# AC1300 DBDC Ceiling-mount AP

## CAP1300, Office 1-2-3, Office +1, Office +3, Office WiFi System, Office WiFi System +1.

# User Manual

04-2015 / v1.1


**Edimax Technology Co., Ltd.**
No.3, Wu-Chuan 3rd Road, Wu-Gu, New Taipei City 24891, Taiwan
Email: support@edimax.com.tw

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

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

# CONTENTS


**OVERVIEW: IMPORTANT ..... 1**

**I. Product Information ..... 2**

I-1. Package Contents ..... 2
I-2. System Requirements ..... 2
I-3. Hardware Overview ..... 3
I-4. LED Status ..... 4
I-5. Reset ..... 5
I-6. Safety Information ..... 6

**II. Hardware Installation ..... 7**

II-1. Connecting the access point to a router or PoE switch ..... 7
II-2. Mounting the access point to a ceiling ..... 8
II-3. T-Rail Mount ..... 11


## AP Mode


**III. Quick Setup ..... 13**

III-1. Initial Setup ..... 13
III-2. Basic Settings ..... 15

**IV. Browser Based Configuration Interface ..... 19**

IV-1. Information ..... 21
IV-1-1. System Information ..... 21
IV-1-2. Wireless Clients ..... 24
IV-1-3. Wireless Monitor ..... 25
IV-1-4. Log ..... 26
IV-2. Network Settings ..... 28
IV-2-1. LAN-Side IP Address ..... 28
IV-2-2. LAN Port ..... 30
IV-2-3. VLAN ..... 31
IV-3. Wireless Settings ..... 32
IV-3-1. 2.4GHz 11bgn ..... 32
IV-3-1-1. Basic ..... 33
IV-3-1-2. Advanced ..... 36
IV-3-1-3. Security ..... 38
IV-3-1-3-1. No Authentication ..... 39

IV-3-1-3-2. WEP ..... 40
IV-3-1-3-3. IEEE802.1x/EAP ..... 40
IV-3-1-3-4. WPA-PSK ..... 40
IV-3-1-3-5. WPA-EAP ..... 41
IV-3-1-3-6. Additional Authentication ..... 41
IV-3-1-4. WDS ..... 43
IV-3-1-5. Schedule ..... 45
IV-3-2. WPS ..... 46
IV-3-3. RADIUS ..... 48
IV-3-3-1. RADIUS Settings ..... 50
IV-3-3-2. Internal Server ..... 51
IV-3-3-3. RADIUS Accounts ..... 53
IV-3-4. MAC Filter ..... 55
IV-3-5. WMM ..... 57
IV-4. Management ..... 59
IV-4-1. Admin ..... 59
IV-4-2. Date and Time ..... 62
IV-4-3. Syslog Server ..... 64
IV-4-4. Ping Test ..... 65
IV-4-5. I'm Here ..... 66
IV-4-6. Operation Mode ..... 67
IV-5. Advanced ..... 68
IV-5-1. LED Settings ..... 68
IV-5-2. Update Firmware ..... 69
IV-5-3. Save/Restore Settings ..... 70
IV-5-4. Factory Default ..... 72
IV-5-5. Reboot ..... 73

## Edimax Pro NMS

**I. Product Information ..... 74**

**II. Quick Setup ..... 75**

**III. Software Layout ..... 81**

**IV. Features ..... 88**

IV-1. LOGIN, LOGOUT & RESTART ..... 88
IV-2. DASHBOARD ..... 90

IV-2-1. System Information ..... 91
IV-2-2. Devices Information ..... 91
IV-2-3. Managed AP ..... 92
IV-2-4. Managed AP Group ..... 93
IV-2-5. Active Clients ..... 94
IV-3. ZONE PLAN ..... 95
IV-4. NMS MONITOR ..... 97
IV-4-1. Access Point ..... 97
IV-4-1-1. Managed AP ..... 97
IV-4-1-2. Managed AP Group ..... 99
IV-4-2. WLAN ..... 101
IV-4-2-1. Active WLAN ..... 101
IV-4-2-2. Active WLAN Group ..... 102
IV-4-3. Clients ..... 102
IV-4-3-1. Active Clients ..... 102
IV-4-4. Rogue Devices ..... 103
IV-4-5. Information ..... 104
IV-4-5-1. All Events/Activities ..... 104
IV-4-5-2. Monitoring ..... 105
IV-5. NMS Settings ..... 106
IV-5-1. Access Point ..... 106
IV-5-2. WLAN ..... 117
IV-5-3. RADIUS ..... 121
IV-5-4. Access Control ..... 127
IV-5-5. Guest Network ..... 130
IV-5-6. Zone Edit ..... 134
IV-5-7. Firmware Upgrade ..... 136
IV-5-8. Advanced ..... 137
IV-5-8-1. System Security ..... 137
IV-5-8-2. Date & Time ..... 137
IV-6. Local Network ..... 139
IV-6-1. Network Settings ..... 139
IV-6-1-1. LAN-Side IP Address ..... 139
IV-6-1-2. LAN Port Settings ..... 142
IV-6-1-3. VLAN ..... 143
IV-6-2. 2.4GHz 11bgn ..... 144
IV-6-2-1. Basic ..... 144
IV-6-2-2. Advanced ..... 146
IV-6-2-3. Security ..... 148
IV-6-2-3-1. No Authentication ..... 149
IV-6-2-3-2. WEP ..... 149

IV-6-2-3-3. IEEE802.1x/EAP ..... 150
IV-6-2-3-4. WPA-PSK ..... 150
IV-6-2-3-5. WPA-EAP ..... 150
IV-6-2-3-6. Additional Authentication ..... 151
IV-6-2-4. WDS ..... 152
IV-6-3. 5GHz 11ac 11an ..... 154
IV-6-3-1. Basic ..... 154
IV-6-3-2. Advanced ..... 156
IV-6-3-3. Security ..... 158
IV-6-3-4. WDS ..... 160
IV-6-4. WPS ..... 162
IV-6-5. RADIUS ..... 163
IV-6-5-1. RADIUS Settings ..... 164
IV-6-5-2. Internal Server ..... 165
IV-6-5-3. RADIUS Accounts ..... 167
IV-6-6. MAC Filter ..... 169
IV-6-7. WMM ..... 171
IV-7. Local Settings ..... 173
IV-7-1. Operation Mode ..... 173
IV-7-2. Network Settings ..... 173
IV-7-2-1. System Information ..... 173
IV-7-2-2. Wireless Clients ..... 176
IV-7-2-3. Wireless Monitor ..... 177
IV-7-2-4. Log ..... 178
IV-7-3. Management ..... 180
IV-7-3-1. Admin ..... 180
IV-7-3-2. Date and Time ..... 182
IV-7-3-3. Syslog Server ..... 183
IV-7-3-4. I’m Here ..... 184
IV-7-4. Advanced ..... 185
IV-7-4-1. LED Settings ..... 185
IV-7-4-2. Update Firmware ..... 185
IV-7-4-3. Save/Restore Settings ..... 187
IV-7-4-4. Factory Default ..... 188
IV-7-4-5. Reboot ..... 188
IV-8. Toolbox ..... 189
IV-8-1. Network Connectivity ..... 189
IV-8-1-1. Ping ..... 189
IV-8-1-2. Trace Route ..... 189

**V. Appendix ..... 190**

V-1. Configuring your IP address ..... 190
V-1-1. Windows XP ..... 191
V-1-2. Windows Vista ..... 193
V-1-3. Windows 7 ..... 195
V-1-4. Windows 8 ..... 199
V-1-5. Mac ..... 203

**V. Best Practice ..... 205**

VI-1. How to Create and Link WLAN & Access Point Groups ..... 205

# OVERVIEW

Your access point can function in three different modes.

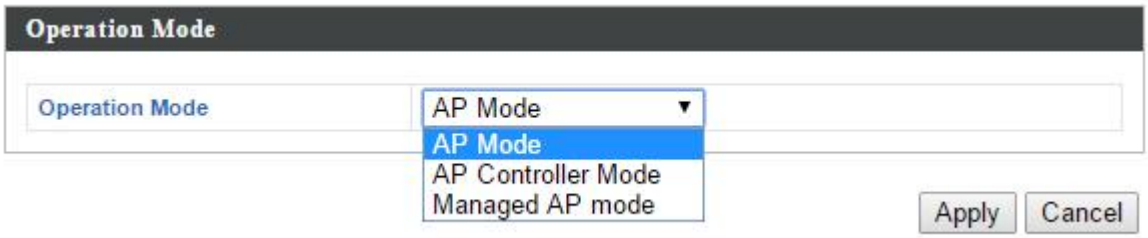
The default mode for your access point is **AP mode**.

**AP mode** is a regular access point for use in your wireless network.

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

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

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

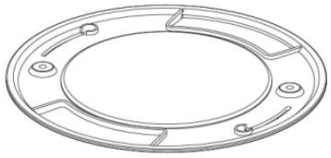



This user manual is split into two parts: **AP mode** (blue) and **Edimax Pro NMS** (grey).

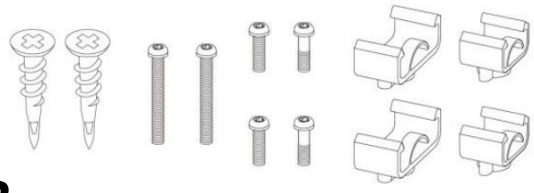
# *I. Product Information*

## I-1. Package Contents

1



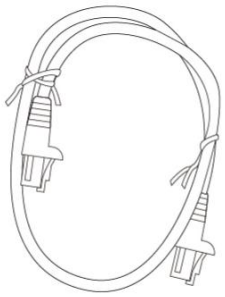
2



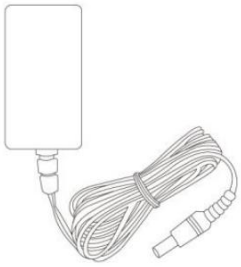
3

4

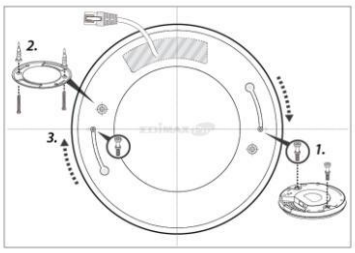
5



6



7



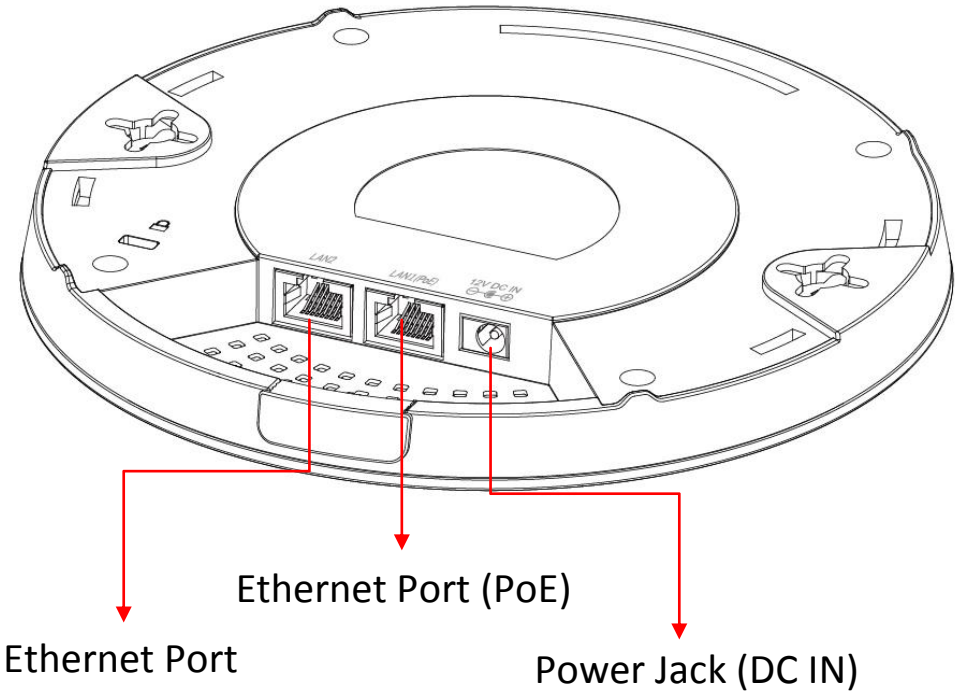

8

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

## I-2. System Requirements

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

## I-3. Hardware Overview



## I-4. LED Status

| LED Color | LED Status | Description |
|---|---|---|
| Blue | On | The access point is on. |
| | Long Flashing | Upgrading firmware. |
| | Short Flashing | Resetting to factory defaults. |
| Amber | On | Starting up. |
| | Flashing | Error. |
| Off | Off | The access point is off. |

## I-5. Reset

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

**1.** Press and hold the reset button on the access point for at least 10 seconds.

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

**2.** Wait for the access point to restart. The access point is ready for setup when the LED is **blue**.

## I-6. Safety Information

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

1. The access point is designed for indoor use only; do not place the access point outdoors.

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

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

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

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

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

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

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

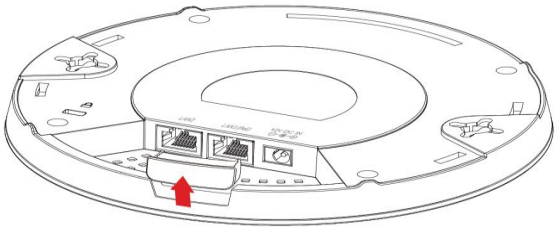
9. If you smell burning or see smoke coming from the access point or power adapter, then disconnect the access point and power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

# II. Hardware Installation

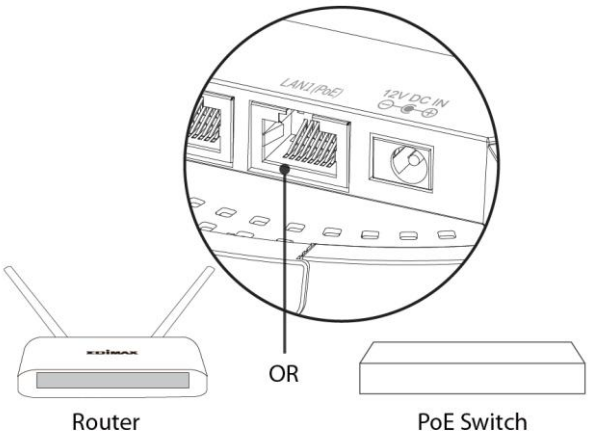
***When using the access point in AP mode it is recommended to configure some basic settings as shown in** III. Quick Setup **before hardware installation.***

## II-1. Connecting the access point to a router or PoE switch

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

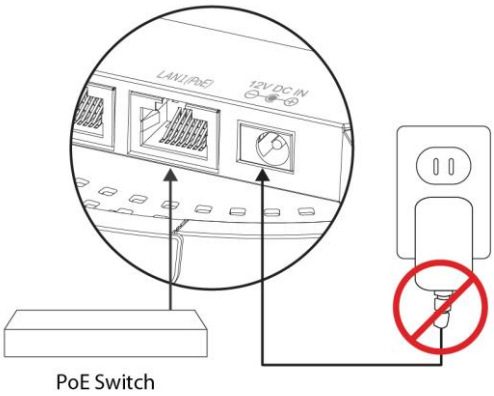


**2.** Connect a router or PoE switch to the access point's **LAN** port using an Ethernet cable.




**3.** If you are using a router, then connect the power adapter to the access point's 12V DC port and plug the power adapter into a power supply.

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



## II-2. Mounting the access point to a ceiling

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

**For Wooden Ceilings (refer to diagram A):**

1. Place the ceiling mount bracket to a ceiling in your desired location and insert screw **iii** through hole **i** (x 2)and tighten to fix the bracket in place.

2. When the ceiling bracket is in place, inset screw **iv** into hole **v** (x 2) on the access point.

3. Fix the access point to the ceiling bracket by inserting the attached screws **iv** into hole **vi** and twisting the access point.

4. Lock the access point firmly into place when by twisting it to align screws **iv** with the grooves in the ceiling mount.

**For Other Ceilings (refer to diagram B):**

1. Place the ceiling mount bracket to a ceiling in your desired location and Insert screw **ii** through hole **i** (x 2) and tighten to fix the bracket in place, as shown in **A**.

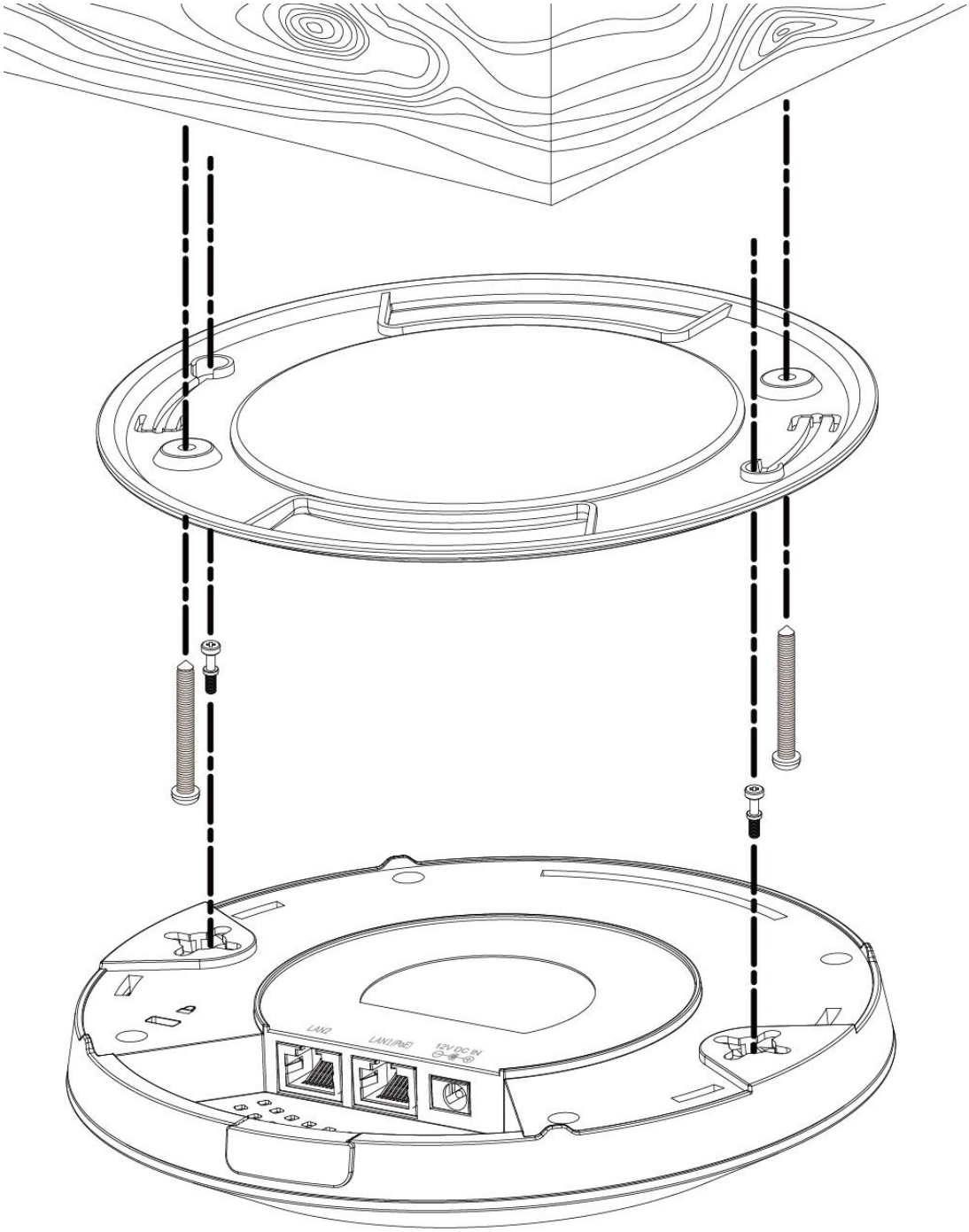
2. Insert screw **iii** through hole **i** and into the rear of screw ii and tighten to provide additional strength.

3. When the ceiling bracket is in place, insert screw **iv** into hole **v** (x 2) on the access point.

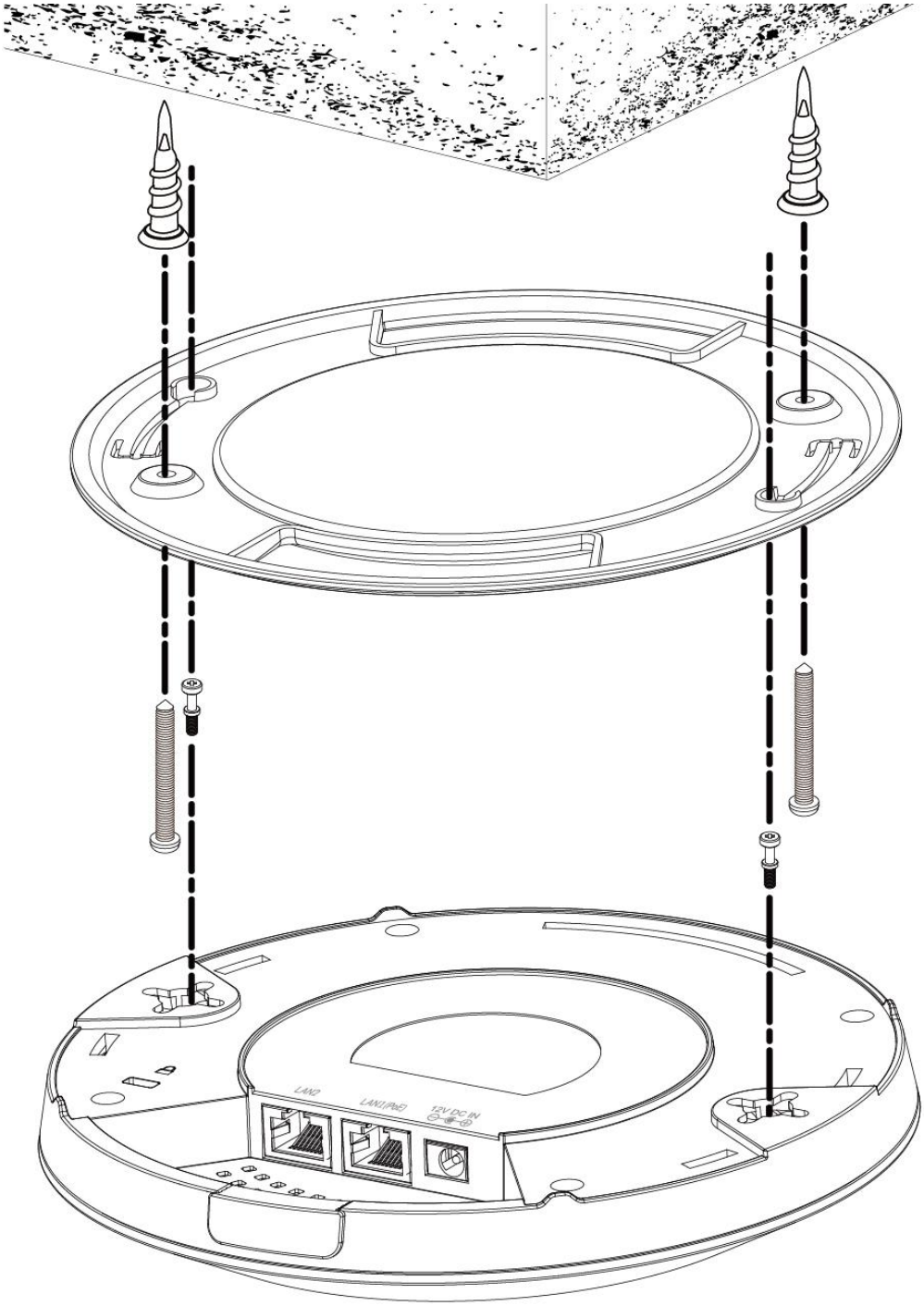
5. Fix the access point to the ceiling bracket by inserting the attached screws **iv** into hole **vi** and twisting the access point.

