COMTREND

# WAP-EN1750W

## NMS User Manual

Version 1.0, November 2015

**FCC Compliance**

This equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the 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 instruction, may cause harmful interference to radio communication. 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:

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

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

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.
This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

**Copyright**



| | |
|---|---|
| **NOTE:** | This document is subject to change without notice. |

**Protect Our Environment**

This symbol indicates that when the equipment has reached the end of
It's useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local

# *I. Product Information*

The 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 5 access points with no additional wireless controller required, reducing costs and facilitating efficient remote access point 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.

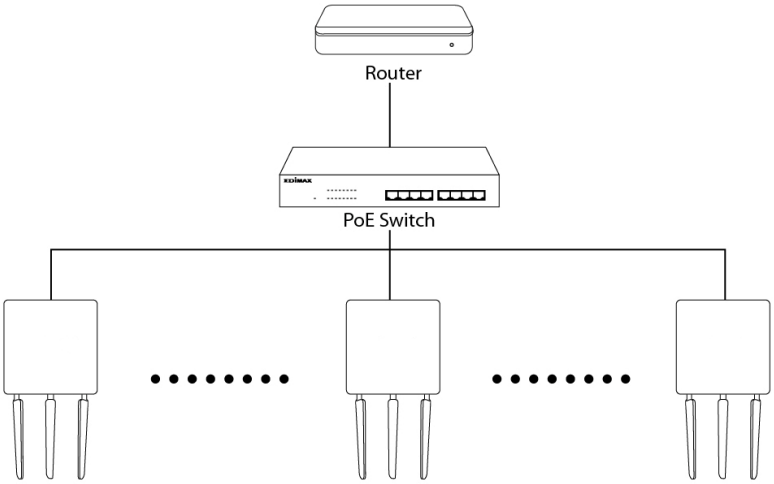
# *II. Quick Setup*

One AP (access point) is designated as the AP Controller (master) and other connected APs are designated as Managed APs (slaves). Using the NMS you can monitor, configure and manage all Managed APs (up to 5) from the single AP Controller.

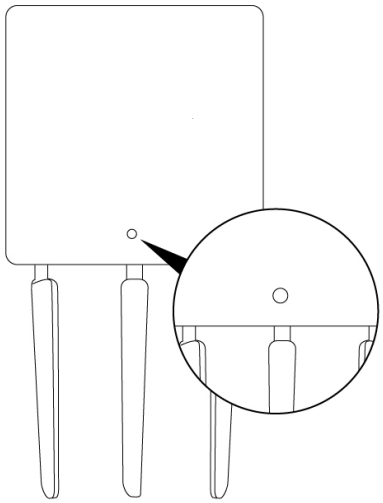
Follow the steps below:

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

***You can use your router as a DHCP server or you can later configure your AP Controller as a DHCP server.***




**2.** Ensure all APs are powered on and check the LED status.



**3.** Designate one AP as the AP Controller which will manage all other connected APs (up to 5).

**4.** Connect a computer to the AP Controller using an Ethernet cable. Connect the AP Controller to power and power on the unit.

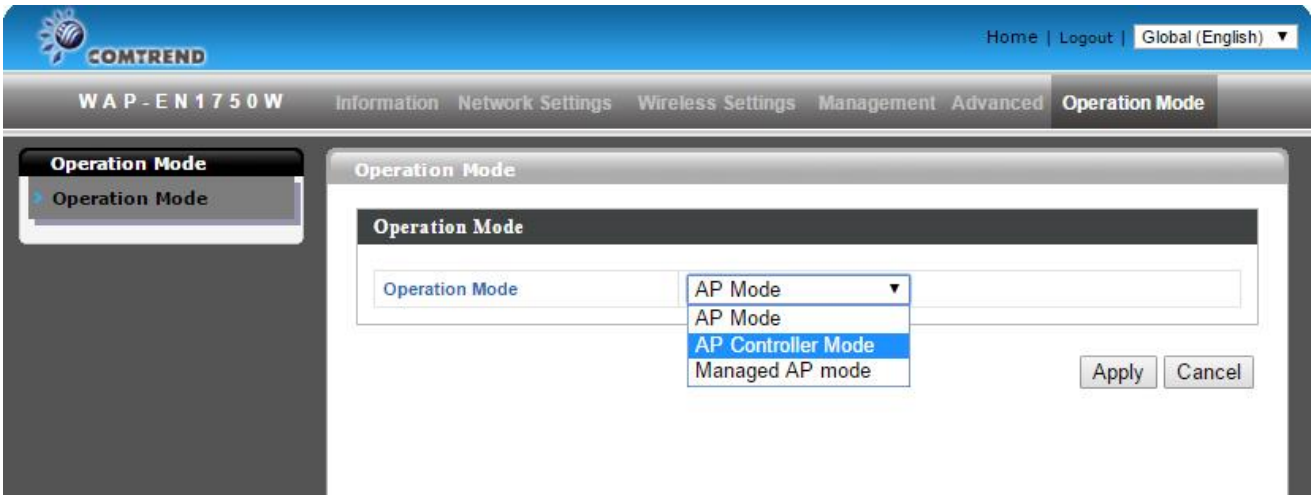
**5.** Open a web browser and enter the AP Controller's IP address in the address field. The default IP address is **192.168.2.2.**

***DHCP is enabled on the access point by default. If no DHCP Service is found, the access point will default to IP address 192.168.2.2.***

***Your computer's IP address must be in the same subnet as the AP Controller. 192.168.2.10 is being used in this example.***


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

**7.** You will arrive at the Access Point Information screen. Go to →**"Operation Mode"** and select **"AP Controller Mode"** from the drop down menu.




**8.** Click “Apply” to save the settings.


**9.** Your Controller AP & Managed APs should be fully functional. Use the top menu to navigate around the NMS.


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

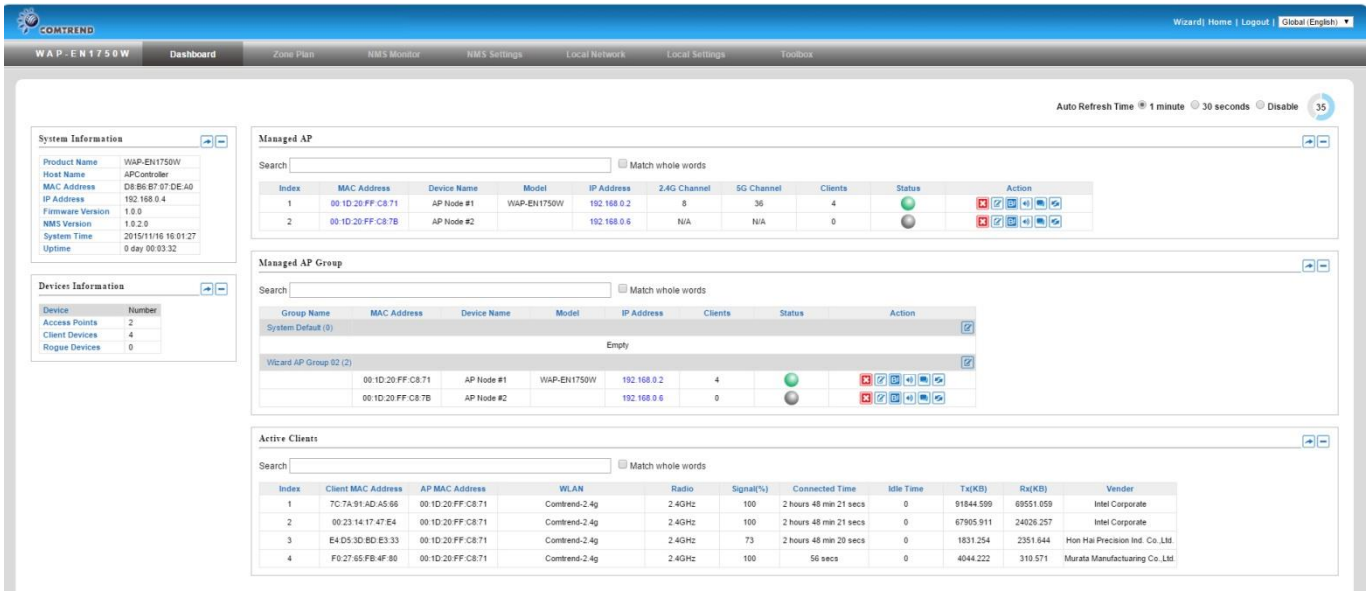
Use ***Dashboard, Zone Plan, NMS Monitor*** & ***NMS Settings*** to configure Managed APs.

Use **Toolbox** to diagnose connection issues.

# *III. Software Layout*

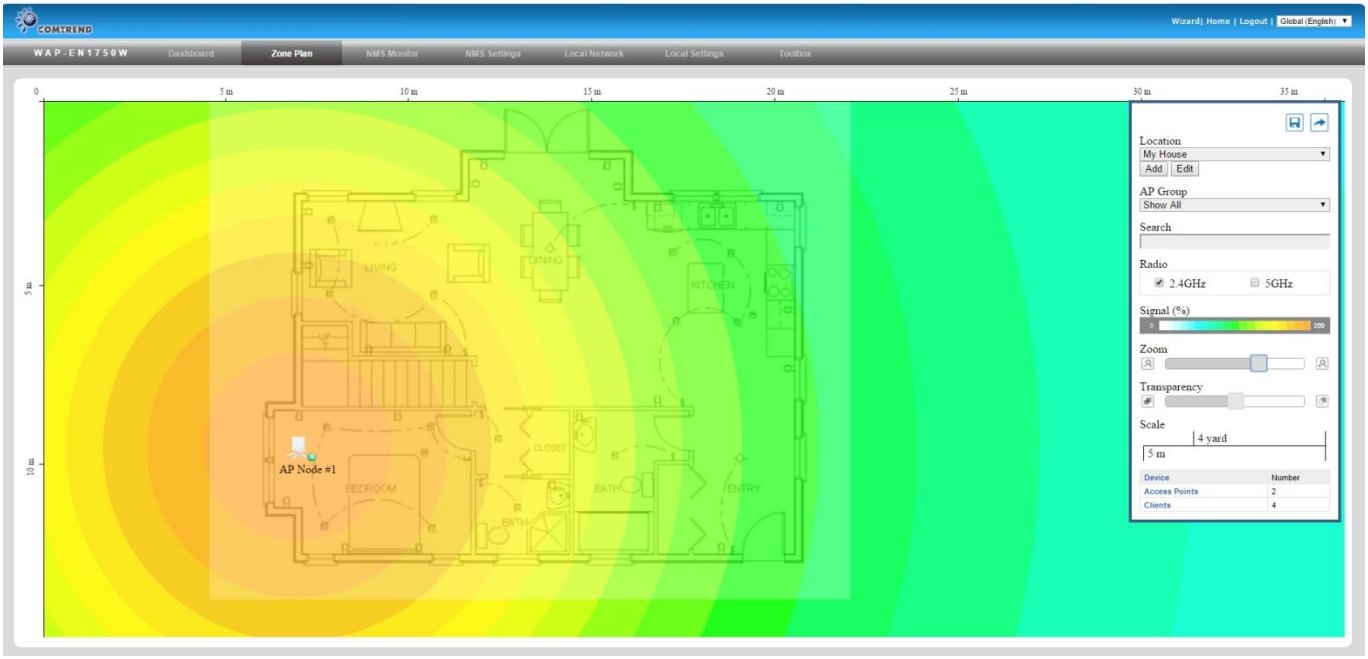
The top menu features 7 panels: *Dashboard, Zone Plan, NMS Monitor, NMS Settings, Local Network, Local Settings & Toolbox.*

## Dashboard



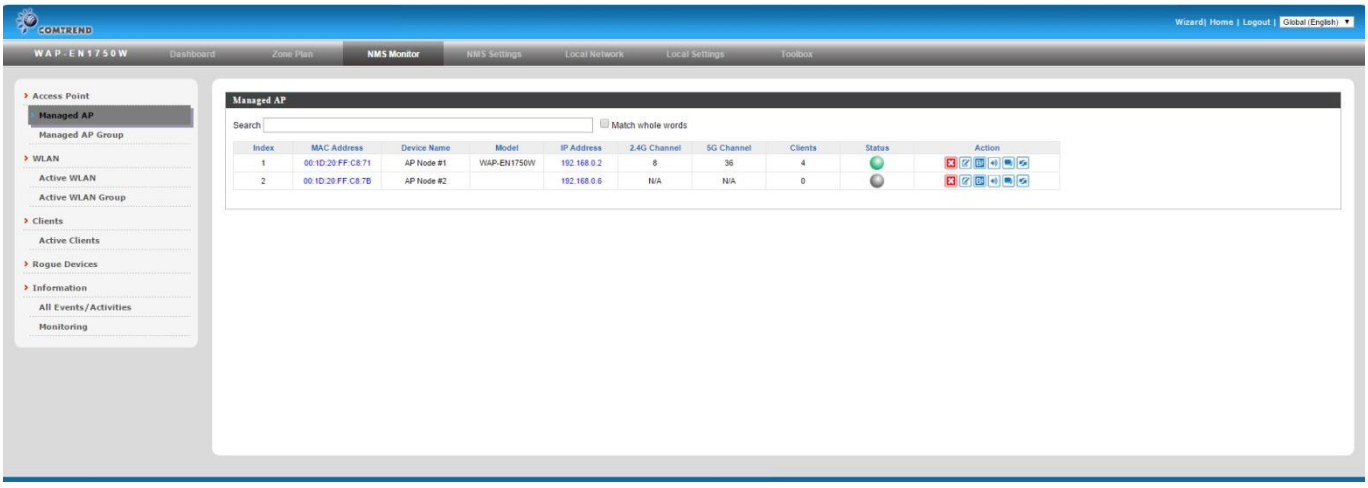

The **Dashboard** panel displays an overview of your network and key system information, with quick links to access configuration options for Managed APs and Managed AP groups. Each panel can be refreshed, collapsed or moved according to your preference.

# Zone Plan



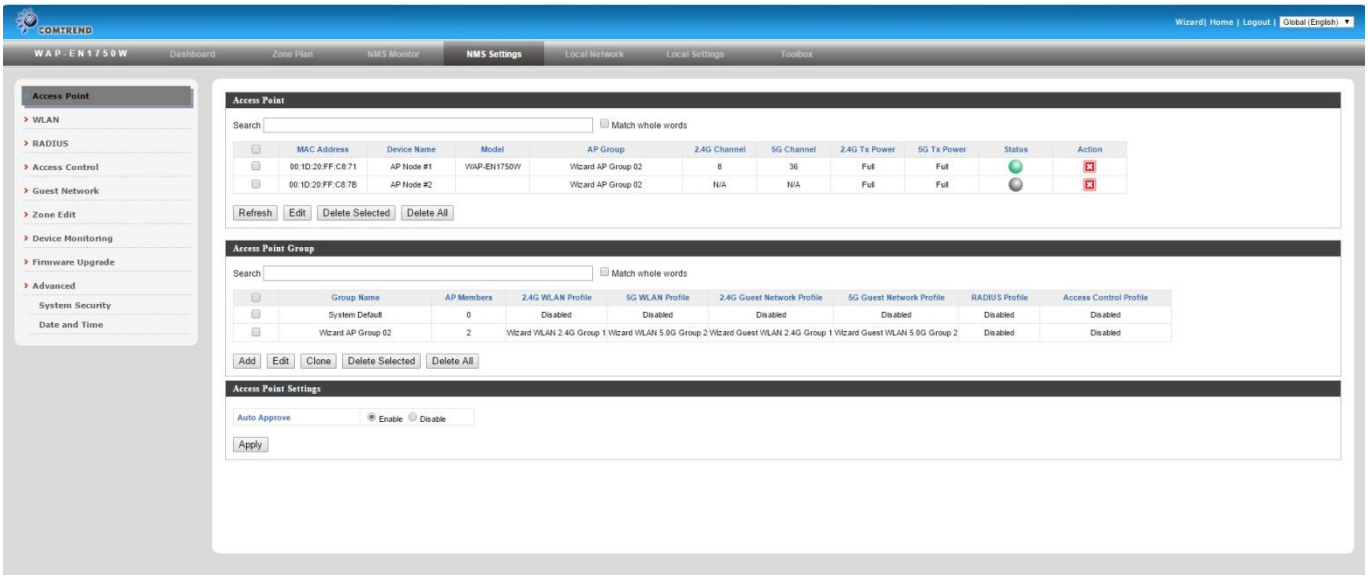

**Zone Plan** displays a customizable live map of Managed APs for a visual representation of your network coverage. Each AP icon can be moved around the map, and a background image can be uploaded for user-defined location profiles using **NMS Settings → Zone Edit**. Options can be configured using the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

# NMS Monitor



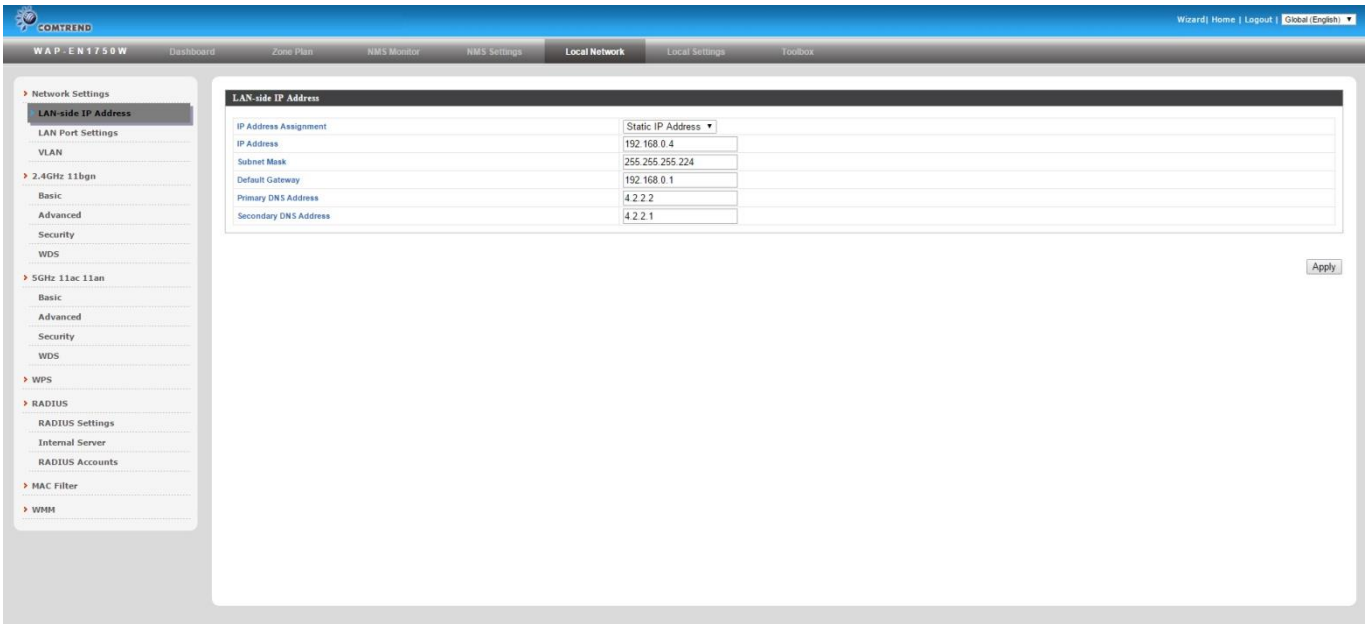

The **NMS Monitor** panel provides more detailed monitoring information about the AP Array than found on the Dashboard, grouped according to categories in the menu down the left side.

# NMS Settings



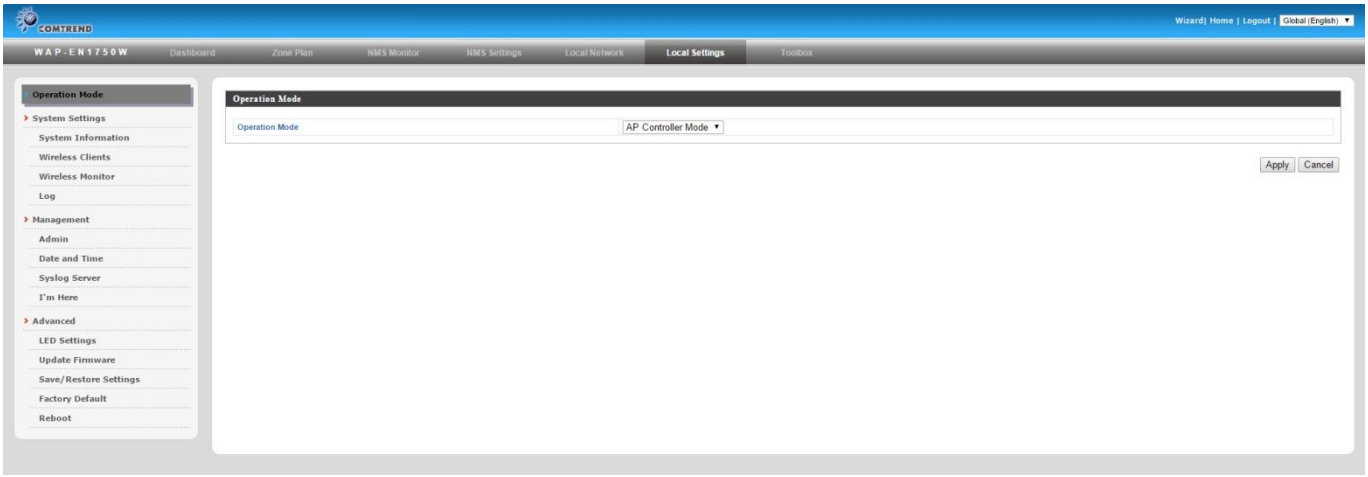

**NMS Settings** provides extensive configuration options for the AP Array. You can manage each access point, assign access points into groups, manage WLAN, RADIUS as well as upgrade firmware across multiple access points. The Zone Plan can also be configured using “Zone Edit”.

# Local Network



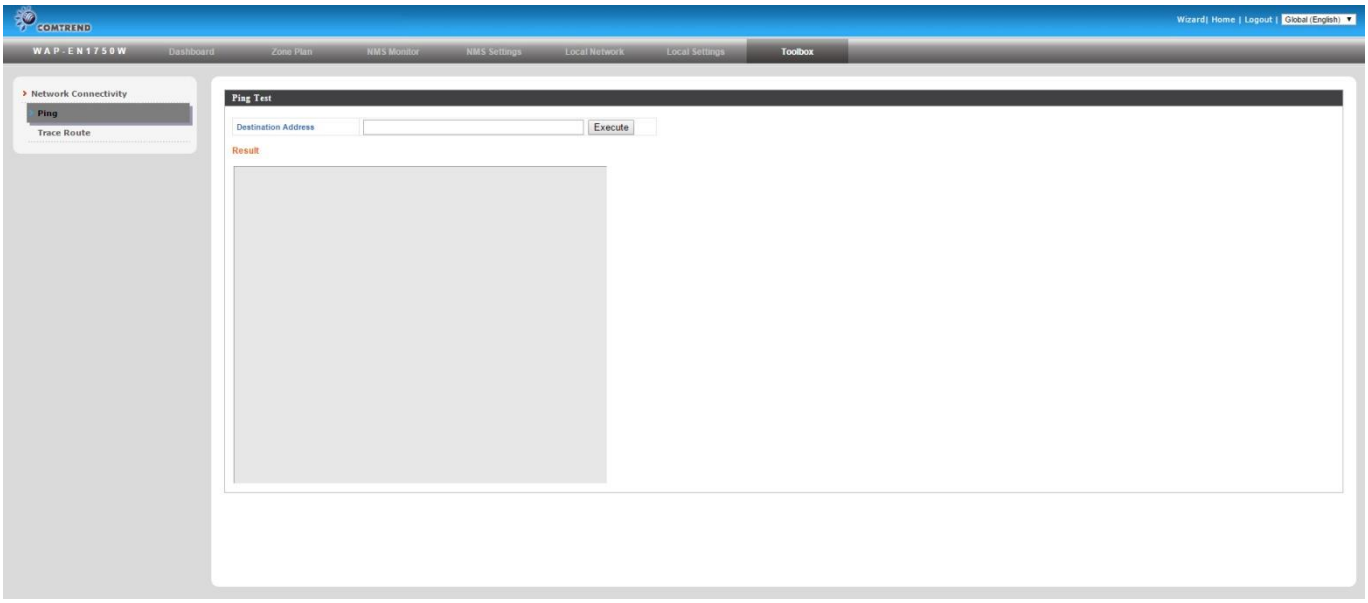

**Local Network** settings are for your AP Controller. You can configure the IP address and DHCP server of the AP Controller in addition to 2.4GHz & 5Ghz Wi-Fi and security, with WPS, RADIUS server, MAC filtering and WMM settings also available.

