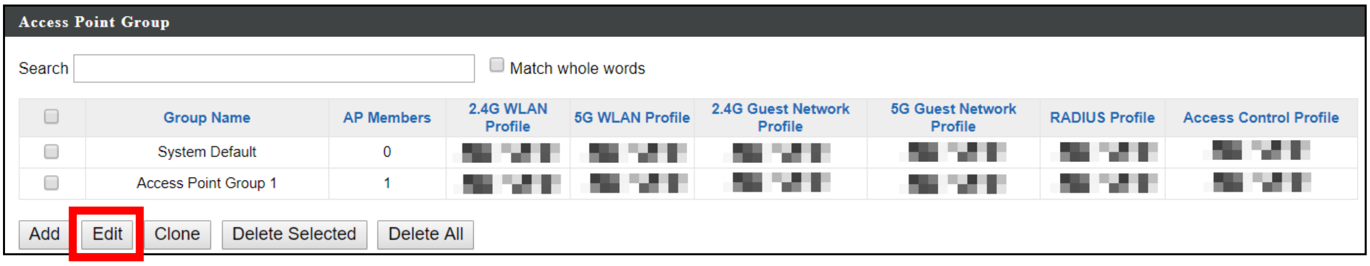
Access Point Group

Search □ Match whole words

□	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
□	System Default	0						
□	Access Point Group 1	1						

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

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

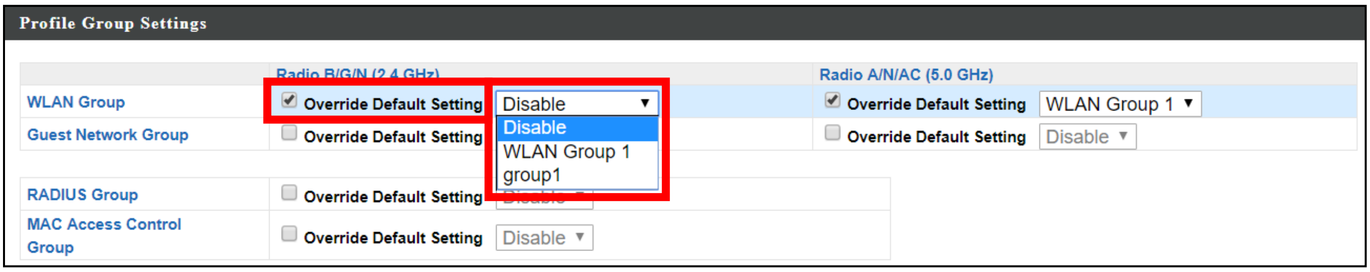


Access Point Group

Search □ Match whole words

□	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
□	System Default	0	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
□	Access Point Group 1	1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

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



Profile Group Settings

	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)	
WLAN Group	☑ Override Default Setting	Disable ▾	☑ Override Default Setting	WLAN Group 1 ▾
Guest Network Group	□ Override Default Setting		□ Override Default Setting	Disable ▾
RADIUS Group	□ Override Default Setting	Disable ▾		
MAC Access Control Group	□ Override Default Setting	Disable ▾		

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

COPYRIGHT

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

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

Federal Communication Commission Interference Statement

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

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

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such as PDAs or lap pads is not authorized. This transmitter is restricted for use with the specific antenna tested in the application for certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

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

EU Countries Intended for Use

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

EU Countries Not Intended for Use

None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 1995/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 1995/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1995/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (1995/5/EK, 2009/125/EK, 2006/95/EK, 2011/65/EK).

Türkçe: Bu cihaz 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 1995/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 1995/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..

Português: Este equipamento cumpre os requesitos essênciais da Directiva 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 1995/5/EG, 2009/125/EG, 2006/95/EG, 2011/65/EG.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.

suomen kieli: Tämä laite täyttää direktiivien 1995/5/EY, 2009/125/EY, 2006/95/EY, 2011/65/EY oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

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

WEEE Directive & Product Disposal

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

Declaration of Conformity

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

Equipment: AC1350 Ceiling Mount Access Point
Model No.: CAP1300

The following European standards for essential requirements have been followed:

Directives 2014/53/EU

Spectrum	:	N 300 328 V2.1.1 (2016-11);

EMC	:	Draft ETSI EN 301 489-1 V2.2.0 (2017-03);
		Draft ETSI EN 301 489-17 V3.2.0 (2017-03);
		EN 301 893 V2.1.1 (2017-05);

EMF	:	EN 62311:2008

Directives 2014/35/EU

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

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

Date of Signature: Sep, 2017

Signature:

Printed Name: Albert Chang

Title: Director
Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

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

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

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

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

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

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

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

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

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

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

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

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

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

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

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

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

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

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

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

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

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

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

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

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

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

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

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

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

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

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

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

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

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

NO WARRANTY

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

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

EDIMAX
NETWORKING PEOPLE TOGETHER