6. Lock the access point firmly into place by twisting it to align screws **iv** with the grooves in the ceiling mount.

**A**



**B**



## II-3. T-Rail Mount

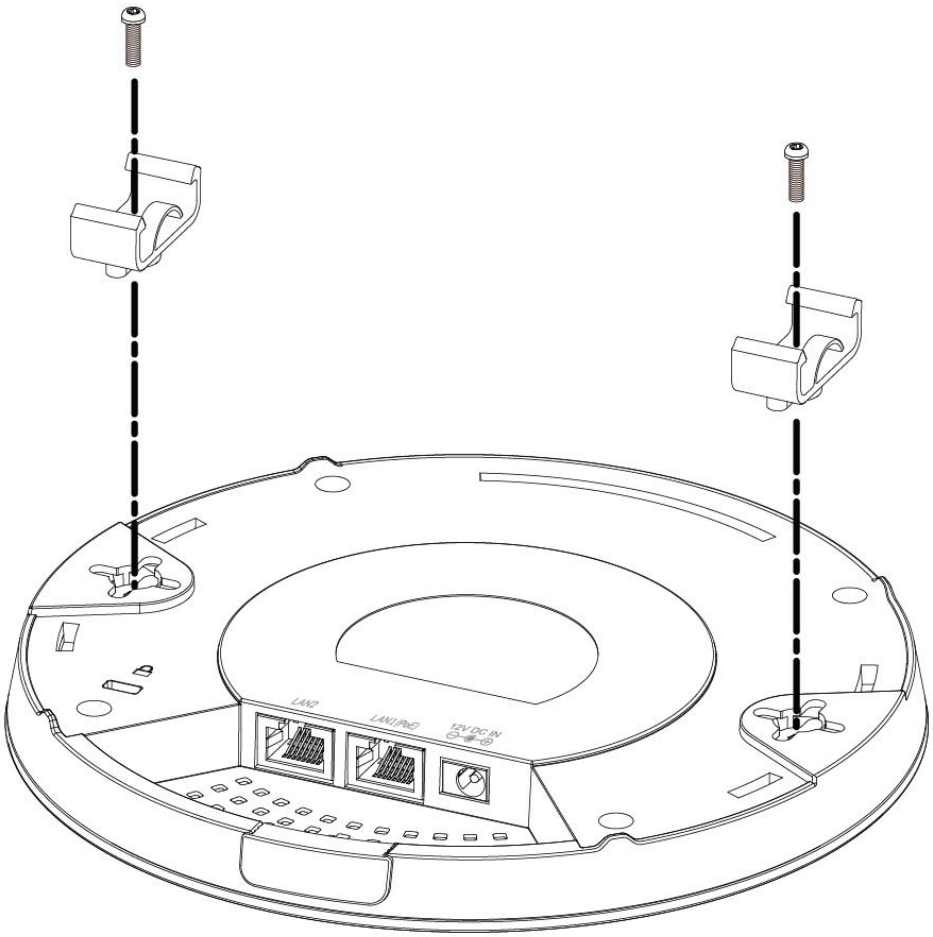
To mount the access point to a T-Rail, please follow the instructions below and refer to diagram **C, D** & **E**.

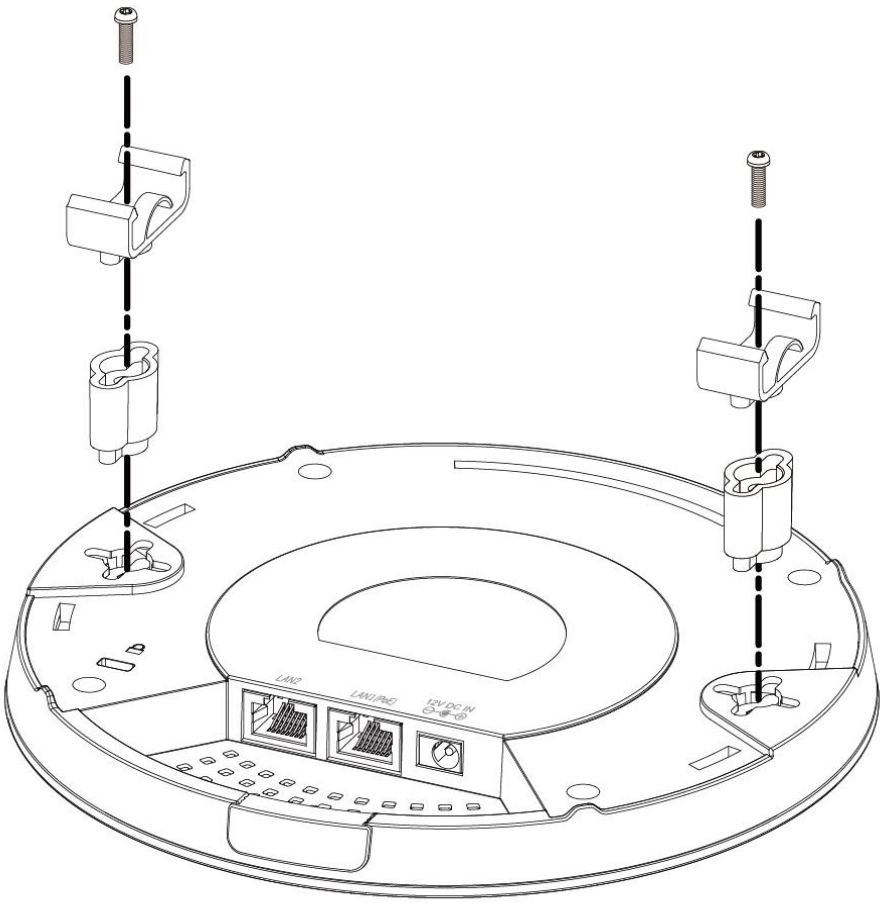
**1.** Select the correct size T-Rail bracket from the two sizes which are included in the package contents.

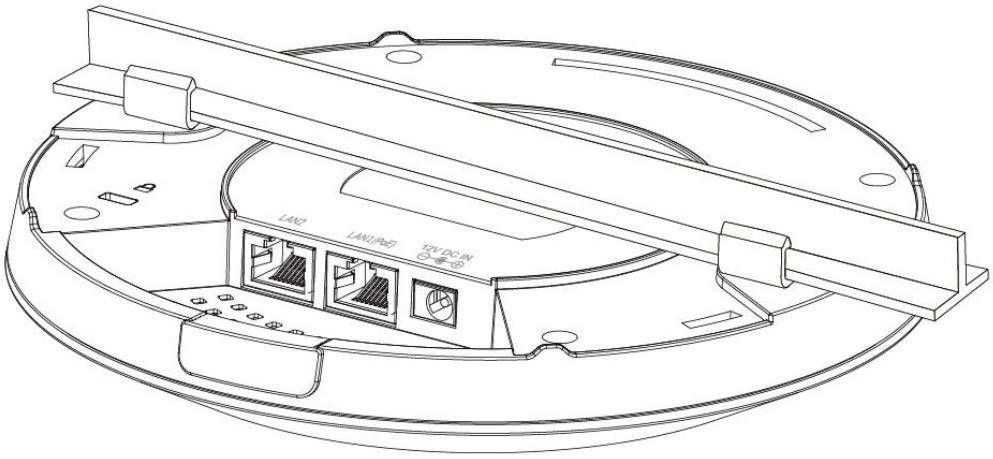
**2.** Attach the T-Rail bracket **i** to hole **ii** using screw **iii** (x 2) as shown in **C**.

***If you need more space between the access point and the T-Rail, then additionally use bracket** iv **between bracket** i **and hole** ii (x 2)**, and use the longer screws (x 2) included in the package contents.***

**3.** Clip the access point onto your T-Rail using the now attached T-Rail bracket.




LAN2
LAN1(PoE)
12V DC IN


LAN2
LAN1(PoE)
12V DC IN

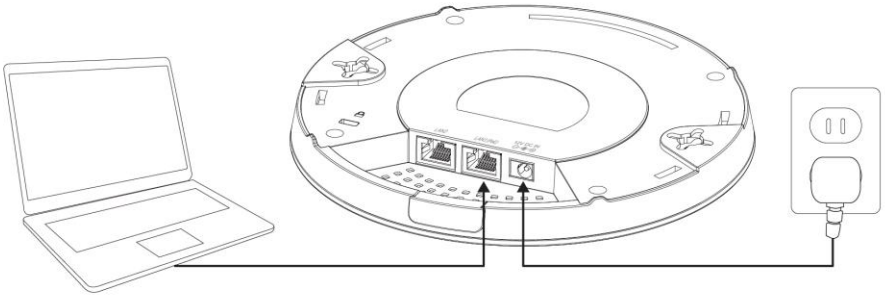
# III. Quick Setup

Your access point can be up and running in just a few minutes. This quick installation guide will help to set up your access point in its default AP mode and configure its basic settings. For use a Managed AP within an AP array no settings are necessary. Configurations can be made from your Controller AP (refer to **Edimax Pro NMS**).

## III-1. Initial Setup

**1.** Connect the access point to a computer via Ethernet cable.

**2.** Connect the power adapter to the access point's 12V DC port and plug the power adapter into a power supply using the included cable.



**3.** Please wait a moment for the access point to start up. The access point is ready when the LED is **blue**.

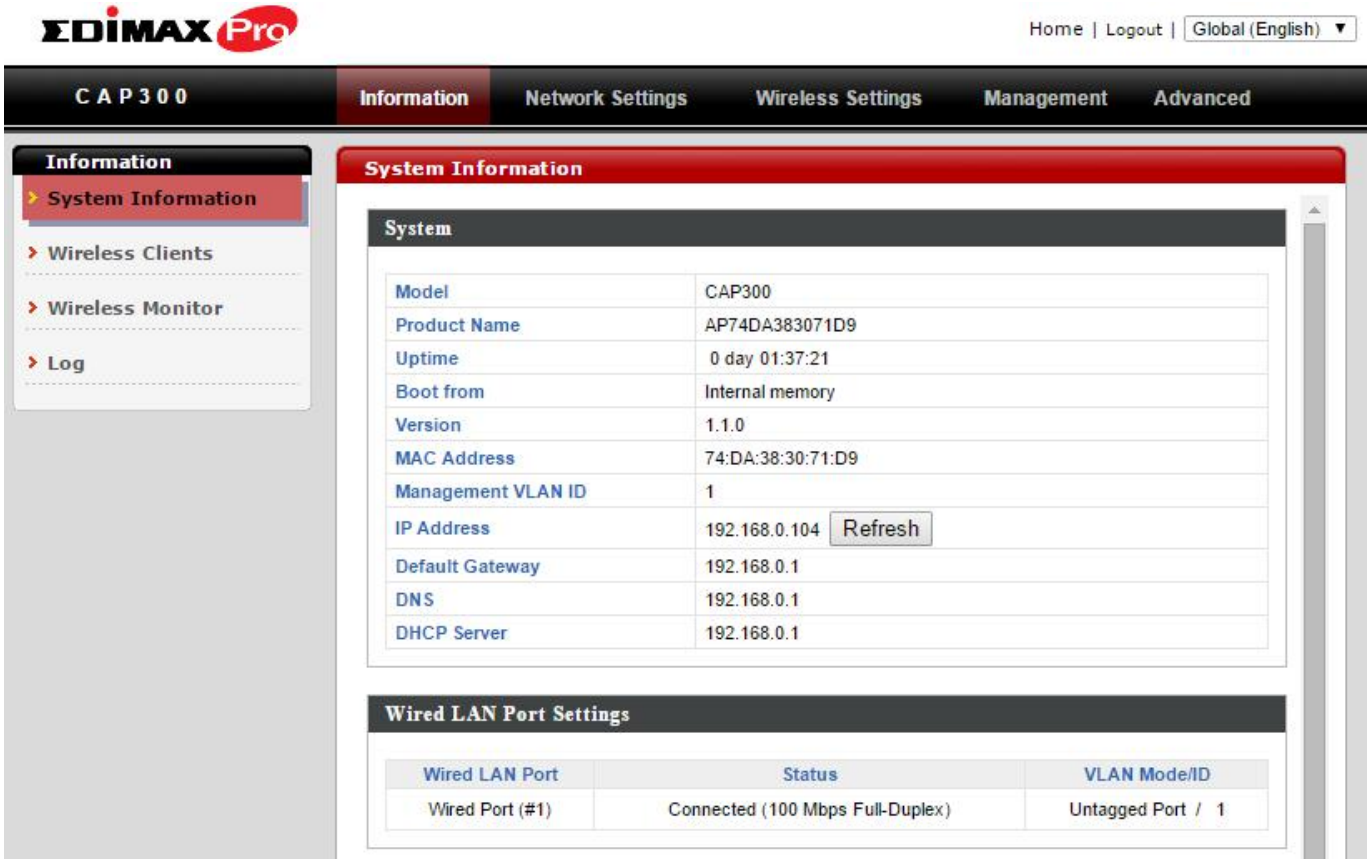
**4.** Set your computer's IP address to **192.168.2.x** where **x** is a number in the range **3 – 100**. If you are unsure how to do this, please refer to the user manual for more information.

***Please ensure there are no other active network connections on your computer (disconnect Wi-Fi connections and Ethernet cables).***

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

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

**7.** You will arrive the “System Information” screen shown below.




**8.** Next, please follow the instructions below in **II-2. Basic Settings** to configure the access point’s basic settings.

***For more advanced configurations, please refer to** IV. Browser Based Configuration Interface.*

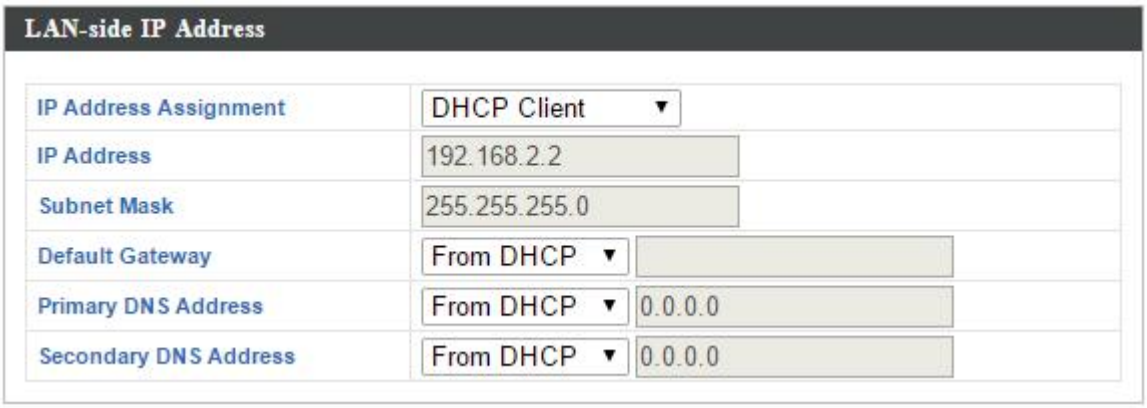
## III-2. Basic Settings

The instructions below will help you to configure the following basic settings of the access point:

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

***It is recommended you configure these settings before using the access point.***

**1.** To change the access point's LAN IP address, go to **"Network Settings" > "LAN-side IP Address"** and you will see the screen below.

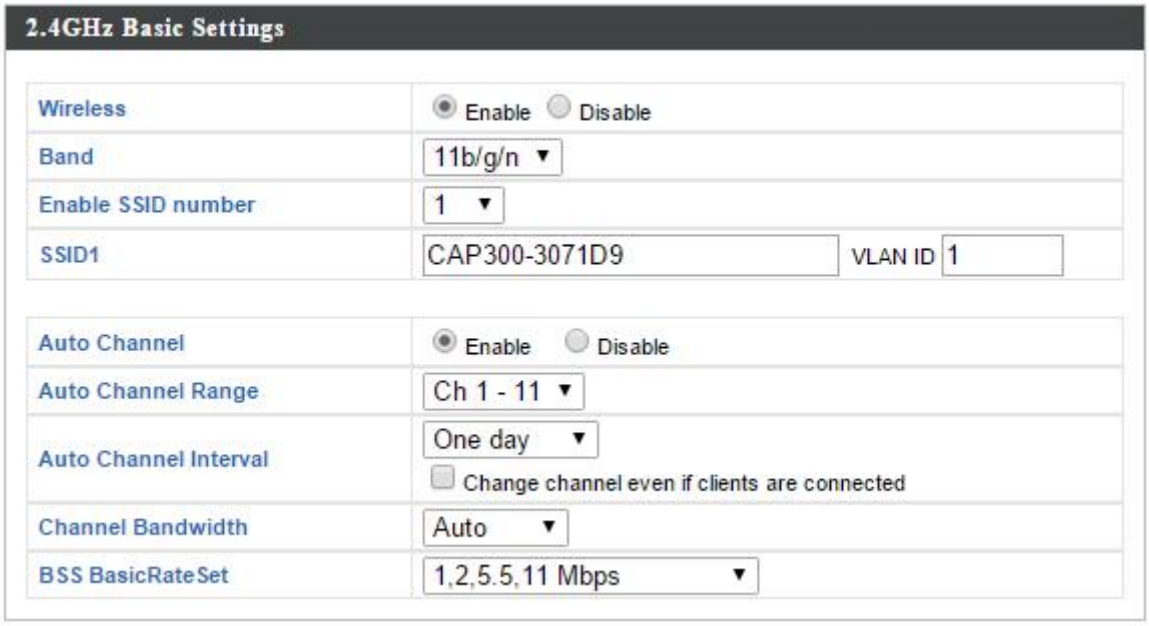



**2.** Enter the IP address settings you wish to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click "Apply" to save the changes and wait a few moments for the access point to reload.

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

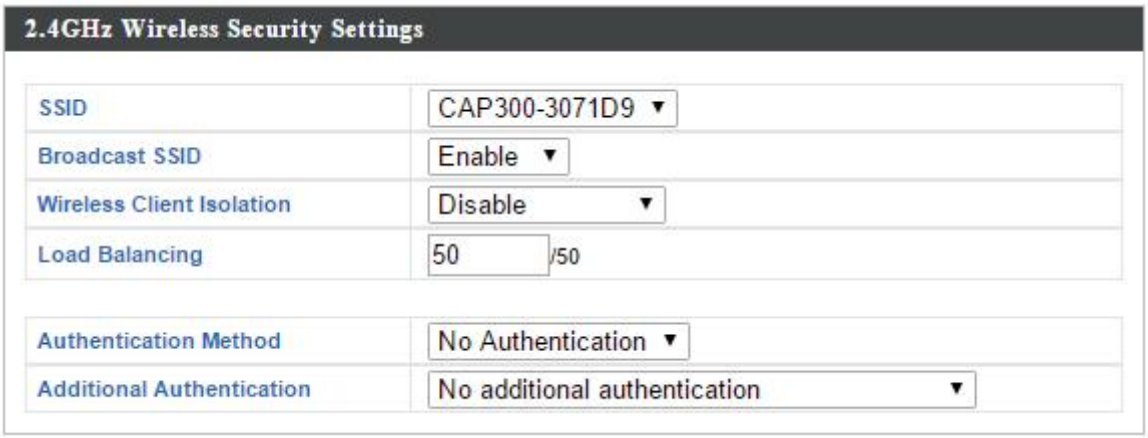
**3.** To change the SSID of your access point's 2.4GHz wireless network(s), go to **"Wireless Setting" > "2.4GHz 11bgn" > "Basic"**. Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".

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

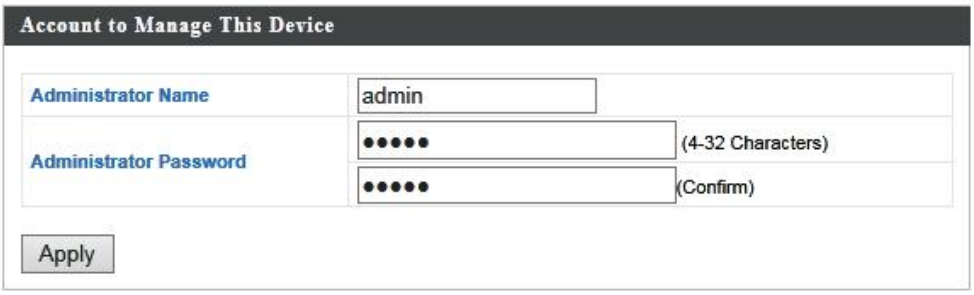



**4.** To configure the security of your access point's 2.4GHz wireless network(s), go to **"Wireless Setting" > "2.4GHz 11bgn" > "Security"**. Select an "Authentication Method" and enter a "Pre-shared Key" or "Encryption Key" depending on your choice, then click "Apply".