# Local Settings




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

# Toolbox




The Toolbox panel provides a network diagnostic tools: *ping* and *trace route*.

# *IV. Features*

Descriptions of the functions of each main panel *Dashboard, Zone Plan, NMS Monitor, NMS Settings, Local Network, Local Settings & Toolbox* can be found below. When using the NMS, click "Apply" to save changes:


***Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.***

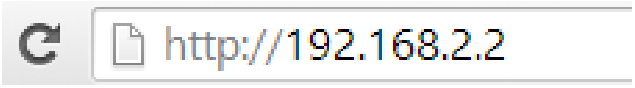
## IV-1. LOGIN, LOGOUT & RESTART

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

**LOGIN**

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

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




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

***DHCP is enabled on the access point by default. If no DHCP Service is found, the access point will default to IP address 192.168.2.2.***

***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.***

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

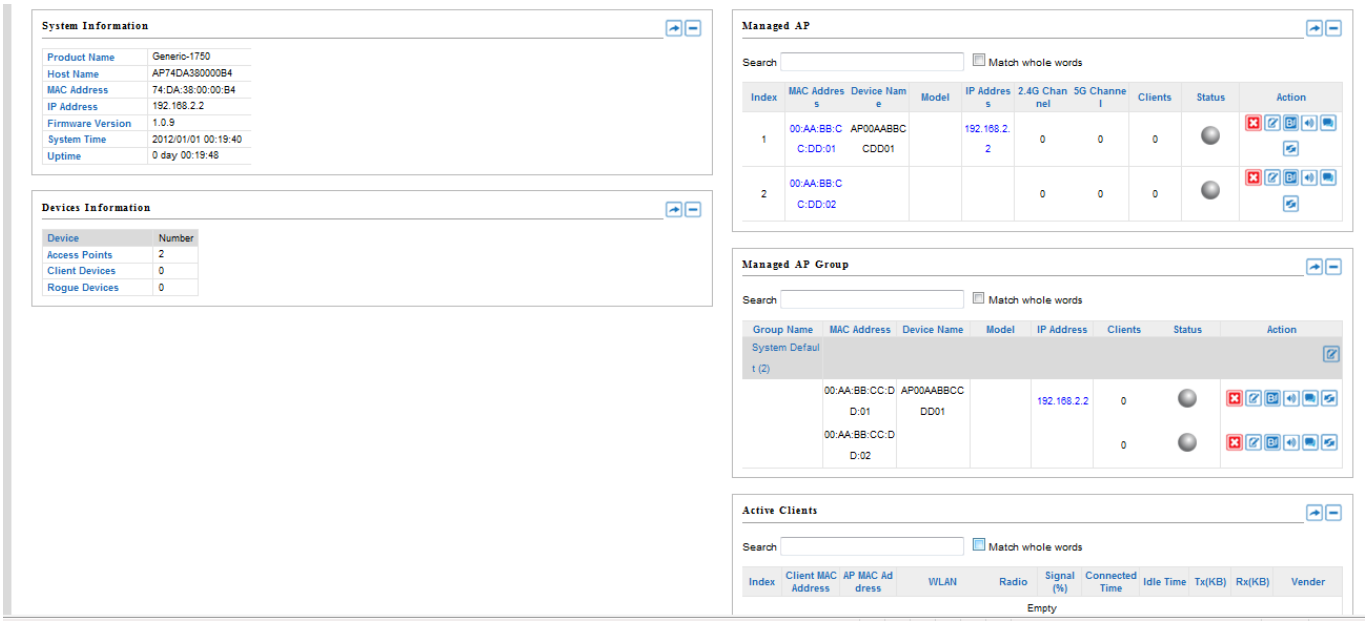
**RESTART**

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

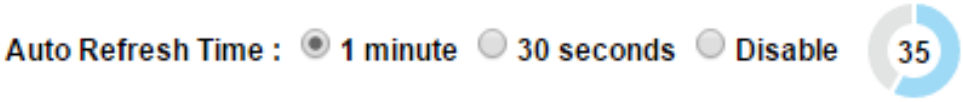
To restart Managed APs click the Restart icon for the specified AP on the Dashboard:

# IV-2. DASHBOARD

The dashboard displays an overview of your AP array:




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



## IV-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 | Generic-1750 |
| Host Name | AP74DA380000B4 |
| MAC Address | 74:DA:38:00:00:B4 |
| IP Address | 192.168.2.2 |
| Firmware Version | 1.0.9 |
| System Time | 2012/01/01 00:20:09 |
| Uptime | 0 day 00:20:17 |

## IV-2-2. Devices Information

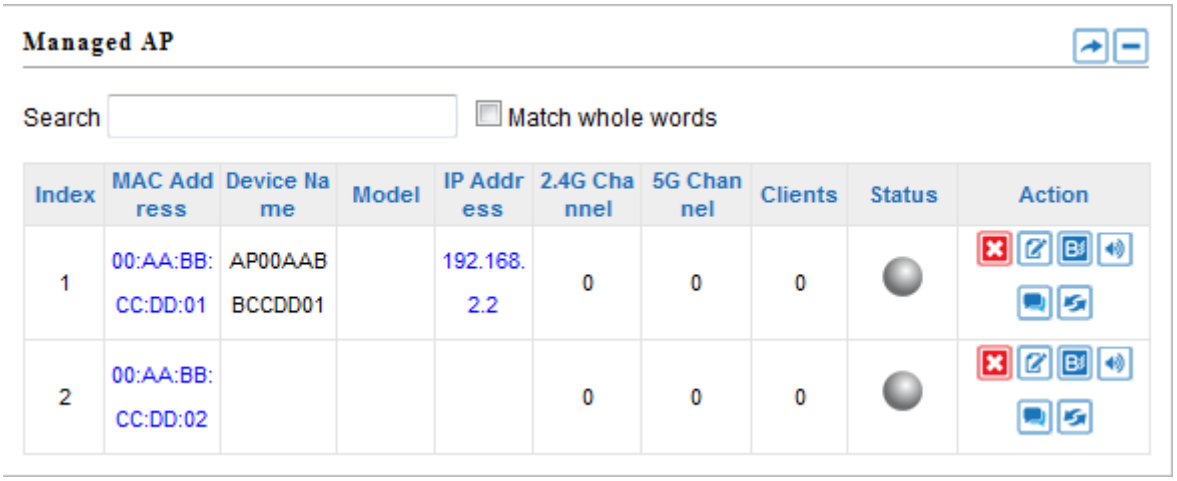
**Devices Information** is a summary of the number of all devices in the local network: *Access Points, Clients Connected, and Rogue (unidentified) Devices.*

**Devices Information**

| Device | Number |
|---|---|
| Access Points | 2 |
| Client Devices | 0 |
| Rogue Devices | 0 |

## IV-2-3. Managed AP

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




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


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

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


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

2. **Edit**
   *Edit various settings for the Managed AP (refer to **IV-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.*

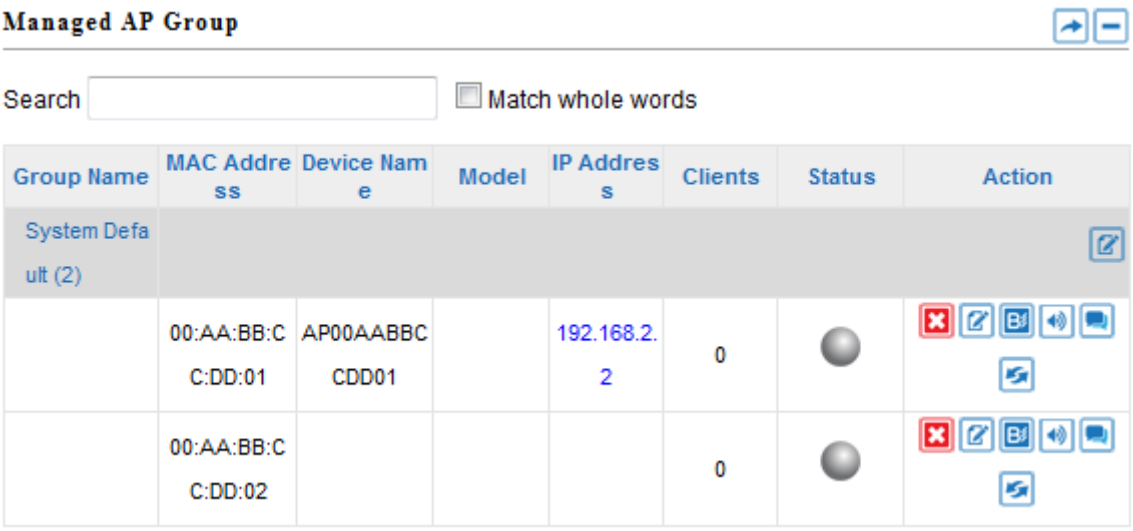
5. **Network Connectivity**
   *Go to the "Network Connectivity" panel to perform a ping or traceroute.*

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

### IV-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 **IV-5-1. Access Point**).




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

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

Each Managed AP 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 **IV-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.*

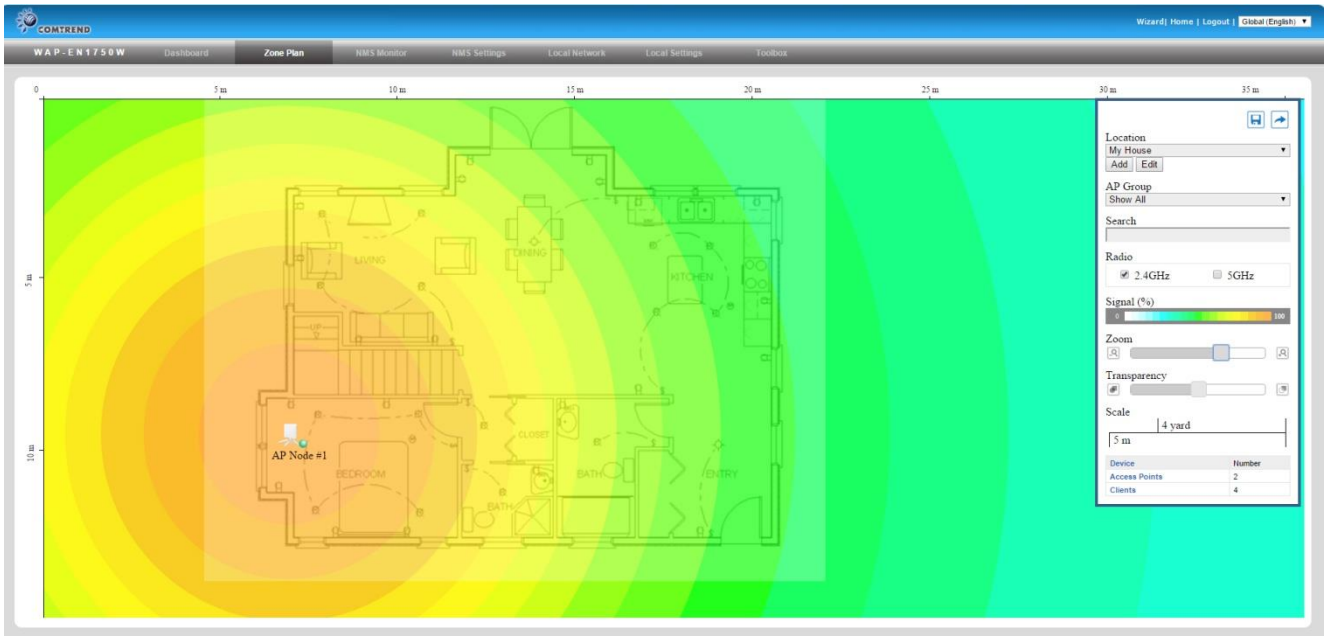
## IV-2-5. Active Clients

**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).*


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

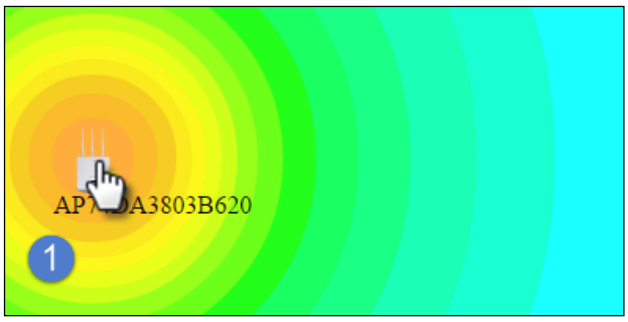
# IV-3. ZONE PLAN

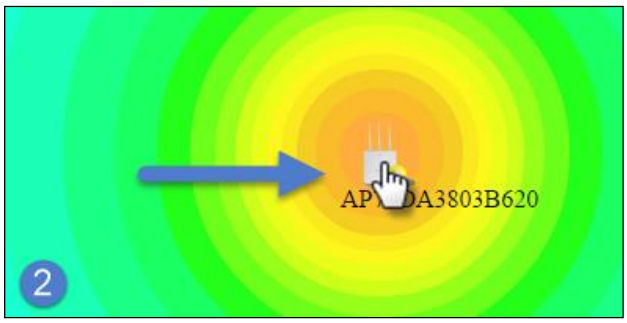
The Zone Plan can be fully customized to match your network environment. You can move the AP icons and select different location images (upload location images in **NMS Settings → Zone Edit**) to create a visual map of your AP array.




Use the menu on the right 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.

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:




| | |
|---|---|
| **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** | Signal strength key for the signal strength display around each AP in the zone map. |
| **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. |

# IV-4. NMS MONITOR

## IV-4-1. Access Point

### IV-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).*


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


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

| Status Icons | | | |
|---|---|---|---|
| **Icon** | **Color** | **Status** | **Definition** |
|  | Grey | Disconnected | Managed AP is disconnected. *Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.* |
|  | Red | Authentication Failed<br><br>Or<br><br>Incompatible NMS Version | System security must be the same for all access points in the AP array. *Please check security settings (refer to **IV-5-8-1. System Security**).*<br><br>Access points must use the same version of NMS: the managed AP will not be able to make configurations. *Please use the AP Controller's firmware upgrade function (refer to **IV-5-7. 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. *Refer to **IV-5-1. Access Point: Auto Approval**. Note: Eight Managed APs are supported. Additional APs will display 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.*

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

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

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

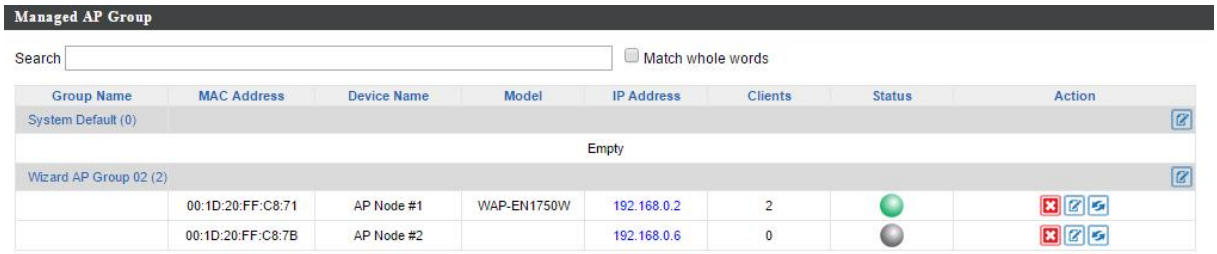
4. **Network Connectivity**
   *Go to the "Network Connectivity" panel to perform a ping or traceroute.*

5. **Restart**
   *Restarts the Managed AP.*

### IV-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 **IV-5-1. Access Point**).




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


The **Status** icon displays *grey* (disconnected), *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 IV-4-1-1. Managed AP:***Status Icons* for full descriptions.

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


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

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

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

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

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

7. **Restart**
   *Restarts the Managed AP.*

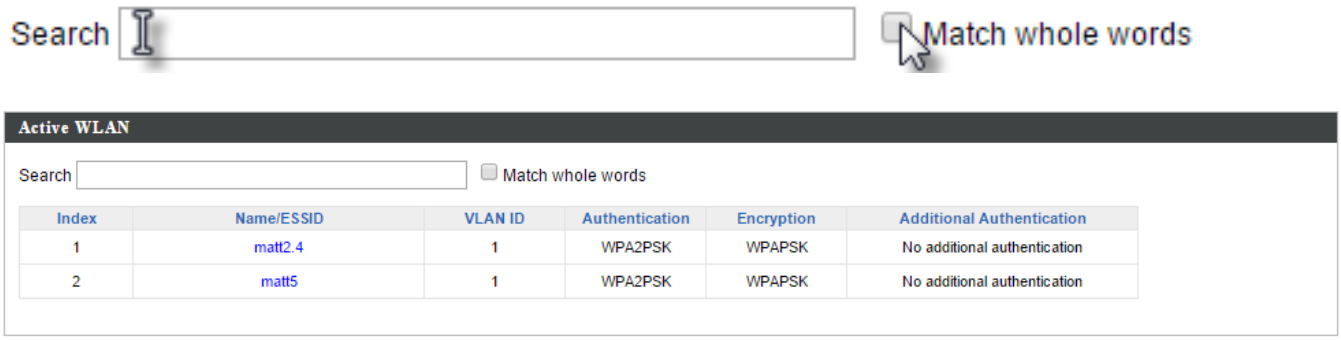
## IV-4-2. WLAN

### IV-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**.

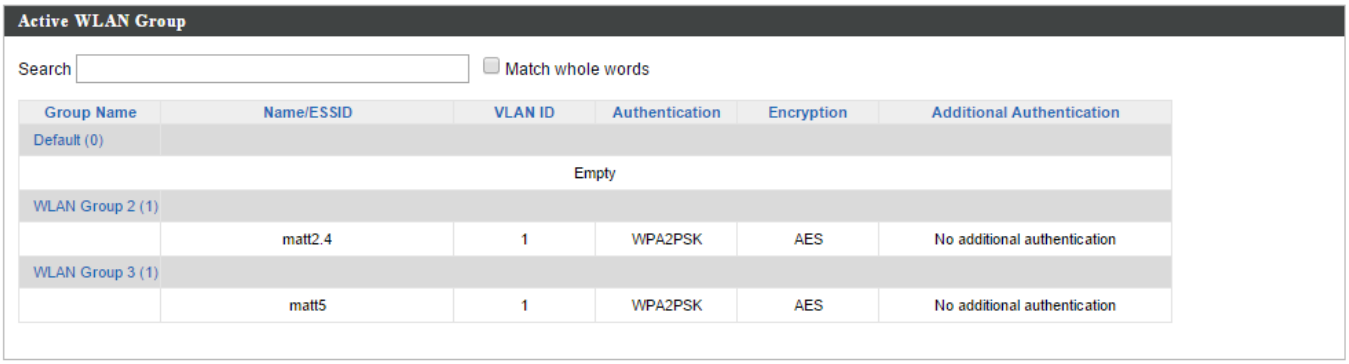
The search function can be used to locate a specific SSID. Type in the search box and the list will update:



### IV-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:

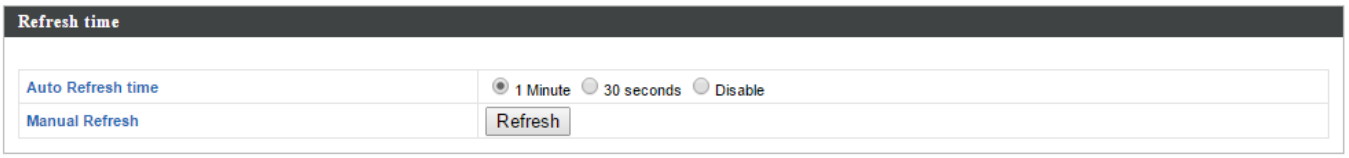

### IV-4-3. Clients

### IV-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:




Active Clients

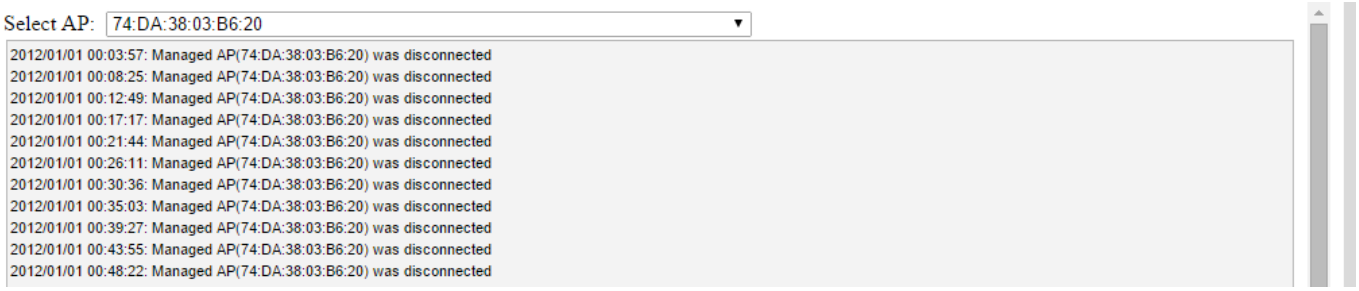
Search Match whole words

| Index | Client MAC Address | AP MAC Address | WLAN | Radio | Signal(%) | Connected Time | Idle Time | Tx(KB) | Rx(KB) | Vender |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 6C:88:14:70:C2:14 | 74:DA:38:00:00:24 | WIZARD_TEST5 | 5GHz | 100 | 3 min 33 secs | 4320 | 17.974 | 627.154 | Intel Corporate |
| 2 | B4:52:7E:84:DB:5B | 00:AA:BB:CC:DD:22 | WIZARD_TEST1 | 2.4GHz | 100 | 6 min 53 secs | 120 | 8.554 | 46.607 | Sony Mobile Communications AB |

## IV-4-4. Information

### IV-4-4-1. 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.

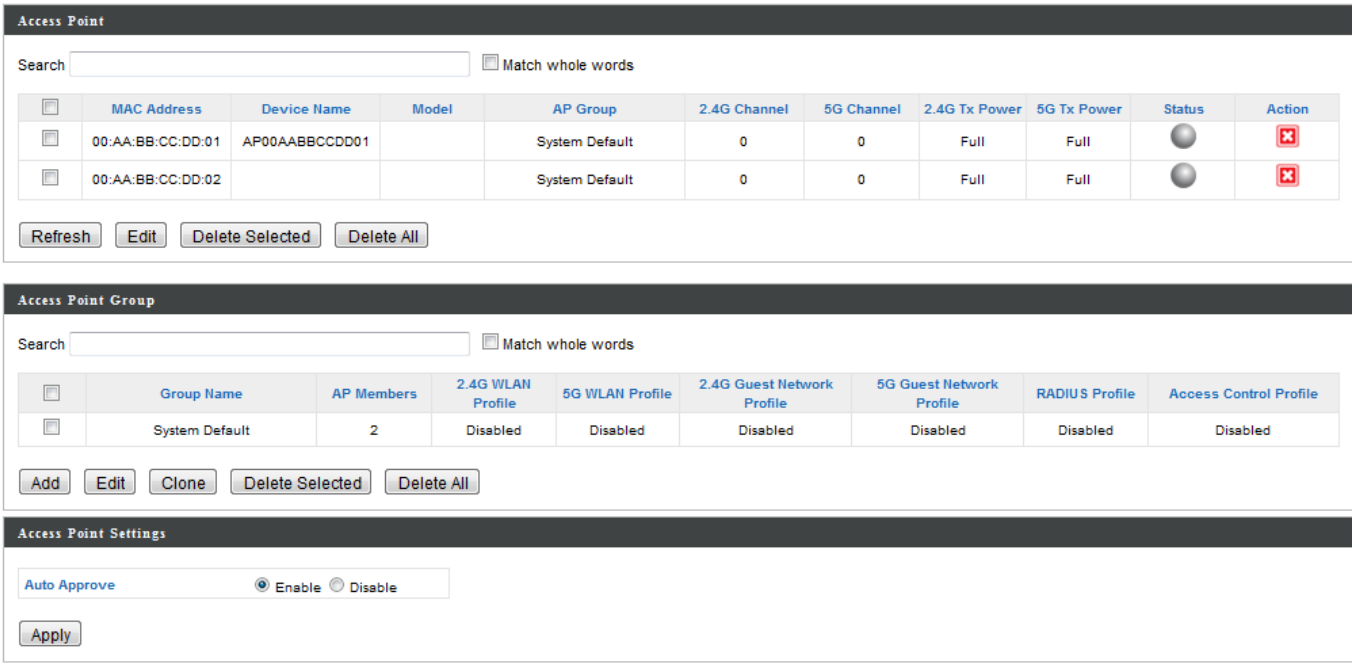


# IV-5. NMS Settings

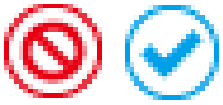
## IV-5-1. Access Point

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:


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 IV-4-1-1. Managed AP:***Status Icons* 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:


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 or disable Auto Approve for all Managed APs. |