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

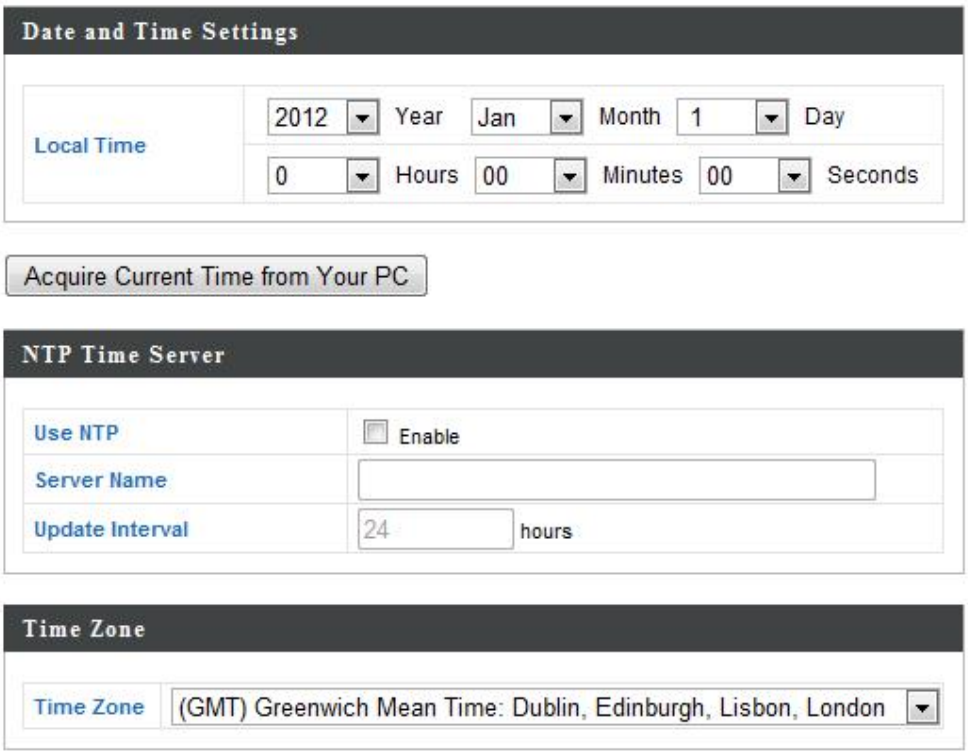


**5.** To change the administrator name and password for the browser based configuration interface, go to **"Management" > "Admin"**.




**6.** Complete the "Administrator Name" and "Administrator Password" fields and click "Apply".

**7.** To set the correct time for your access point, go to **"Management" > "Date and Time"**.




**8.** Set the correct time and time zone for your access point using the drop down menus. The access point also supports NTP (Network Time Protocol) so alternatively you can enter the host name or IP address of a time server. Click "Apply" when you are finished.

***You can use the "Acquire Current Time from your PC" button if you wish to set the access point to the same time as your PC.***

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

# IV. Browser Based Configuration Interface

***In Managed AP mode some functions of the browser based configuration interface are disabled. Please use Edimax Pro NMS on your Controller AP to configure your Managed AP(s).***

The browser-based configuration interface enables you to configure the access point's advanced features. The CAP1300 features a range of advanced functions such as MAC filtering, MAC RADIUS authentication, VLAN configurations, up to 32 SSIDs and many more. To access the browser based configuration interface:

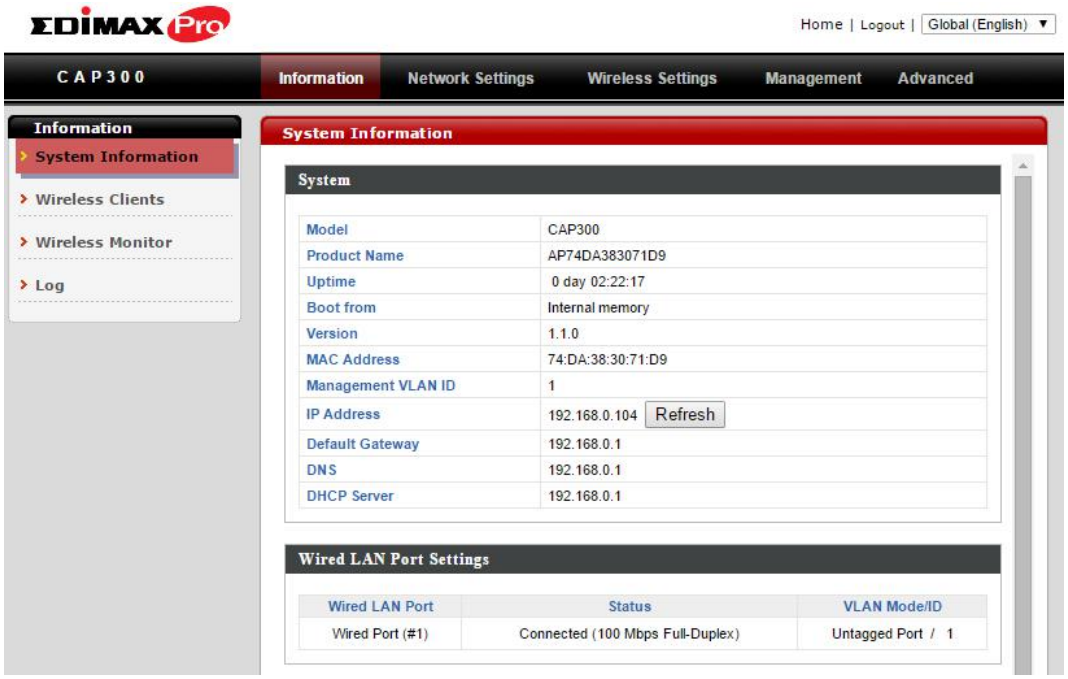
**1.** Connect a computer to your access point using an Ethernet cable.

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

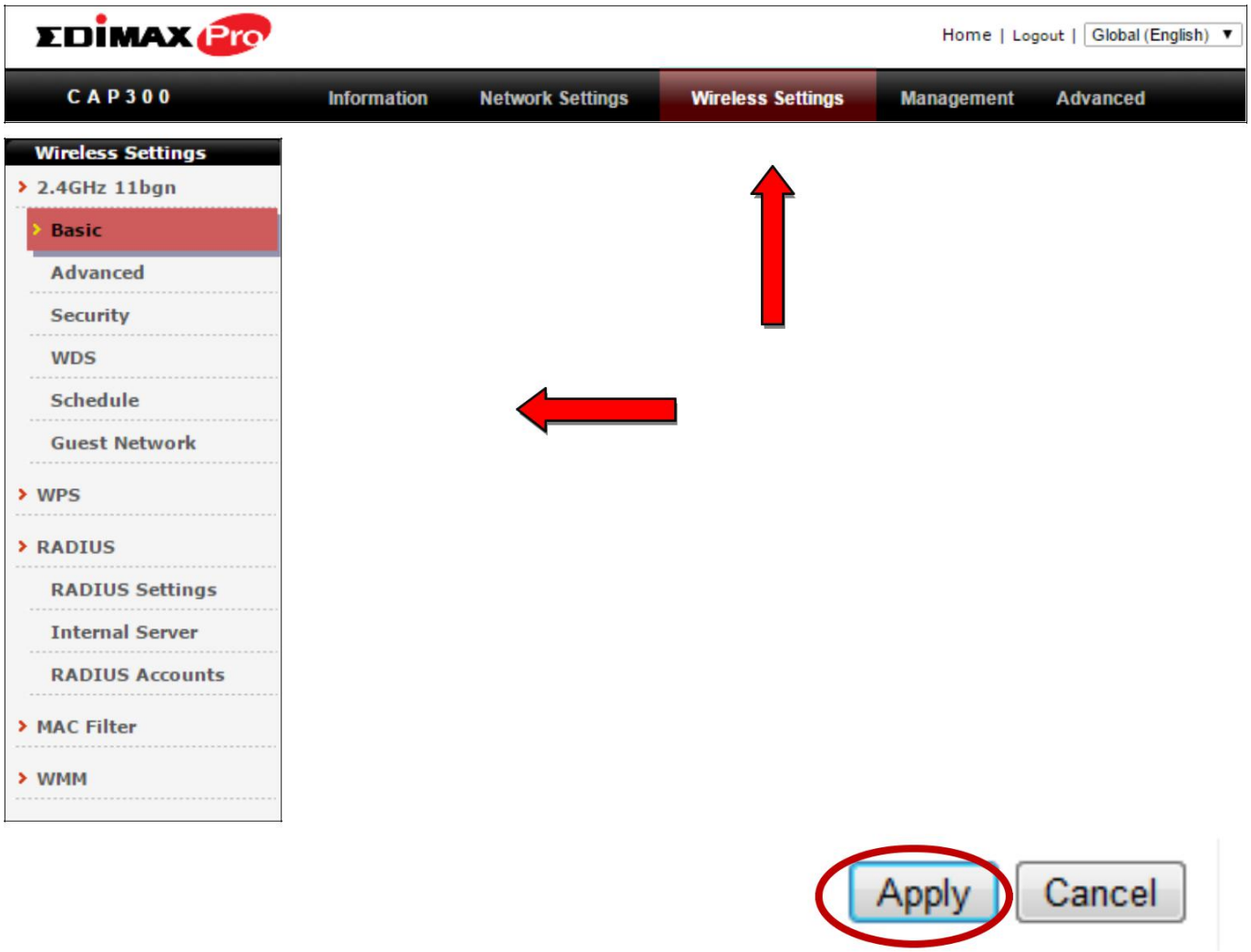
**3.** You will be prompted for a username and password. The default username is "admin" and the default password is "1234", though it was recommended that you change the password during setup (see **III-2. Basic Settings**).

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

**4.** You will arrive at the "System Information" screen shown below.

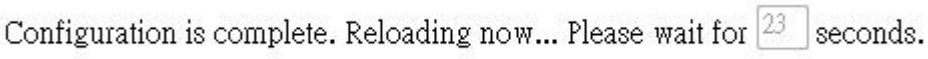


**5.** Use the menu across the top and down the left side to navigate.




**6.** Click "Apply" to save changes and reload the access point, or "Cancel" to cancel changes.

***Please wait a few seconds for the access point to reload after you "Apply" changes, as shown below.***




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

# IV-1. Information

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

## IV-1-1. System Information

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

**System**

| | |
|---|---|
| Model | CAP300 |
| Product Name | AP74DA383071D9 |
| Uptime | 0 day 03:19:17 |
| Boot from | Internal memory |
| Version | 1.1.0 |
| MAC Address | 74:DA:38:30:71:D9 |
| Management VLAN ID | 1 |
| IP Address | 192.168.0.104 Refresh |
| Default Gateway | 192.168.0.1 |
| DNS | 192.168.0.1 |
| DHCP Server | 192.168.0.1 |

**Wired LAN Port Settings**

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

**Wireless 2.4GHz**

| | |
|---|---|
| Status | Enabled |
| MAC Address | 00:AA:BB:CC:DD:10 |
| Channel | Ch 3 + 7 (Auto) |
| Transmit Power | 100% |

**Wireless 2.4GHz /SSID**

| SSID | Authentication Method | Encryption Type | VLAN ID | Additional Authentication | Wireless Client Isolation |
|---|---|---|---|---|---|
| CAP300-CCDD10 | No Authentication | No Encryption | 1 | No additional authentication | Disabled |

**Wireless 2.4GHz /**

| 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 the firmware version. |
| **MAC Address** | Displays the access point’s MAC address. |
| **Management VLAN ID** | Displays the management VLAN ID. |
| **IP Address** | Displays the IP address of this device. Click “Refresh” to update this value. |
| **Default Gateway** | Displays the IP address of the default gateway. |
| **DNS** | IP address of DNS (Domain Name Server) |
| **DHCP Server** | IP address of DHCP Server. |

| Wired LAN Port Settings | |
|---|---|
| **Wired LAN Port** | Specifies which LAN port (1 or 2). |
| **Status** | Displays the status of the specified LAN port (connected or disconnected). |
| **VLAN Mode/ID** | Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port. See **IV-2-3. VLAN** |

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

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

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

## IV-1-2. Wireless Clients

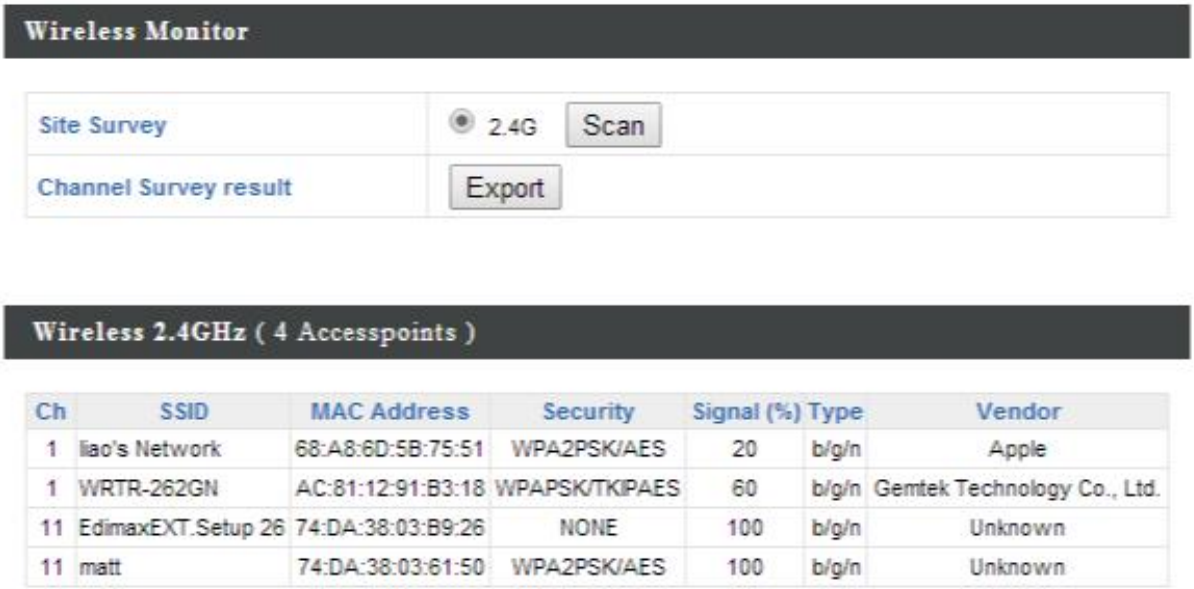
The "Wireless Clients" page displays information about all wireless clients connected to the access point on the 2.4GHz frequency.

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

## IV-1-3. Wireless Monitor

Wireless Monitor is a tool built into the 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** | Click “Scan” to begin the survey. |
| **Channel Survey Result** | After a scan is complete, click “Export” to save the results to local storage. |

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

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

```
Jan  1 00:02:49 [SYSTEM]: LAN, Port[1] link status is changed to down
Jan  1 00:02:25 [SYSTEM]: LAN, Port[1] link is changed to 100Mbps-Full-Duplex
Jan  1 00:00:58 [SYSTEM]: WLAN[2.4G], Best channel selection start, switch to channel 1 + 5
Jan  1 00:00:38 [SYSTEM]: WLAN[5G], Skip Best channel selection and wait for next time
Jan  1 00:00:12 [SYSTEM]: LAN, Port[1] link status is changed to down
Jan  1 00:00:12 [SYSTEM]: LAN, Port[0] link status is changed to down
Jan  1 00:00:11 [SYSTEM]: TFTP server, Stopping
Jan  1 00:00:11 [SYSTEM]: FTP server, Stopping
Jan  1 00:00:11 [SYSTEM]: HTTPS, start
Jan  1 00:00:11 [SYSTEM]: HTTP, start
Jan  1 00:00:11 [SYSTEM]: LAN, Firewall Disabled
Jan  1 00:00:11 [SYSTEM]: LAN, NAT Disabled
Jan  1 00:00:11 [SYSTEM]: NET, Firewall Disabled
Jan  1 00:00:11 [SYSTEM]: NET, NAT Disabled
Jan  1 00:00:10 [SYSTEM]: LEDs, light on specific LEDs
Jan  1 00:00:07 [SYSTEM]: WLAN[5G], Channel = AutoSelect
Jan  1 00:00:07 [SYSTEM]: WLAN[5G], Wireless Mode = 11ACVHT80
Jan  1 00:00:02 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan  1 00:00:02 [SYSTEM]: WLAN[2.4G], Wireless Mode = 11NGHT40MINUS
Jan  1 00:00:02 [SYSTEM]: DHCPC, start
Jan  1 00:00:02 [SYSTEM]: LAN, start
Jan  1 00:00:02 [SYSTEM]: Bridge, start
```

Save Clear Refresh

| | |
|---|---|
| **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*

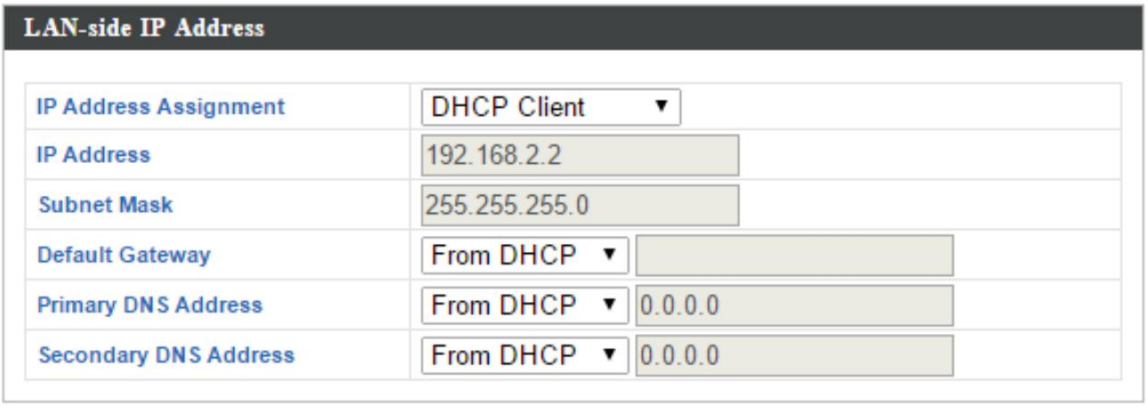
## IV-2. Network Settings

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

### IV-2-1. LAN-Side IP Address

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

***The access point's default IP address is 192.168.2.2.***




| LAN-side IP Address | |
|---|---|
| **IP Address Assignment** | Select "DHCP Client" for your access point to be assigned a dynamic IP address from your router's DHCP server, or select "Static IP" to manually specify a static/fixed IP address for your access point (below). |
| **IP Address** | Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address. |
| **Subnet Mask** | Specify a subnet mask. The default value is 255.255.255.0 |

| | |
|---|---|
| **Default Gateway** | For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank. |

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

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

## IV-2-2. LAN Port

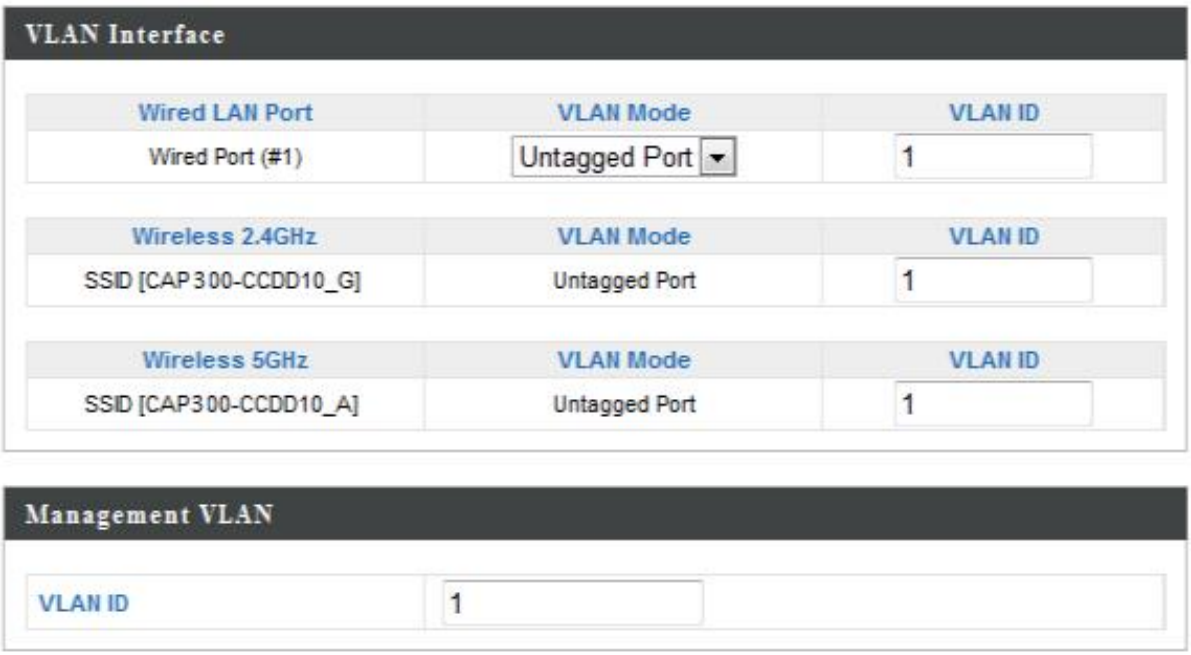
The “LAN Port” page allows you to configure the settings for your access point’s two wired LAN (Ethernet) ports.

| | |
|---|---|
| **Wired LAN Port** | Identifies LAN port 1 or 2. |
| **Enable** | Enable/disable specified LAN port. |
| **Speed & Duplex** | Select a speed & duplex type for specified LAN port, or use the “Auto” value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packets transfer/receive. |
| **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-2-3. VLAN

The "VLAN" (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other. VLAN IDs 1 – 4095 are supported.

***VLAN IDs in the range 1 – 4095 are supported.***




| VLAN Interface | |
|---|---|
| **Wired LAN Port/Wireless** | Identifies LAN port 1 or 2 and wireless SSIDs. |
| **VLAN Mode** | Select "Tagged Port" or "Untagged Port" for specified LAN interface. |
| **VLAN ID** | Set a VLAN ID for specified interface, if "Untagged Port" is selected. |

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

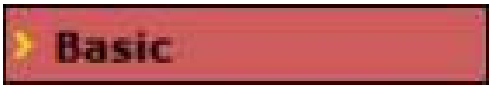
## IV-3. Wireless Settings

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

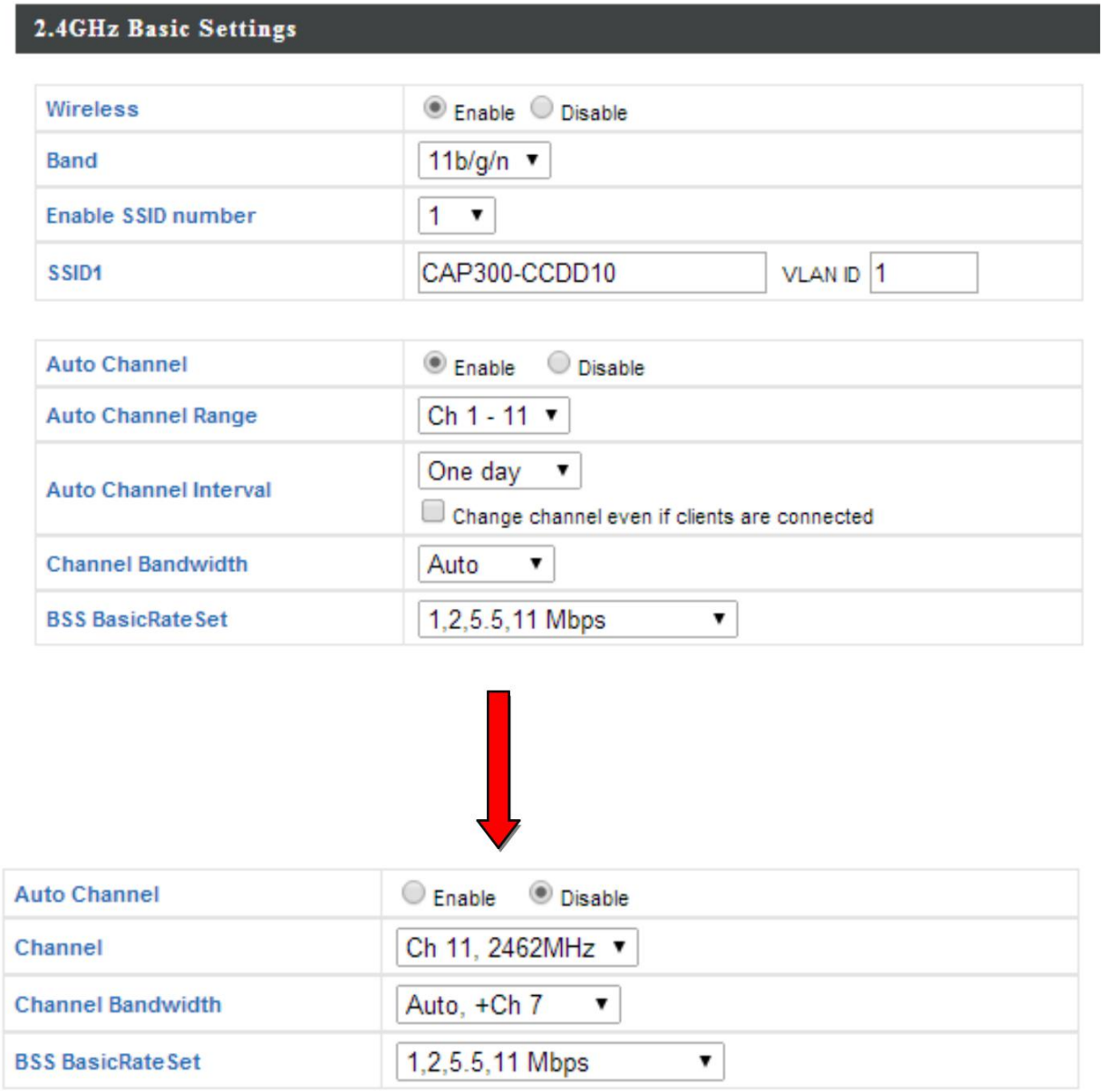
### IV-3-1. 2.4GHz 11bgn

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

## IV-3-1-1. Basic




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



| | |
|---|---|
| **Wireless** | Enable or disable the access point's 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active. |
| **Band** | Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g & 802.11n can be selected. |
| **Enable SSID Number** | Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of 16 can be enabled. |
| **SSID#** | Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters. |
| **VLAN ID** | Specify a VLAN ID for each SSID. |
| **Auto Channel** | Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz 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), 40MHz (higher performance but potentially higher interference) or Auto (automatically select based on interference level). |
| **BSS BasicRateSet** | Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients. |

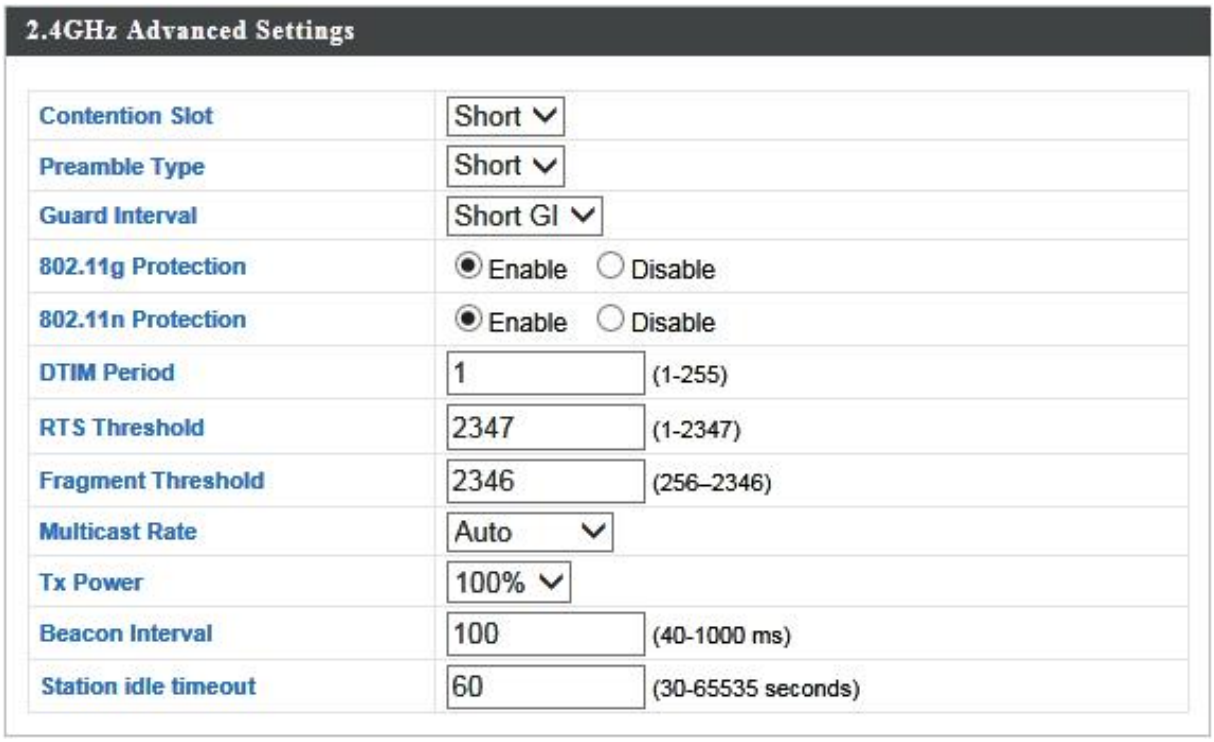
When auto channel is disabled, select a wireless channel manually:

| | |
|---|---|
| **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-3-1-2. Advanced

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

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




| | |
|---|---|
| **Contention Slot** | Select “Short” or “Long” – this value is used for contention windows in WMM (see **IV-3-6. WMM**). |
| **Preamble Type** | Set the wireless radio preamble type. The preamble type in 802.11 based wireless 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. |

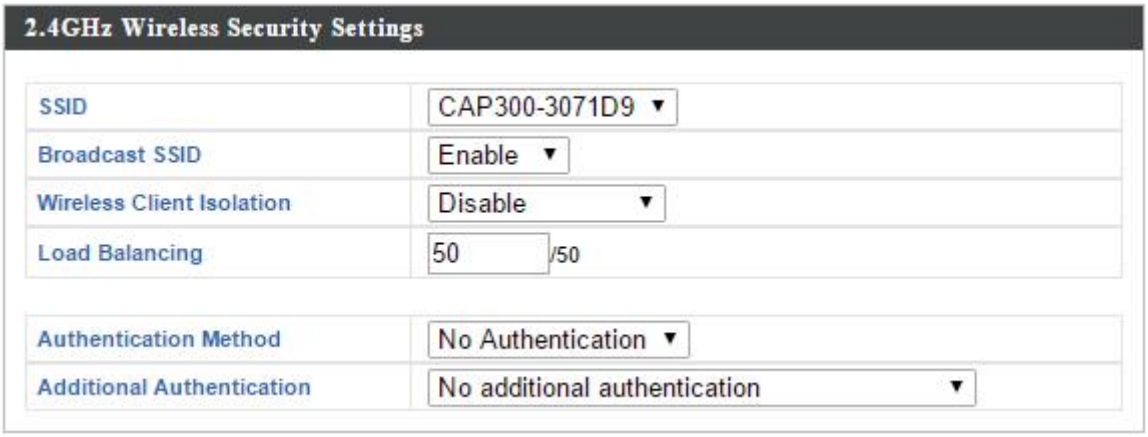
| | |
|---|---|
| **802.11g Protection** | Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.) |
| **802.11n Protection** | 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 distant areas will not be able to access your signal. |
| **Beacon Interval** | Set the beacon interval of the wireless radio. The default value is 100. |
| **Station idle timeout** | Set the interval for keepalive messages from the access point to a wireless client to verify if the station is still alive/active. |

### IV-3-1-3. Security

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

***It'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 Selection** | Select which SSID to configure security settings for. |
| **Broadcast SSID** | Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID. |
| **Wireless Client Isolation** | Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords. |
| **Load Balancing** | Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 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-3-1-3-6.**) appropriate for your method. |

### IV-3-1-3-1. 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-3-1-3-2. WEP

WEP (Wired Equivalent Privacy) is a basic 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” (any alphanumerical character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F). |
| **Default Key** | Select which encryption key (1 – 4 below) is the default key. For security purposes, you can set up to four keys (below) and change which is the default key. |
| **Encryption Key 1 – 4** | Enter your encryption key/password according to the format you selected above. |

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

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

### IV-3-1-3-4. WPA-PSK

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

| | |
|---|---|
| **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 and A-F). |
| **Pre-Shared Key** | Please enter a security key/password according to the format you selected above. |

### IV-3-1-3-5. WPA-EAP

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

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

### IV-3-1-3-6. Additional Authentication

Additional wireless authentication methods can also be used:

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

**MAC Address Filter**

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

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

**MAC Filter & MAC-RADIUS Authentication**

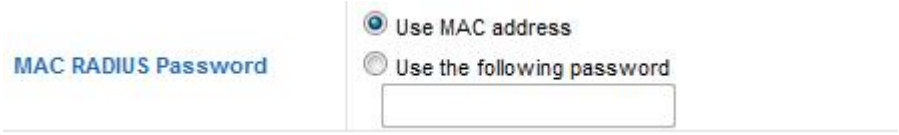
Restrict wireless clients access using both of the above MAC filtering & RADIUS authentication methods.

**MAC-RADIUS Authentication**

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

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

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



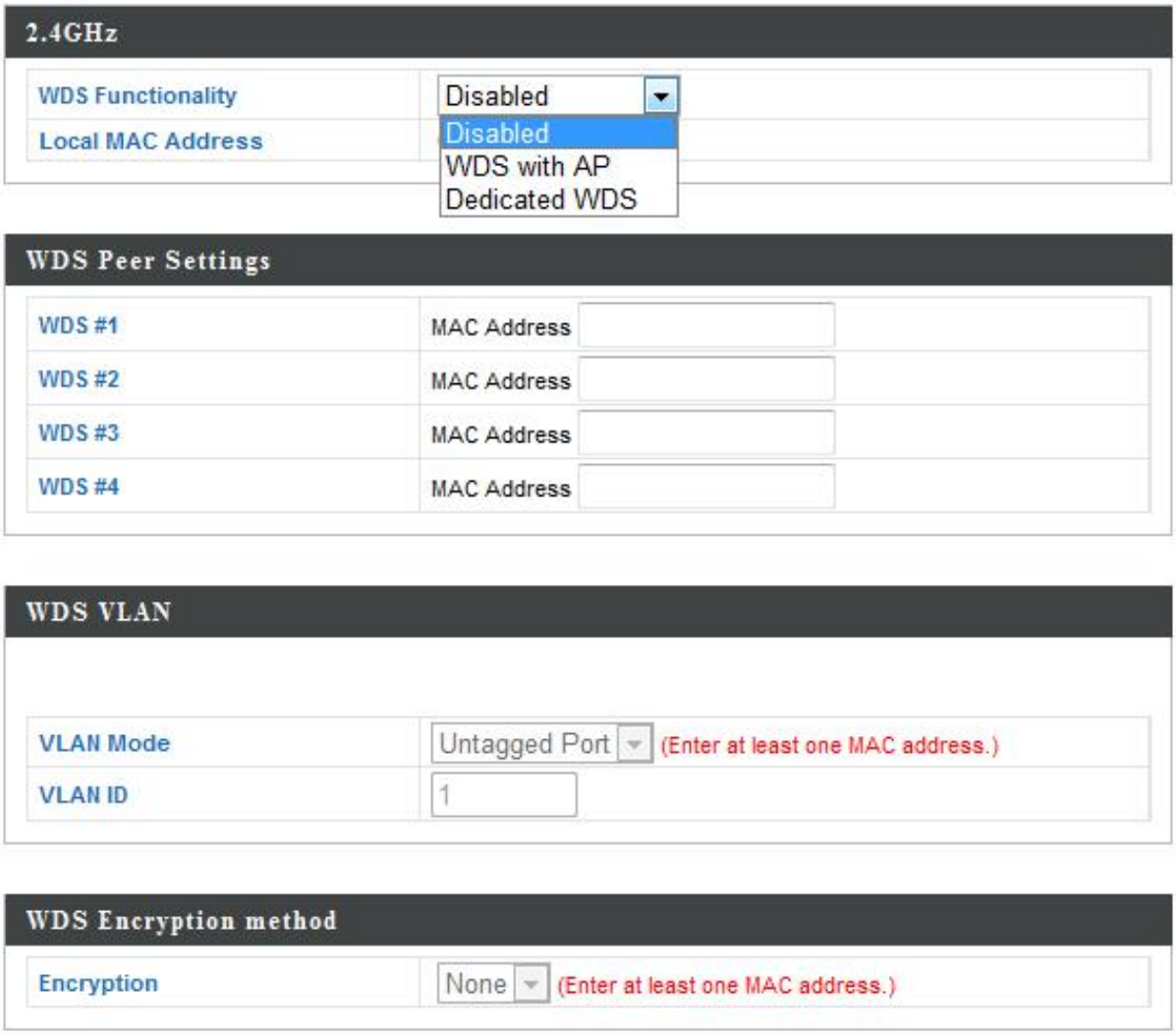

| | |
|---|---|
| **MAC RADIUS Password** | Select whether to use MAC address or password authentication via RADIUS server. If you select “Use the following password”, enter the password in the field below. The password should match the “Shared Secret” used in **IV-3-4. RADIUS**. |

## IV-3-1-4. WDS

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

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

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



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

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

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

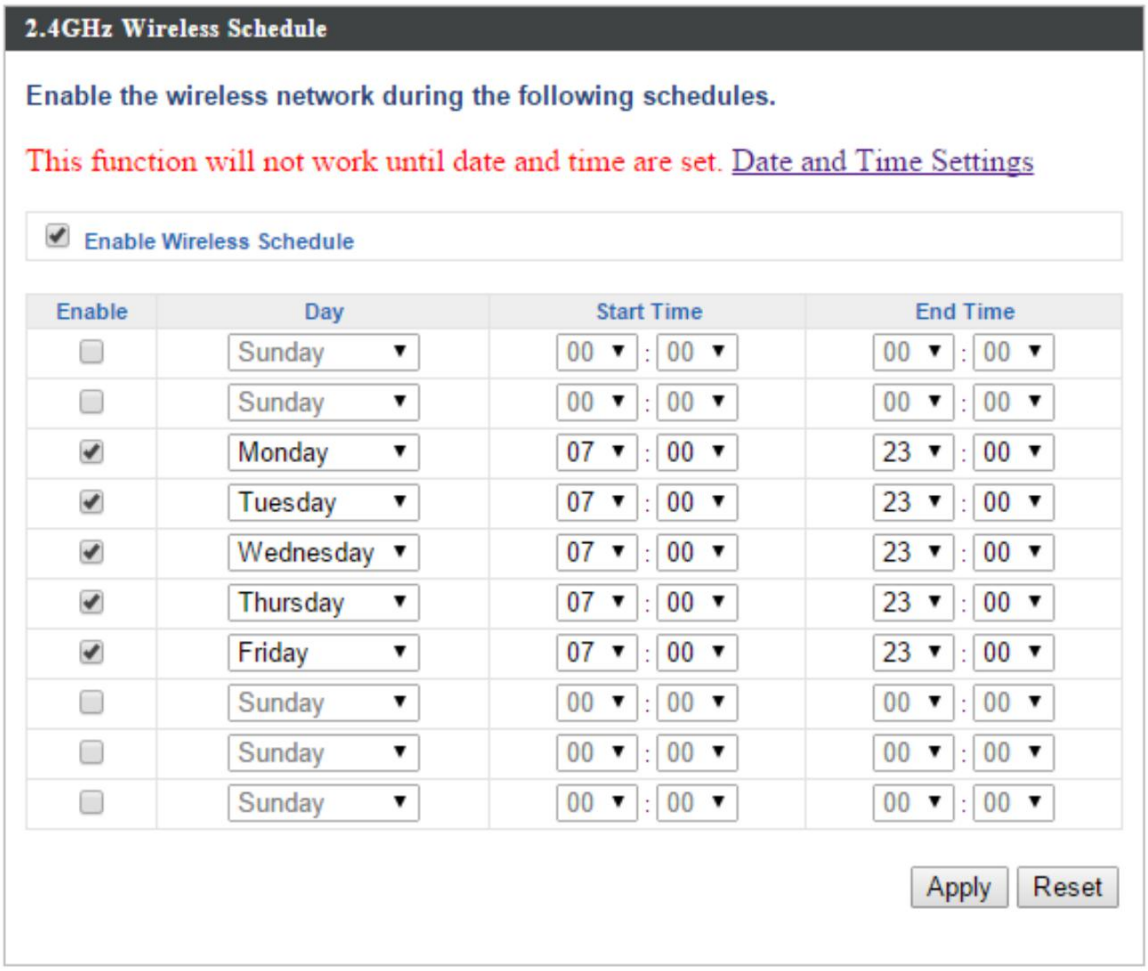
| WDS Encryption method | |
|---|---|
| **Encryption** | Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES consisting of 8-63 alphanumeric characters. |

## IV-3-1-5. Schedule

The schedule feature allows you to automate the wireless network for specified times.

Check/uncheck the box "Enable Wireless Schedule" to enable/disable the wireless scheduling function.

***The access point's time and date settings must be set in order to use this function.***




***Wireless scheduling can save energy and increase the security of your network.***

**1.** Use the "Enable" checkboxes to select schedule(s).

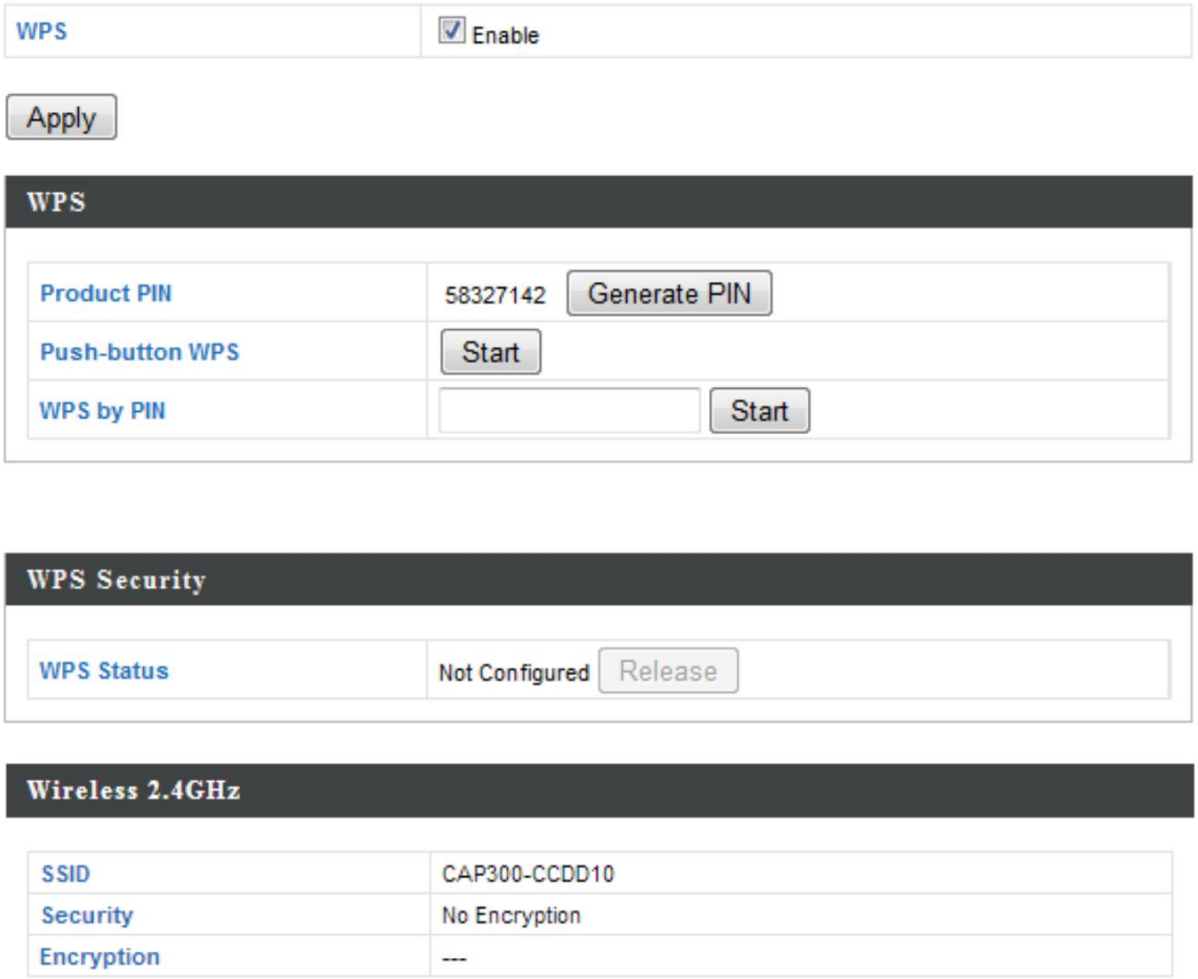
**2.** Specify a day, start time and end time for the schedule using the drop-down menus.

**3.** Click "Apply" to save the schedules or "Reset" to reset all values back to default.

## IV-3-2. 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-3-1-3-6 & IV-3-4**). |

| WPS | |
|---|---|
| **Product PIN** | Displays the WPS PIN code of the device, used for PIN code WPS. You will be required to enter this PIN code into another WPS device for PIN code WPS. Click “Generate PIN” to generate a new WPS PIN code. |
| **Push-Button WPS** | Click “Start” to activate WPS on the access point for approximately 2 minutes. 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 Security | |
|---|---|
| **WPS Status** | WPS security status is displayed here. Click “Release” to clear the existing status. |

| Wireless 2.4GHz | |
|---|---|
| **SSID** | Displays the SSID name(s) for the specified frequency. |
| **Security** | Displays the security for the specified SSID. |
| **Encryption** | Displays the encryption type for the specified SSID. See **IV-3. Wireless Settings** |

## IV-3-3. RADIUS

| RADIUS |
|---|

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

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

The access point can utilize both a primary and secondary (backup) external RADIUS server.