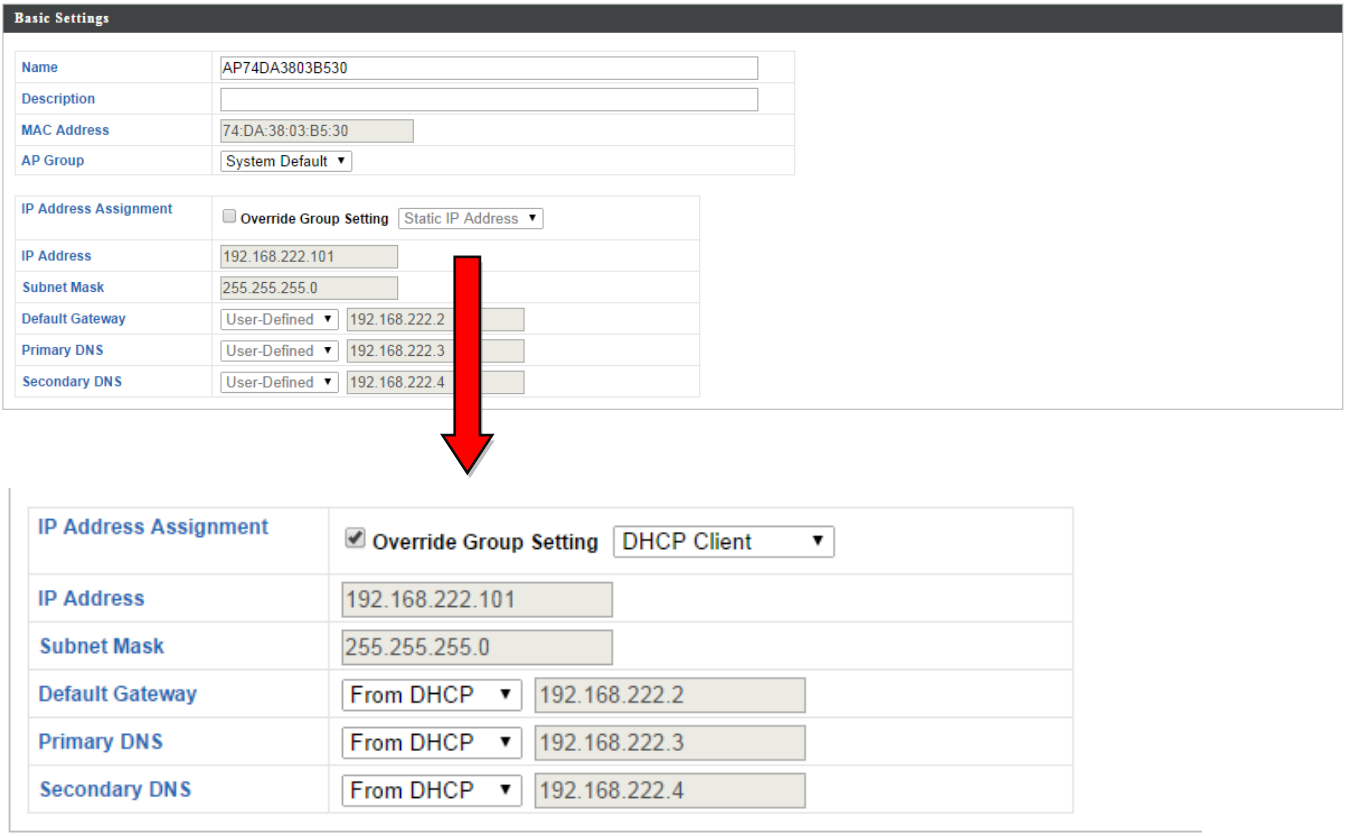
To manually approve a Managed AP, use the *allow* "Action" icon for the specified access point:

**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. An events log is displayed at the bottom of the page.

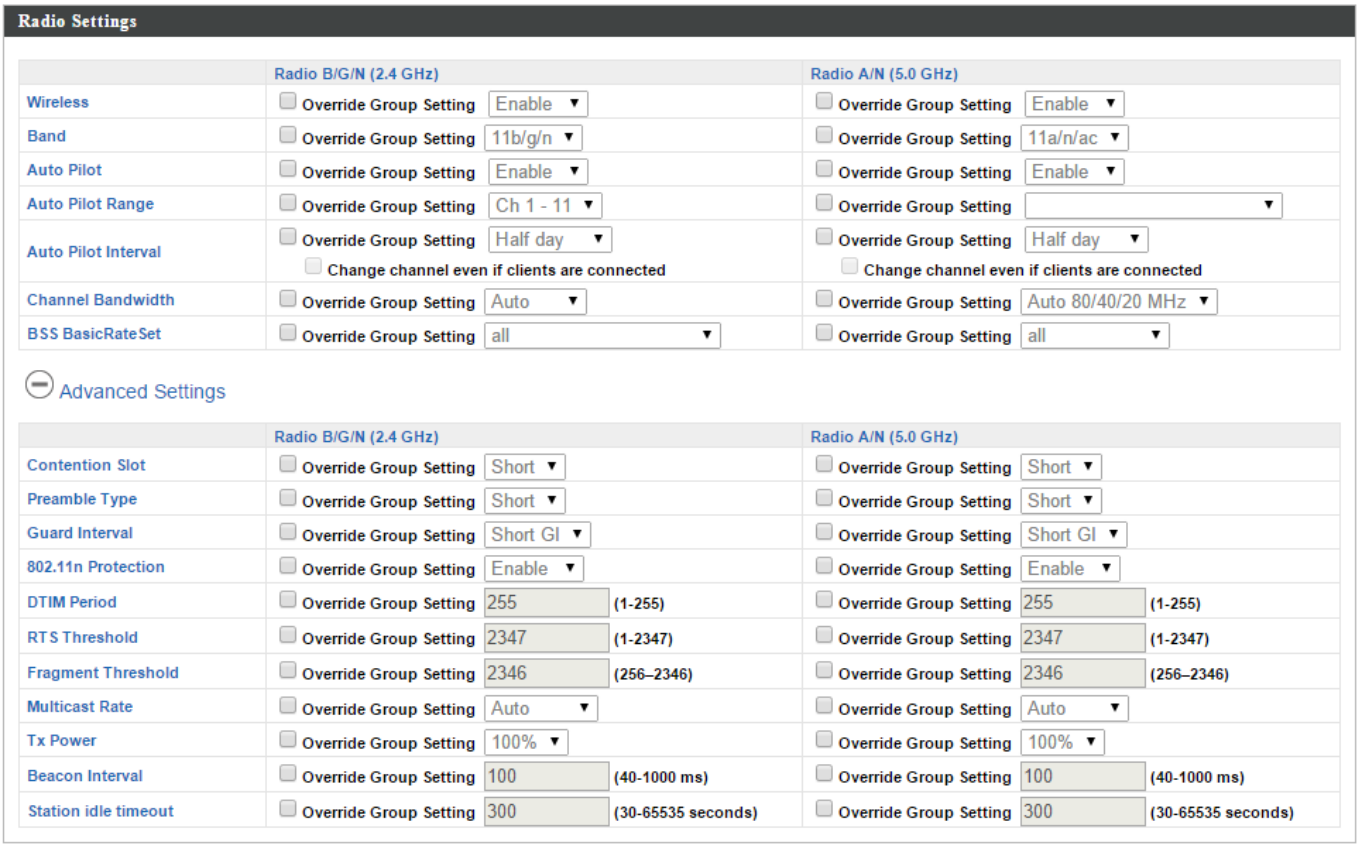
You can also use **Profile Settings** to assign the access point to WLAN, RADIUS and Access Control groups independently from Access Point Group settings.

Check the "**Override Group Settings**" box to use different individual settings for access points assigned to AP Groups:




| 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. |




| 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 |

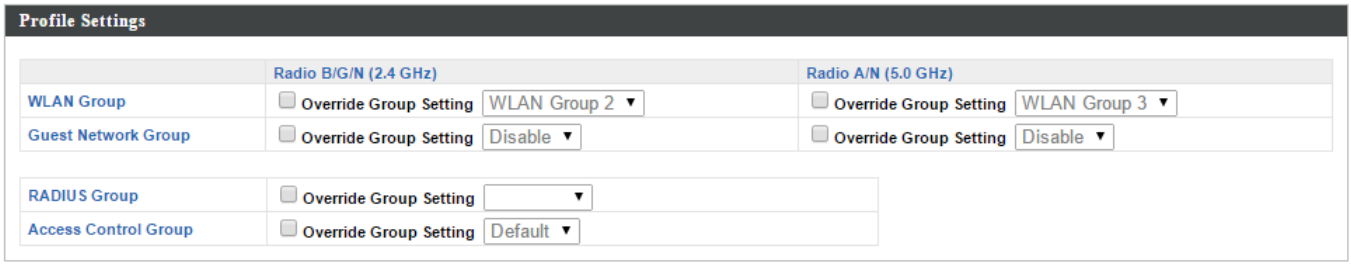
| | |
|---|---|
| | channel selection will automatically set the wireless channel for the access point's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually. |
| **Auto Pilot Range** | Select a range from which the auto channel setting (above) 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 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 **IV-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. |

| | |
|---|---|
| **802.11g 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. |
| **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 distantareas 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. |



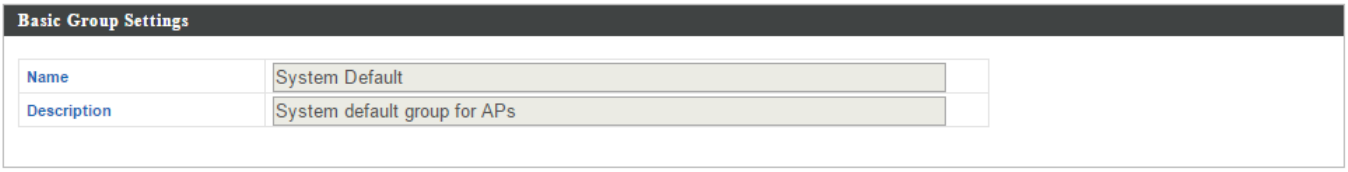
| Profile Settings | |
|---|---|
| **WLAN Group** | Assign the access point's 2.4GHz or 5GHz SSID(s) to a WLAN Group. You can edit WLAN groups in **NMS Settings → WLAN**. |
| **RADIUS Group** | Assign the access point's 2.4GHz SSID(s) to a RADIUS group. You can edit RADIUS groups in **NMS Settings → RADIUS**. |
| **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** |

## Add/Edit Access Point Group

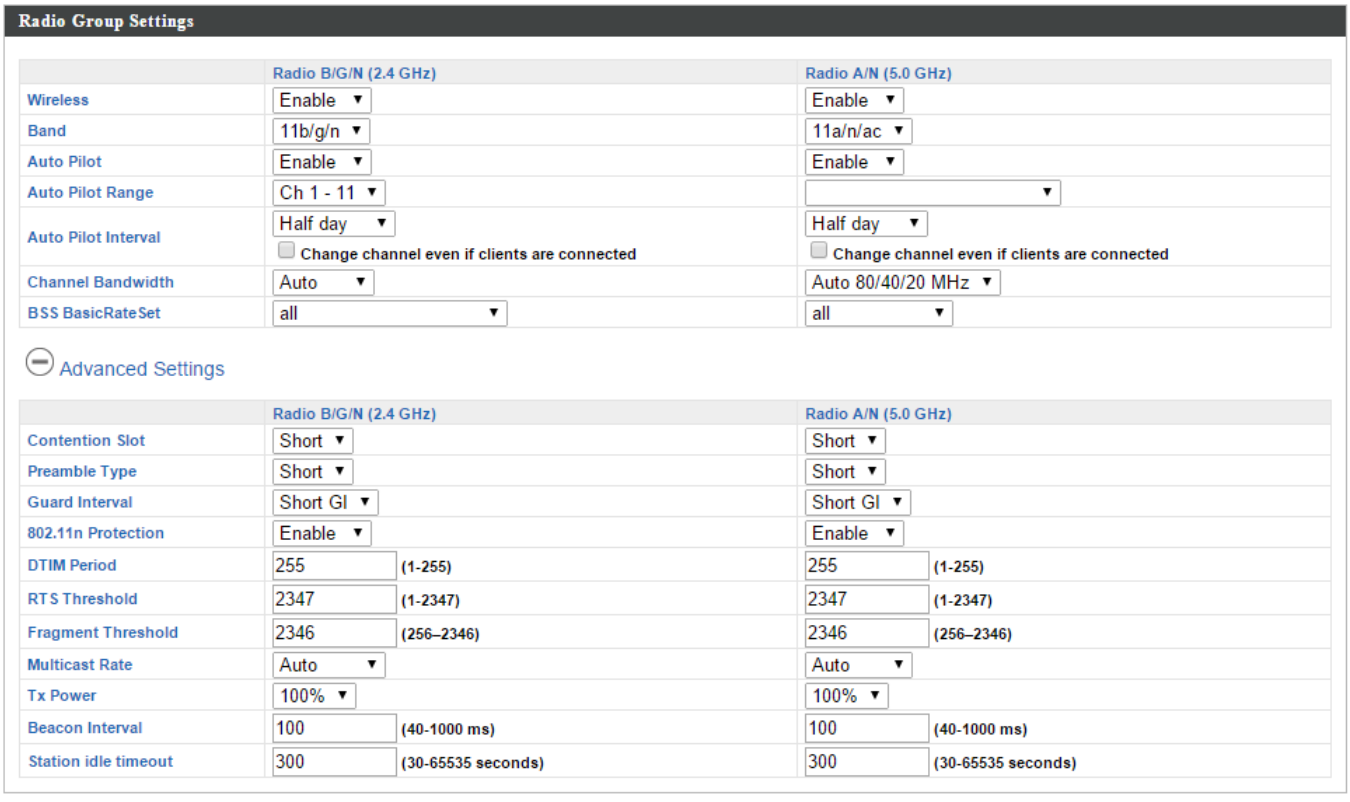
Configure your selected access point group. Access point group settings apply to all access points in the group, unless individually set to override group settings.

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

The **Group Settings** panel can be used to quickly move access points between exsiting 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** | Edit the access point group name. |
| **Description** | Enter a description of the access point group for reference e.g. 2nd Floor Office Group. |



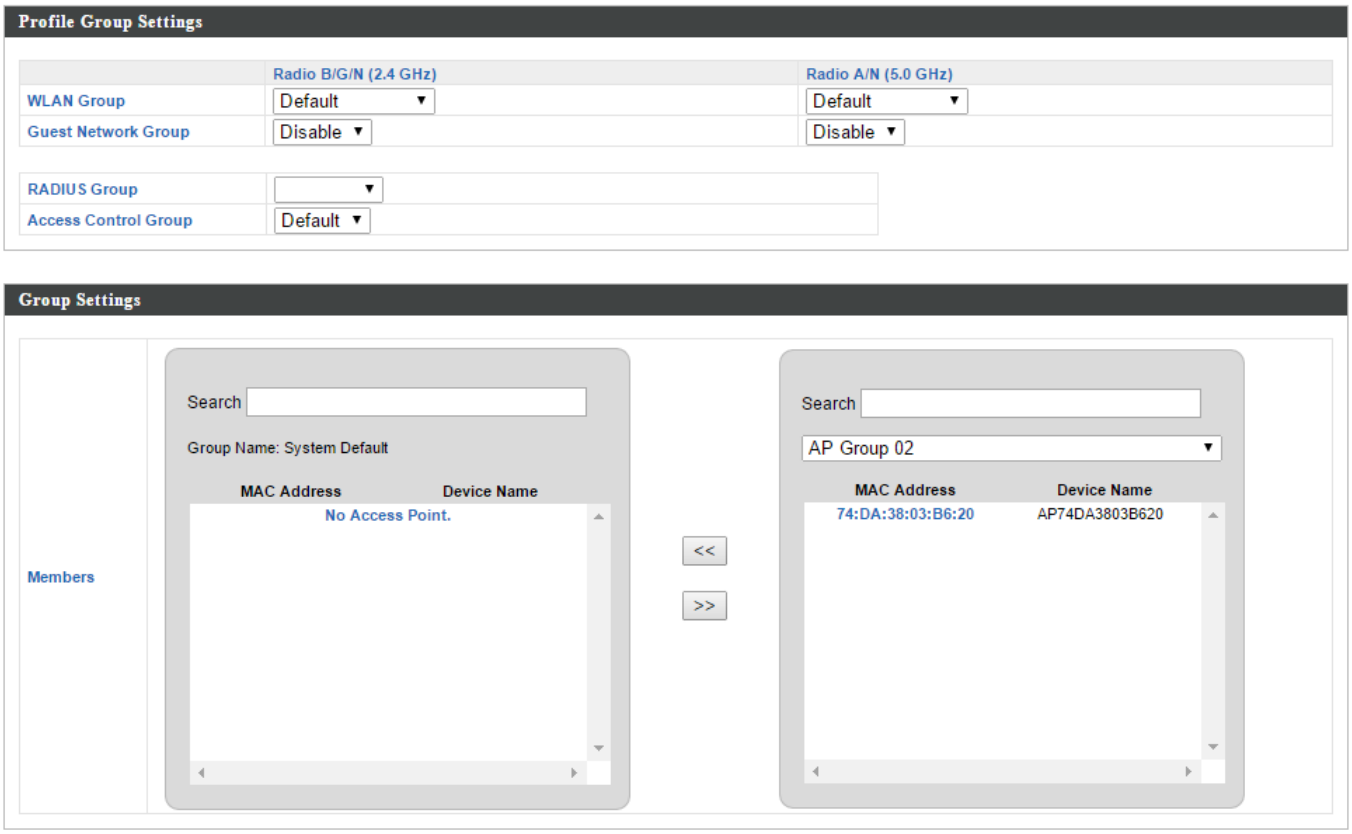
| Radio Group Settings | |
|---|---|
| **Wireless** | Enable or disable the access point group's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active. |
| **Band** | Select the wireless standard used for the access point group. Combinations of 802.11b, 802.11g, 802.11n & 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 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 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 **IV-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. |
| **802.11g 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. |
| **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 distantareas 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. |

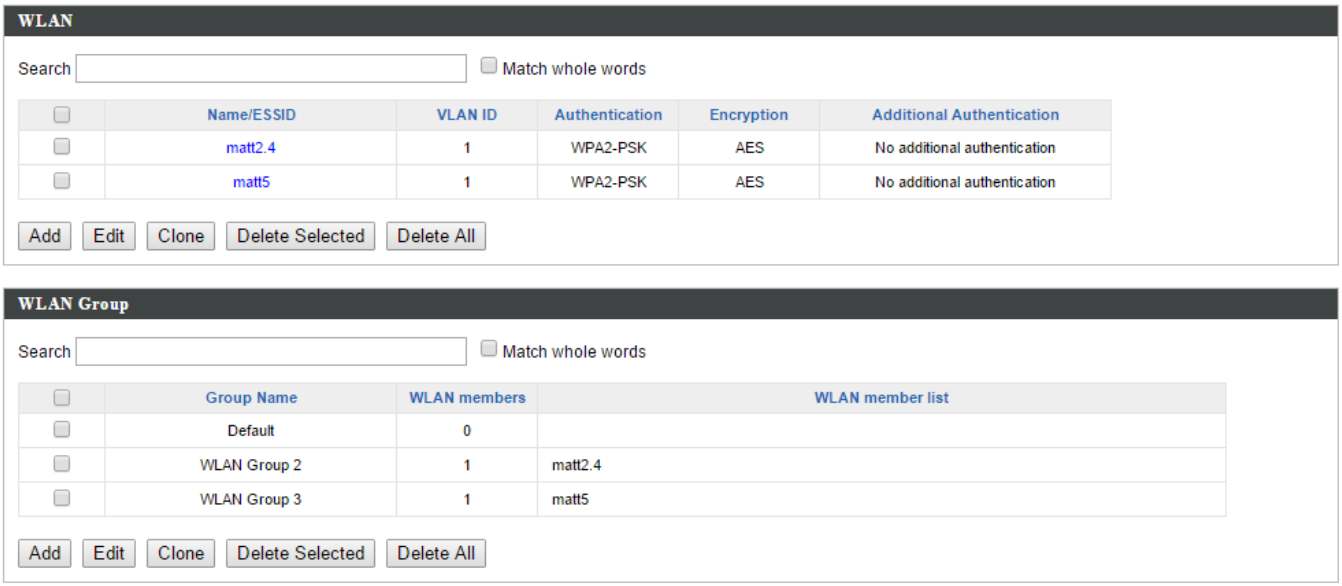



| Profile Group Settings | |
|---|---|
| **WLAN Group** | Assign the access point group's 2.4GHz or 5GHz SSIDs to a WLAN Group. You can edit WLAN groups in **NMS Settings → WLAN**. |
| **RADIUS Group** | Assign the access point group's 2.4GHz SSIDs to a RADIUS group. You can edit RADIUS groups in **NMS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

## IV-5-2. WLAN

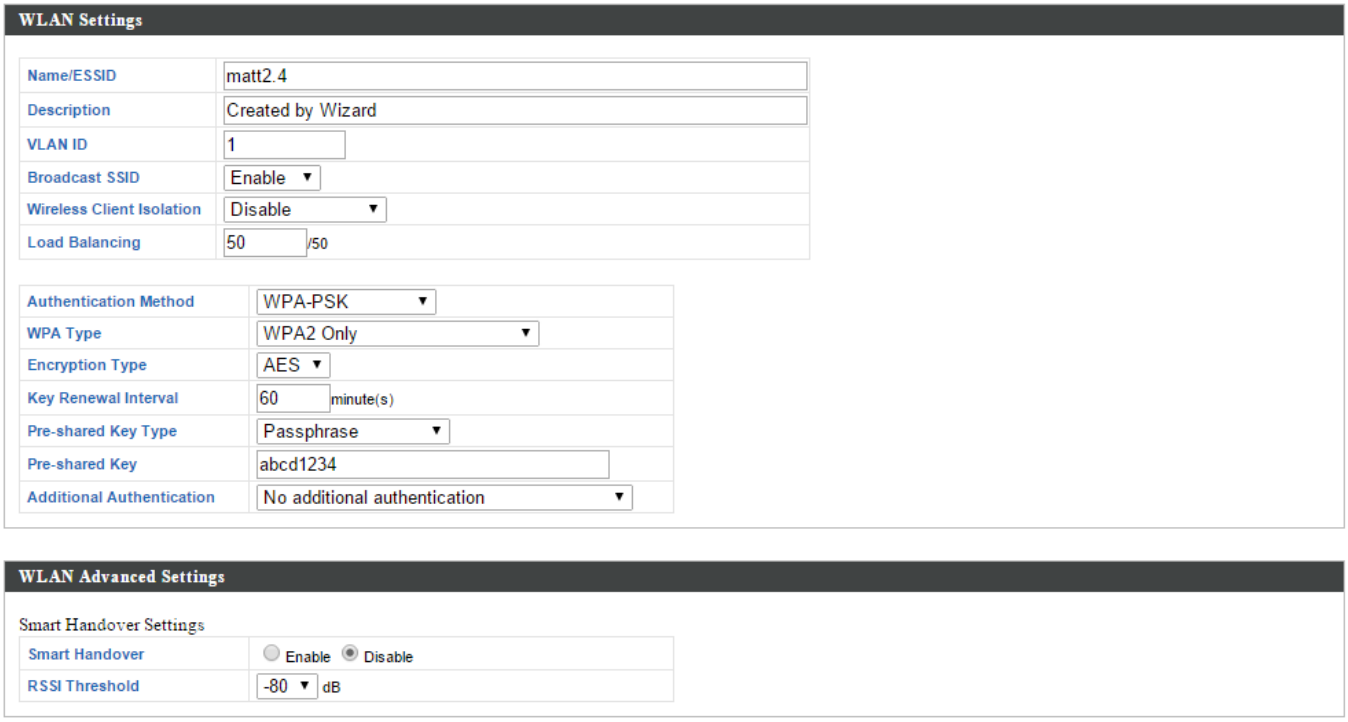
Displays information about each WLAN and WLAN group in the local network and allows you to add or edit WLANs & WLAN Groups. When you add a WLAN Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings**& access point group **Profile Group Settings**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


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

## Add/Edit WLAN




| WLAN Settings | |
|---|---|
| **Name/ESSID** | Edit the WLAN name (SSID). |
| **Description** | Enter a description of the SSID for reference e.g. 2nd Floor Office HR. |
| **SSID** | Select which SSID to configure security settings for. |
| **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. |
| **Load Balancing** | Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50). |
| **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's essential to configure wireless security in order to prevent unauthorised access to your network.***