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

**RADIUS Server (2.4GHz)**

| Primary RADIUS Server | |
|---|---|
| RADIUS Server | |
| Authentication Port | 1812 |
| Shared Secret | |
| Session Timeout | 3600 second(s) |
| Accounting | Enable Disable |
| Accounting Port | 1813 |

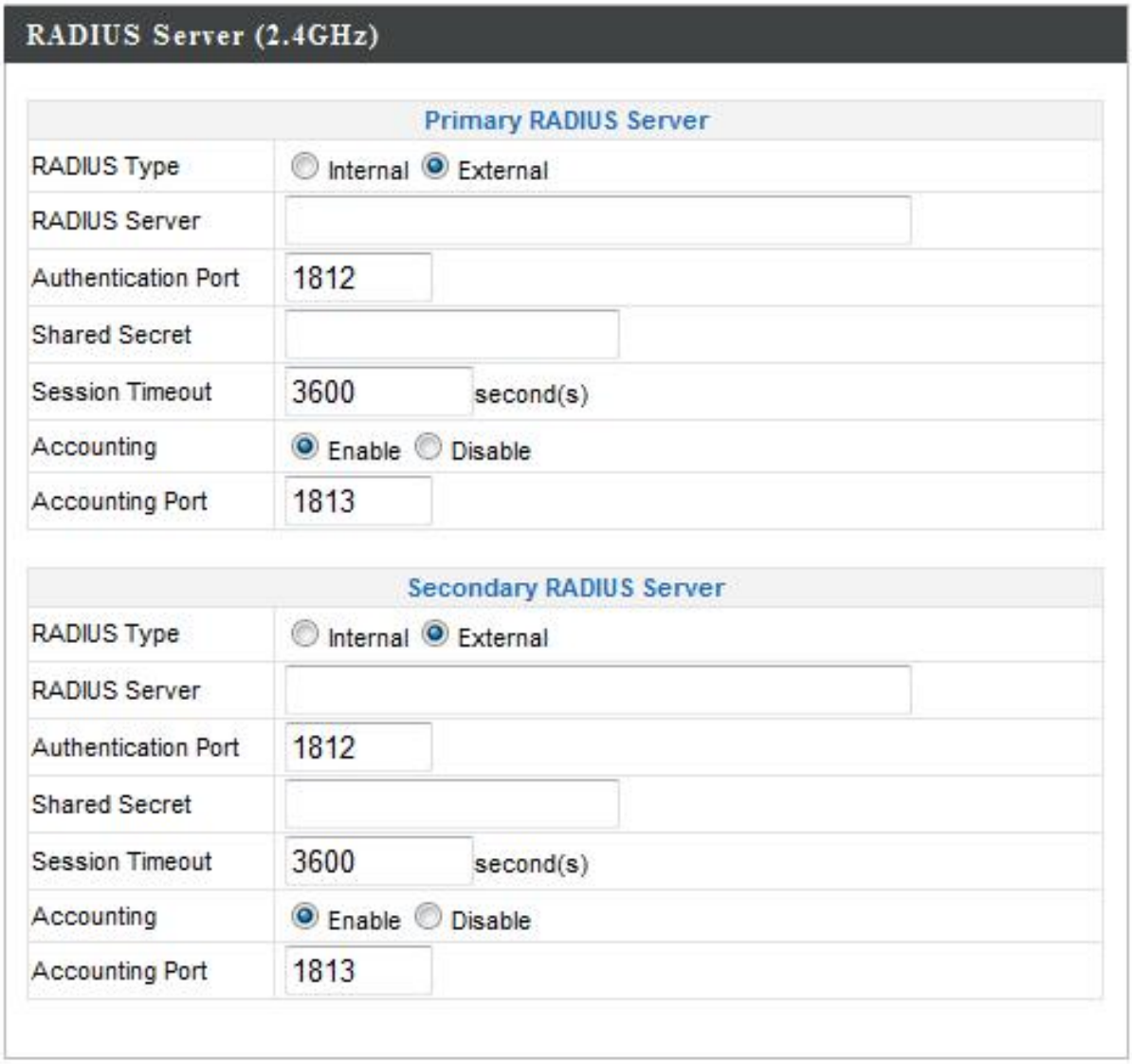
| Secondary RADIUS Server | |
|---|---|
| RADIUS Server | |
| Authentication Port | 1812 |
| Shared Secret | |
| Session Timeout | 3600 second(s) |
| Accounting | Enable Disable |
| Accounting Port | 1813 |

| | |
|---|---|
| **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-3-3-1. RADIUS Settings

Configure the RADIUS server settings for 2.4GHz. 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. |

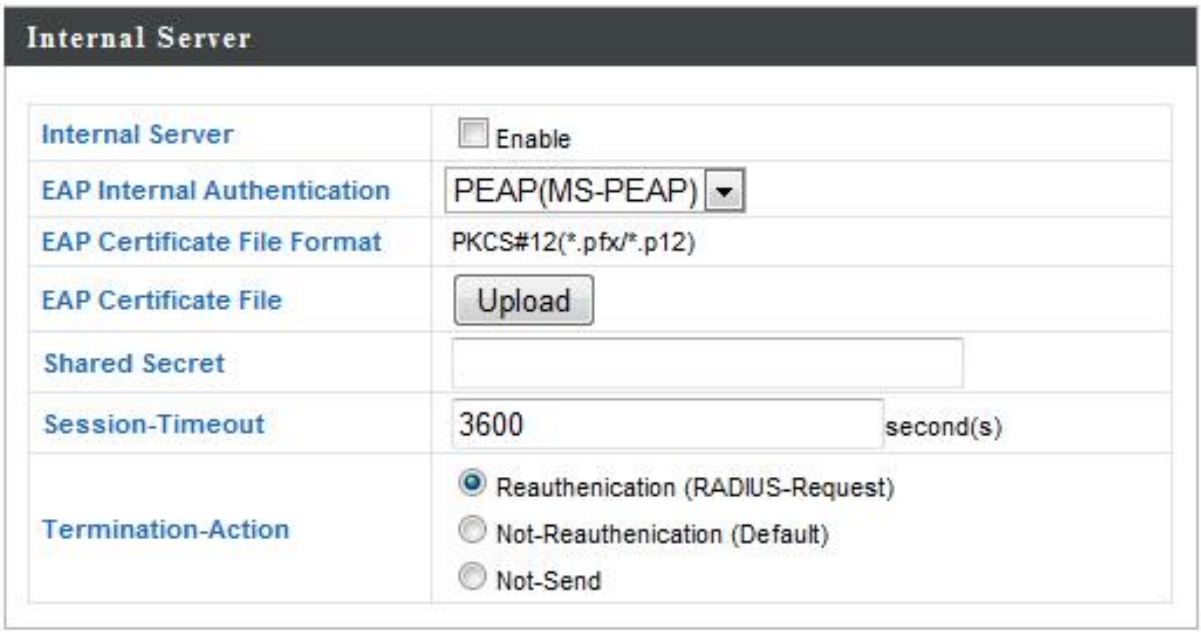
| | |
|---|---|
| **Shared Secret** | Enter a shared secret/password between 1 – 99 characters in length. This should match the "MAC-RADIUS" password used in **IV-3-1-3-6** or **IV-3-2-3**. |
| **Session Timeout** | Set a duration of session timeout in seconds between 0 – 86400. |
| **Accounting** | 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-3-3-2. Internal Server

**Internal Server**

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

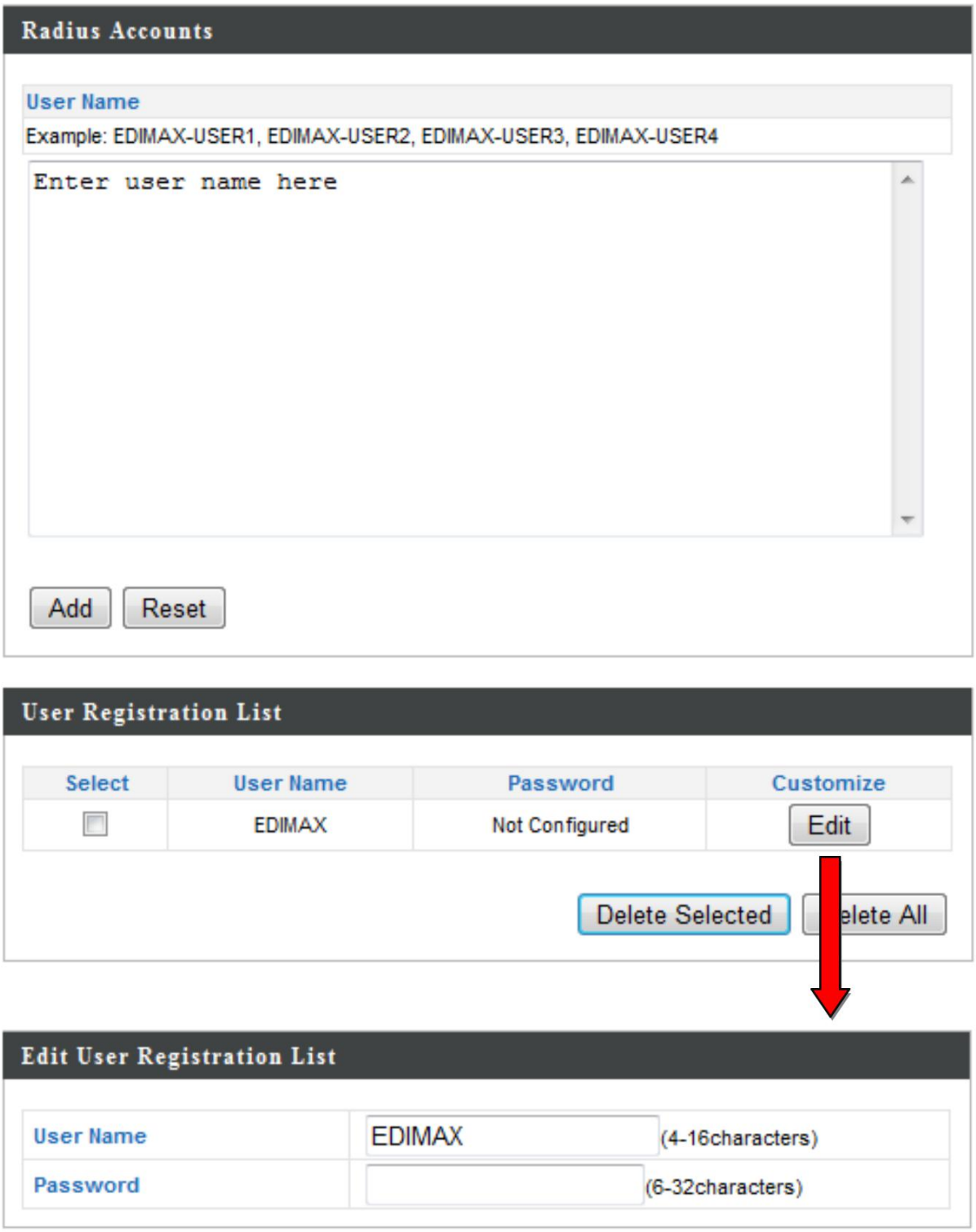
***To use RADIUS servers, go to** "Wireless Settings" → "Security" **and select** "MAC RADIUS Authentication" → "Additional Authentication" **and select** "MAC RADIUS Authentication" **(see** IV-3-1-3. **&** IV-3-2-3**).***



| | |
|---|---|
| **Internal Server** | Check/uncheck to enable/disable the access point's internal RADIUS server. |
| **EAP Internal Authentication** | Select EAP internal authentication type from the drop down menu. |
| **EAP Certificate File Format** | Displays the EAP certificate file format: PCK#12(*.pfx/*.p12) |
| **EAP Certificate File** | Click "Upload" to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate. |
| **Shared Secret** | Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 – 99 characters in length. This should match the "MAC-RADIUS" password used in **IV-3-1-3-6** or **IV-3-2-3**. |
| **Session Timeout** | Set a duration of session timeout in seconds between 0 – 86400. |
| **Termination Action** | Select a termination-action attribute: "Reauthentication" sends a RADIUS request to the access point, "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-3-3-3. 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. |

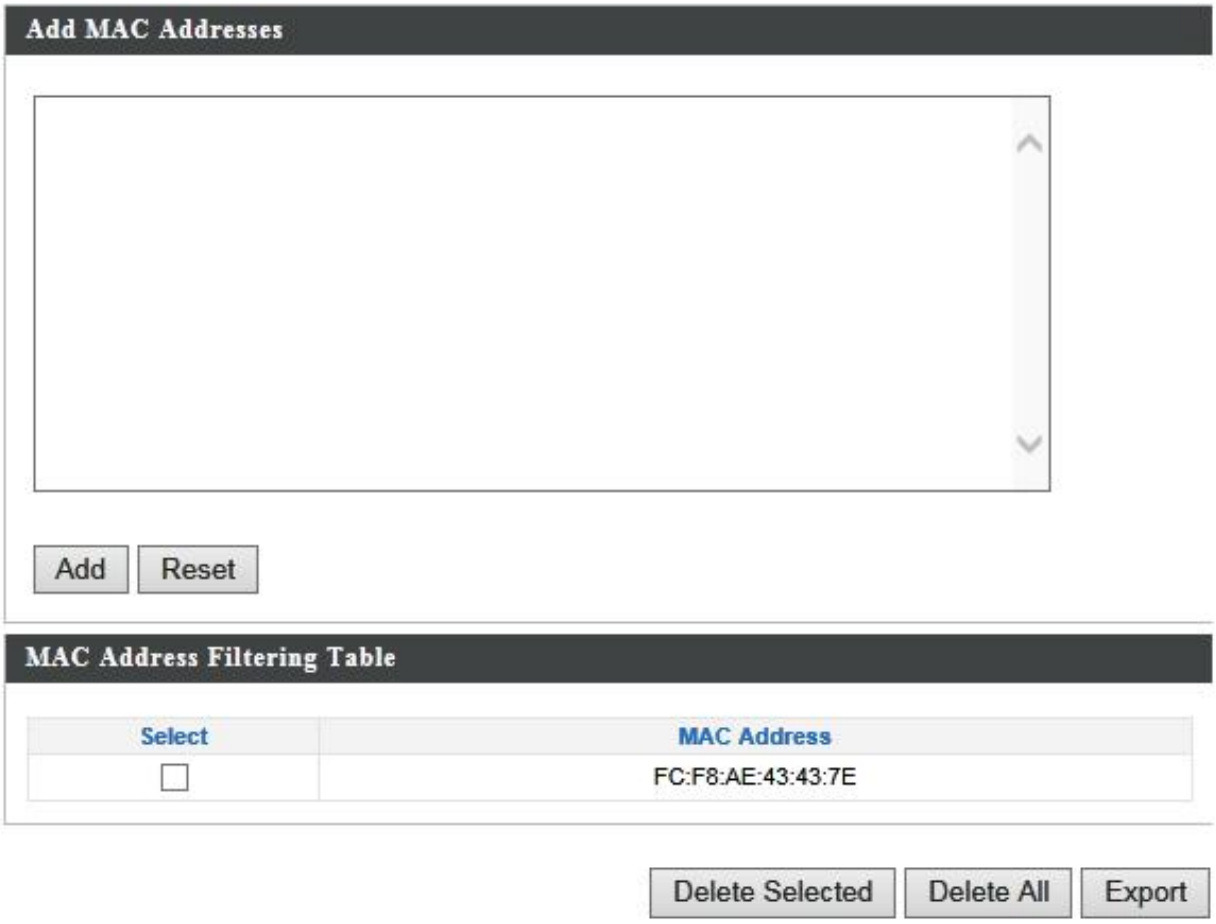
## IV-3-4. MAC Filter

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

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

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

The MAC address filtering table is displayed below:




| | |
|---|---|
| **Add MAC Address** | Enter a MAC address of computer or network device manually e.g. 'aa-bb-cc-dd-ee-ff' or enter multiple MAC addresses separated with |

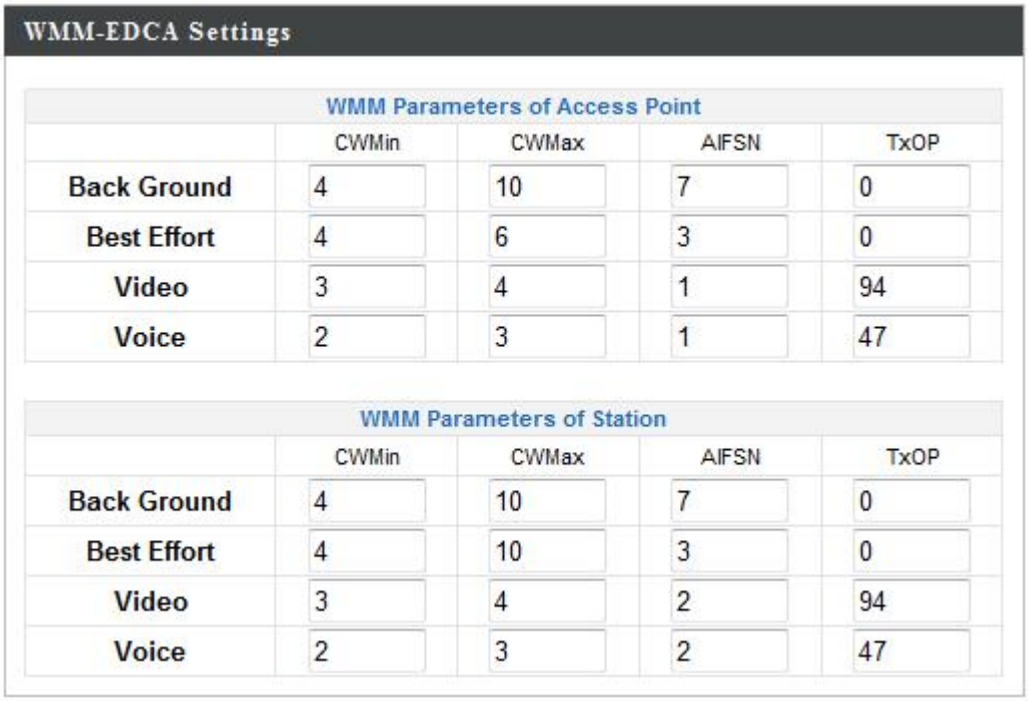
| | |
|---|---|
| | commas, e.g. ‘aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg’ |
| **Add** | Click “Add” to add the MAC address to the MAC address filtering table. |
| **Reset** | Clear all fields. |

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

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

## IV-3-5. WMM

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



WMM-EDCA Settings

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

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

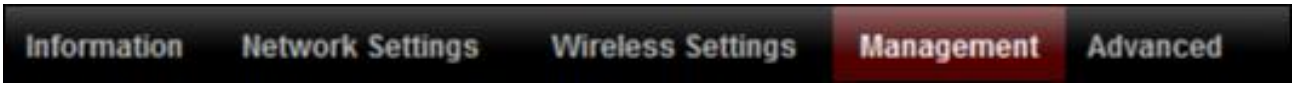
Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

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

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can 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-4. Management




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

### IV-4-1. Admin

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

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

**Account to Manage This Device**

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

Apply

**Advanced Settings**

| | |
|---|---|
| Product Name | AP00AABBCCDD10 |
| Management Protocol | ☑ HTTP<br>☐ TELNET<br>☐ SNMP |
| SNMP Version | v1/v2c ▼ |
| SNMP Get Community | public |
| SNMP Set Community | private |
| SNMP Trap | Disabled ▼ |
| SNMP Trap Community | public |
| SNMP Trap Manager | |

| 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 preference consisting of 1-32 alphanumeric characters. This name is used for reference purposes. |
| **Management Protocol** | Check/uncheck the boxes to enable/disable specified management interfaces (see below). |

| | |
|---|---|
| | When SNMP is enabled, complete the SNMP fields below. |
| **SNMP Version** | Select SNMP version appropriate for your SNMP manager. |
| **SNMP Get Community** | Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests. |
| **SNMP Set Community** | Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests. |
| **SNMP Trap** | Enable or disable SNMP Trap to notify SNMP manager of network errors. |
| **SNMP Trap Community** | Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests. |
| **SNMP Trap Manager** | Specify the IP address or sever name (2-128 alphanumeric characters) of the SNMP manager. |