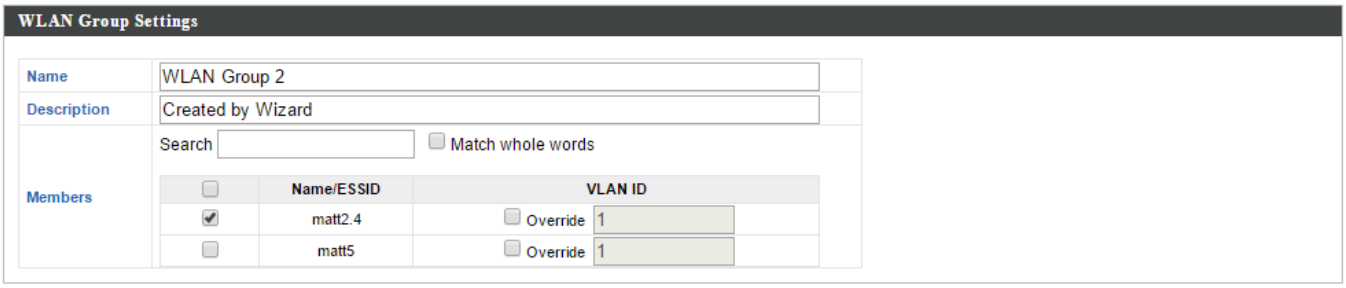
***Select hard-to-guess passwords which include combinations of numbers, letters and symbols, and change your password regularly.***

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

| WLAN Advanced Settings | |
|---|---|
| **RSSI Threshold** | Set a RSSI Threshold level. |

## 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** (**IV-5-1.**)



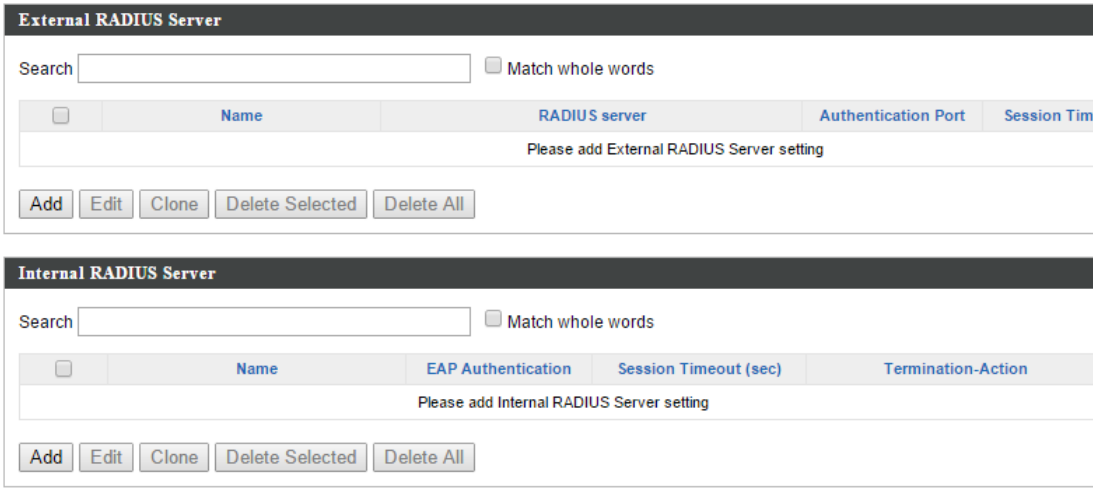

| WLAN Group Settings | |
|---|---|
| **Name** | Edit the WLAN Group name. |
| **Description** | Enter a description of the WLAN Group for reference e.g. 2nd Floor Office HR Group. |
| **Members** | Select SSIDs to include in the group using the checkboxes and assign VLAN IDs. |

## IV-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** (**IV-5-1.**)

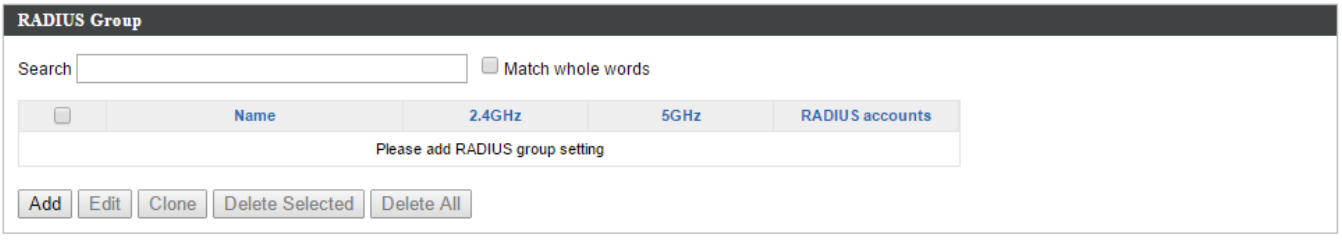
The **search** function can be used to locate a RADIUS Server, Account or Group. Type in the search box and the list will update:


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

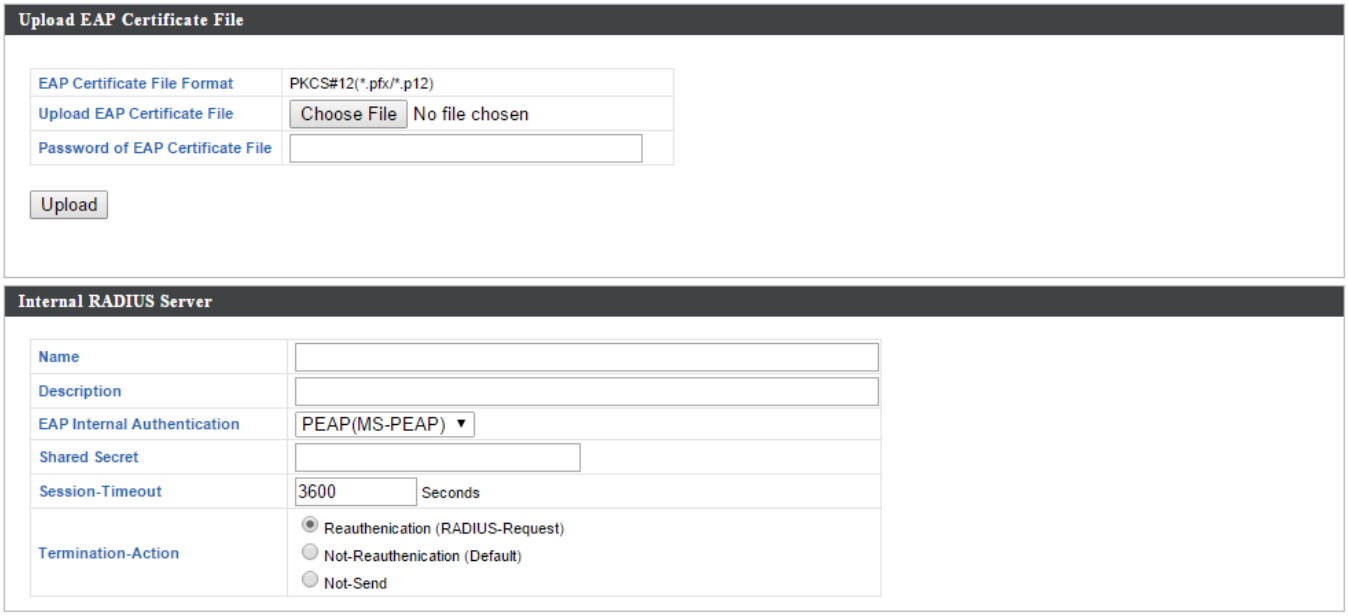




## Add/Edit External RADIUS Server


| | |
|---|---|
| **Name** | Enter a name for the RADIUS Server. |
| **Description** | Enter a description of the RADIUS Server for reference. |
| **RADIUS Server** | Enter the RADIUS server host IP address. |
| **Authentication Port** | Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535. |
| **Shared Secret** | Enter a shared secret/password between 1 – 99 characters in length. This should match the "MAC-RADIUS" password used in **IV-3-1-3-6** or **IV-3-2-3**. |
| **Session Timeout** | Set a duration of session timeout in seconds between 0 – 86400. |
| **Accounting** | Enable or disable RADIUS accounting. |
| **Accounting Port** | When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between 1 – 65535. |




## Add/Edit Internal RADIUS Server

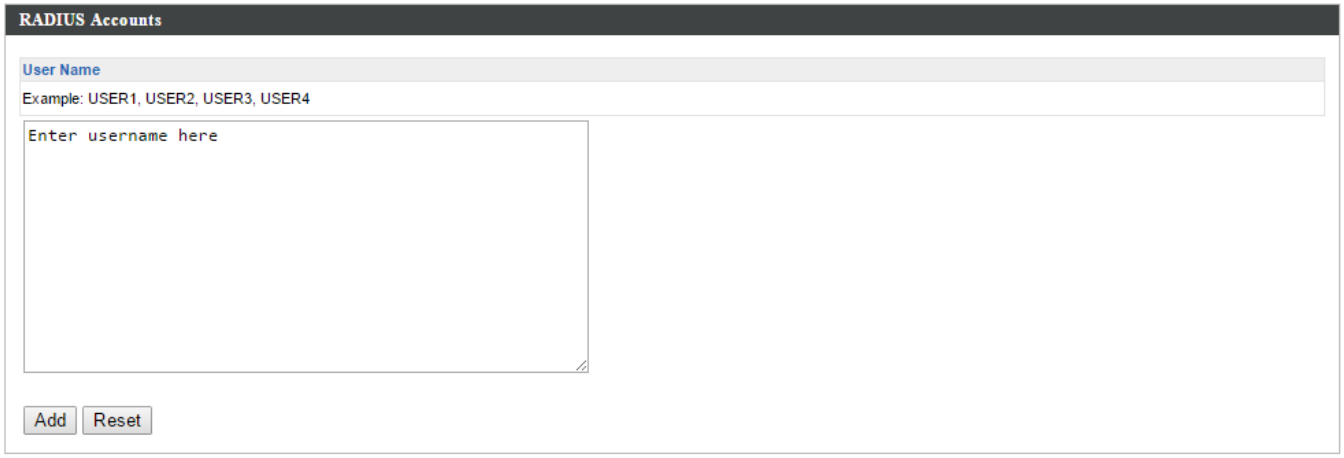
| Upload EAP Certificate File | |
|---|---|
| **EAP Certificate File Format** | Displays the EAP certificate file format: PCK#12(*.pfx/*.p12) |
| **EAP Certificate File** | Click “Upload” to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded,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

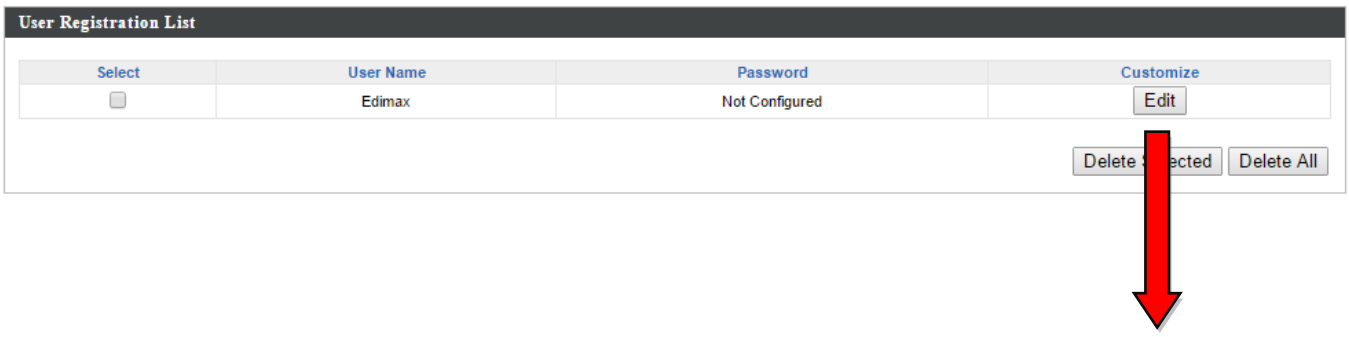
| **Internal RADIUS Server** | |
|---|---|
| **Name** | Enter a name for the Internal RADIUS Server. |
| **Description** | Enter a description of the Internal RADIUS Server for reference. |
| **EAP Certificate File Format** | Displays the EAP certificate file format: PCK#12(*.pfx/*.p12) |
| **EAP Certificate 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. |

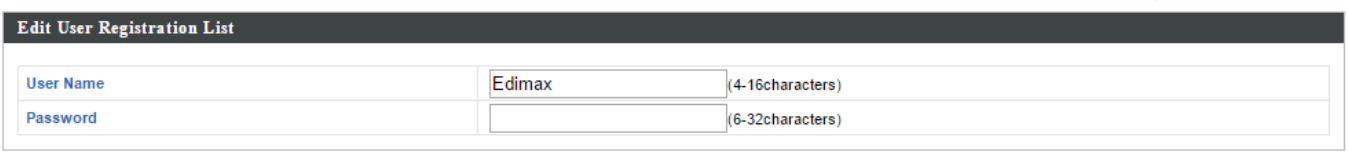
| | |
|---|---|
| **Shared Secret** | Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length. |
| **Session Timeout** | Set a duration of session timeout in seconds between 0 – 86400. |
| **Termination Action**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

## Add/Edit 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** | 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. |

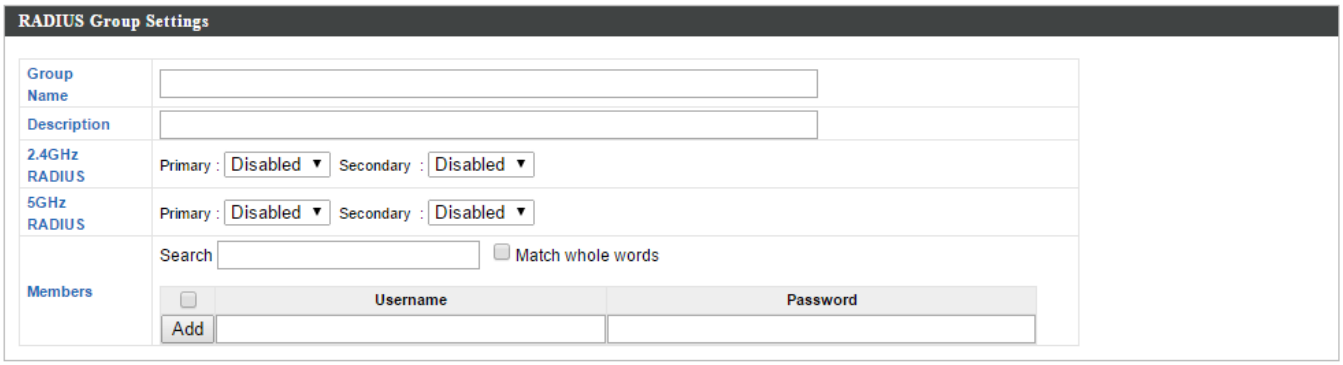
| User Registration List | |
|---|---|
| **Select** | Check the box to select a user. |
| **User Name** | Displays the user name. |
| **Password** | Displays if specified user name has a password (configured) or not (not configured). |
| **Customize** | Click “Edit” to open a new field to set/edit a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

| 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. |

## 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** (**IV-5-1.**)




| 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(Maximun 5). |

## IV-5-4. Access Control

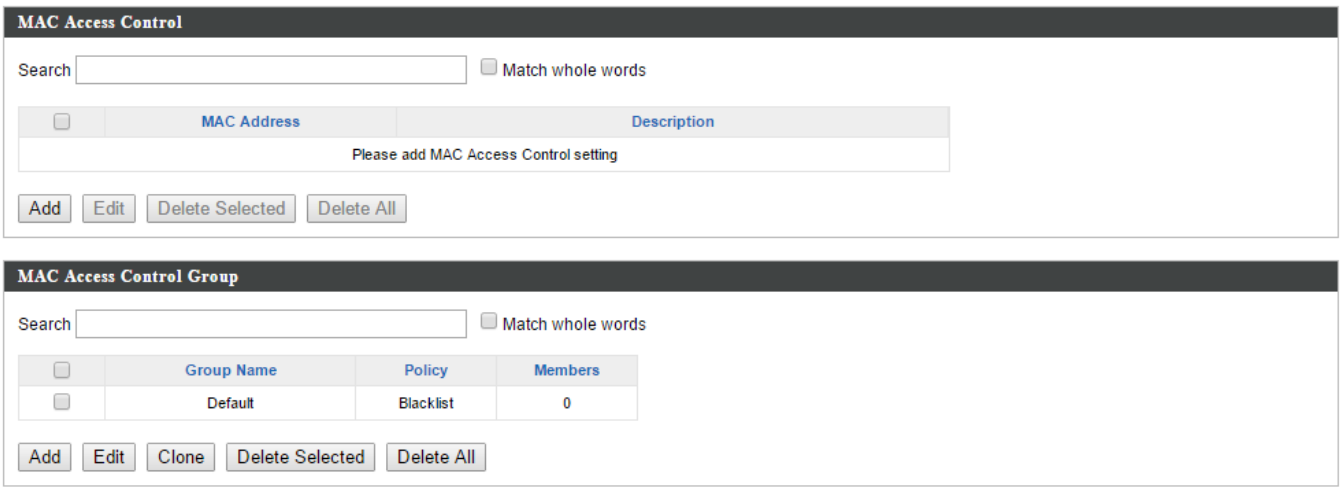
MAC Access Control is a security feature that can help to prevent unauthorized users from connecting to your access point.

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

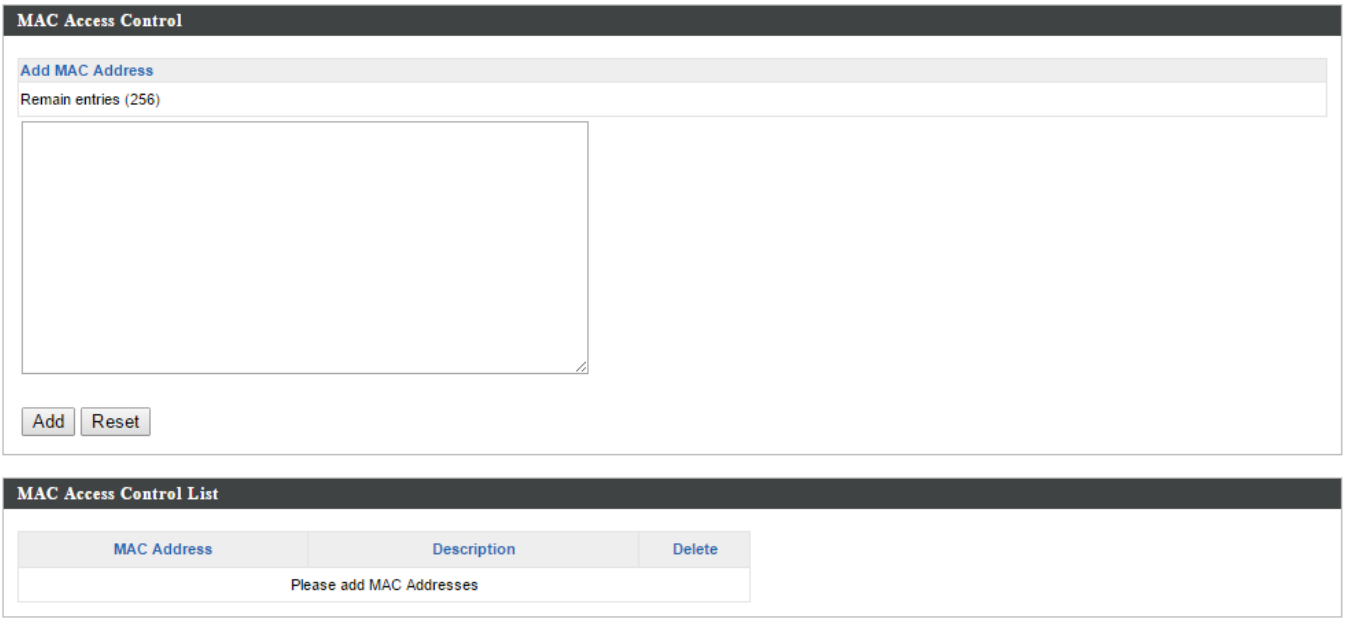
TheAccess Control paneldisplays information about MAC Access Control & MAC Access Control Groups and Groups and allows you to add or edit MAC Access Control & MAC Access Control Group settings. When you add an Access Control Group, it will be available for selection in **NMS Settings → Access Point** access point **Profile Settings**& access point group **Profile Group Settings** (**IV-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:


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

## Add/Edit MAC Access Control



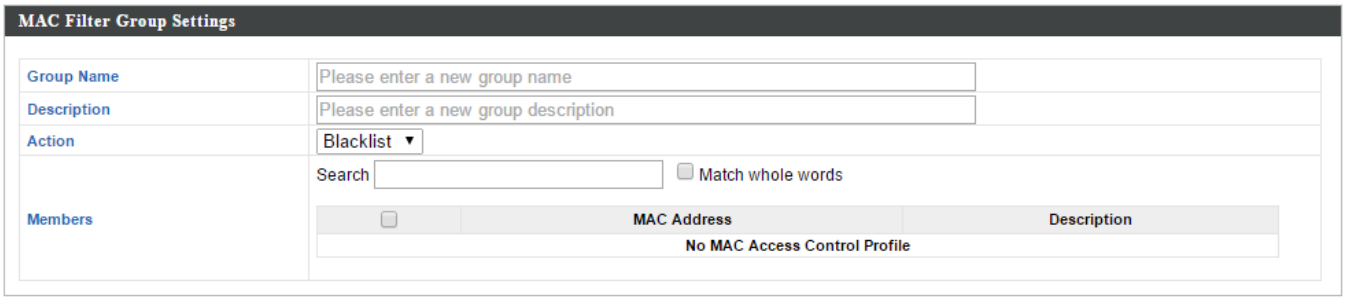

| | |
|---|---|
| **Add MAC Address** | Enter a MAC address of computer or network device manually e.g. ‘aa-bb-cc-dd-ee-ff’ or enter multiple MAC addresses separated with commas, e.g. ‘aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg’ |
| **Add** | Click “Add” to add the MAC address to the MAC address filtering table.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

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

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

## Add/Edit 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** (**IV-5-1.**)

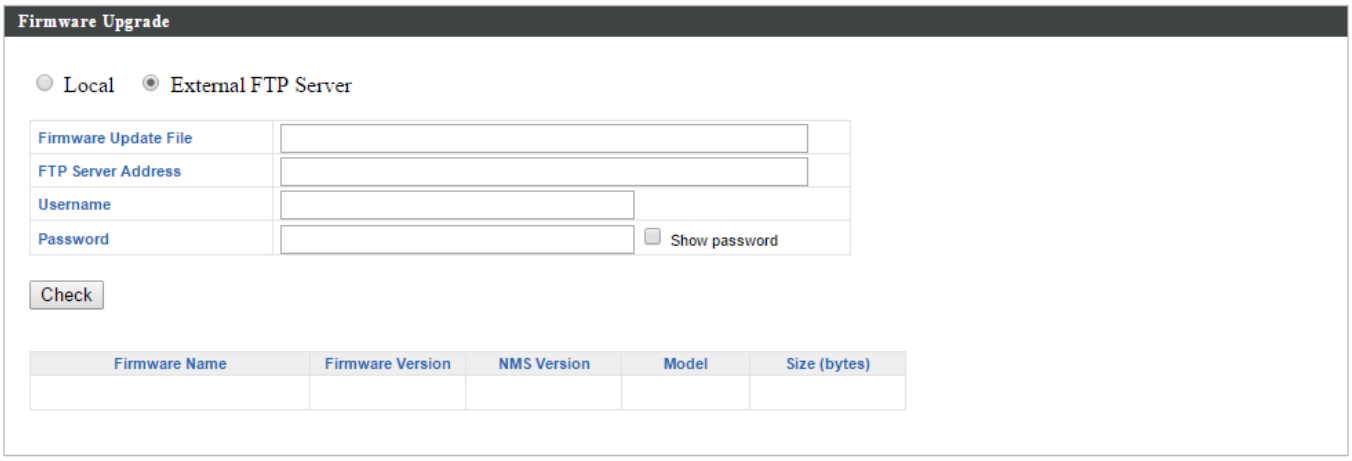


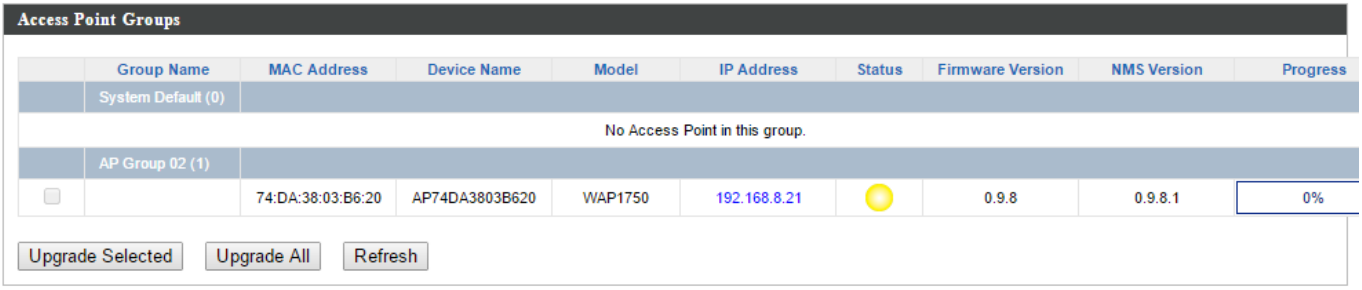

| MAC Filter Group Settings | |
|---|---|
| **Group Name** | Edit the MAC Access Control Group name. |
| **Description** | Enter a description of the MAC Access Control Group for reference. |
| **Action** | Select “Blacklist” to deny access to specified MAC addresses in the group, and select “Whitelist”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

## IV-5-5. 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.



## IV-5-6. Advanced

### IV-5-6-1. System Security

Configure the NMS system login name and password.