**HTTP**

*Internet browser HTTP protocol management interface*

**TELNET**

*Client terminal with telnet protocol management interface*

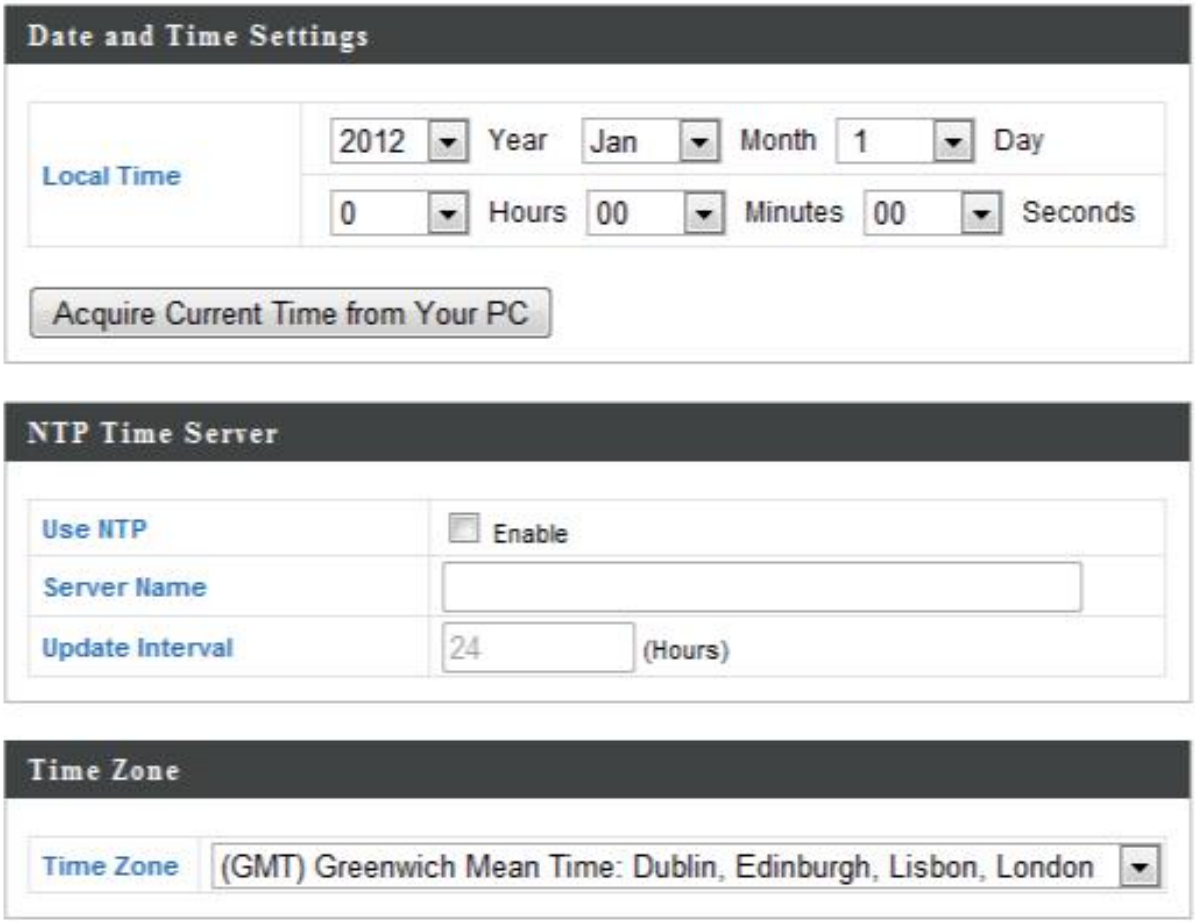
**SNMP**

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

## IV-4-2. Date and Time

**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. |

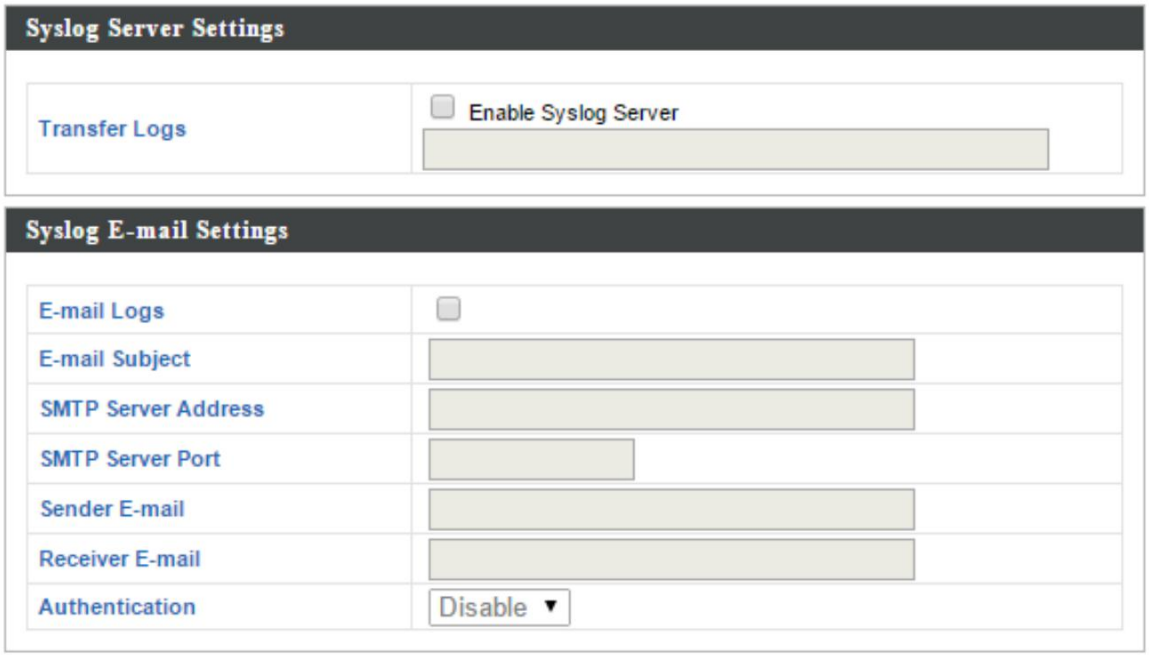
| | |
|---|---|
| **Server Name** | Enter the host name or IP address of the time server if you wish. |
| **Update Interval** | Specify a frequency (in hours) for the access point to update/synchronize with the NTP server. |

| 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-4-3. Syslog Server

**Syslog Server**

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




| 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. |

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

## IV-4-4. Ping Test

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

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

## IV-4-5. I’m Here

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

***The buzzer is loud!***

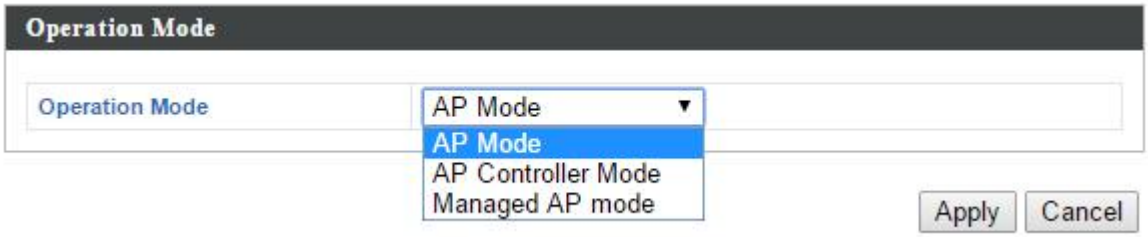
| | |
|---|---|
| **Duration of Sound** | Set the duration for which the buzzer will sound when the “Sound Buzzer” button is clicked. |
| **Sound Buzzer** | Activate the buzzer sound for the above specified duration of time. |

## IV-4-6. Operation Mode

The access point can function in three different modes. Set the operation mode of the access point here. 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. Refer back to **Overview** and **Edimax Pro NMS I. Product Information** for more help.

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

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



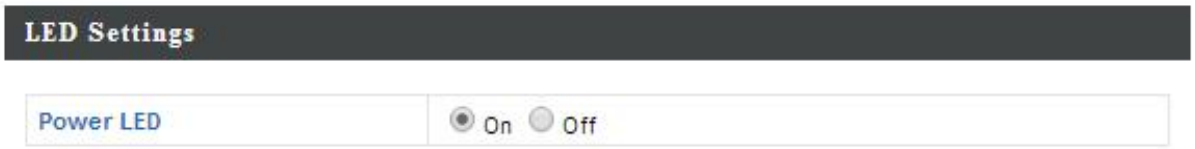

| | |
|---|---|
| **Operation Mode** | AP Mode is a standard access point in a wireless network.<br><br>AP Controller Mode is the master of an AP array and controls all other managed APs (below) using Edimax Pro NMS.<br><br>Managed AP mode is an AP which is part of the AP array and is managed by the Controller AP. |

## IV-5. Advanced

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

### IV-5-1. LED Settings

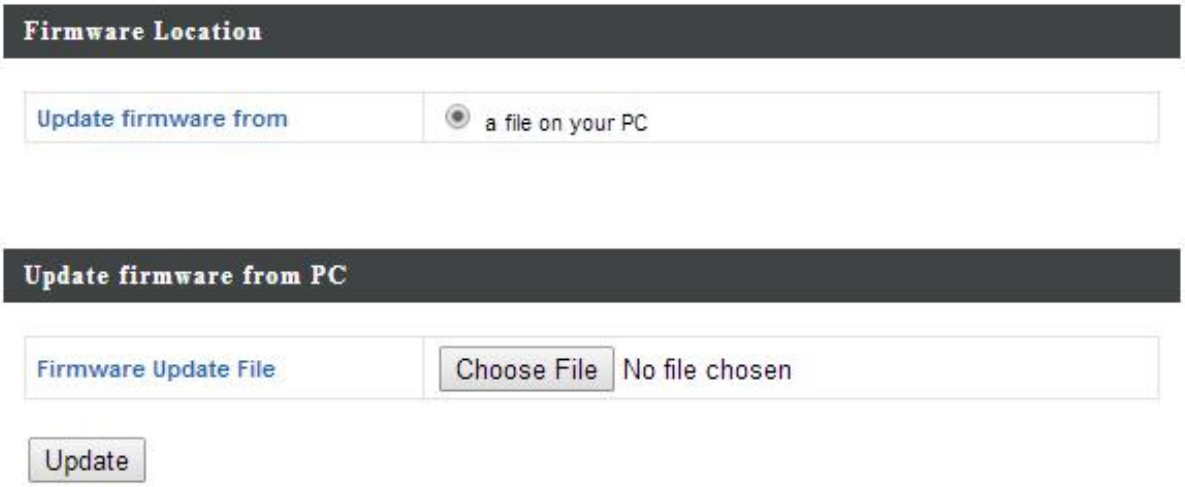
The access point's LEDs can be manually enabled or disabled according to your preference.




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

## IV-5-2. 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. You can download the latest firmware from the Edimax website.

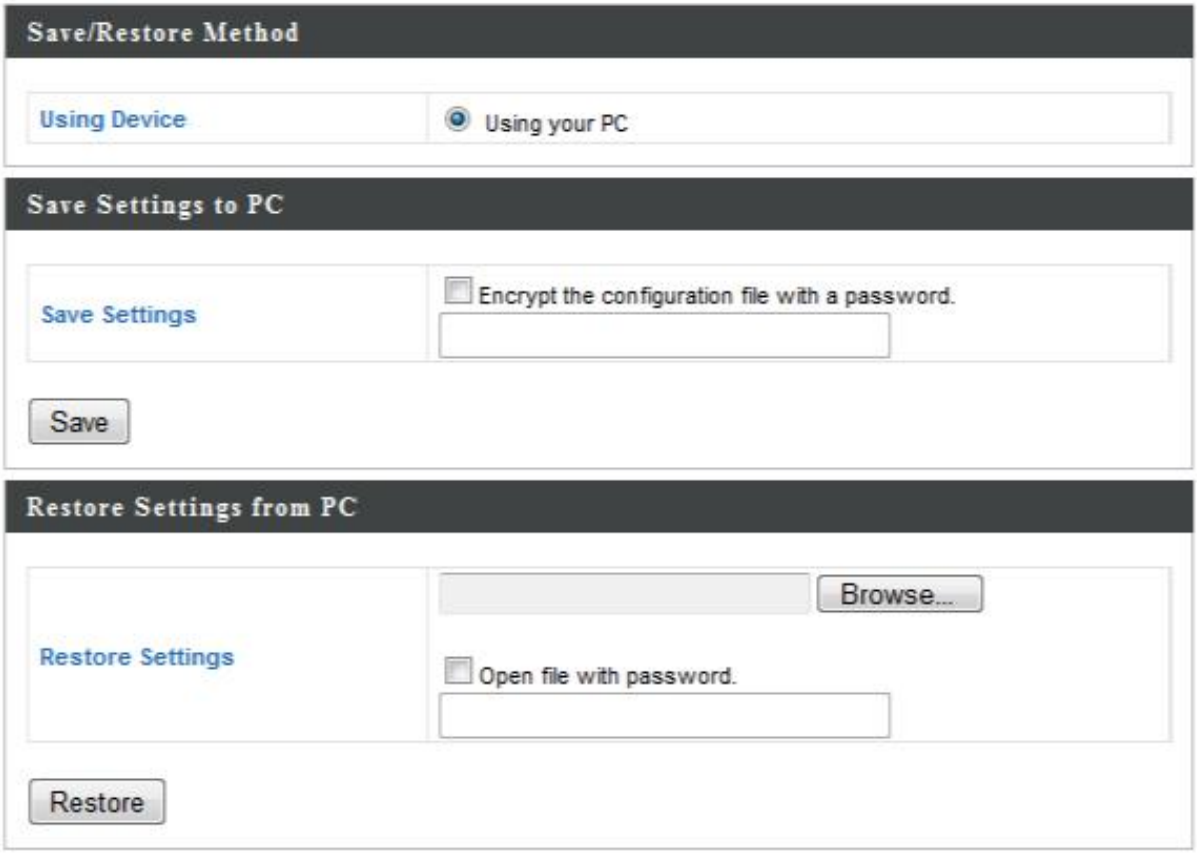



***Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.***

| | |
|---|---|
| **Update Firmware From** | Select "a file on your PC" to upload firmware from your local computer. |
| **Firmware Update File** | Click "Choose File" 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-5-3. 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. |

| 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-5-4. Factory Default

If the access point malfunctions or is not responding, then it is recommended that you reboot the device (see **IV-5.5**) 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-5-5. Reboot

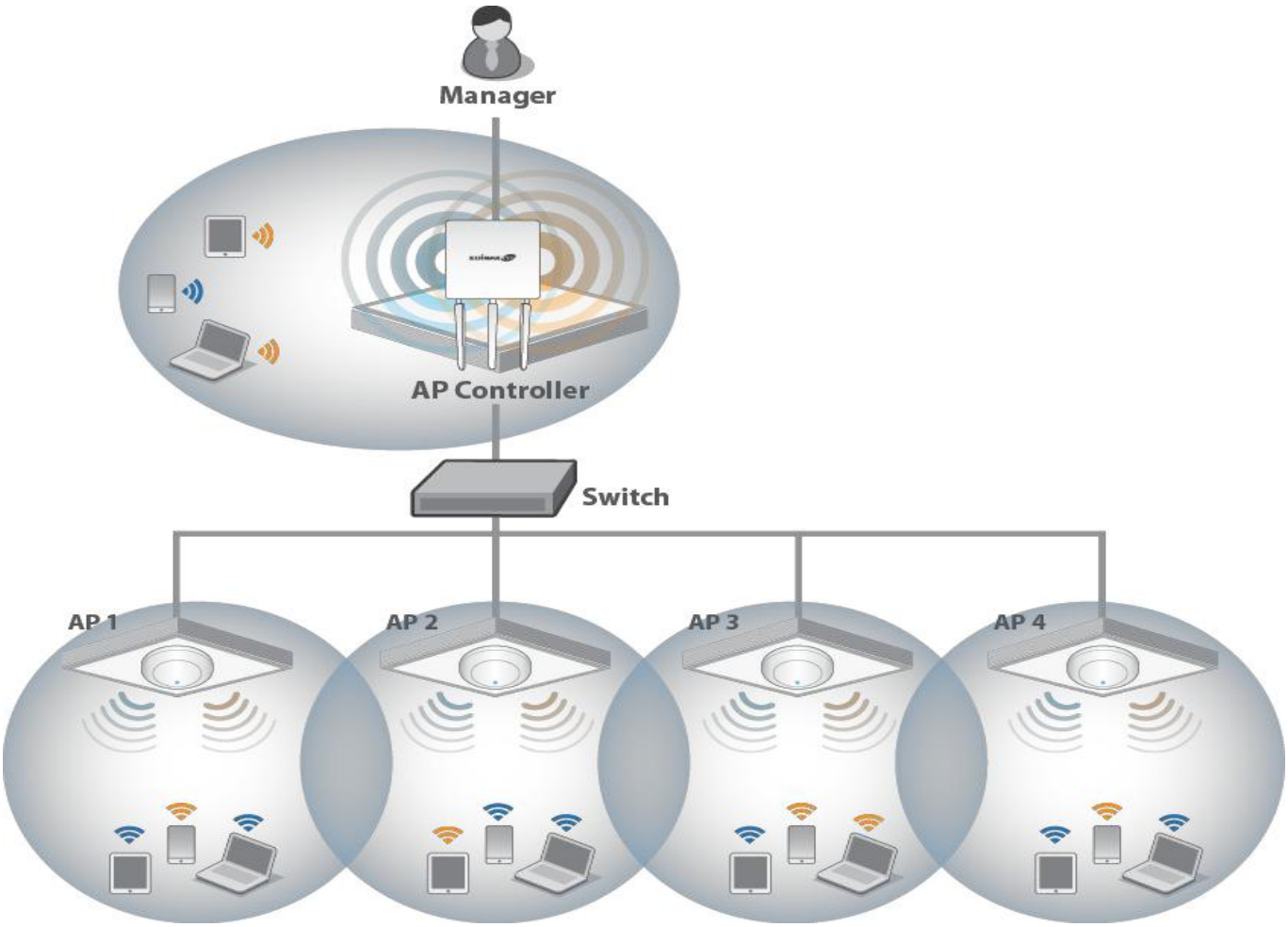
If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the access point back to its factory default settings (see **IV-5-4**). You can reboot the access point remotely using this feature.

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

# I. Product Information

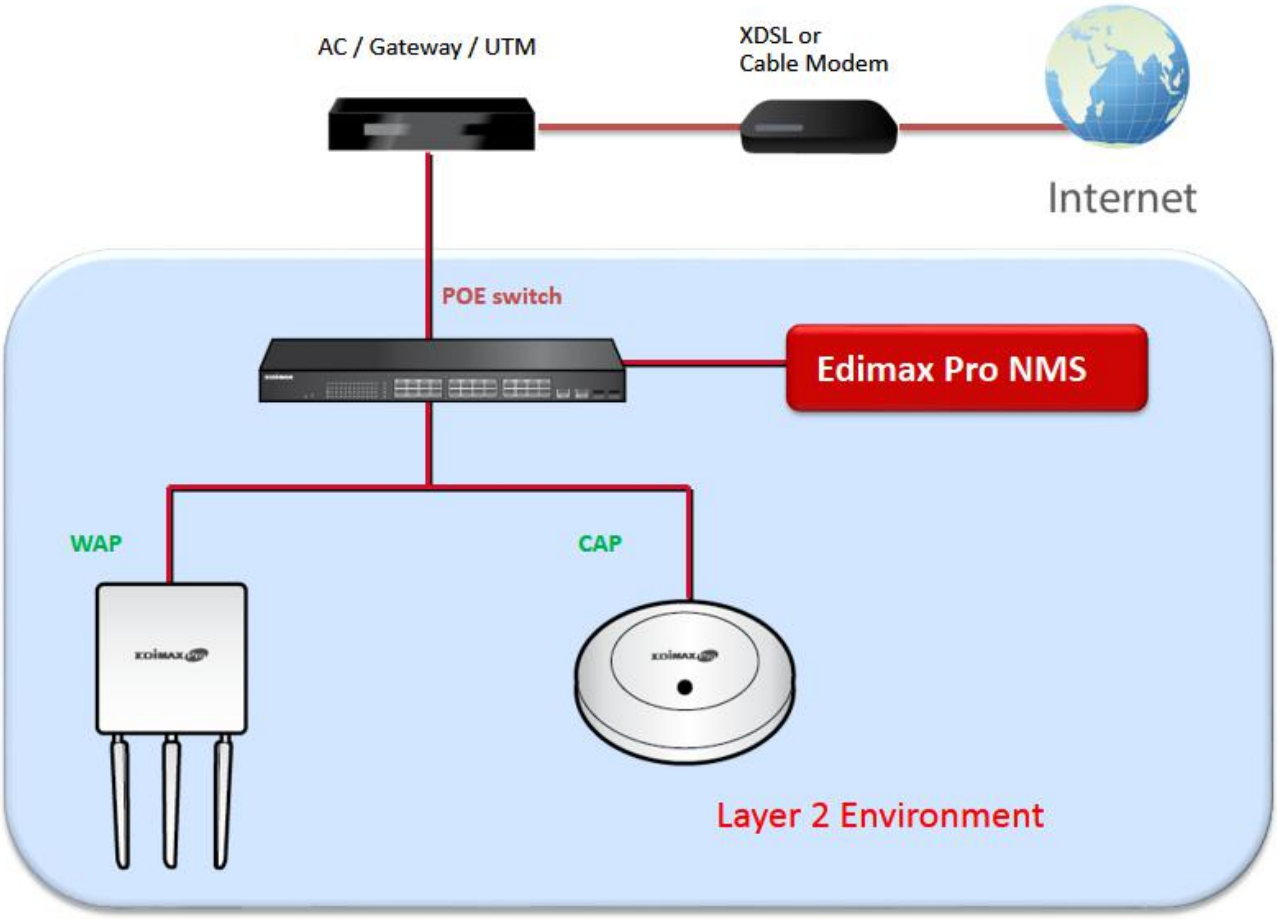
Edimax Pro Network Management Suite (NMS) supports the central management of a group of access points, otherwise known as an AP Array. NMS can be installed on one access point and support up to 8 Edimax Pro access points with no additional wireless controller required, reducing costs and facilitating efficient remote AP management.

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



# II. Quick Setup

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

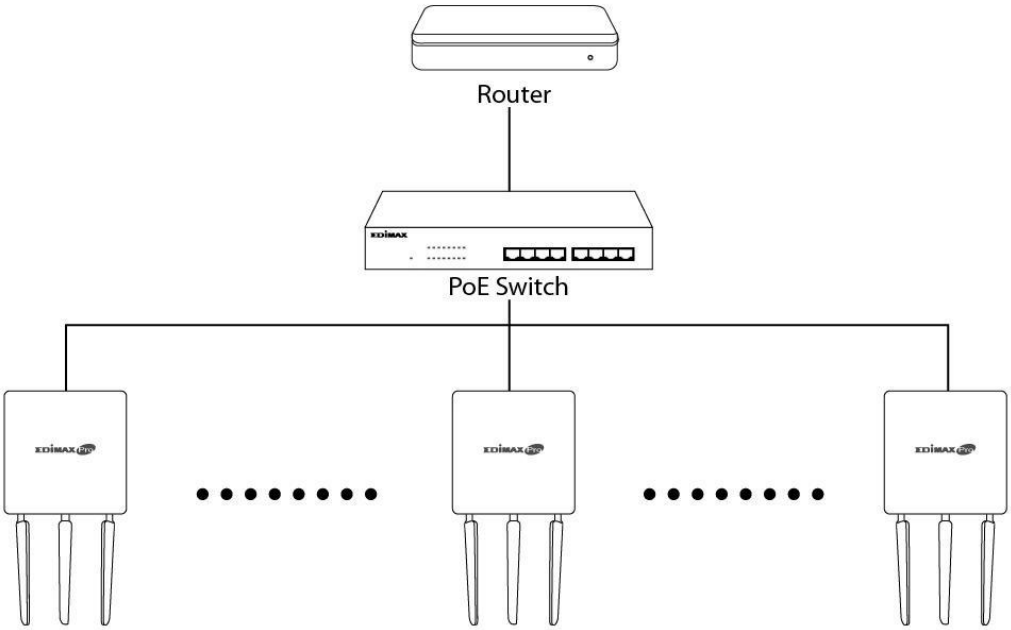



One AP (access point) is designated as the AP Controller (master) and other connected Edimax Pro APs are automatically designated as Managed APs (slaves). Using Edimax Pro NMS you can monitor, configure and manage all Managed APs (up to 8) from the single AP Controller.