# IV-6. Local Network

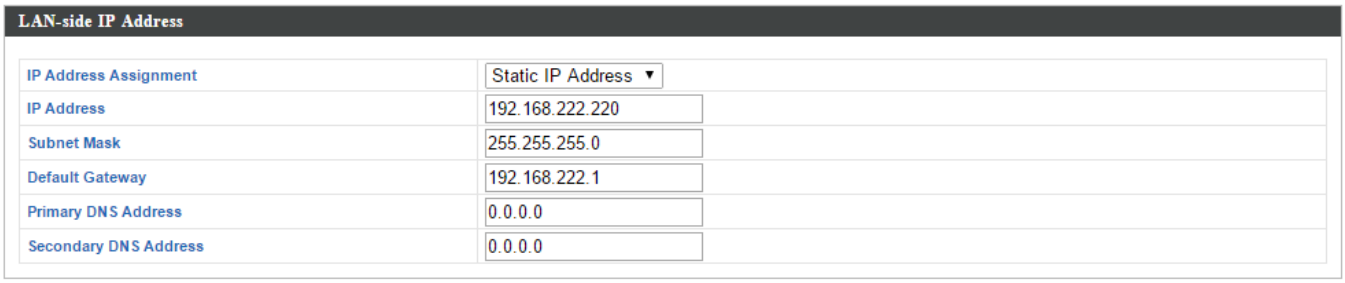
## IV-6-1. Network Settings

### IV-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.

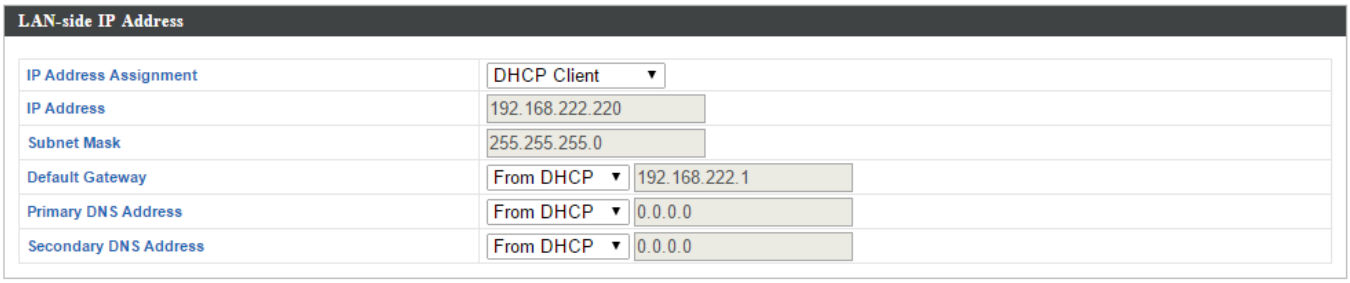
***The access point’s default IP address is 192.168.2.2***

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

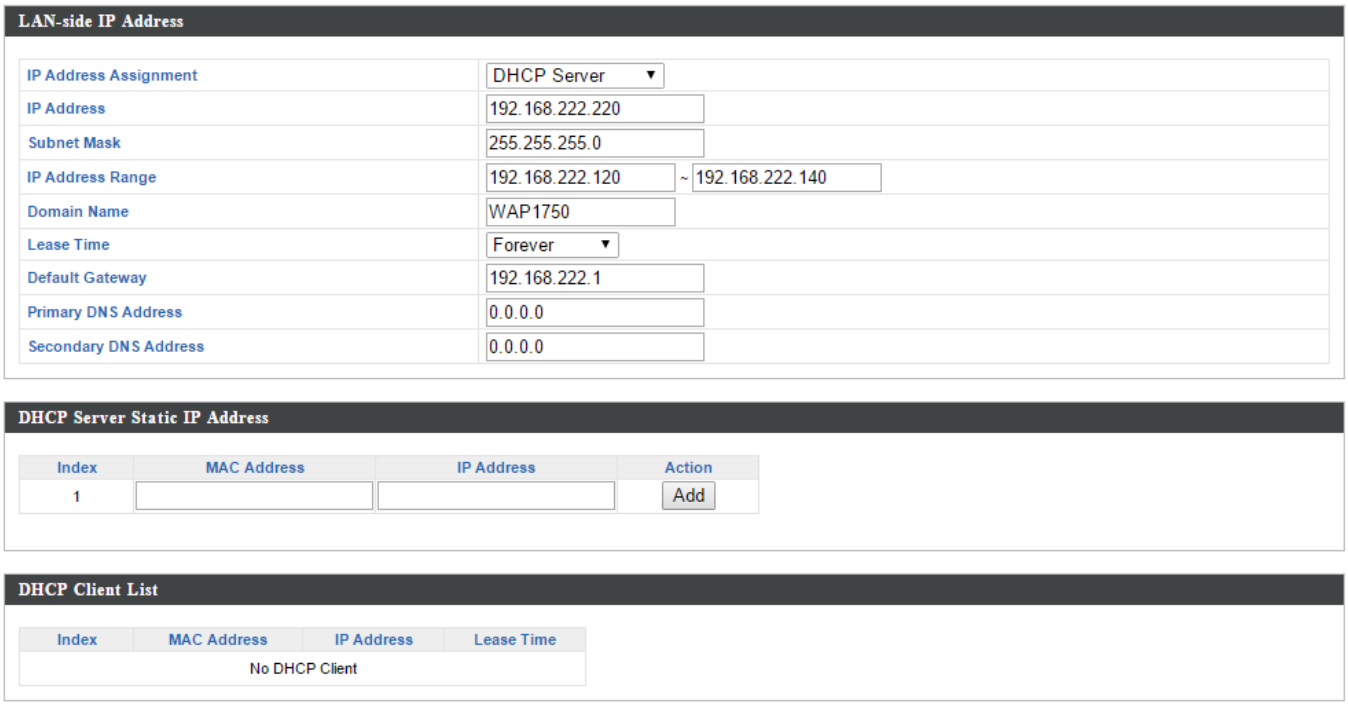



| LAN-side IP Address | |
|---|---|
| **IP Address Assignment** | Select “Static IP” to manually specify a static/fixed IP address for your access point. Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server, or select “DHCP Server” for your access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




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



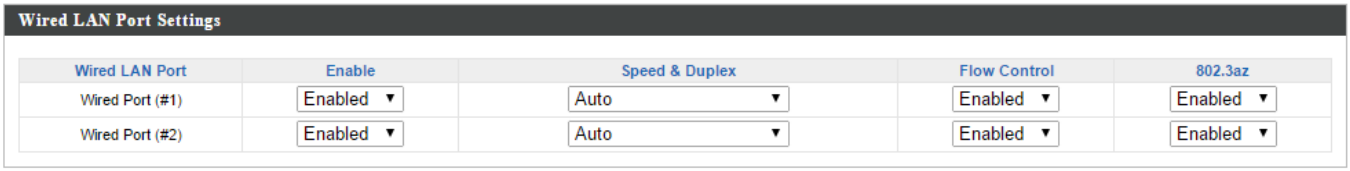

| DHCP Server | |
|---|---|
| **IP Address** | Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address. |
| **Subnet Mask** | Specify a subnet mask. The default value is 255.255.255.0 |
| **IP Address Range** | Enter the start and end 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. |

### IV-6-1-2. LAN Port Settings

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

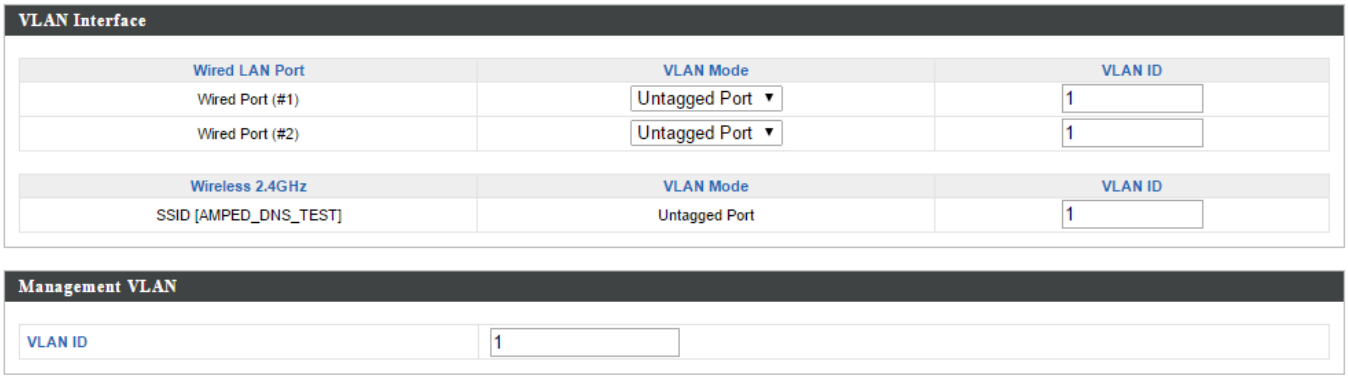



| **Wired LAN Port** | Identifies LAN port 1 or 2. |
|---|---|
| **Enable** | Enable/disable specified LAN port. |
| **Speed & Duplex** | Select a speed & duplex type for specified LAN port, or use the “Auto” value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packets 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. |

## IV-6-1-3. VLAN

The “VLAN” (Virtual Local Area Network) page 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 1 – 4094 are supported.

***VLAN IDs in the range 1 – 4094 are supported.***




| VLAN Interface | |
|---|---|
| **Wired LAN Port/Wireless** | Identifies LAN port 1 or 2 and wireless SSIDs (2.4GHz or 5GHz). |
| **VLAN Mode** | Select “Tagged Port” or “Untagged Port” for specified LANinterface. |
| **VLAN ID** | Set a VLAN ID for specified interface, if “Untagged Port” is selected. |

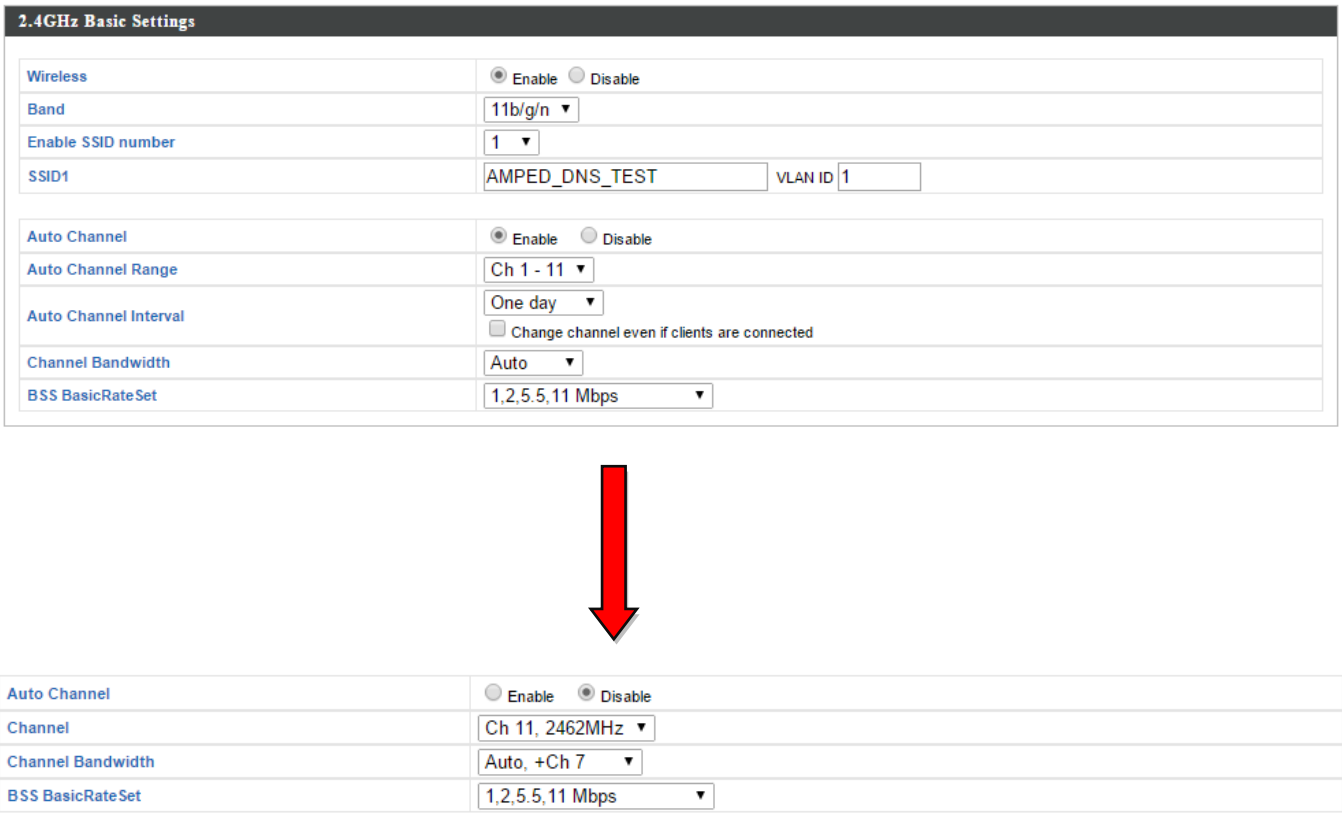
| Management VLAN | |
|---|---|
| **VLAN ID** | Specify the VLAN ID of the management VLAN. Only the hosts belonging to the sameVLAN can manage the device. |

## IV-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 four categories: Basic, Advanced, Security and WDS.

### IV-6-2-1. Basic

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



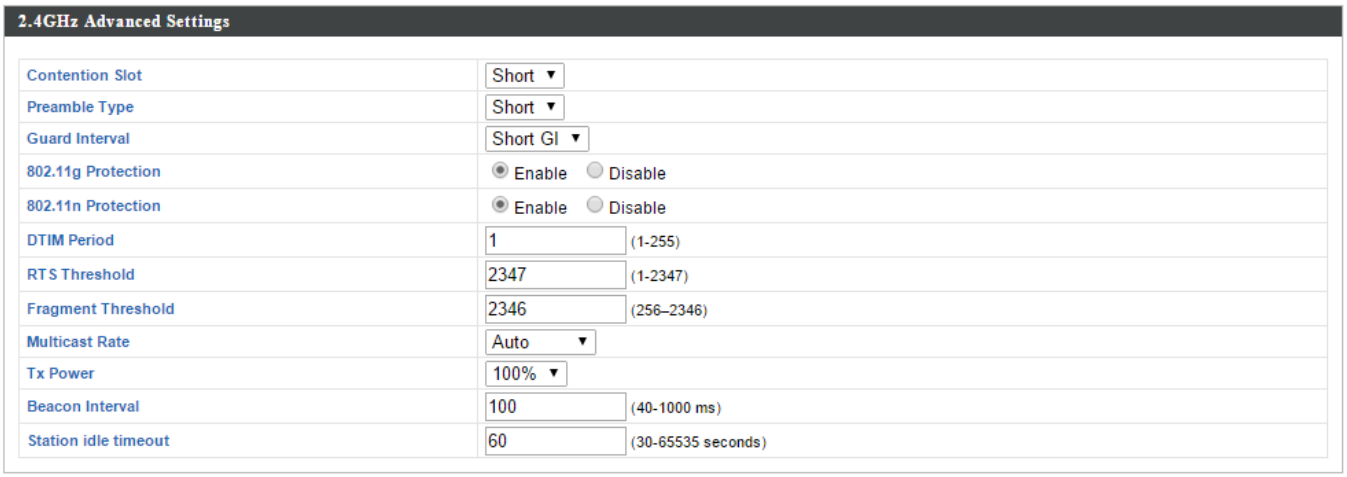

When auto channel is disabled, select a wireless channel manually:

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

## IV-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.***




| | |
|---|---|
| **Contention Slot** | Select “Short” or “Long” – this value is used for contention windows in WMM (see **IV-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. |
| **802.11g 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.) |

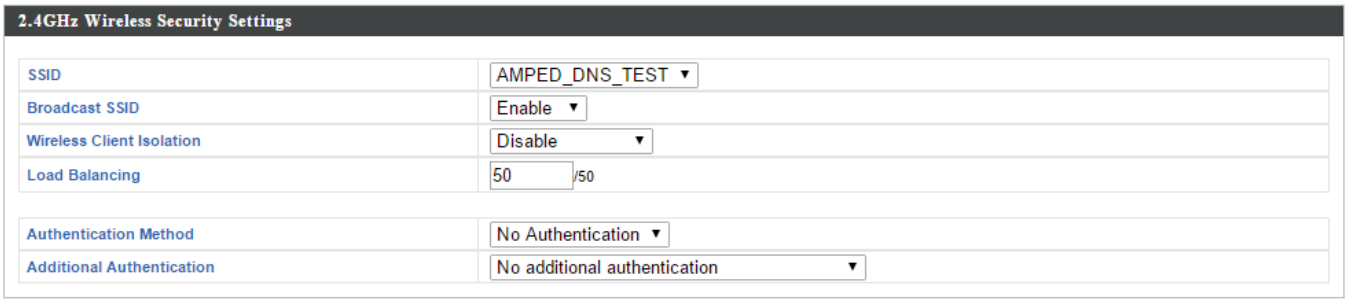
| | |
|---|---|
| **802.11n Protection** | Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.) |
| **DTIM Period** | Set 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. |
| **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 distantareas 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. |

### IV-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's 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.***




| | |
|---|---|
| **SSID** | 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 50). |
| **Authentication Method** | Select an authentication method from the drop down menu and refer to the information below appropriate for your method. |
| **Additional Authentication** | Select an additional authentication method from the drop down menu and refer to the information below (**IV-6-2-3-6.**) appropriate for your method. |

### IV-6-2-3-1. No Authentication

Authentication is disabled and no password/key is required to connect to the access point.

***Disabling wireless authentication is not recommended. When disabled, anybody within range can connect to your device's SSID.***

### IV-6-2-3-2. WEP

WEP (Wired Equivalent Privacy) is abasic encryption type. For a higher level of security consider using WPA encryption.

| | |
|---|---|
| **Key Length** | Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended. |
| **Key Type** | Choose from "ASCII" (anyalphanumericalcharacter0-9,a-zandA-Z) or "Hex" (any characters from 0-9,a-f andA-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. |

### IV-6-2-3-3. IEEE802.1x/EAP

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

### IV-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.

| | |
|---|---|
| **WPA Type** | Select from WPA/WPA2 Mixed Mode-PSK, WPA2 or WPA only. WPA2 is safer than WPA only, but 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 andA-F). |
| **Pre-Shared Key** | Please enter a security key/password according to the format you selected above. |

### IV-6-2-3-5. WPA-EAP

| | |
|---|---|
| **WPA Type** | Select from WPA/WPA2 Mixed Mode-EAP, WPA2-EAP or WPA-EAP. |
| **Encryption** | 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.***

### IV-6-2-3-6. Additional Authentication

Additional wireless authentication methods can also be used:

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

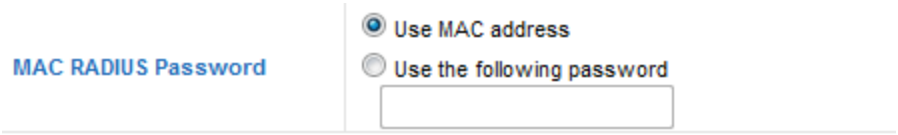
***See** IV-6-6.MAC Filter **to configure MAC filtering.***

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

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

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

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



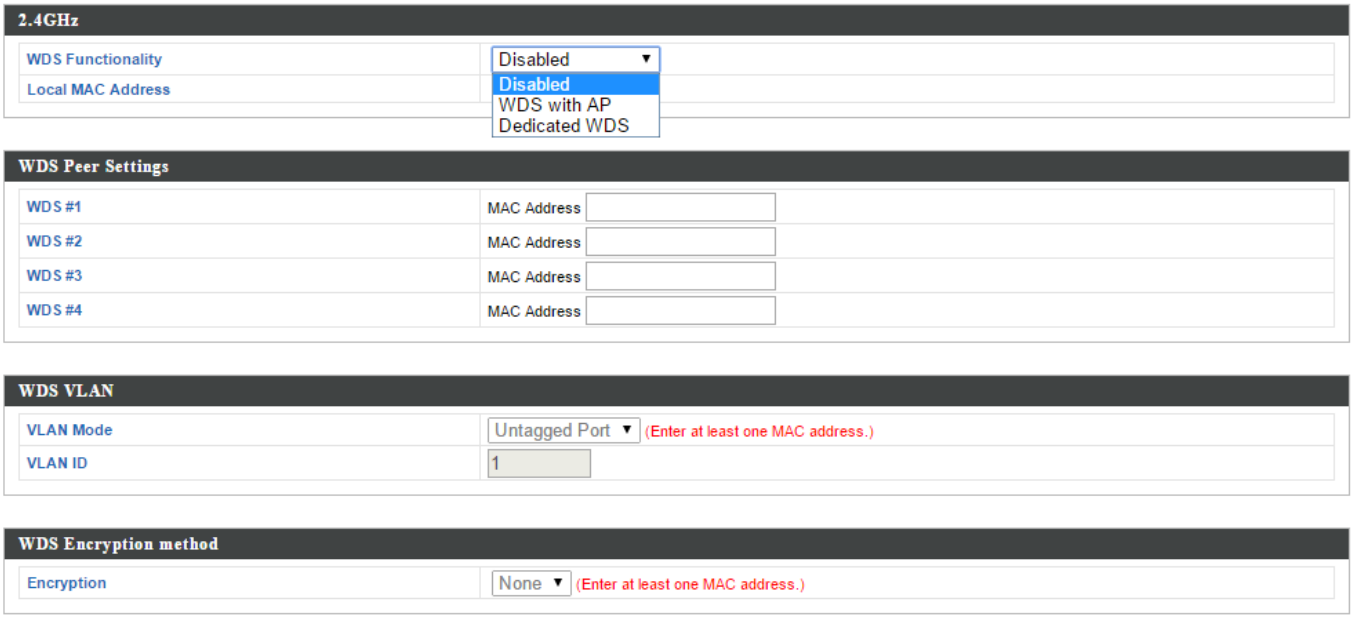

| | |
|---|---|
| **MAC RADIUS Password** | Select whether to use MAC address or password authentication via RADIUS server. If you select “Use the following password”, enter the password in the field below. The password should match the “Shared Secret” used in **IV-6-5. RADIUS**. |

## IV-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** | 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. |

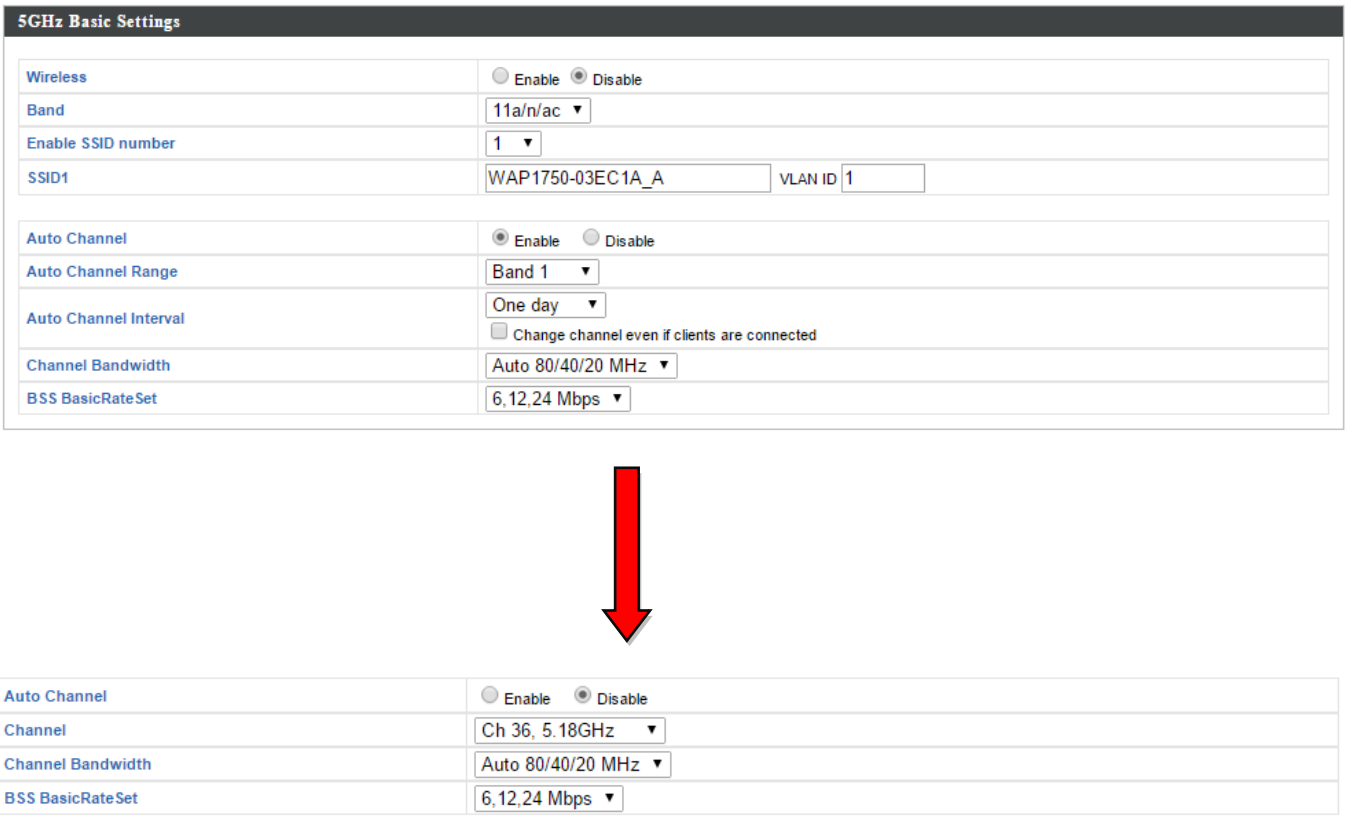
| WDS Encryption method | |
|---|---|
| **Encryption** | Select whether to use “None” or “AES” encryption and enter a pre-shared key for AESconsisting of 8-63 alphanumeric characters. |

## IV-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 four categories: Basic, Advanced, Security and WDS.

### IV-6-3-1. Basic

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




| | |
|---|---|
| **Wireless** | Enable or disable the access point’s 5GHz wireless radio. When disabled, no 5GHz SSIDs will be active. |
| **Band** | Select the 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 5GHz frequency from the drop down menu. A maximum of 16 can be enabled. |

| | |
|---|---|
| **SSID#** | Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters. |
| **VLAN ID** | Specify a VLAN ID for each SSID. |
| **Auto Channel** | Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 5GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table. |
| **Auto Channel Range** | Select a range from which the auto channel setting (above) will choose a channel. |
| **Auto Channel 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 Bandwidth** | Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level). |
| **BSS BasicRate Set** | Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients. |

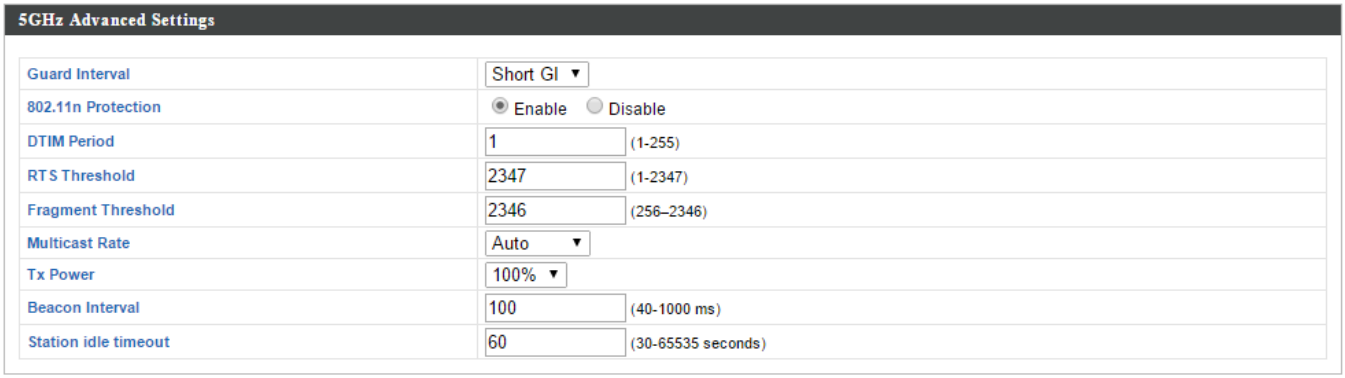
When auto channel is disabled, select a wireless channel manually:

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

## IV-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.***




| | |
|---|---|
| **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 distantareas will not be able to access your signal. |

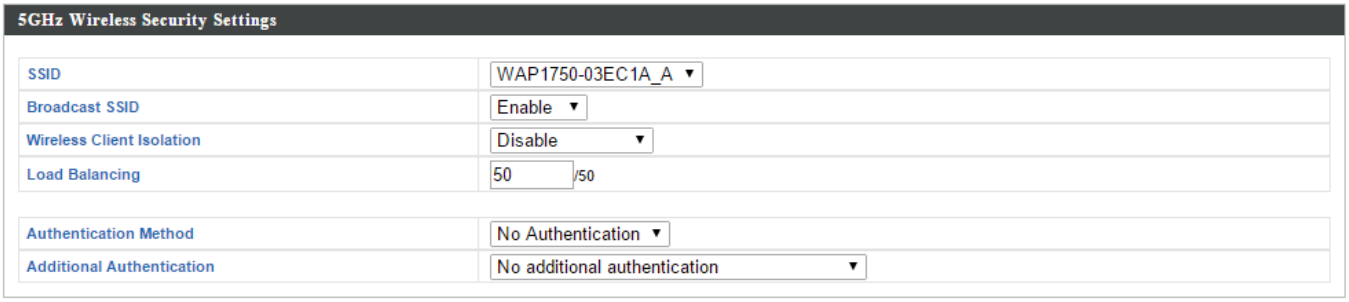
| | |
|---|---|
| **Beacon Interval** | Set the beacon interval of the wireless radio. The default value is 100. |
| **Station idle timeout** | Set the interval for keepalive messages from the access point to a wireless client to verify if the station is still alive/active. |

### IV-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.***

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




| | |
|---|---|
| **SSID** | 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 50). |
| **Authentication Method** | Select an authentication method from the drop down menu and refer to the information below appropriate for your method. |
| **Additional Authentication** | Select an additional authentication method from the drop down menu and refer to the information below appropriate for your method. |

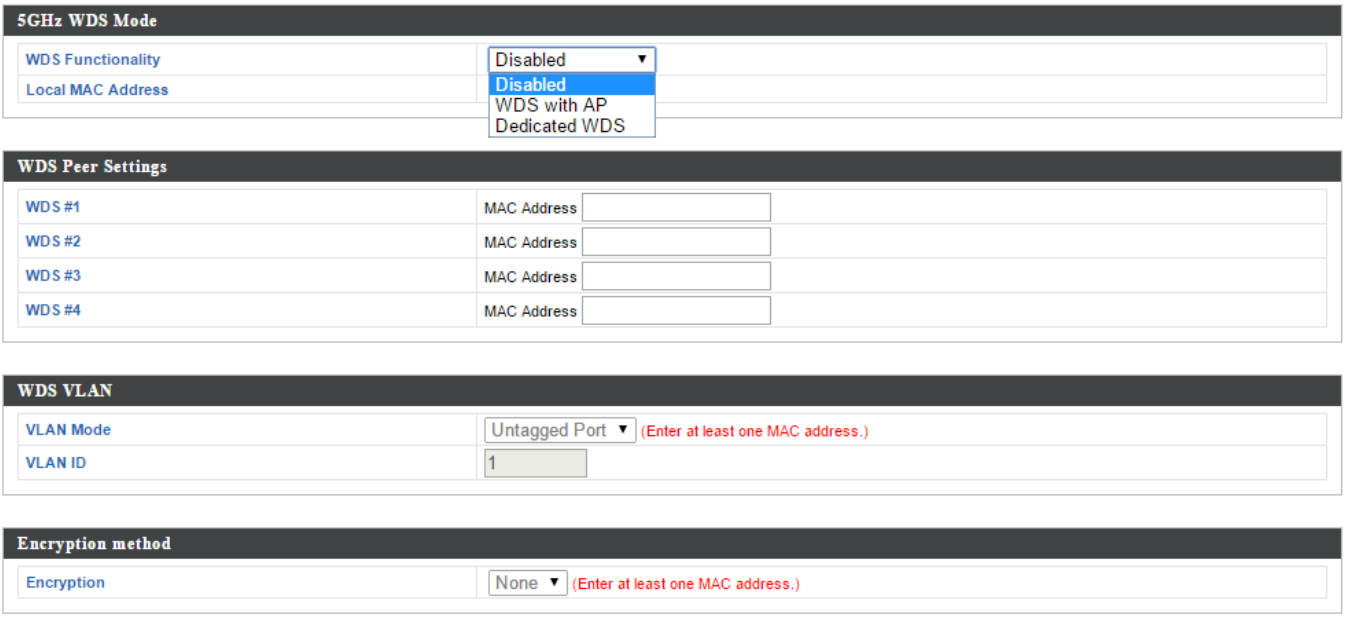
Please refer back to **IV-6-2-3. Security** for more information on authentication and additional authentication types.

## IV-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** | 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. |

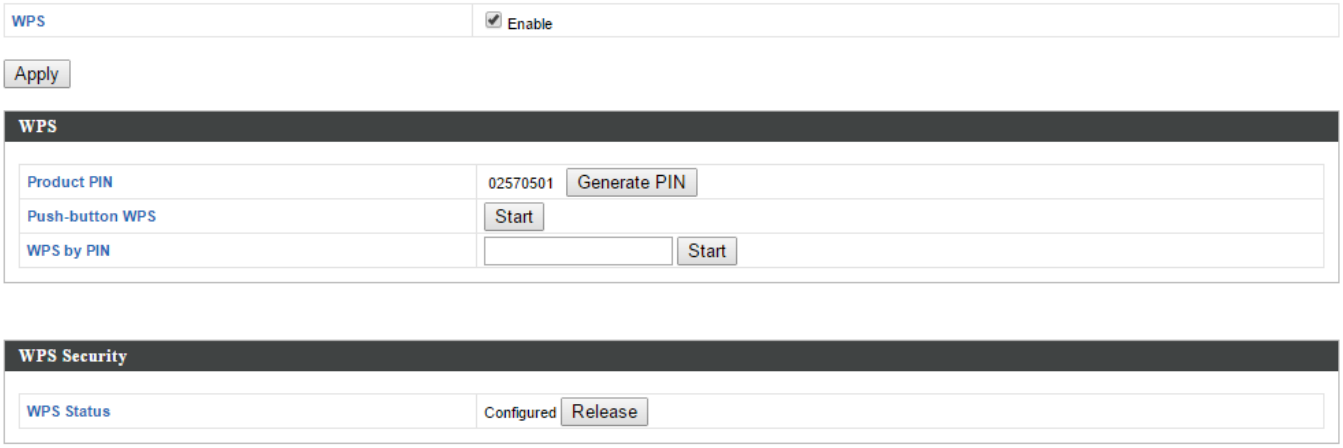
| WDS VLAN | |
|---|---|
| **VLAN Mode** | Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”. |
| **VLAN ID** | Specify the WDS VLAN ID when “Untagged Port” is selected above. |

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

## IV-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 device or from within the device's firmware/configuration interface (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

***Please refer to manufacturer's instructions for your other WPS device.***




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

| | |
|---|---|
| **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. This has the same effect as physically pushing the access point's WPS button. |
| **WPS by PIN** | Enter the PIN code of another WPS device and click "Start" to attempt to establish a WPS connection for approximately 2 minutes. |

| | |
|---|---|
| **WPS Status** | WPS security status is displayed here. Click "Release" to clear the existing status. |

### IV-6-5. RADIUS

The RADIUS sub menu allows you to configure the access point's RADIUS server settings, categorized into three submenus: RADIUS settings, Internal Server and RADIUS accounts.

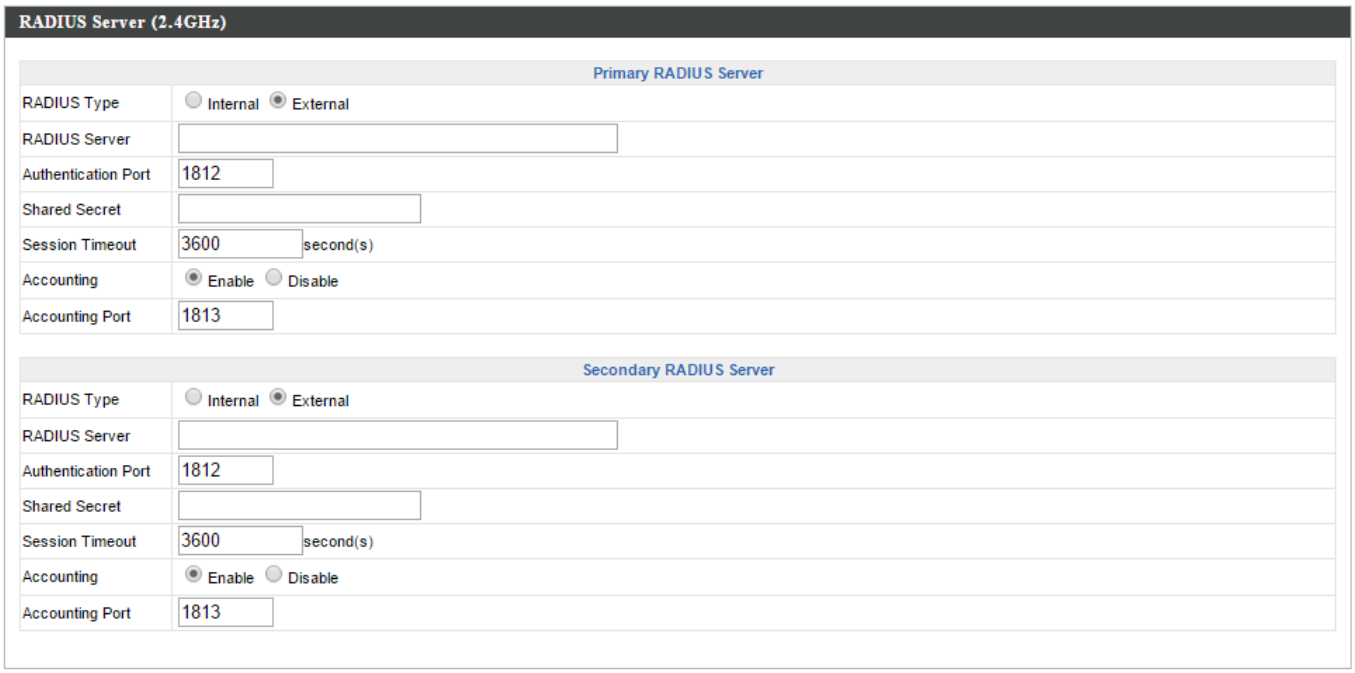
A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

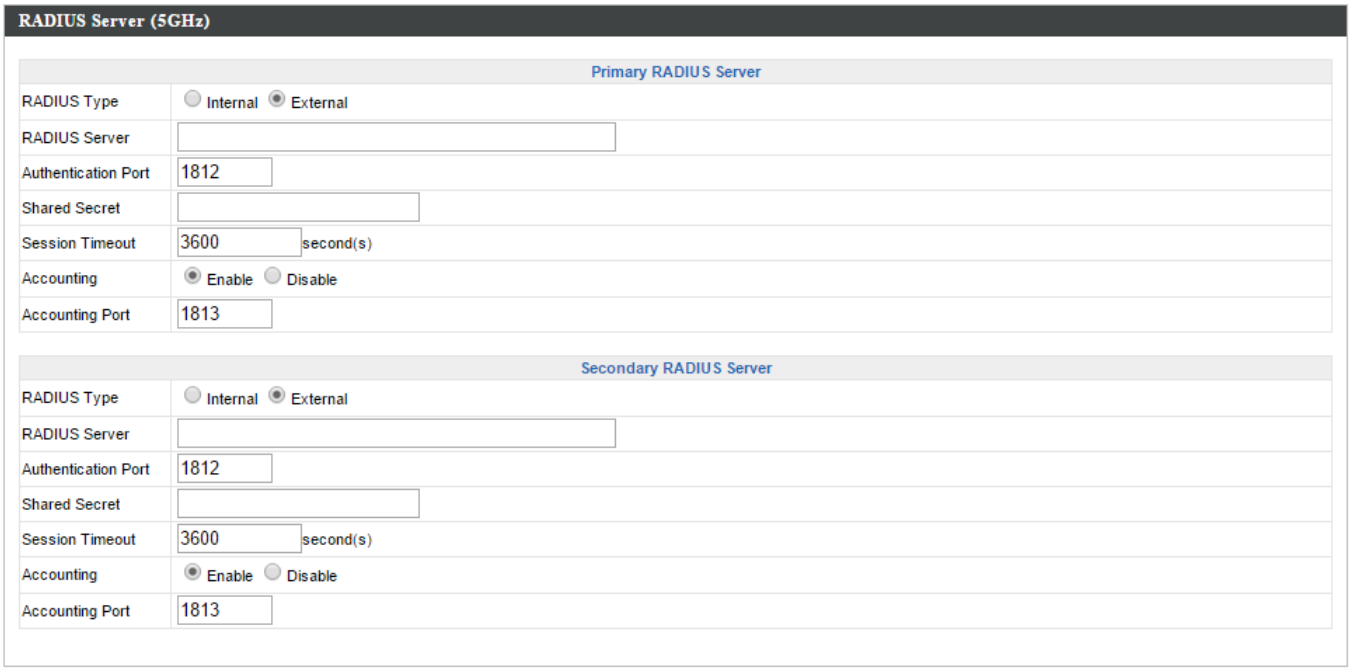
The access point can utilize both a primary and secondary (backup) RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz). External RADIUS servers can be used or the access point's internal RADIUS server can be used.

***To use RADIUS servers, go to*** *"Local Network"* →*"Security"* →*"Additional Authentication"* ***and select*** *"MAC RADIUS Authentication"* ***(see*** *IV-6-2-3.* ***&****IV-6-3-3****).***

## IV-6-5-1. RADIUS Settings

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



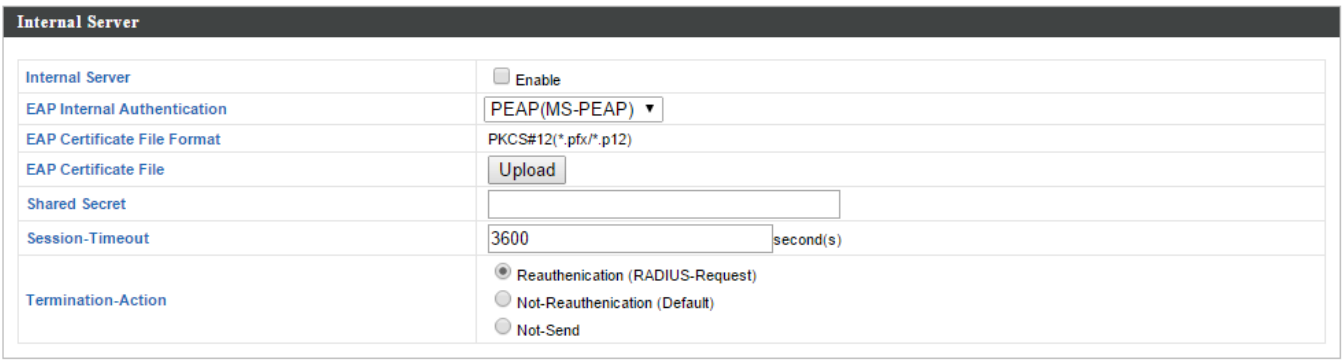

| | |
|---|---|
| **RADIUS Type** | Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server. |

| | |
|---|---|
| **RADIUS Server** | Enter the RADIUS server host IP address. |
| **Authentication Port** | Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535. |
| **Shared Secret** | Enter a shared secret/password between 1 – 99 characters in length. This should match the "MAC-RADIUS" password used in **IV-3-1-3-6** or **IV-3-2-3**. |
| **Session Timeout** | Set a duration of session timeout in seconds between 0 – 86400. |
| **Accounting** | Enable or disable RADIUS accounting. |
| **Accounting Port** | When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between 1 – 65535. |

### IV-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 "Local Network" → "RADIUS Settings" menu.

***To use RADIUS servers, go to** "Wireless Settings"→"Security""Additional Authentication" **and select** "MAC RADIUS Authentication" **(see** IV-6-2-3.**&**IV-6-3-3**).***

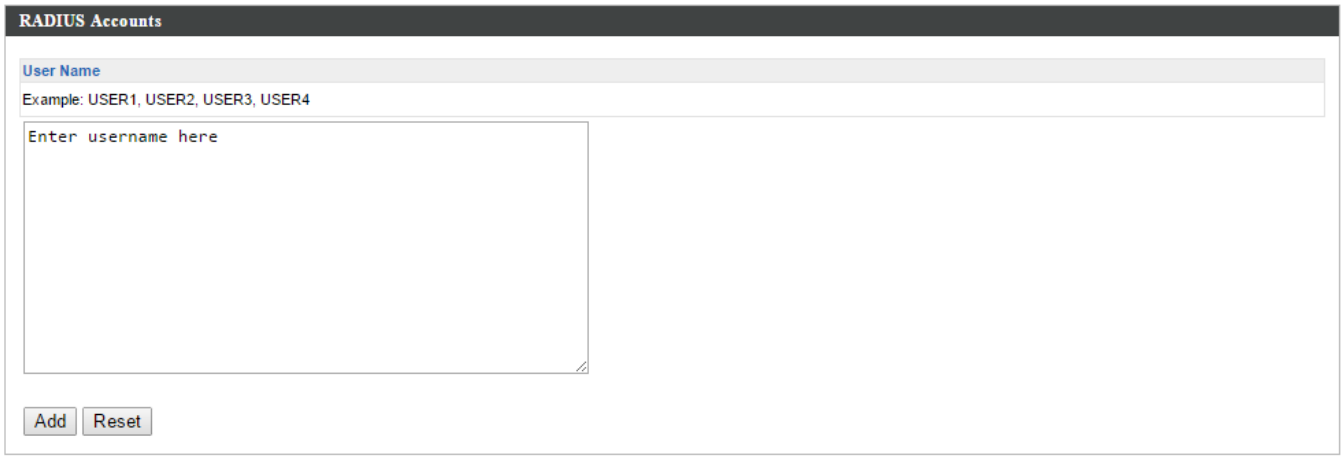


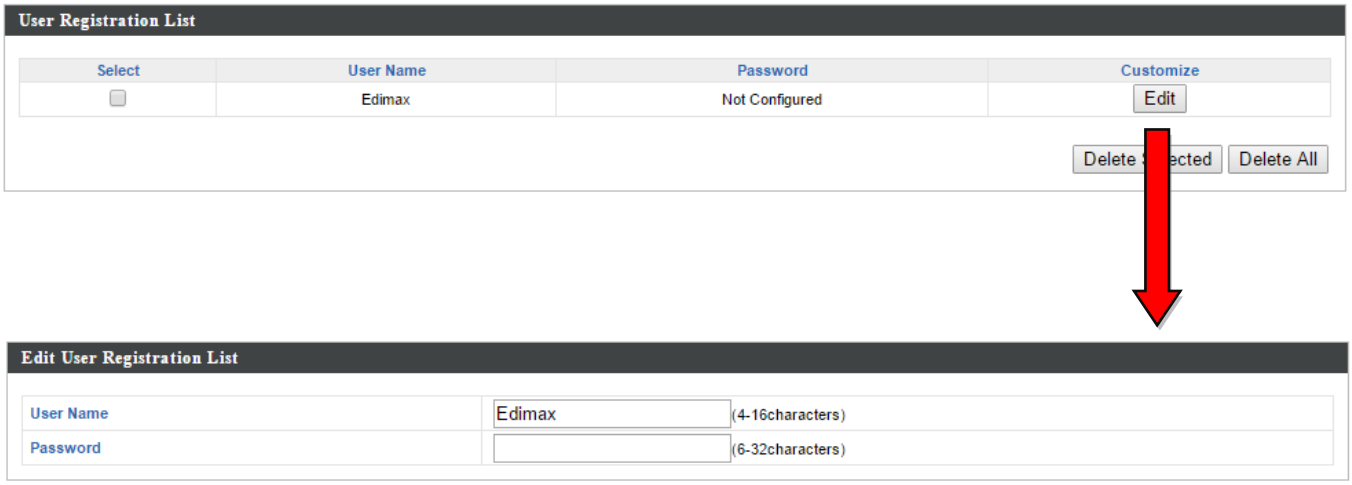

| | |
|---|---|
| **Internal Server** | Check/uncheck to enable/disable the access point's internal RADIUS server. |
| **EAP Internal Authentication** | Select EAP internal authentication type from the drop down menu. |

| | |
|---|---|
| **EAP Certificate File Format** | Displays the EAP certificate file format: PCK#12(*.pfx/*.p12) |
| **EAP Certificate File** | Click “Upload” to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate. |
| **Shared Secret** | Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in **IV-6-2-3-6** or **IV-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, “Not-Reathentication” sends a default termination-action attribute to the access point, “Not-Send” no termination-action attribute is sent to the access point. |