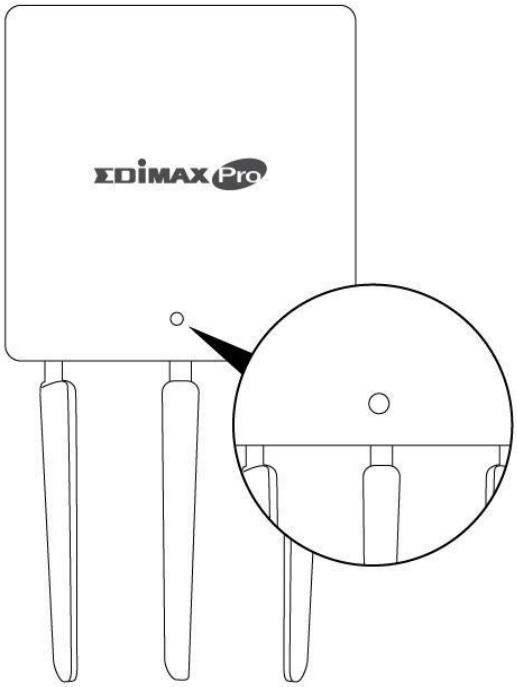
Follow the steps below:

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

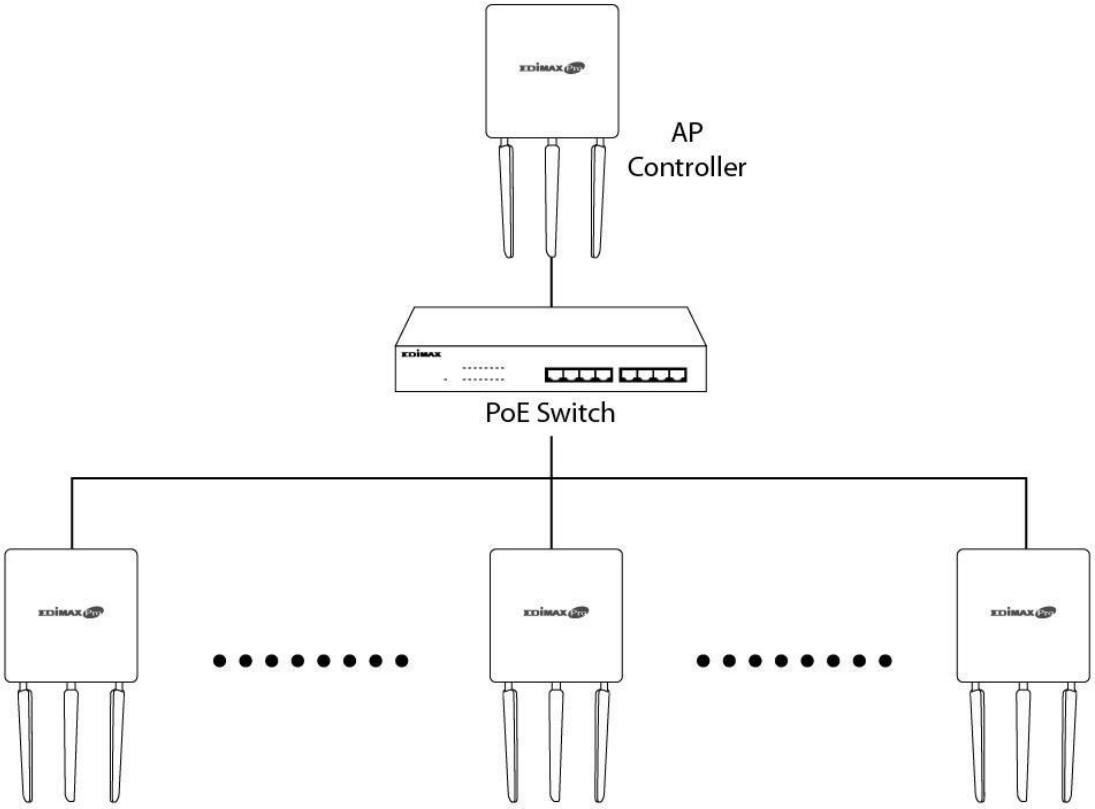
**1.** Connect all APs to an Ethernet or PoE switch which is connected to a gateway/router.



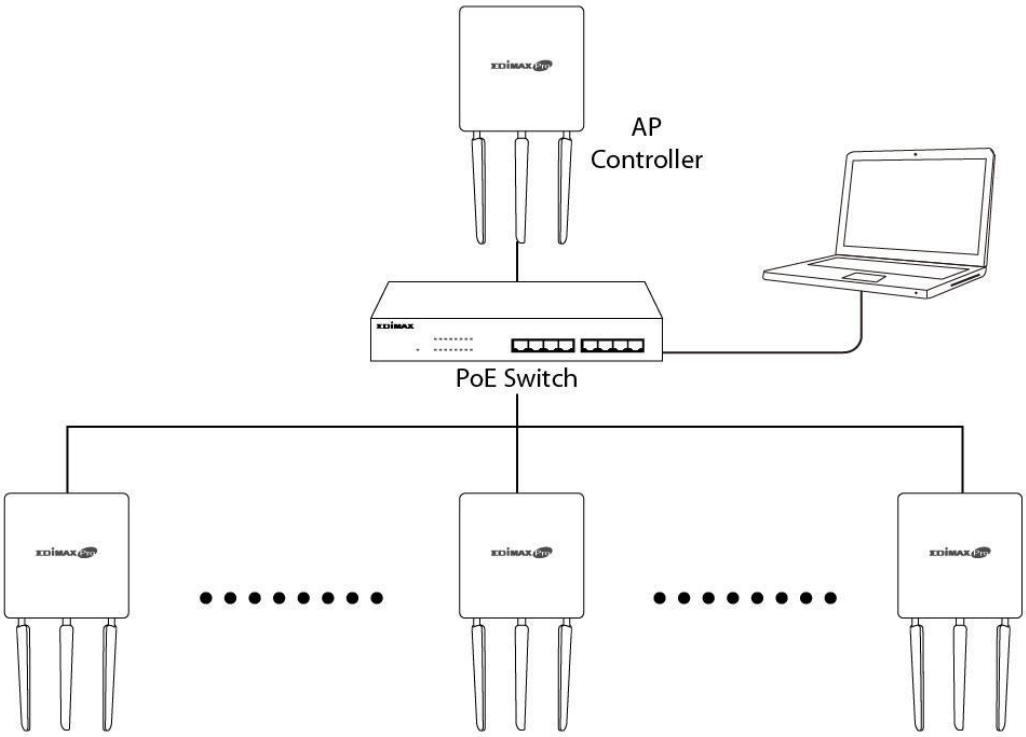

**2.** Ensure all APs are powered on and check LEDs.



**3.** Designate one AP as the AP Controller which will manage all other connected APs (up to 8).




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



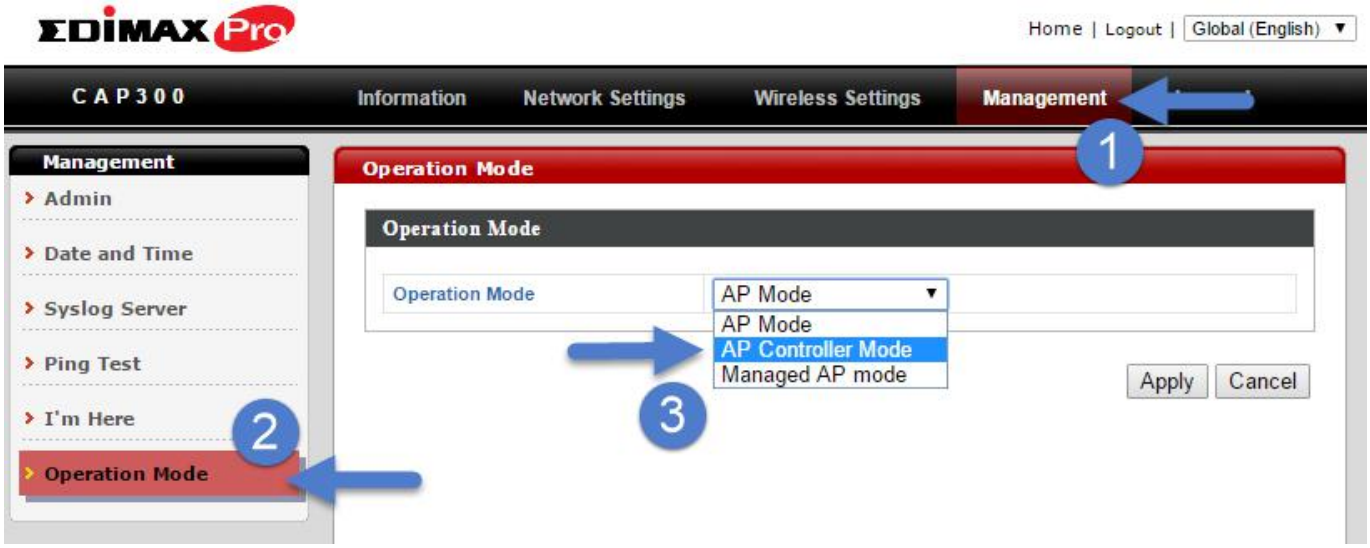
**5.** Open a web browser and enter the AP Controller's IP address in the address field. The default IP address is **192.168.2.2**

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

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

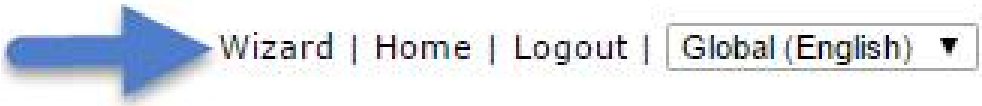
**6.** Enter the username & password to login. The default username & password are **admin** & **1234**.

**7.** You will arrive at the Edimax Pro NMS Dashboard. Go to **"Management"** → **"Operation Mode"** and select **"AP Controller Mode"** from the drop down menu.

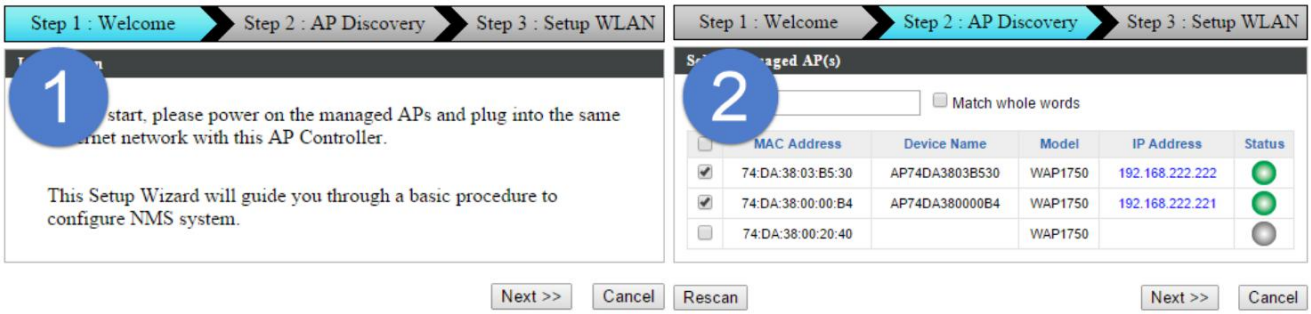


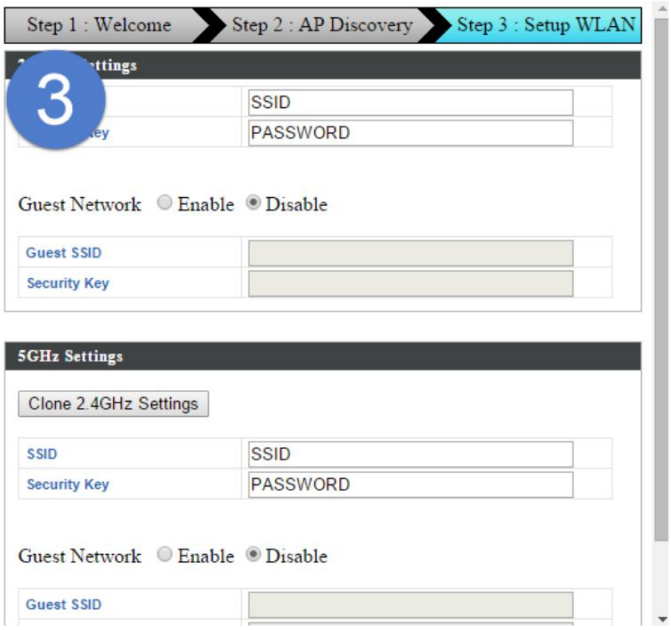

**8.** Click "Apply" to save the settings.

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



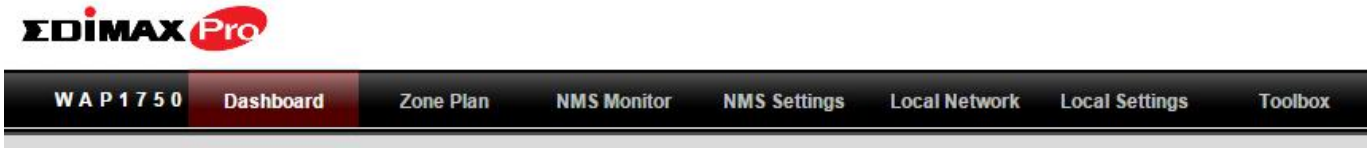

**10.** Follow the instructions on-screen to complete **Steps 1, 2 & 3** and click **"Finish"** to save the settings.




***If any of your Managed APs are not found*** *during Step 2 AP Discovery****, reset the Managed AP to its factory default settings.***

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



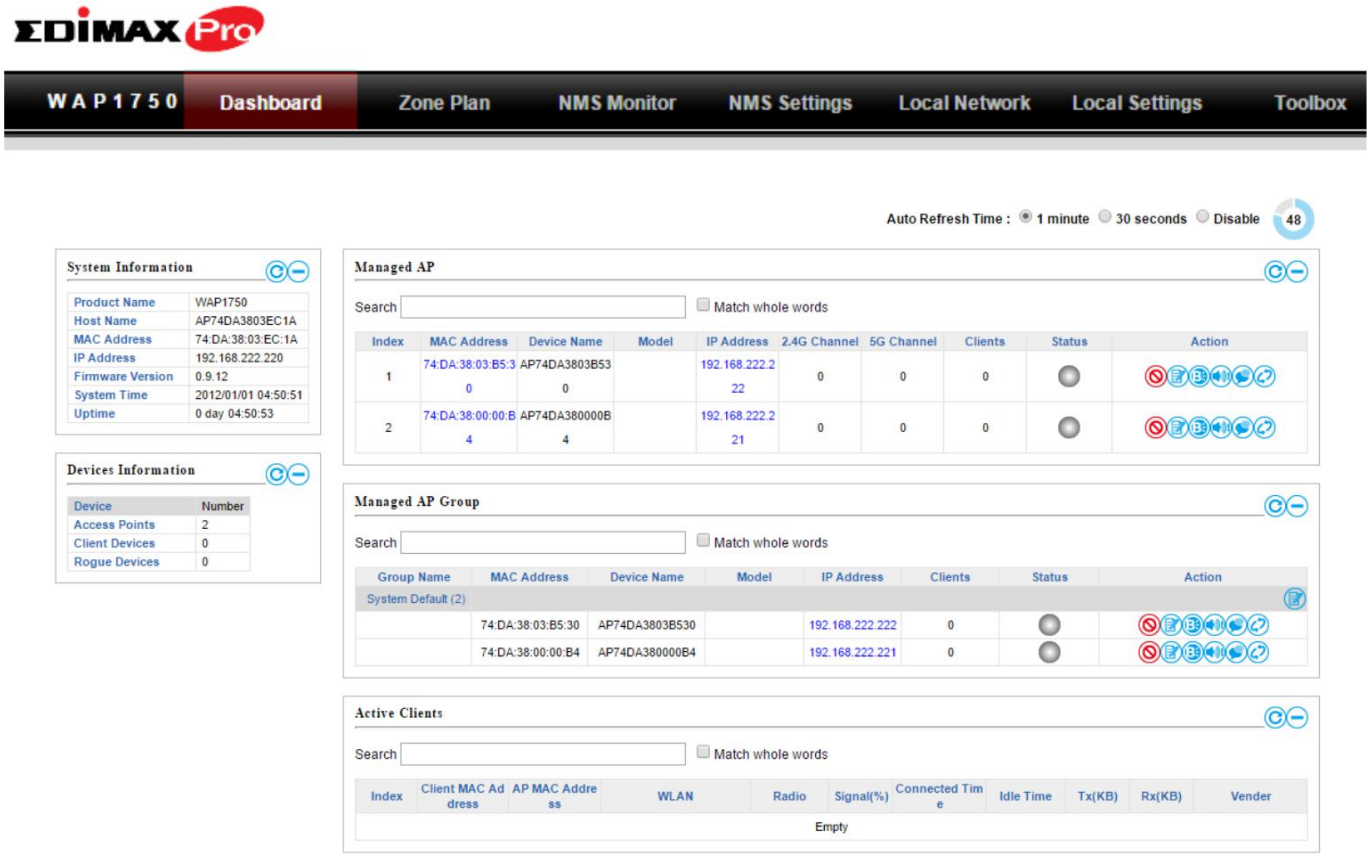

Use ***Dashboard***, ***Zone Plan***, ***NMS Monitor*** & ***NMS Settings*** to configure Managed APs.

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

# III. Software Layout

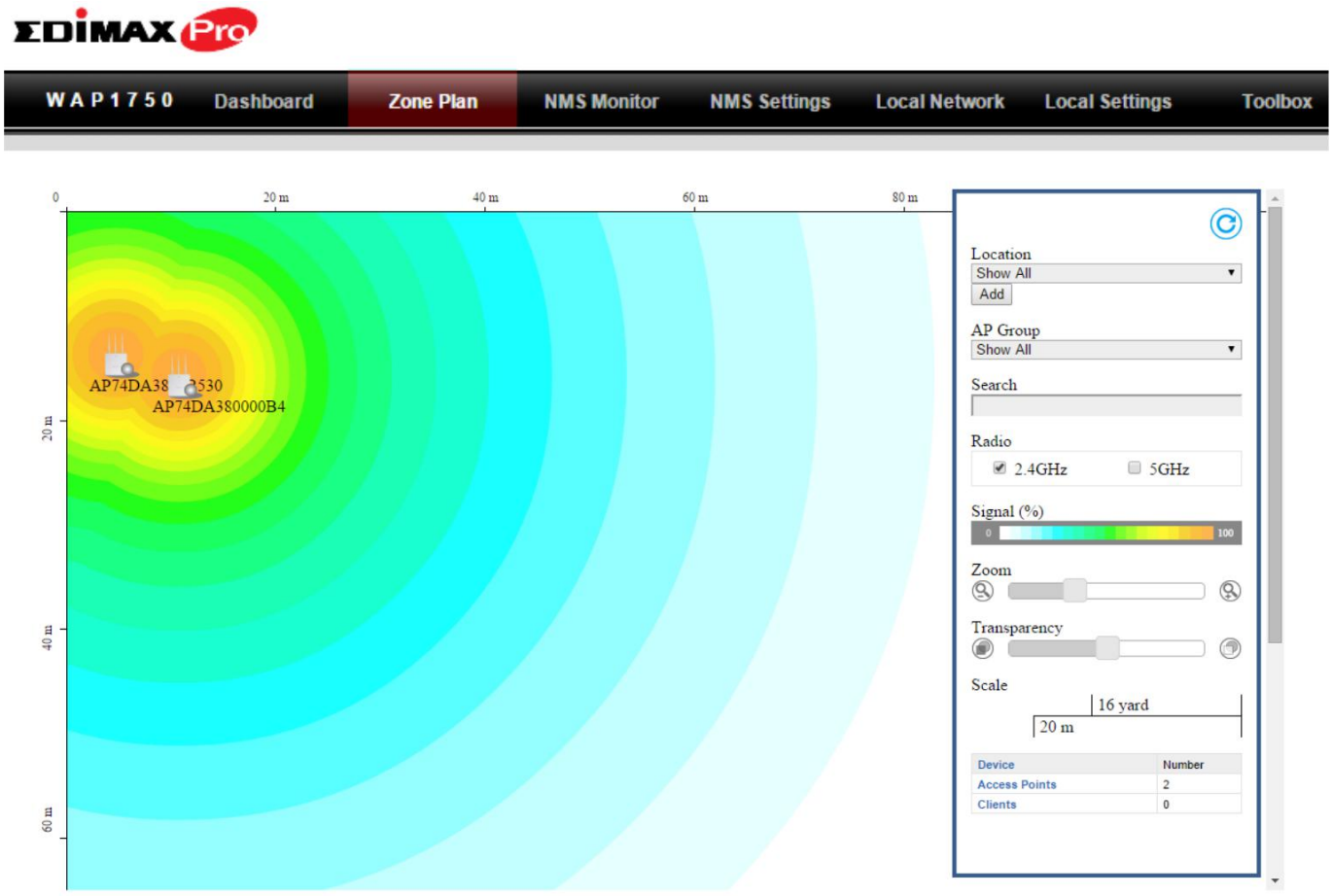
The top menu features 7 panels: *Dashboard, Zone Plan, NMS Monitor, NMS Settings, Local Network, Local Settings & Toolbox.*

## Dashboard



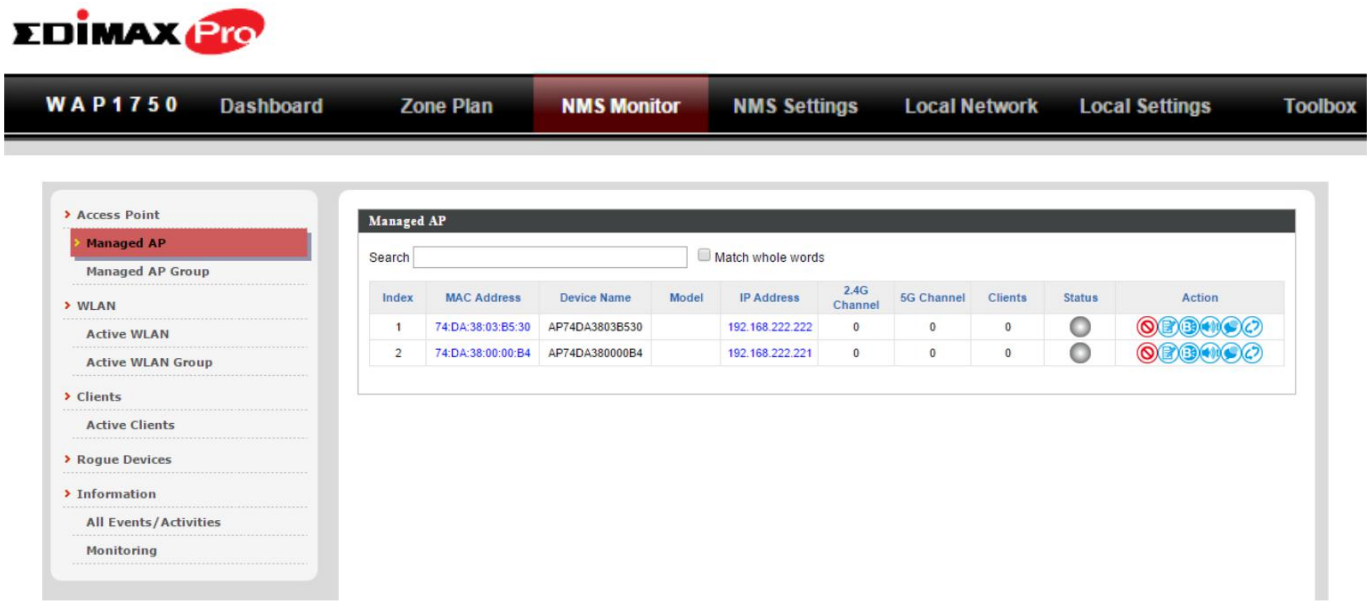

The **Dashboard** panel displays an overview of your network and key system information, with quick links to access configuration options for Managed APs and Managed AP groups. Each panel can be refreshed, collapsed or moved according to your preference.