## IV-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.







| | |
|---|---|
| **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. |

**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. |

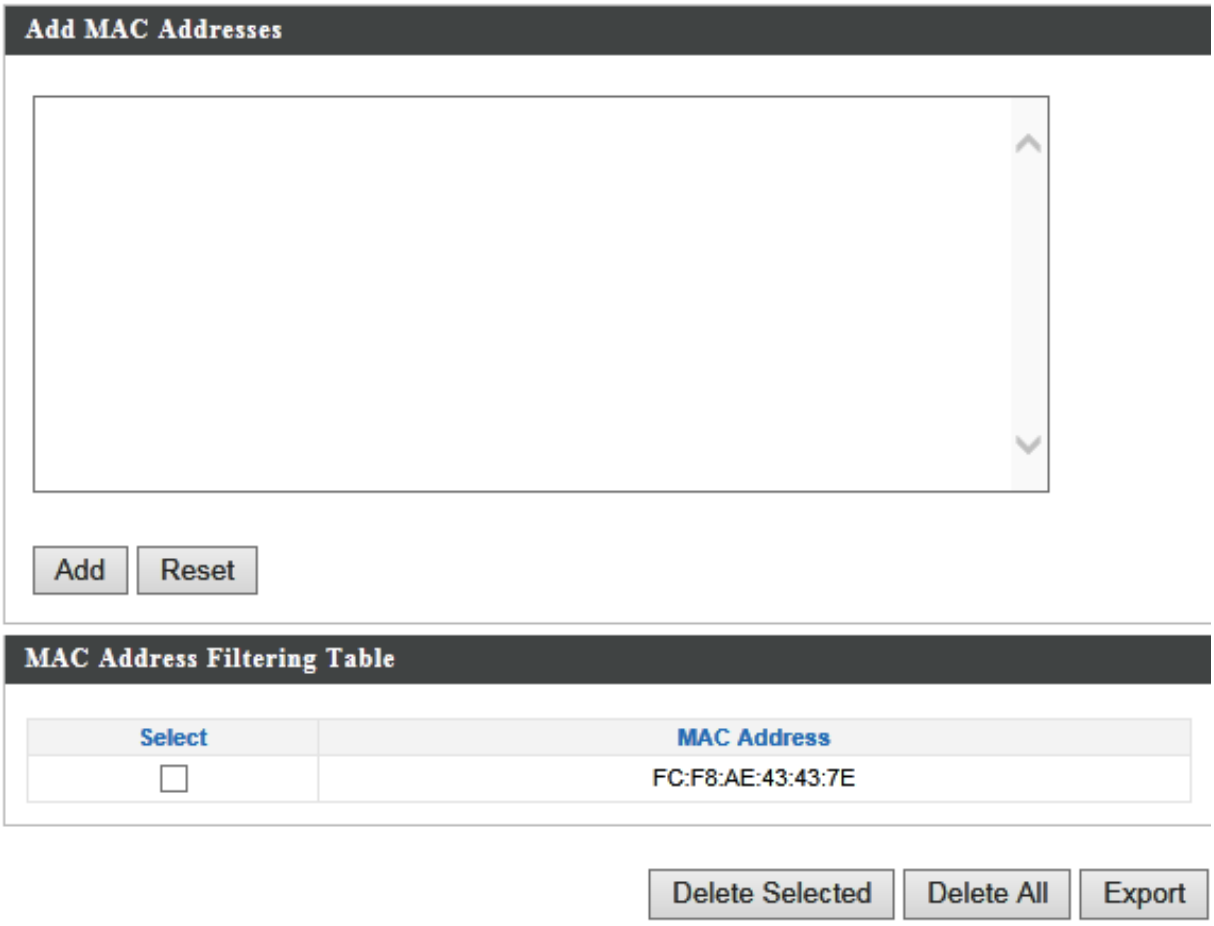
### IV-6-6. MAC Filter

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*** *"Local Settings"* →*"Security"* → *"Additional Authentication"* ***and select*** *"MAC Filter"* ***(see*** *IV-6-2-3.****&****IV-6-3-3****).***

The MAC address filtering table is displayed below:



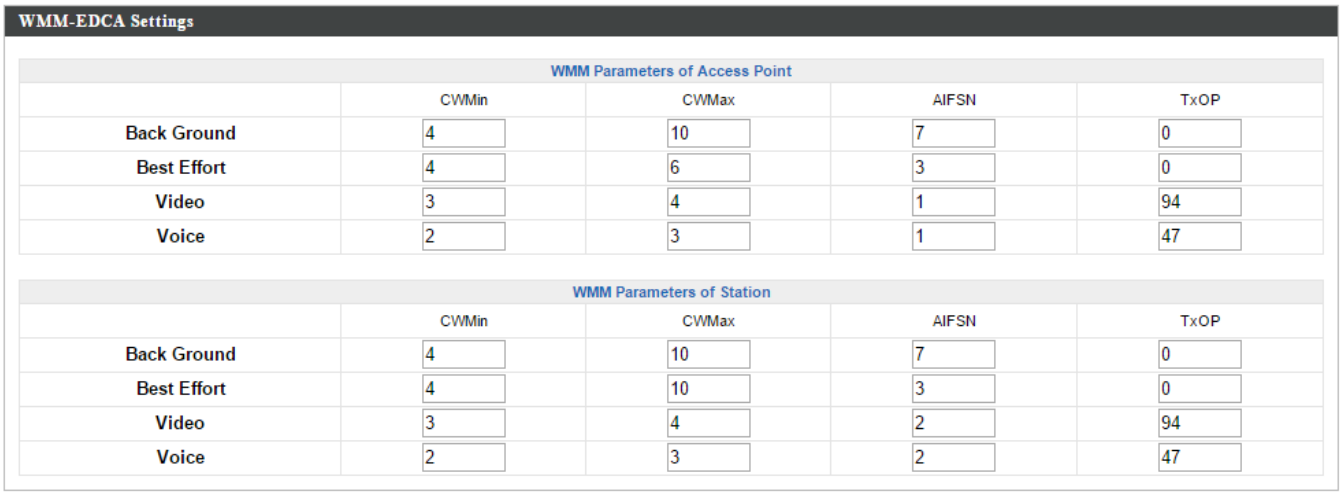
| | |
|---|---|
| **Add MAC Address** | Enter a MAC address of computer or network device manually e.g. ‘aa-bb-cc-dd-ee-ff’ or enter multiple MAC addresses separated with commas, e.g. ‘aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg’ |
| **Add** | Click “Add” to add the MAC address to the MAC address filtering table.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

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

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

## IV-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.




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. |

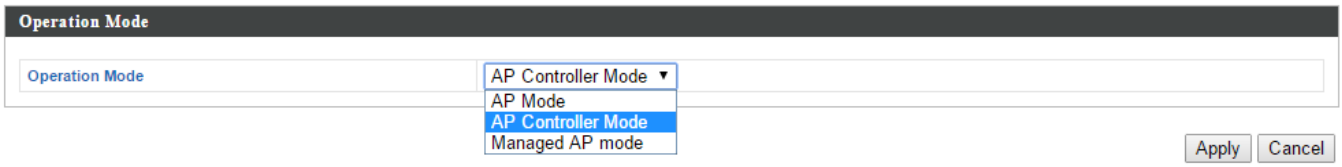
Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can further be adjusted manually:

| | |
|---|---|
| **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 effects higher priority. |

# IV-7. Local Settings

## IV-7-1. Operation Mode

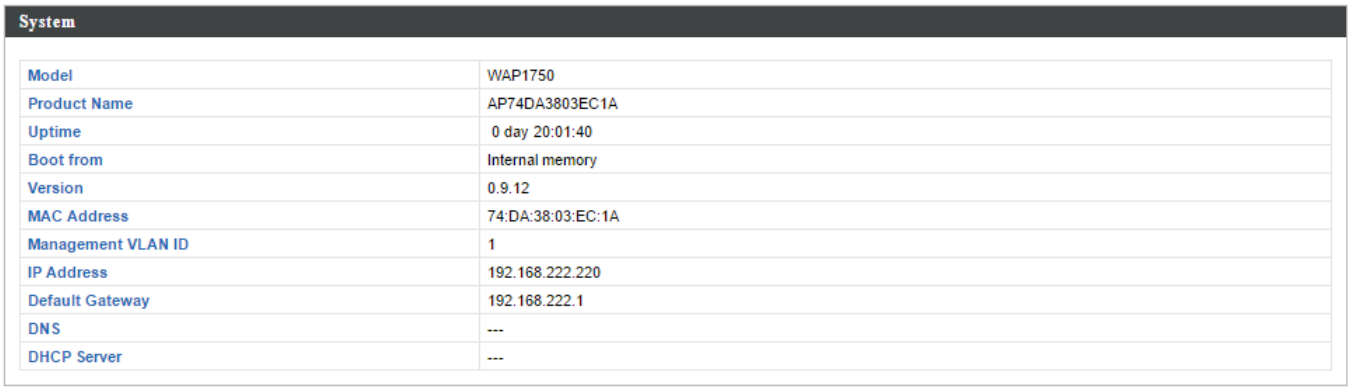
Set the operation mode of the access point. AP mode is a standalone access point, AP controller mode acts as the designated master of the AP array, and Managed AP mode acts as a slave AP within the AP array.

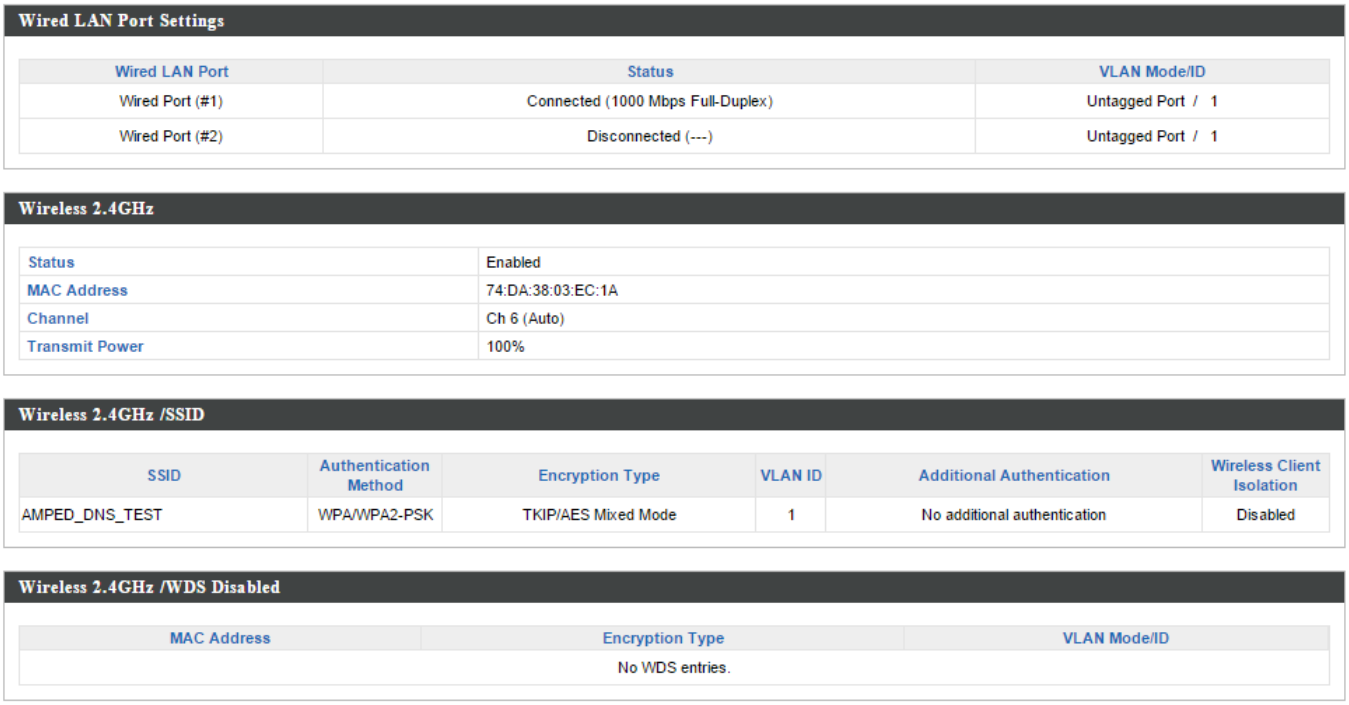



## IV-7-2. Network Settings

### IV-7-2-1. System Information

The “System Information” page displays basic system information about the access point.





**Wired LAN Port Settings**

| Wired LAN Port | Status | VLAN Mode/ID |
|---|---|---|
| Wired Port (#1) | Connected (1000 Mbps Full-Duplex) | Untagged Port / 1 |
| Wired Port (#2) | Disconnected (---) | Untagged Port / 1 |

**Wireless 2.4GHz**

| | |
|---|---|
| Status | Enabled |
| MAC Address | 74:DA:38:03:EC:1A |
| Channel | Ch 6 (Auto) |
| Transmit Power | 100% |

**Wireless 2.4GHz /SSID**

| SSID | Authentication Method | Encryption Type | VLAN ID | Additional Authentication | Wireless Client Isolation |
|---|---|---|---|---|---|
| AMPED_DNS_TEST | WPA/WPA2-PSK | TKIP/AES Mixed Mode | 1 | No additional authentication | Disabled |

**Wireless 2.4GHz /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. |
| **Boot From** | Displays information for the booted hardware, booted from either USB or internal memory. |
| **Version** | Displays thefirmware version. |
| **MAC Address** | Displays the access point’s MAC address. |
| **Management VLAN ID** | Displays the management VLAN ID. |
| **IP Address** | Displays the IP address of this device. Click “Refresh” to update this value. |
| **Default Gateway** | Displays the IP address of the default gateway. |
| **DNS** | IP address of DNS (Domain Name Server) |
| **DHCP Server** | IP address of DHCP Server. |

| Wired LAN Port Settings | |
|---|---|
| **Wired LAN Port** | Specifies which LAN port (1 or 2). |
| **Status** | Displays the status of the specified LAN port (connected or disconnected). |

| | |
|---|---|
| **VLAN Mode/ID** | Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port. See **IV-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. |

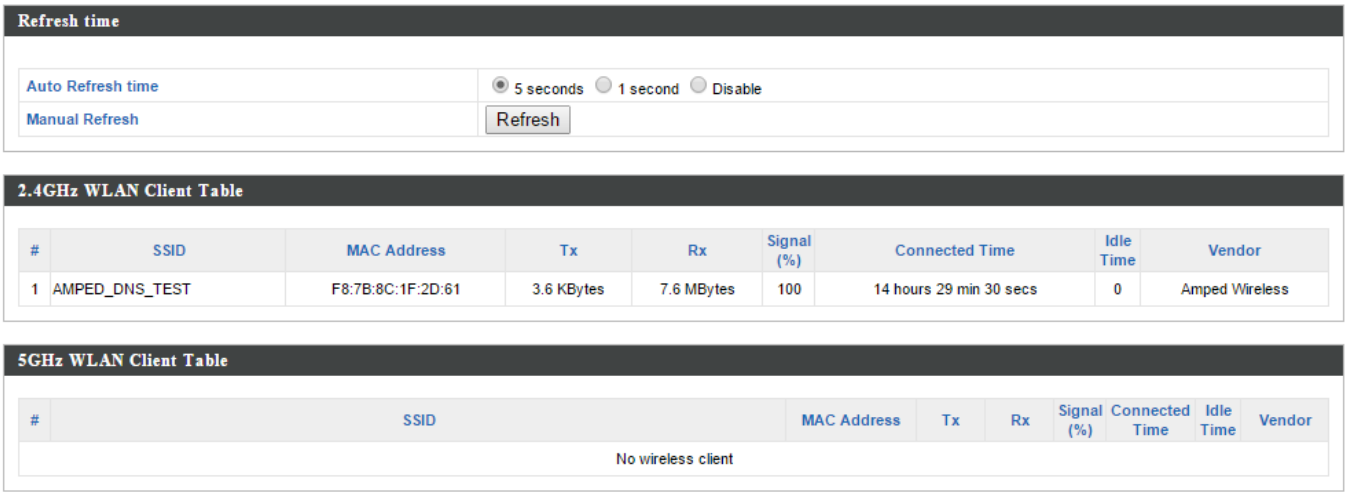
| Wireless 2.4GHZ (5GHz) / SSID | |
|---|---|
| **SSID** | Displays the SSID name(s) for the specified frequency. |
| **Authentication Method** | Displays the authentication method for the specified SSID. See **IV-6. Wireless Settings** |
| **Encryption Type** | Displays the encryption type for the specified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

| Wireless 2.4GHZ (5GHz) / WDS Status | |
|---|---|
| **MAC Address** | Displays thepeer access point's MAC address. |
| **Encryption Type** | Displays the encryption type for the specified WDS. See **IV-6-2-4. WDS** |
| **VLAN Mode/ID** | Displays the VLAN ID for the specified WDS. See **IV-6-2-4. WDS** |

| | |
|---|---|
| **Refresh** | Click to refresh all information. |

## IV-7-2-2. Wireless Clients

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

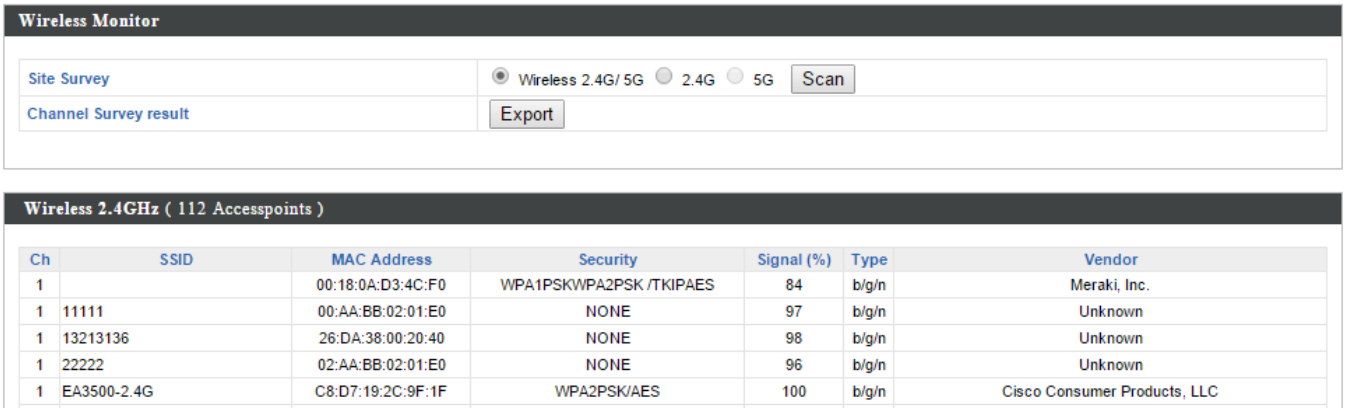



| Refresh time | |
|---|---|
| **Auto Refresh Time** | Select a time interval for the client table list to automatically refresh. |
| **Manual Refresh** | Click refresh to manually refresh the client table. |

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

## IV-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.



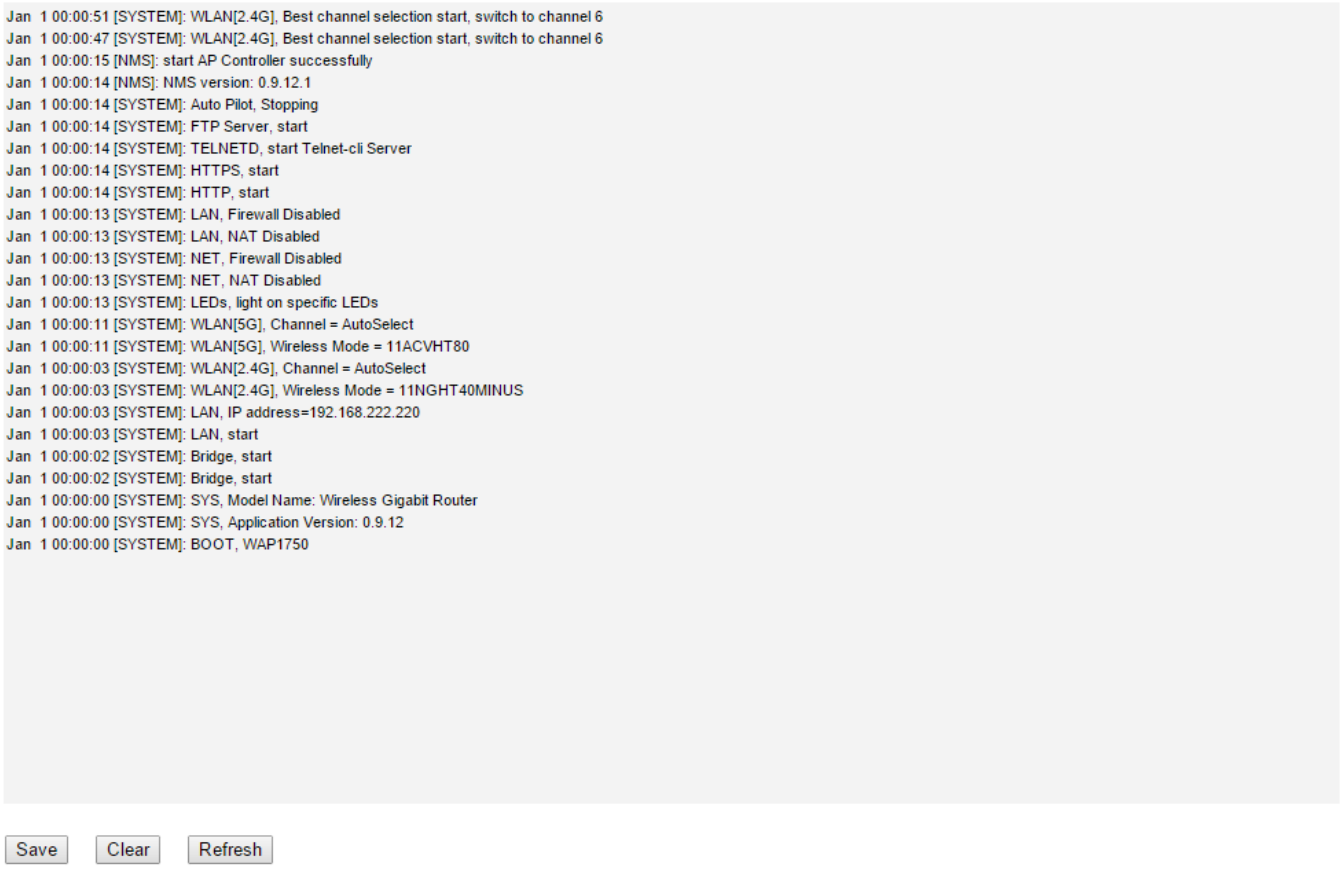

| Wireless Monitor | |
|---|---|
| **Site Survey** | Select which frequency (or both) to scan, and click “Scan” to begin. |
| **Channel Survey Result** | After a scan is complete, click “Export” to save the results to local storage. |

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

## IV-7-2-4. Log

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

***When the log is full, old entries are overwritten.***




| | |
|---|---|
| **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:

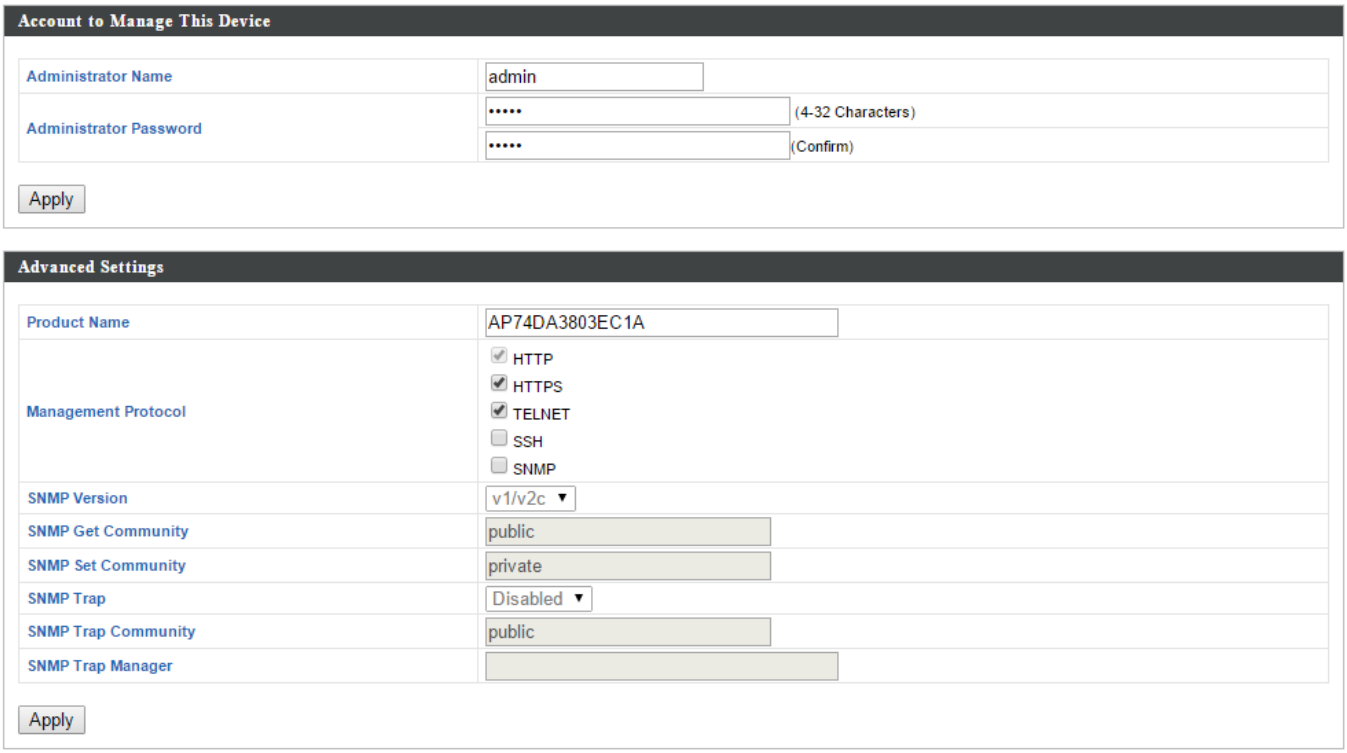
- **USB**
  *Mount & unmount*
- **Wireless Client**
  *Connected &disconnected*
  *Key exchange success & fail*
- **Authentication**
  *Authentication fail or successful*.
- **Association**
  *Success or fail*
- **WPS**
  *M1 - M8 messages*
  *WPS success*
- **Change Settings**
- **System Boot**
  *Displays 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*
- **ADT**

## IV-7-3. Management

### IV-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*** *IV-7-4-4. Factory Default* ***for how to reset the access point.***




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

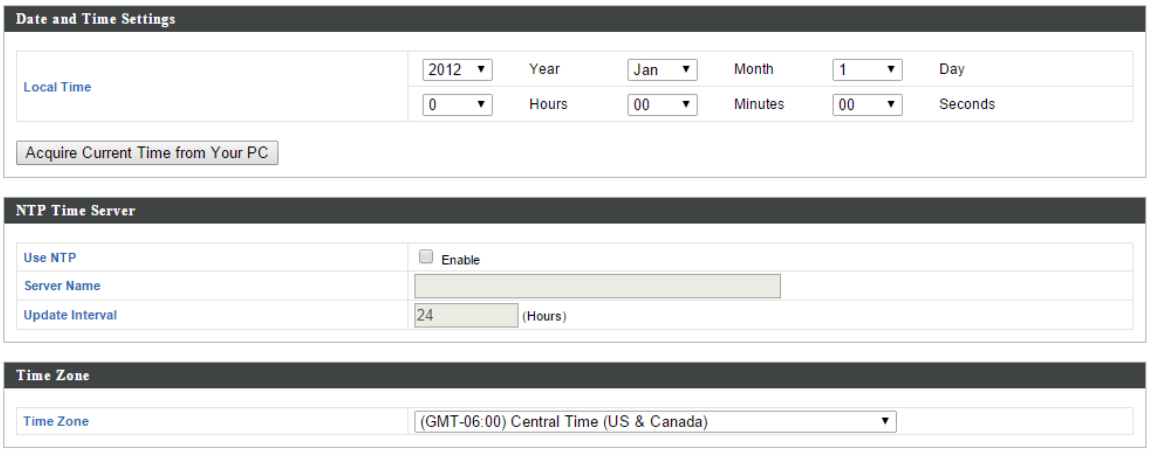
| Advanced Settings |
|---|

| | |
|---|---|
| **Product Name** | Edit the product name according to your preferenceconsisting 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*
**HTTPS**
*Internet browser HTTPS protocol management interface*
**TELNET**
*Client terminal with telnet protocol management interface*
**SSH**
*Client terminal with SSH protocol version 1 or 2 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.*

## IV-7-3-2. Date and Time

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



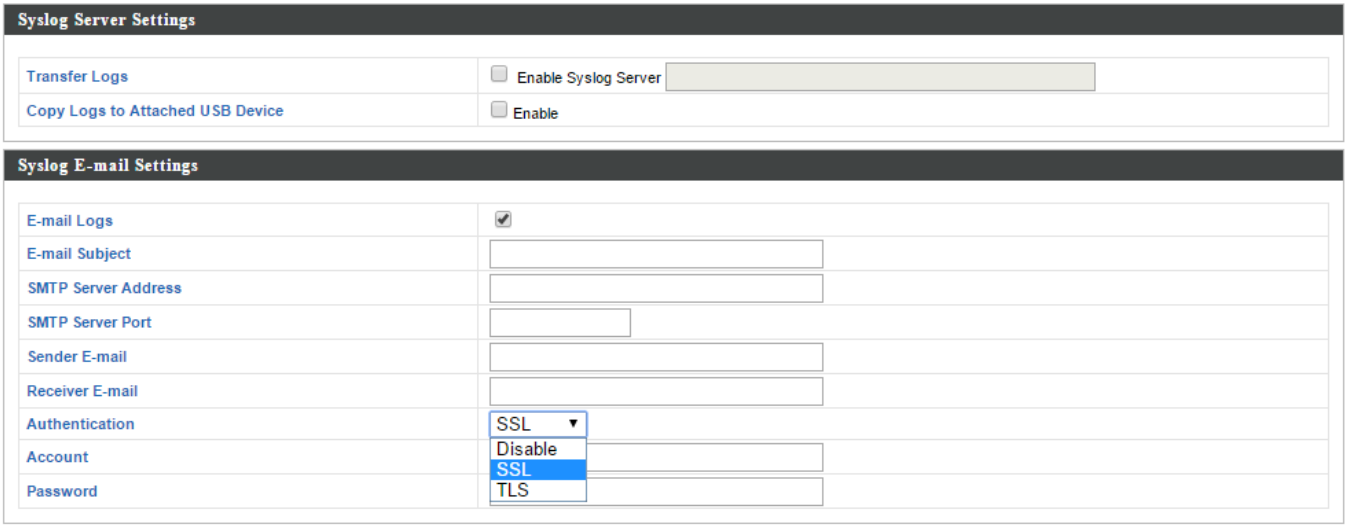

| Date and Time Settings | |
|---|---|
| **Local Time** | Set the access point's date and time manually using the drop down menus. |
| **Acquire Current Time from your PC** | Click "Acquire Current Time from Your PC" to enter the required values automatically according to your computer's current time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

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

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

## IV-7-3-3. Syslog Server

The system log can be sent to a server, attached to USB storage or sent via email.



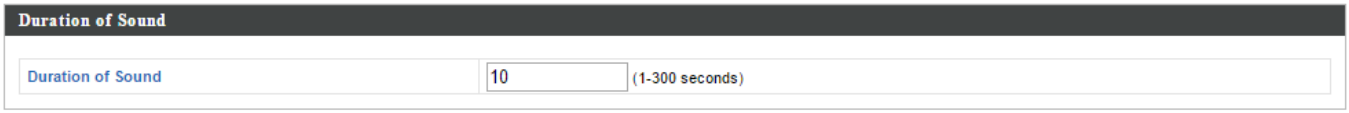

| Syslog Server Settings | |
|---|---|
| **Transfer Logs** | Check/uncheck the box to enable/disable the use of a syslog server, and enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters. |
| **Copy Logs to Attached USB Device** | Check/uncheck the box to enable/disable copying logs to attached USB storage. |

| Syslog Email Settings | |
|---|---|
| **Email Logs** | Check/uncheck the box to enable/disable email logs. When enabled, the log will be emailed according to the settings below. |
| **Email Subject** | Enter the subject line of the email which will be sent containing the log. |
| **SMTP Server Address** | Specify the SMTP server address for the sender email account. |
| **SMTP Server Port** | Specify the SMTP server port for the sender email account. |
| **Sender Email** | Enter the sender's email address. |
| **Receiver Email** | Specify the email recipient of the log. |
| **Authentication** | Select "Disable", "SSL" or "TLS" according to your email authentication. |

| | |
|---|---|
| **Account** | When authentication is used above, enter the account name. |
| **Password** | When authentication is used above, enter the password. |

### IV-7-3-4. I’m Here

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




***The buzzer is loud!***

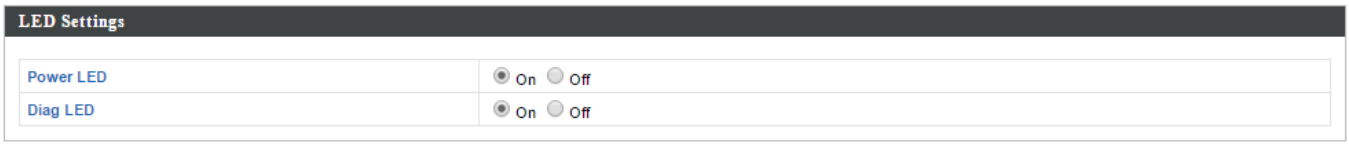
| | |
|---|---|
| **Duration of Sound** | Set the duration for which the buzzer will sound when the “Sound Buzzer” button is clicked. |
| **Sound Buzzer** | Activate the buzzer sound for the above specified duration of time. |

## IV-7-4. Advanced

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.

### IV-7-4-1. LED Settings

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

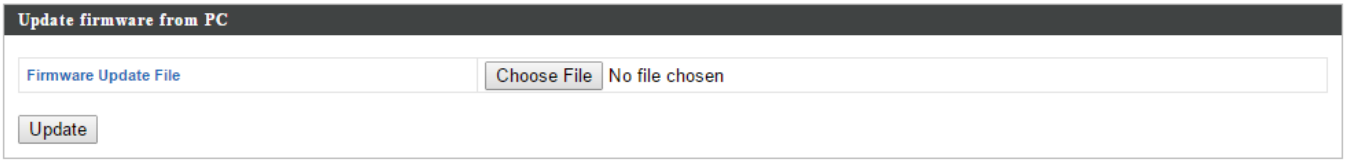



| | |
|---|---|
| **Power LED** | Select on or off. |
| **Diag LED** | Select on or off. |

### IV-7-4-2. Update Firmware

The "Firmware" page allows you to update the system firmware to a more recent version. Updated firmware versions often offer increased performance and security, as well as bug fixes.

***This firmware update is for an individual access point. To update firmware for multiple access points in the AP array, go to NMS Settings → Firmware Upgrade.***

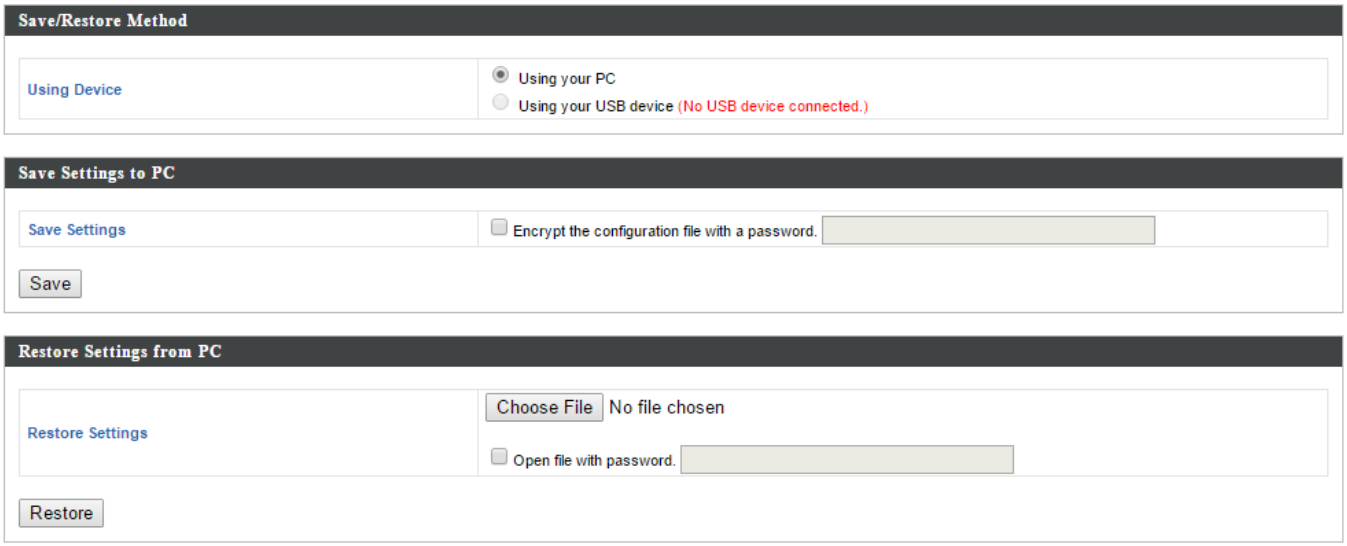




***Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.***

| | |
|---|---|
| **Update Firmware From** | Select “a file on your PC” to upload firmware from your local computer or from an attached USB device. |
| **Firmware Update File** | Click “Browse” to open a new window to locate and select the firmware file in your computer. |
| **Update** | Click “Update” to upload the specified firmware file to your access point. |

### IV-7-4-3. Save/Restore Settings

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




| Save / Restore Settings | |
|---|---|
| **Using Device** | Select "Using your PC" to save the access point's settings to your local computer or to an attached USB device. |
| Save Settings to PC | |
| **Save Settings** | Click "Save" to save settings and a new window will open to specify a location to save the settings file. You can also check the "Encrypt the configuration file with a password" box and enter a password to protect the file in the field underneath, if you wish. |
| Restore Settings from PC | |
| **Restore Settings** | Click the browse button to find a previously saved settings file on your computer, then click "Restore" to replace your current settings. If your settings file is encrypted with a password, check the "Open file with password" box and enter the password in the field underneath. |

### IV-7-4-4. Factory Default

If the access point malfunctions or is not responding, then it is recommended that you reboot the device (see **IV-7-4-5.**) or reset the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the location of the access point is not convenient to access the reset button.


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

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

### IV-7-4-5. Reboot

If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the access point back to its factory default settings (see **IV-7-4-4**). You can reboot the access point remotely using this feature.


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

# IV-8. Toolbox

## IV-8-1. Network Connectivity

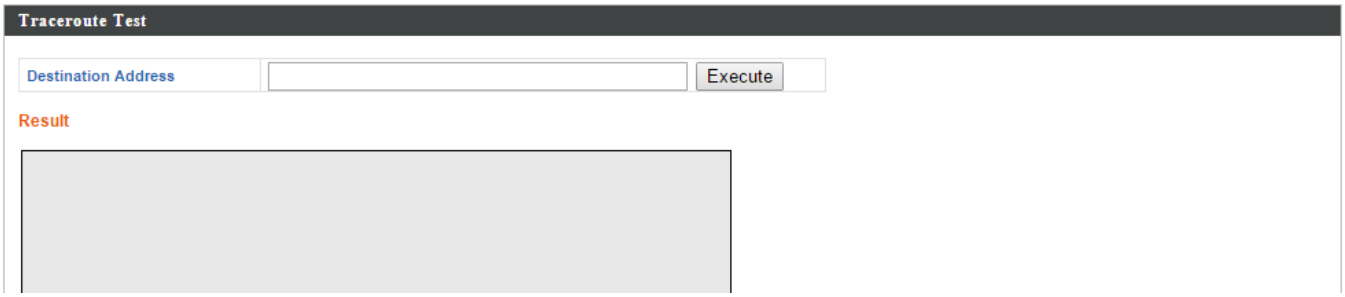
### IV-8-1-1. Ping

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. |

### IV-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. |

# *V. Best Practice*

**How to Create and Link WLAN & Access Point Groups**

You can use NMS 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.

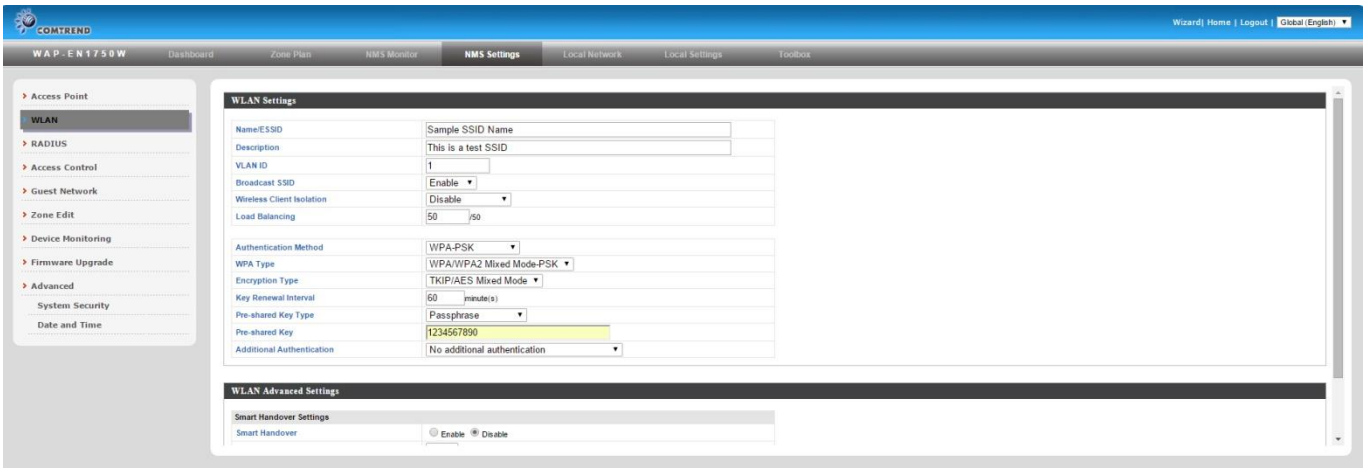
Follow the example below to:

**A.** Create a WLAN group.
**B.** Create an access point group.
**C.** Assign the access point group to use the SSID group settings.

**A.**

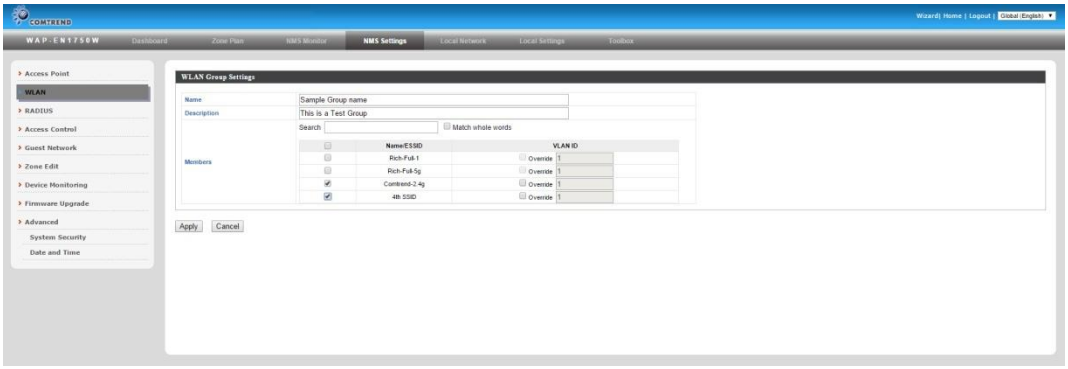
1. Go to **NMS Settings → WLAN** and click **"Add"** in the **WLAN** panel:

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




3. The new SSID will be displayed in the **WLAN** panel. **Repeat** to add additional SSIDs according to your preference, and then click **"Add"** in the **WLAN Group** panel:

4. Enter a **name** for the **SSIDgroup** and **check the boxes** to select which SSIDs to include within the group. Click "**Apply**" when done.

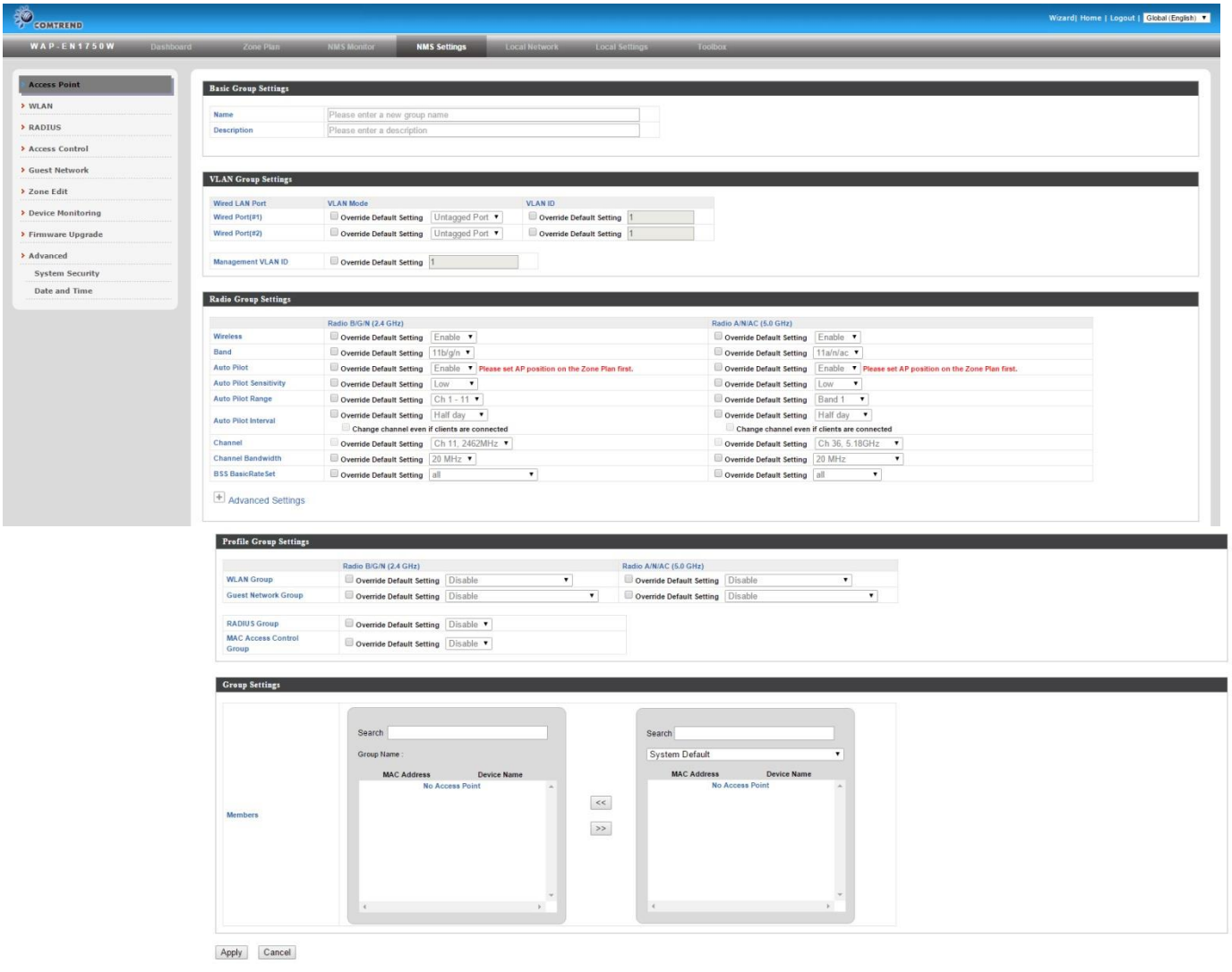



5. The new **WLAN group** will be displayed in the **WLAN Group** panel. **Repeat** to add additional WLAN groups according to your preference:

**B.**

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

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



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

**C.**

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

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

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