# Zone Plan



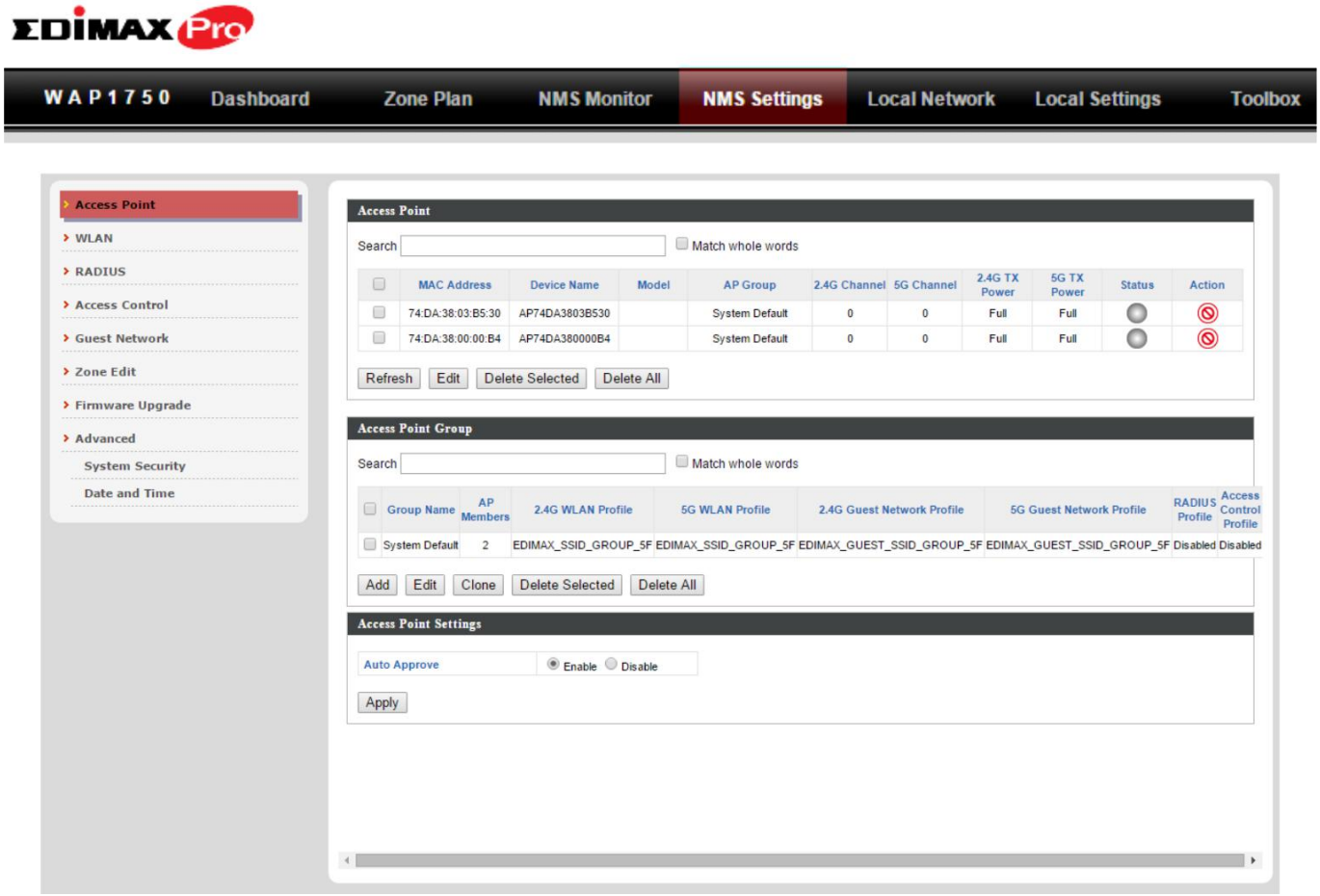

**Zone Plan** displays a customizable live map of Managed APs for a visual representation of your network coverage. Each AP icon can be moved around the map, and a background image can be uploaded for user-defined location profiles using **NMS Settings** → **Zone Edit**. Options can be configured using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

# NMS Monitor



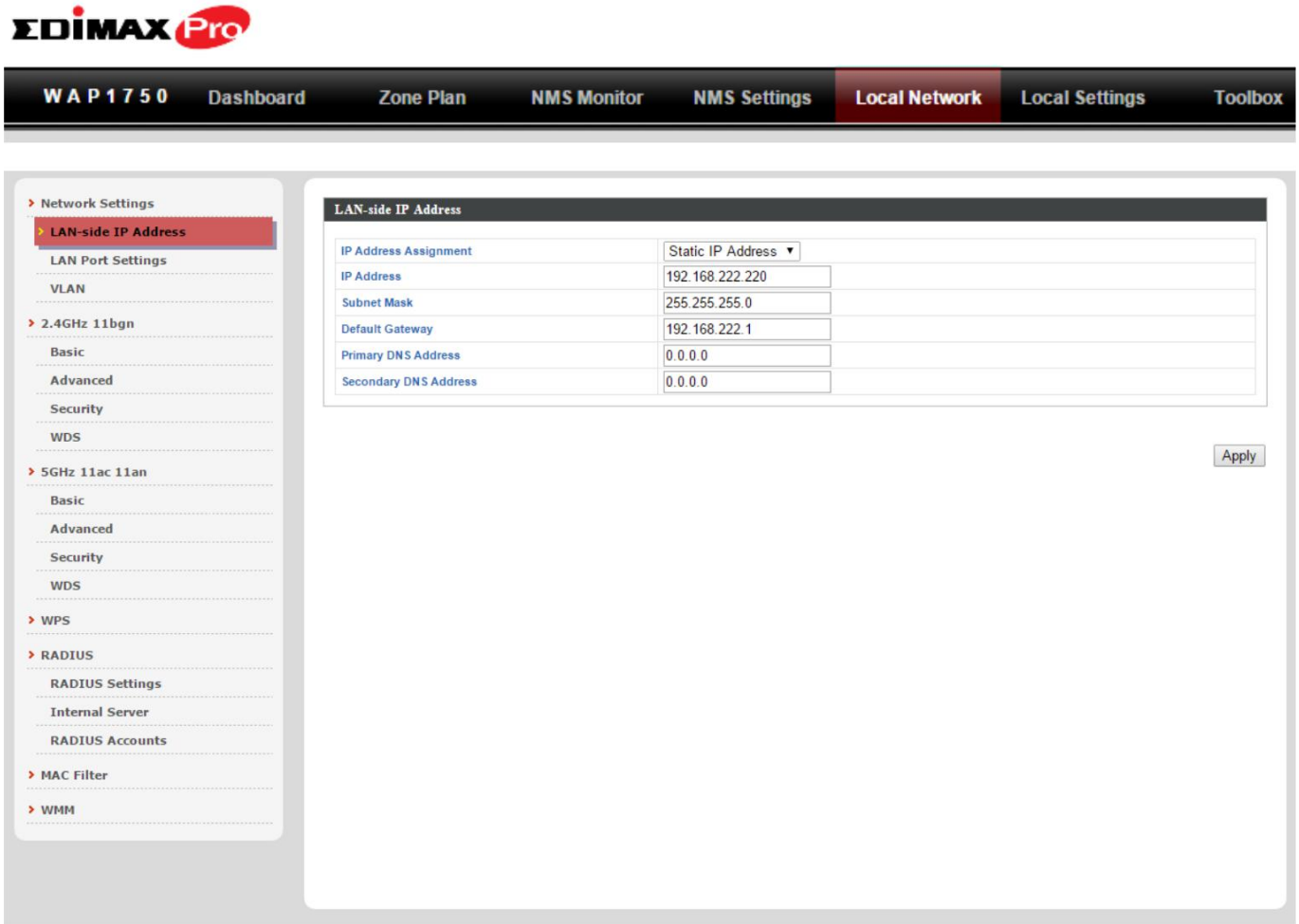

The **NMS Monitor** panel provides more detailed monitoring information about the AP Array than found on the Dashboard, grouped according to categories in the menu down the left side.

# NMS Settings



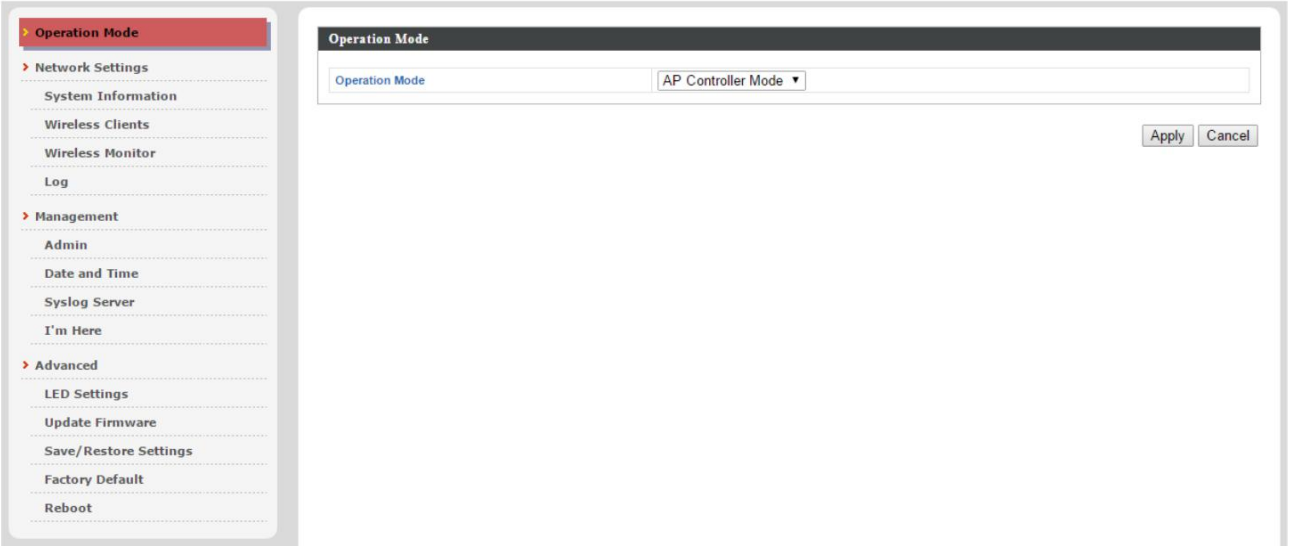

**NMS Settings** provides extensive configuration options for the AP Array. You can manage each access point, assign access points into groups, manage WLAN, RADIUS & guest network settings as well as upgrade firmware across multiple access points. The Zone Plan can also be configured using “Zone Edit”.

# Local Network



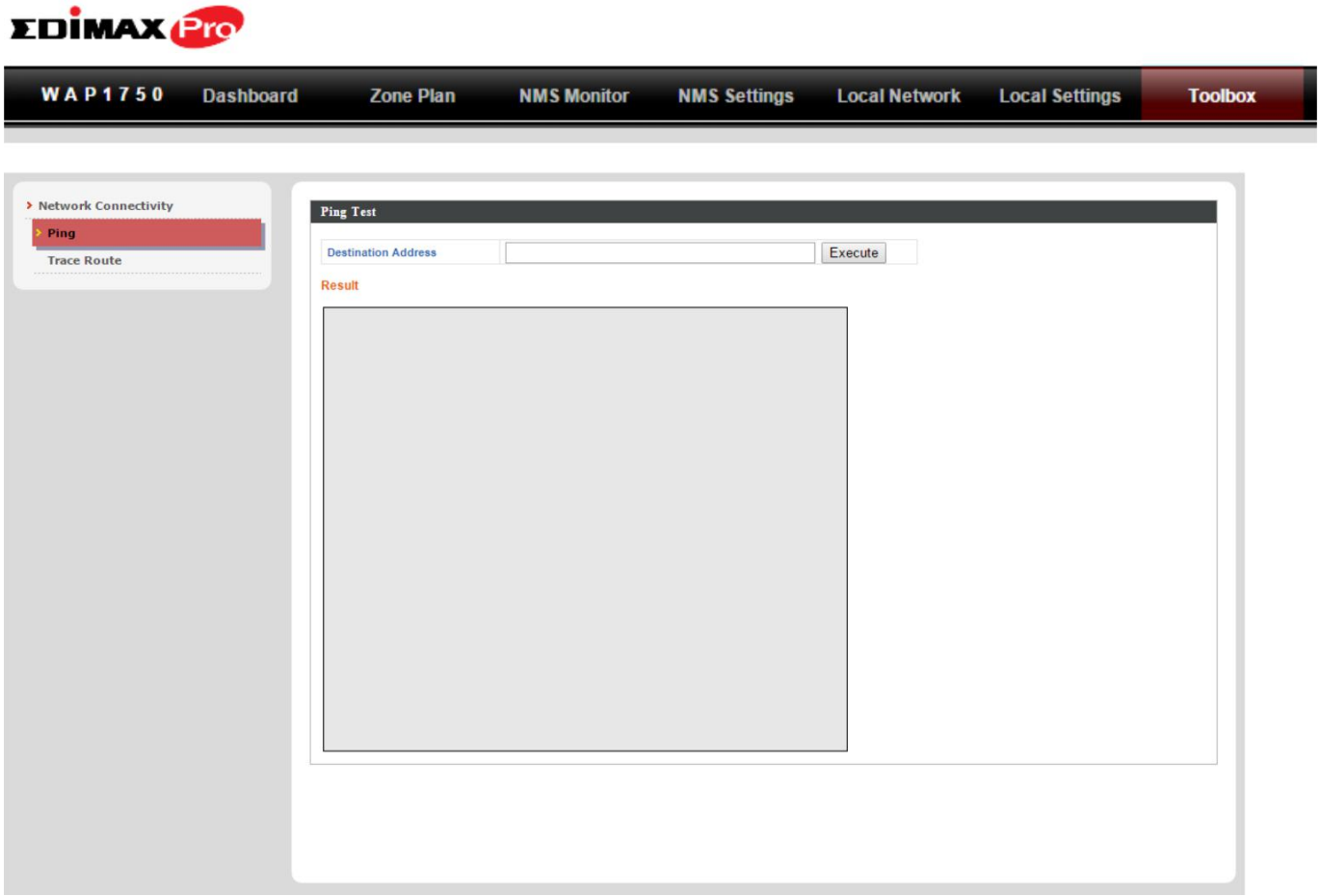

**Local Network** settings are for your AP Controller. You can configure the IP address and DHCP server of the AP Controller in addition to 2.4GHz & 5Ghz Wi-Fi and security, with WPS, RADIUS server, MAC filtering and WMM settings also available.

# 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 *traceroute*.

# 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 Edimax NMS, click "Apply" to save changes:

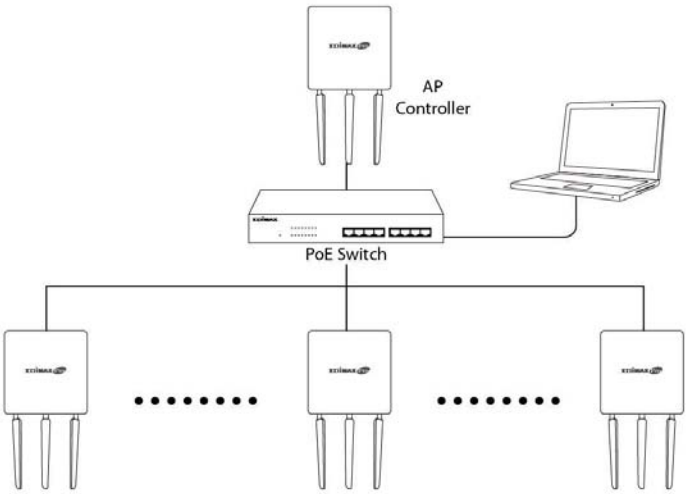
***Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.***

## 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.***

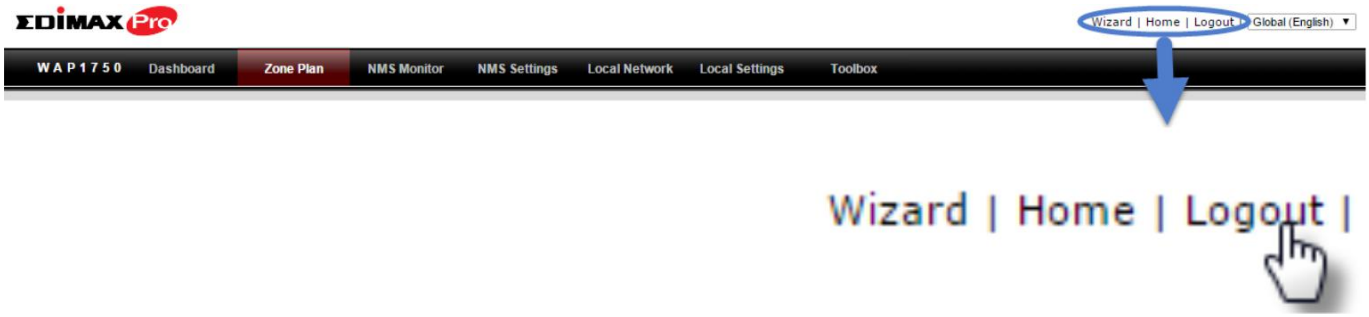
***If you changed the AP Controller's IP address, or if your gateway/router uses a DHCP server, ensure you enter the correct IP address. Refer to your gateway/router's settings.***

***If 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**.

## LOGOUT

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



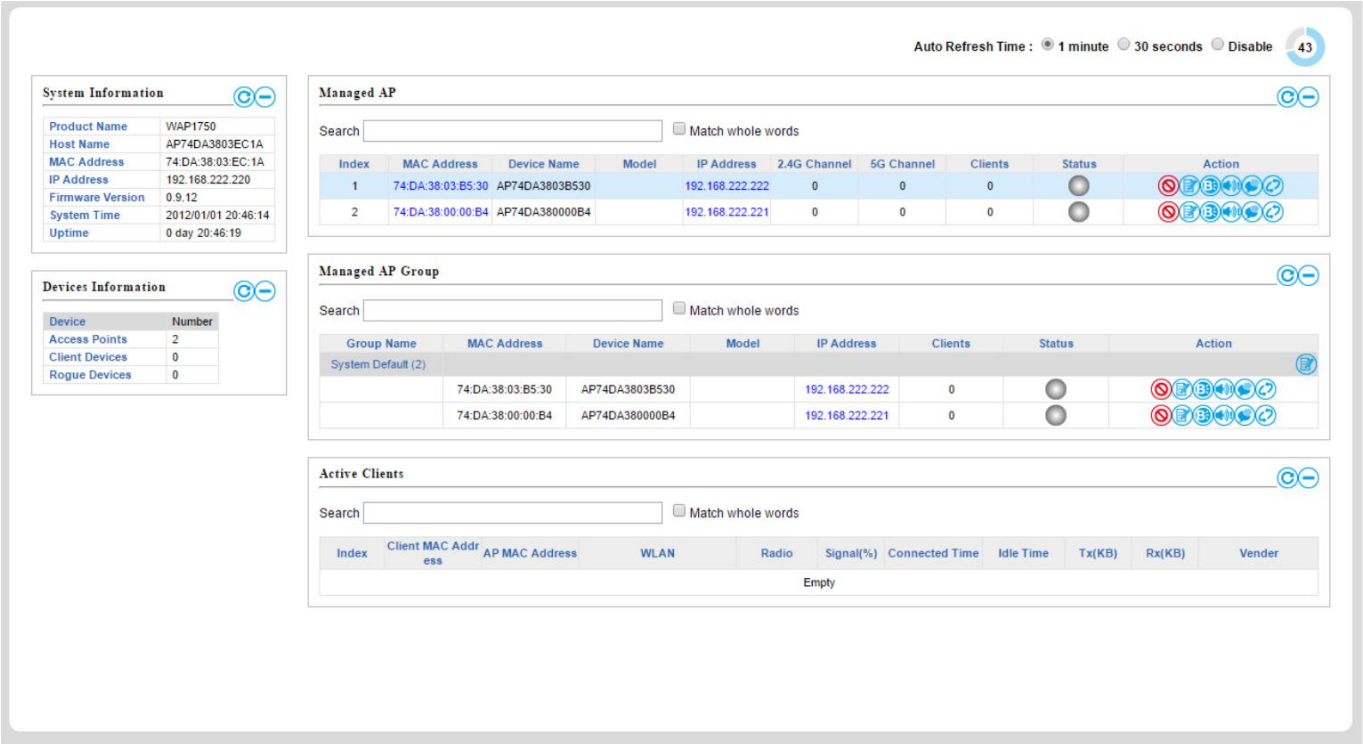

## RESTART

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

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

# 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 | WAP1750 |
| Host Name | AP74DA3803EC1A |
| MAC Address | 74:DA:38:03:EC:1A |
| IP Address | 192.168.222.220 |
| Firmware Version | 0.9.12 |
| System Time | 2012/01/01 20:49:25 |
| Uptime | 0 day 20:49:31 |

## 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).*

| Index | MAC Address | Device Name | Model | IP Address | 2.4G Channel | 5G Channel | Clients | Status | Action |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 74:DA:38:03:B5:30 | AP74DA3803B530 | | 192.168.222.222 | 0 | 0 | 0 | | |
| 2 | 74:DA:38:00:00:B4 | AP74DA380000B4 | | 192.168.222.221 | 0 | 0 | 0 | | |

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: