

APC500

User Manual

08-2021 / v1.1

Edimax Technology Co., Ltd.

No. 278, Xinhua 1st Rd., Neihu Dist., Taipei City, Taiwan

Email: support@edimax.com.tw

Edimax Technology Europe B.V.

Fijenhof 2, 5652 AE Eindhoven, The Netherlands

Email: support@edimax.nl

Edimax Computer Company

530 Technology Drive Suite 100, Irvine, CA 92618, USA

Email: support@edimax.us

CONTENTS

I. Product Information.....	1
I-1. Package Contents	2
I-2. System Requirements.....	3
I-3. Hardware Overview	3
I-4. LED Status	4
I-5. Reset	4
I-6. Console/HyperTerminal.....	5
I-7. Safety Information	6
II. Hardware Installation.....	7
II-1. Wall Mount	7
II-2. Rack Mount.....	8
III. Quick Setup.....	9
IV. Software Layout	16
V. Features.....	23
V-1. LOGIN, LOGOUT & RESTART	23
V-2. DASHBOARD	25
V-2-1. System Information	26
V-2-2. Devices Information.....	26
V-2-3. Managed AP.....	27
V-2-4. Managed AP Group.....	28
V-2-5. Active Clients	29
V-2-6. Active Users	30
V-3. ZONE PLAN.....	31
V-4. NMS MONITOR	33
V-4-1. Access Point	33
V-4-1-1. Managed AP.....	33
V-4-1-2. Managed AP Group.....	35
V-4-2. WLAN	37
V-4-2-1. Active WLAN	37
V-4-2-2. Active WLAN Group	38
V-4-3. Clients	38
V-4-3-1. Active Clients	38
V-4-4. Users	39
V-4-4-1. Active Users	39

V-4-4-2.	Users Log.....	39
V-4-5.	Rogue Devices.....	40
V-4-6.	Information	41
V-4-6-1.	All Events/Activities	41
V-4-6-2.	Monitoring	42
V-5.	NMS Settings.....	43
V-5-1.	Access Point	43
V-5-2.	WLAN	56
V-5-2-1.	No Authentication	58
V-5-2-2.	WEP	58
V-5-2-3.	IEEE802.1x/EAP	59
V-5-2-4.	WPA-PSK	59
V-5-2-5.	WPA-EAP	60
V-5-2-6.	Additional Authentication	60
V-5-3.	RADIUS.....	62
V-5-4.	Access Control	68
V-5-5.	Guest Network.....	71
V-5-6.	Users	75
V-5-7.	Guest Portal	78
V-5-7-1.	Add/Edit Guest Portal	79
V-5-7-1-1.	Front Desk URL	80
V-5-7-1-2.	Front Desk Printout	82
V-5-7-1-3.	Guest Portal Type	83
V-5-7-1-4.	Guest Portal Customization.....	84
V-5-8.	Zone Edit	85
V-5-9.	Schedule.....	87
V-5-10.	Device Monitoring	89
V-5-11.	Firmware Upgrade	90
V-5-12.	Advanced	91
V-5-12-1.	System Security.....	91
V-5-12-2.	Date & Time	91
V-6.	Local Network.....	93
V-6-1.	Network Settings	93
V-6-1-1.	LAN-Side IP Address.....	93
V-6-1-2.	LAN Port Settings	96
V-6-1-3.	VLAN	97
V-7.	Local Settings	98
V-7-1.	System Settings.....	98
V-7-1-1.	System Information	98
V-7-1-2.	Log.....	100
V-7-2.	Management	101

V-7-2-1.	Admin.....	101
V-7-2-2.	Date and Time.....	103
V-7-2-3.	Syslog Server	105
V-7-2-4.	I'm Here	106
V-7-3.	Advanced	107
V-7-3-1.	LED Settings	107
V-7-3-2.	Update Firmware	107
V-7-3-3.	Save/Restore Settings.....	109
V-7-3-4.	Factory Default	110
V-7-3-5.	Reboot	110
V-8.	Toolbox	111
V-8-1.	Network Connectivity	111
V-8-1-1.	Ping	111
V-8-1-2.	Trace Route.....	111

VI. Appendix112

VI-1.	Configuring your IP address.....	112
VI-1-1.	Windows XP	113
VI-1-2.	Windows Vista	115
VI-1-3.	Windows 7	117
VI-1-4.	Windows 8	121
VI-1-5.	Mac	125

VII. Best Practice127

VII-1.	How to Create and Link WLAN & Access Point Groups.....	127
--------	--	-----

Federal Communication Commission Interference Statement ..錯誤! 尚未定

義書籤。

I. Product Information

The APC500 supports central management for up to 200 Edimax Pro access points, **suitable for SMBs/SMEs**. Functions include:

<i>L2/L3 AP Management</i>	<i>Captive Portal/Guest Policy</i>
<i>QoS by SSID</i>	<i>Local Radius (AAA)</i>
<i>Batch Setup/Configuration</i>	<i>Group Firmware Upgrade/Restart</i>
<i>Channel/RF Power/Load Optimization</i>	<i>Edimax NMS</i>

Edimax Pro Network Management Suite (NMS) supports the central management of a group of access points, otherwise known as an AP Array. NMS can be installed on one access point and support up to 16 Edimax Pro access points with no additional wireless controller required. The APC500 is a standalone AP Controller with support for up to 200 Edimax Pro APs.

Edimax Pro NMS	CAP Series	WAP Series	APC500
<i>Platform</i>	Software	Software	Standalone Box
<i>Segment</i>	Entry	Middle	High
<i>Managed AP Capacity</i>	1 – 8	1 – 16	1 - 200

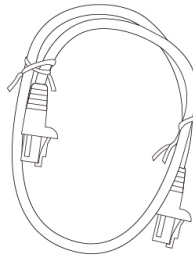
The APC500 Controller connects to a network via a switch or directly to a router, and other connected Edimax Pro access points are automatically designated as Managed APs. Using the APC500 you can configure, monitor and manage all Managed APs (up to 200 connected by switches) from the single AP Controller.

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.

I-1. Package Contents



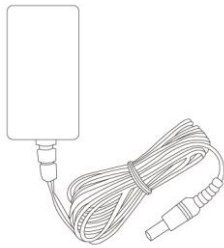
1



2



3



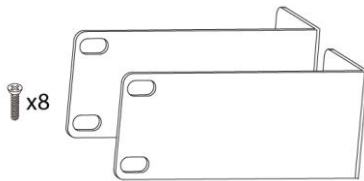
4



5



6



7



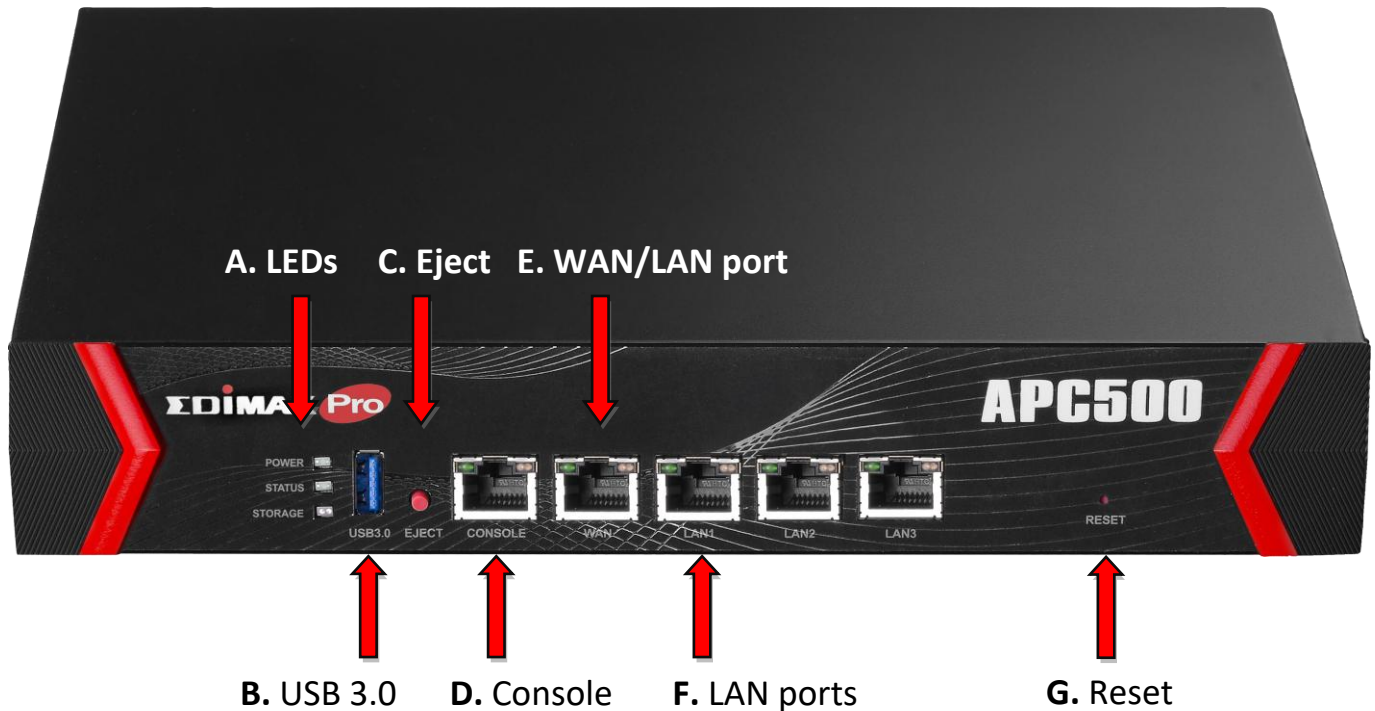
8

- | | |
|-------------------|-----------------------------|
| 1. APC500 | 5. CD |
| 2. Ethernet Cable | 6. Quick Installation Guide |
| 3. Console Cable | 7. Rack-Mount Kit |
| 4. Power Adapter | 8. Wall-Mount Kit |

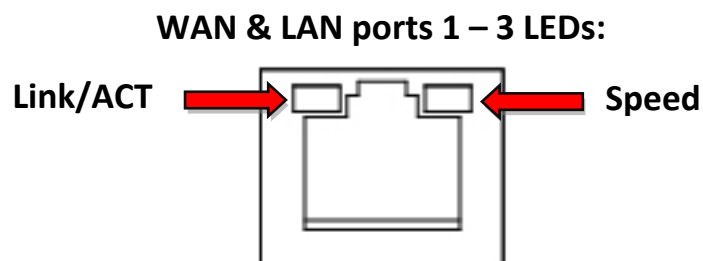
I-2. System Requirements

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

I-3. Hardware Overview



- A.** Power, status & storage LEDs.
- B.** USB 3.0 port for system log and save/restore settings.
- C.** Eject an attached USB device.
- D.** Connect a management console.
- E.** WAN/LAN port 0.
- F.** LAN ports 1 – 3.
- G.** Reset the controller to factory default settings.



I-4. LED Status

LED	LED Color	LED Status	Description
Power	Blue	On	The controller is on.
		Flashing	The controller is starting up.
		Off	The controller is off.
Status	Blue	On	The controller is working properly.
		Flashing	Transferring/receiving data.
		Off	The controller is offline.
Storage	Blue	On	USB storage attached.
		Flashing	USB activity.
		Off	No USB storage attached.
Link/ACT	Green	On	Active link.
		Flashing	Network activity.
		Off	Inactive link.
Speed	Green	On	1000 Mbps
		Off	10/100 Mbps

I-5. Reset

If you experience problems with your controller, 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 front of the controller 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 controller to restart. The controller is ready for setup when the **blue** power LED is **on**.

I-6. Console/HyperTerminal

The controller can be configured via the “Console” port located on the access point’s side panel using a terminal or a PC-based terminal-emulation program (e.g. HyperTerminal).

Use a DB9 straight cable to connect the Console (RS-232 serial port) of the APC500 and the RS-232 serial port of a terminal or PC.

Use the following configuration settings for terminal-emulation programs:

Baud Rate	115200
Data	8 bit
Parity	None
Stop	1 bit
Flow Control	None



The console cable pin definition is compatible with Cisco console cables.

I-7. 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 controller is designed for indoor use only; do not place the controller outdoors.
2. Do not place the controller 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 controller.
4. Handle the controller with care. Accidental damage will void the warranty of the controller.
5. The device contains small parts which are a danger to small children under 3 years old. Please keep the controller out of reach of children.
6. Do not place the controller on paper, cloth, or other flammable materials. The controller may become hot during use.
7. There are no user-serviceable parts inside the controller. If you experience problems with the controller, please contact your dealer of purchase and ask for help.
8. The controller 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 controller or power adapter, then disconnect the controller and power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

II. Hardware Installation

II-1. Wall Mount

The APC500 includes screws to mount your controller to a wall.

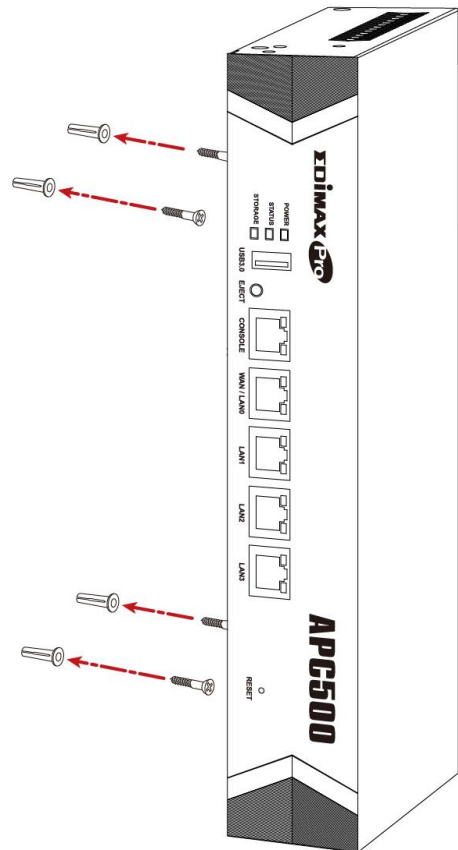


Remove the rubber feet from the underside of the APC500 by pulling gently before using the wall mount.

1. Identify and mark correct screw positions on your selected wall.
2. Attach the APC500 to your wall using the included screws, as shown in the diagram.
3. Ensure the APC500 is fixed to the wall firmly and oriented correctly, with the controller's Edimax logo as shown in the diagram.



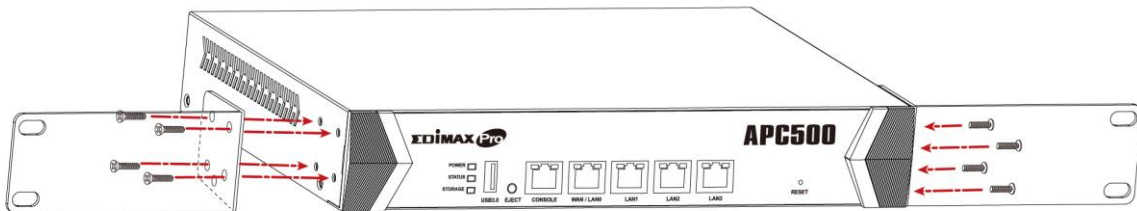
Ensure your controller is securely attached to the wall.



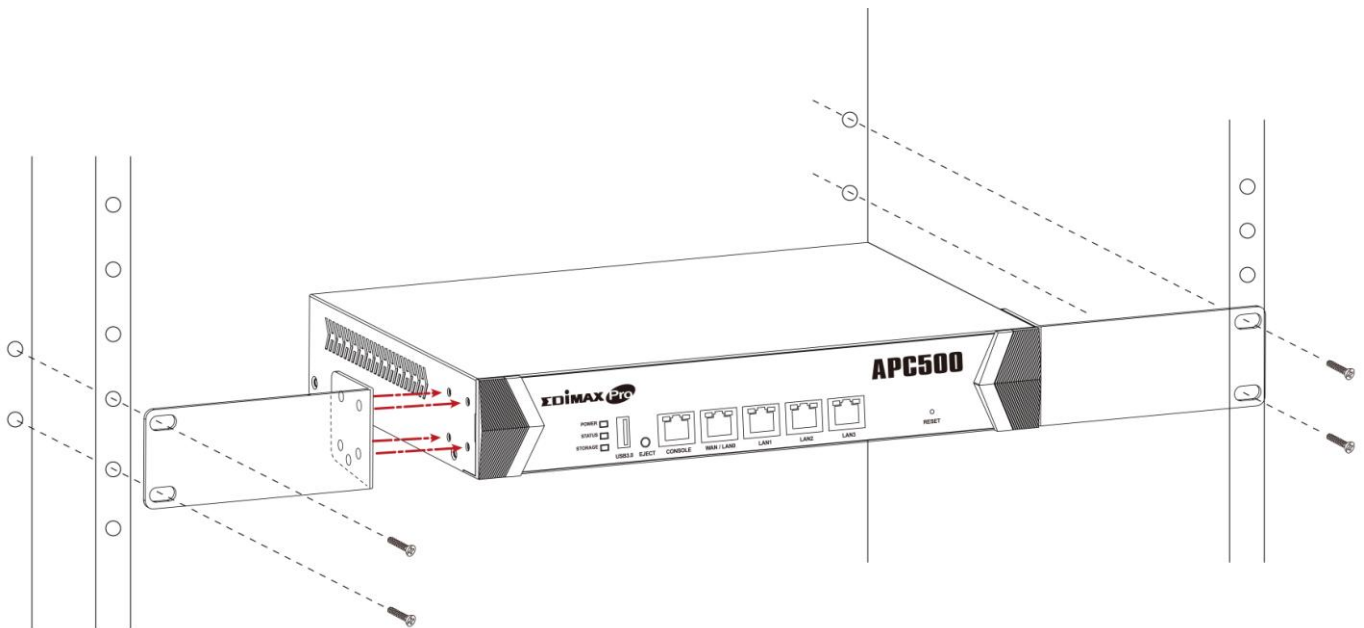
II-2. Rack Mount

The controller can be mounted in a rack which can be placed in a wiring closet with other equipment. To install the switch, please follow these steps:

1. Attach the mounting brackets on the controller's side panels (one on each side) and secure them with the screws provided.



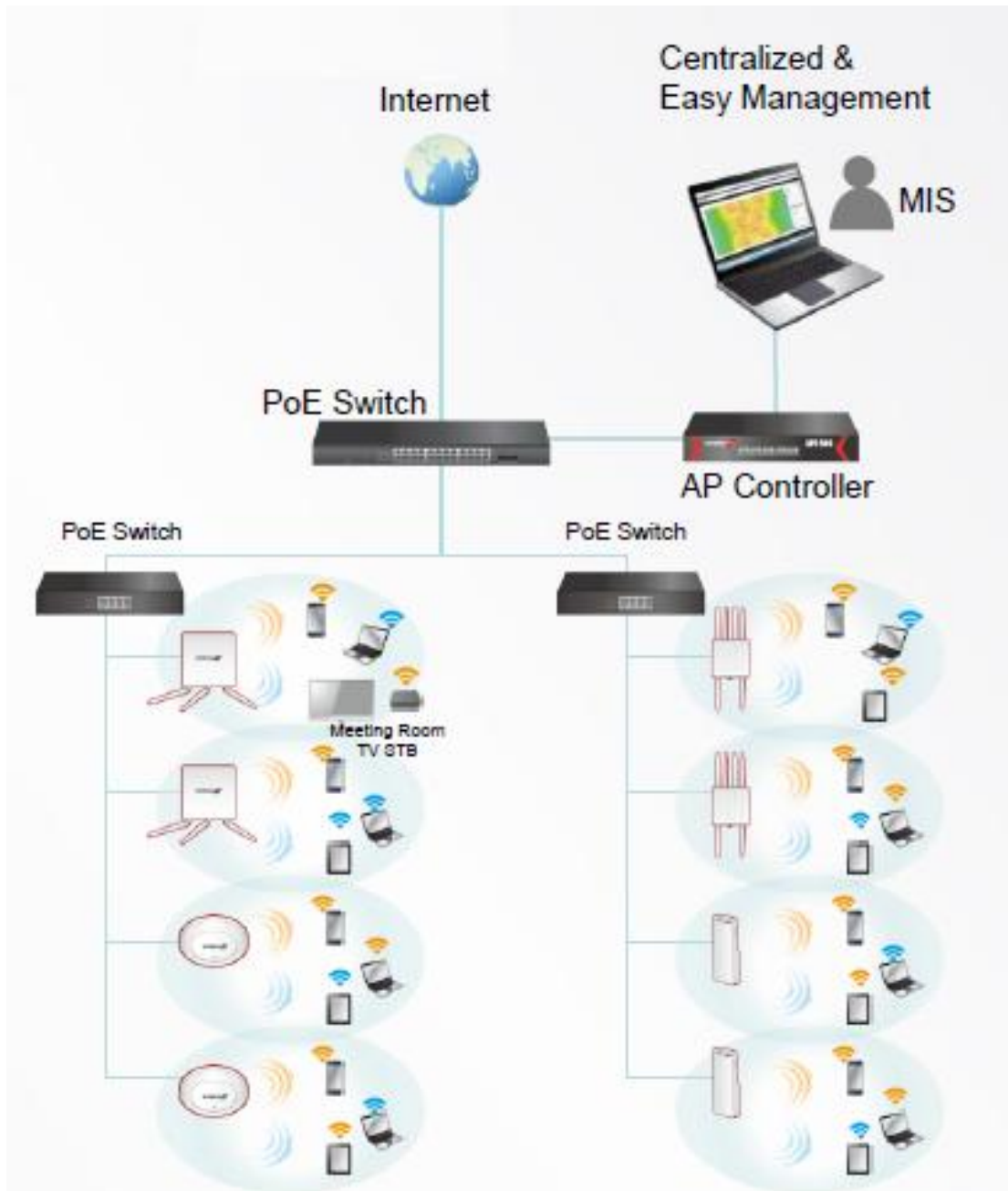
2. Use the screws provided with your equipment rack to mount the controller on the rack and tighten it.



III. Quick Setup

The APC500 supports central management for up to 200 Edimax Pro access points including both indoor and outdoor APs, reducing costs and facilitating efficient remote AP management.

APC500 is simple to setup. An overview of a recommended network is shown below:



The APC500 Controller connects to a network via a switch or directly to a router, and other connected Edimax Pro access points are automatically designated as Managed APs. Using the APC500 you can configure, monitor and manage all Managed APs (up to 200 connected by switches) from the single AP Controller.

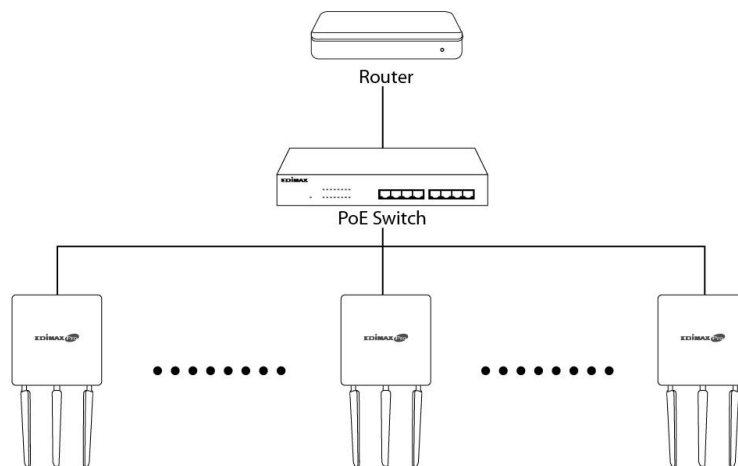


Ensure you have the latest firmware from the Edimax website for your Edimax Pro products.

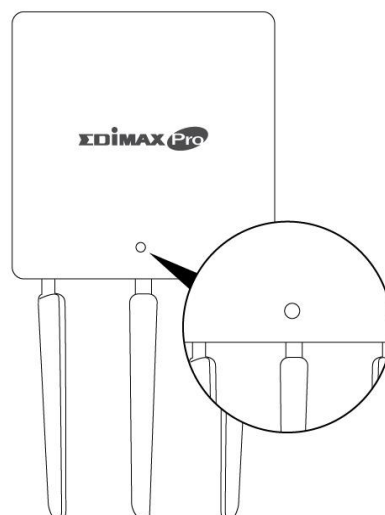
- 1.** Connect all APs to a PoE switch which is connected to a gateway/router.



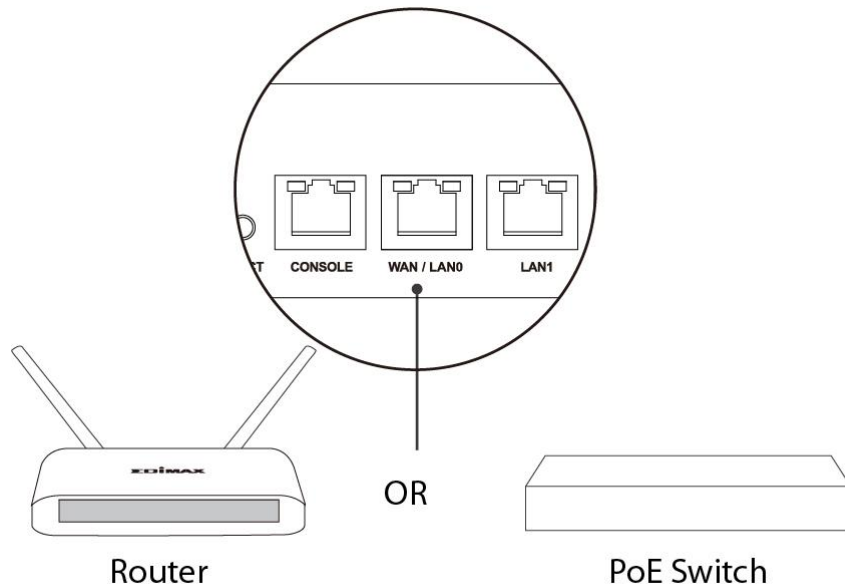
You can use your router as a DHCP server or you can later configure your AP Controller as a DHCP server.



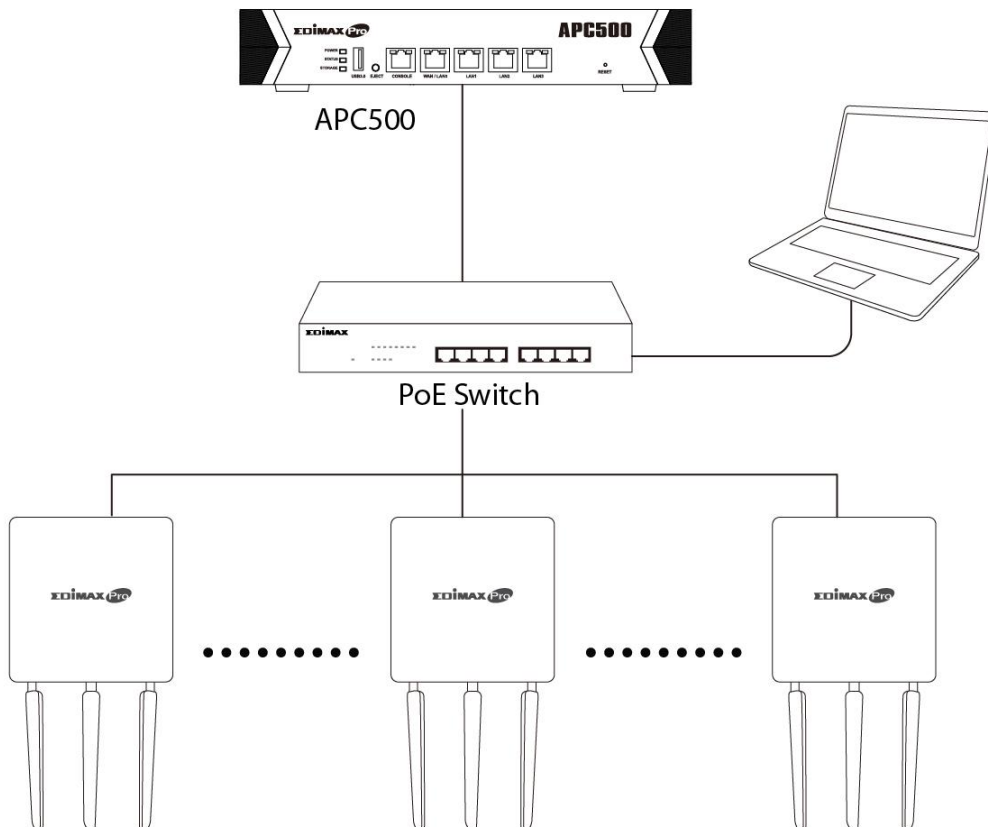
- 2.** Ensure all APs are powered on and check LEDs.



3. Connect the APC500 to the PoE switch (LAN port) or gateway/router (WAN port) and connect the power supply.



4. Connect a computer to the APC500 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 **192.168.2.1**



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.



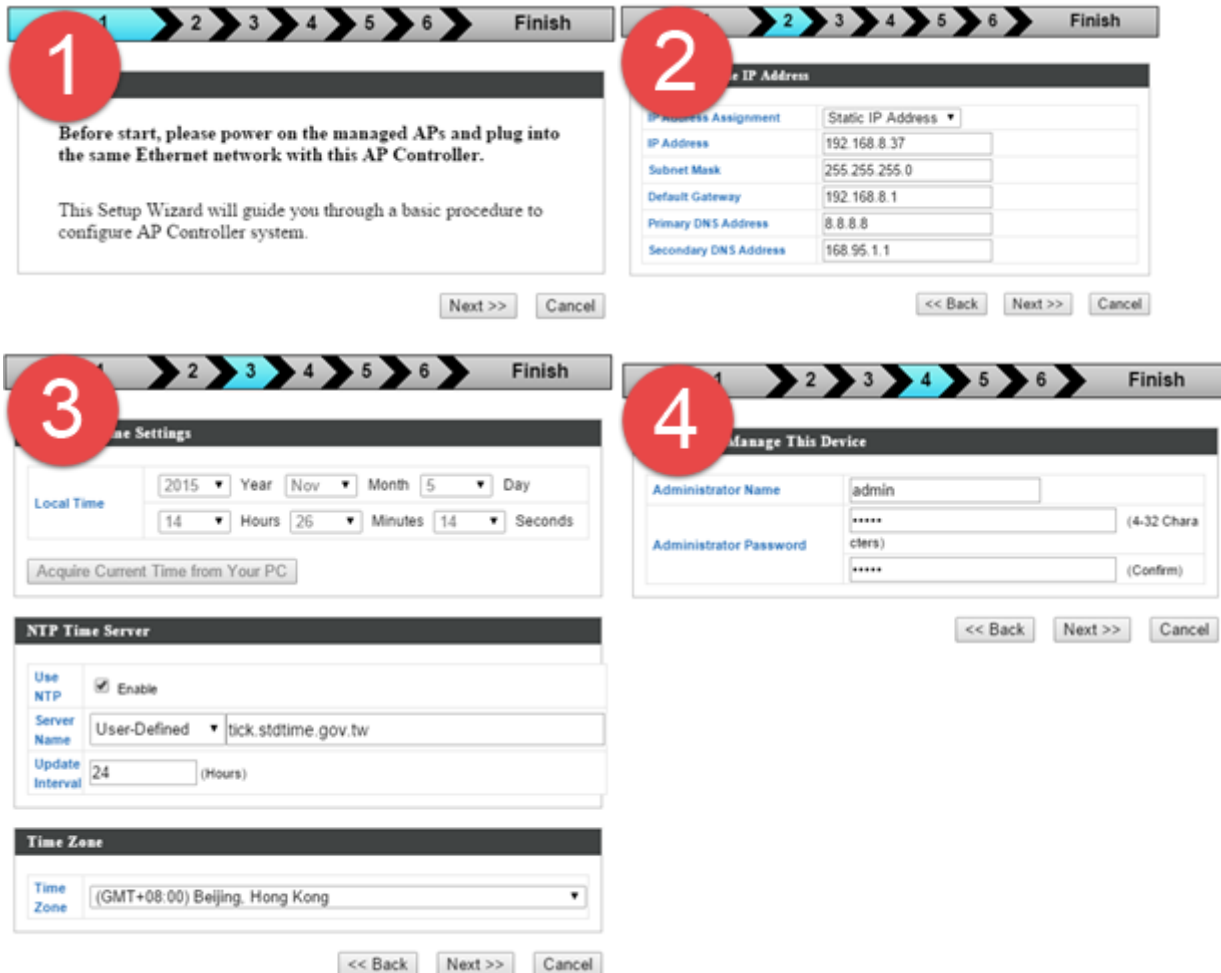
If you changed the AP Controller's IP address, or if your gateway/router uses a DHCP server, ensure you enter the correct IP address. Refer to your gateway/router's settings.

6. Enter the username & password to login. The default username & password are **admin & 1234**.
7. You will arrive at the APC500 Dashboard. APC500 includes a wizard to quickly setup the LAN IP address, admin login & time/date settings for the APC500, as well as SSID & security for Managed APs. Click "Wizard" in the top right corner to begin.



Wizard | Home | Logout | Global (English) ▼

8. Follow the instructions on-screen to complete **Steps 1 - 7** and click **“Finish”** to save the settings. The wizard will help you set up LAN IP address, 2.4GHz & 5GHz SSID and security, administrator name & password, time & date settings and Managed APs.



The image displays four sequential screenshots of the EDIMAX Pro Setup Wizard, each with a red circle and a number indicating the step.

Step 1: The first screen shows a progress bar at the top with steps 1 through 6, and a 'Finish' button. The main text reads: "Before start, please power on the managed APs and plug into the same Ethernet network with this AP Controller. This Setup Wizard will guide you through a basic procedure to configure AP Controller system." At the bottom are 'Next >>' and 'Cancel' buttons.

Step 2: The second screen is titled 'Set IP Address'. It features a progress bar with step 2 highlighted. The main content includes a dropdown for 'IP Address Assignment' set to 'Static IP Address', and input fields for 'IP Address' (192.168.8.37), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.8.1), 'Primary DNS Address' (8.8.8.8), and 'Secondary DNS Address' (168.95.1.1). At the bottom are '<< Back', 'Next >>', and 'Cancel' buttons.

Step 3: The third screen is titled 'Time Settings'. It features a progress bar with step 3 highlighted. The main content includes a 'Local Time' section with dropdowns for Year (2015), Month (Nov), Day (5), Hours (14), Minutes (26), and Seconds (14), and a button 'Acquire Current Time from Your PC'. Below this is the 'NTP Time Server' section with 'Use NTP' checked, 'Server Name' set to 'User-Defined' and 'tick.stdtime.gov.tw', and 'Update Interval' set to 24 (Hours). At the bottom are '<< Back', 'Next >>', and 'Cancel' buttons.

Step 4: The fourth screen is titled 'Manage This Device'. It features a progress bar with step 4 highlighted. The main content includes input fields for 'Administrator Name' (admin), 'Administrator Password' (masked with asterisks), and a confirmation field. At the bottom are '<< Back', 'Next >>', and 'Cancel' buttons.

Step 1 > **2** > **3** > **4** > **5** > **6** > **Finish**

5

Search ☐ Match whole words

MAC Address	Device Name	Model	IP Address	Status
☒ 74-DA-38-3E-79-10	AP74DA383E7910	CAP1200	192.168.8.102	☐
☒ 74-DA-38-3E-78-C0	AP74DA383E78C0	CAP1200	192.168.8.100	☐
☐ 74-DA-38-40-E0-E4		CAP1200		☐
☐ 74-DA-38-30-71-D8		CAP300		☐
☐ 74-DA-38-3E-7B-E6		CAP1200		☐
☐ 74-DA-38-06-E1-AA		WAP1750		☐
☐ 80-1F-02-F1-95-D2		WAP1200		☐

Managed AP(s)

Search ☐ Match whole words

MAC Address	Device Name	Model	IP Address	Status
74-DA-38-1E-54-30		CAP1200		☐
74-DA-38-1E-54-3E		CAP1200		☐
74-DA-38-64-CD-32		CAP1200		☐

Rescan << Back Next >> Cancel

Step 1 > **2** > **3** > **4** > **5** > **6** > **Finish**

6

2.4GHz Settings

SSID

Security Key

Guest Network: ☒ Enable ☐ Disable

Guest SSID

Security Key

5GHz Settings

Clone 2.4GHz Settings

SSID

Security Key

Guest Network: ☒ Enable ☐ Disable

Guest SSID

Security Key

<< Back Next >> Cancel

Step 1 > **2** > **3** > **4** > **5** > **6** > **Finish**

7

Configuration

Management IP

IP Address Assignment

IP Address

Date and Time

Local Time

Time Zone

Administrator Account

Administrator Name

Managed AP(s)

MAC Address	Device Name	Model	IP Address	Status
74-DA-38-27-1B-54	AP74DA38271B54	CAP1200	192.168.2.124	☒
74-DA-38-03-23-9C	AP74DA3803239C	WAP1750	192.168.2.102	☒

2.4GHz Settings

SSID

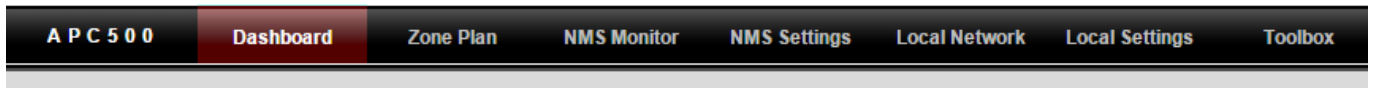
Security Key

Guest Network



If any of your Managed APs are not found during Step 5 Select Free APs, reset the Managed AP to its factory default settings. Refer to the AP's user manual for help.

9. Your APC500 Controller & Managed APs should be fully functional with all of the basic settings configured. Use the top menu to navigate around Edimax Pro NMS (Network Management Suite) settings.



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

Use *Local Network & Local Settings* to configure your APC500.

IV. Software Layout

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

Dashboard



A P C 5 0 0
Dashboard
Zone Plan
NMS Monitor
NMS Settings
Local Network
Local Settings
Toolbox

Auto Refresh Time 1 minute 30 seconds Disable 53

System Information

Product Name	APC500
Host Name	AP00AA8BCCDD10
MAC Address	00-AA-BB-CC-DD-10
IP Address	192.168.2.1
Firmware Version	1.3.1
System Time	2015/11/06 15:23:51
Uptime	0 day 03:18:56
CPU Usage	3%
Memory Usage	9%

Managed AP

Search ☐ Match whole words

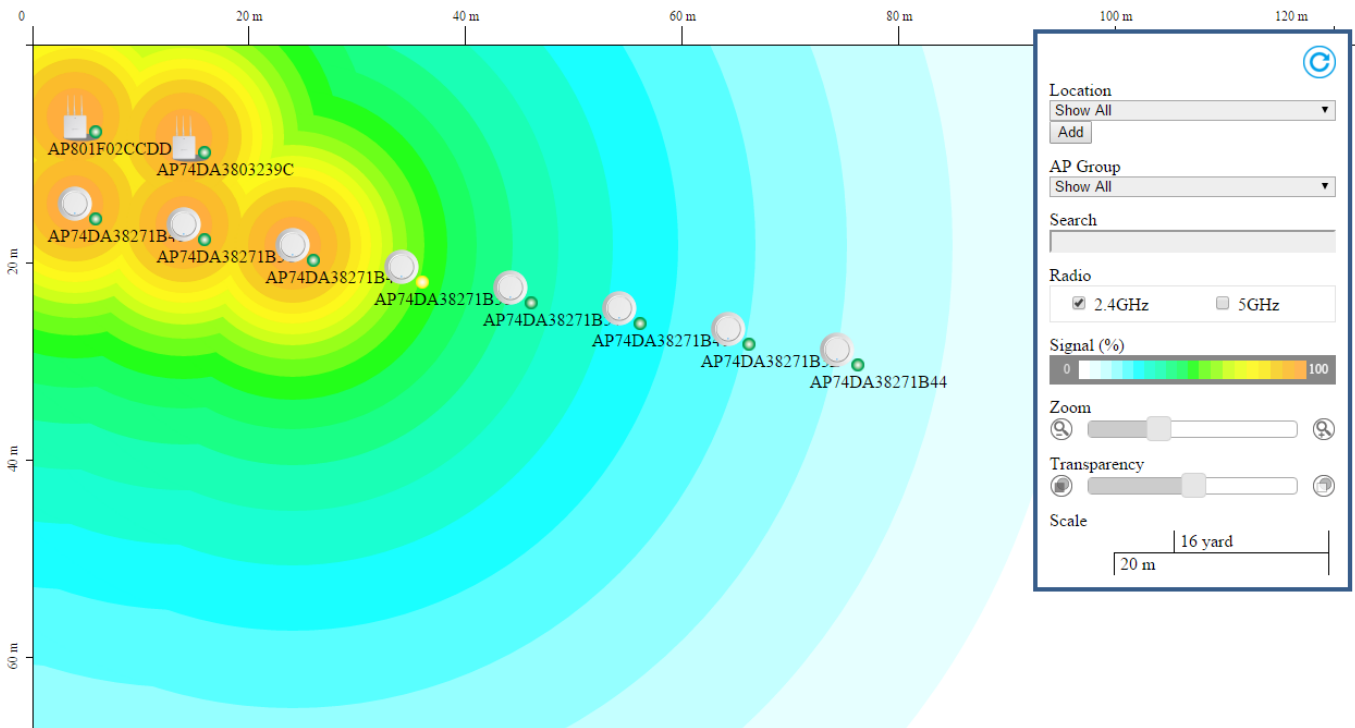
Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74-DA-38-27-1B-54	AP74DA38271B54	CAP1200	192.168.2.124	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
2	74-DA-38-03-23-9C	AP74DA3803239C	WAP1750	192.168.2.102	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
3	74-DA-38-27-1B-48	AP74DA38271B48	CAP1200	192.168.2.120	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
4	74-DA-38-27-1B-38	AP74DA38271B38	CAP1200	192.168.2.118	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
5	74-DA-38-27-1B-3C	AP74DA38271B3C	CAP1200	192.168.2.110	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
6	80-1F-02-CC-DD-10	AP801F02CCDD10	WAP1750	192.168.2.105	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
7	74-DA-38-27-1B-46	AP74DA38271B46	CAP1200	192.168.2.121	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
8	74-DA-38-27-1B-40	AP74DA38271B40	CAP1200	192.168.2.126	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
9	74-DA-38-27-1B-44	AP74DA38271B44	CAP1200	192.168.2.127	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞
10	74-DA-38-27-1B-3E	AP74DA38271B3E	CAP1200	192.168.2.128	11	36	0	●	⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞ ⊞

Devices Information

Device	Number
Access Points	10
Client Devices	0
Rogue Devices	0

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



Access Point

Managed AP

Managed AP Group

WLAN

Active WLAN

Active WLAN Group

Clients

Active Clients

Users

Active Users

Users Log

Rogue Devices

Information

All Events/Activities

Monitoring

Managed AP

Search ☐ Match whole words

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74 DA:38 27:1B 54	AP74DA38271B54	CAP1200	192.168.2.124	11	36	0		
2	74 DA:38 03:23 9C	AP74DA3803239C	WAP1750	192.168.2.102	11	36	0		
3	74 DA:38 27:1B 48	AP74DA38271B48	CAP1200	192.168.2.120	11	36	0		
4	74 DA:38 27:1B 38	AP74DA38271B38	CAP1200	192.168.2.118	11	36	0		
5	74 DA:38 27:1B 3C	AP74DA38271B3C	CAP1200	192.168.2.110	11	36	0		
6	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	192.168.2.105	11	36	0		
7	74 DA:38 27:1B 46	AP74DA38271B46	CAP1200	192.168.2.121	11	36	0		
8	74 DA:38 27:1B 40	AP74DA38271B40	CAP1200	192.168.2.126	11	36	0		
9	74 DA:38 27:1B 44	AP74DA38271B44	CAP1200	192.168.2.127	11	36	0		
10	74 DA:38 27:1B 3E	AP74DA38271B3E	CAP1200	192.168.2.128	11	36	0		

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



Access Point

WLAN

RADIUS

Access Control

Guest Network

Users

Guest Portal

Zone Edit

Schedule

Device Monitoring

Firmware Upgrade

Advanced

System Security

Date and Time

Access Point

Search

Match whole words

	MAC Address	Device Name	Model	AP Group	2.4G Channel	5G Channel	2.4G Tx Power	5G Tx Power	Status	Action
☐	74-DA-38-27-1B-54	AP74DA38271B54	CAP1200	System Default	11	36	Full	Full		
☐	74-DA-38-03-23-9C	AP74DA3803239C	WAP1750	System Default	11	36	Full	Full		
☐	74-DA-38-27-1B-48	AP74DA38271B48	CAP1200	System Default	11	36	Full	Full		
☐	74-DA-38-27-1B-38	AP74DA38271B38	CAP1200	System Default	11	36	Full	Full		
☐	74-DA-38-27-1B-3C	AP74DA38271B3C	CAP1200	System Default	11	36	Full	Full		
☐	80-1F-02-CC-DD-10	AP801F02CCDD10	WAP1750	System Default	11	36	Full	Full		
☐	74-DA-38-27-1B-46	AP74DA38271B46	CAP1200	System Default	11	36	Full	Full		
☐	74-DA-38-27-1B-40	AP74DA38271B40	CAP1200	System Default	11	36	Full	Full		
☐	74-DA-38-27-1B-44	AP74DA38271B44	CAP1200	System Default	11	36	Full	Full		
☐	74-DA-38-27-1B-3E	AP74DA38271B3E	CAP1200	System Default	11	36	Full	Full		

Refresh
Edit
Delete Selected
Delete All

Access Point Group

Search

Match whole words

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, guest network, users and scheduling settings as well as upgrade firmware across multiple access points. The Zone Plan can also be configured using “Zone Edit”.

Local Network



A P C 5 0 0

Dashboard

Zone Plan

NMS Monitor

NMS Settings

Local Network

Local Settings

Toolbox

> Network Settings

LAN-side IP Address

LAN Port Settings

VLAN

LAN-side IP Address

IP Address Assignment

Static IP Address

IP Address

192.168.2.1

Subnet Mask

255.255.255.0

Default Gateway

192.168.2.3

Primary DNS Address

8.8.8.8

Secondary DNS Address

0.0.0.0

Local Network settings are for your AP Controller. You can configure the IP address and DHCP server of the AP Controller in addition to LAN Port and VLAN settings.

Local Settings



AP C 5 0 0

Dashboard

Zone Plan

NMS Monitor

NMS Settings

Local Network

Local Settings

Toolbox

System Settings

System Information

Log

Management

Admin

Date and Time

Syslog Server

I'm Here

Advanced

LED Settings

Update Firmware

Save/Restore Settings

Factory Default

Reboot

System

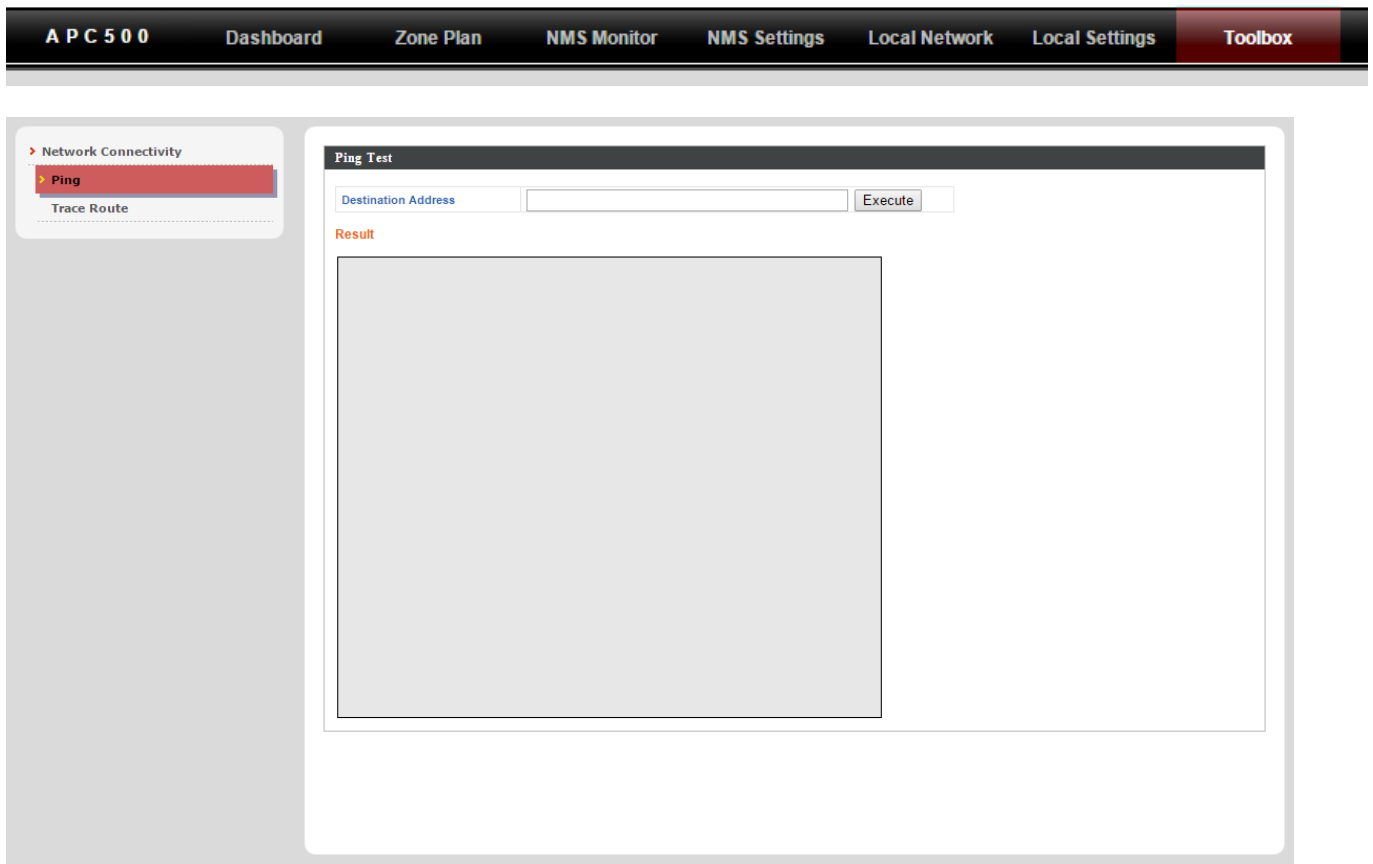
Model	APC500
Product Name	AP00AABBCCDD10
Uptime	0 day 03:23:27
System Time	2015/11/06 15:28:23
Boot from	Internal memory
Firmware Version	1.3.1
MAC Address	00:AA:BB:CC:DD:10
Management VLAN ID	1
IP Address	192.168.2.1
Default Gateway	192.168.2.3
DNS	---
DHCP Server	---
Internal Storage	Not detected

Wired LAN Port Settings

Wired LAN Port	Status	VLAN ModeID
LAN0	Disconnected (---)	Untagged Port / 1
LAN1	Disconnected (---)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1
LAN3	Connected (100 Mbps Full-Duplex)	Untagged Port / 1

Local Settings are for your AP Controller. You can view basic system settings 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 two network diagnostic tools: *ping* and *traceroute*.

V. 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.

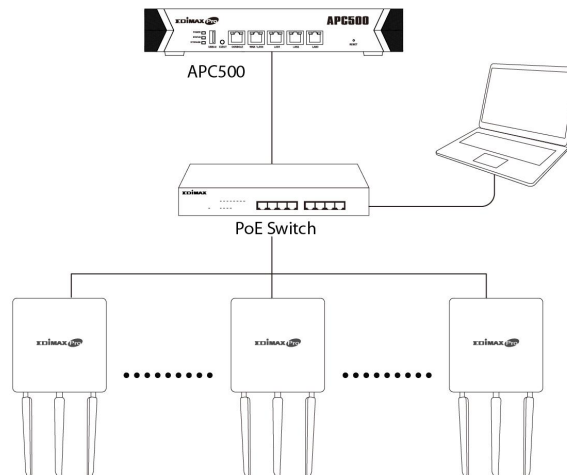
V-1. LOGIN, LOGOUT & RESTART



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 **192.168.2.1**





Your computer's IP address must be in the same subnet as the AP Controller. Refer to VI-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.

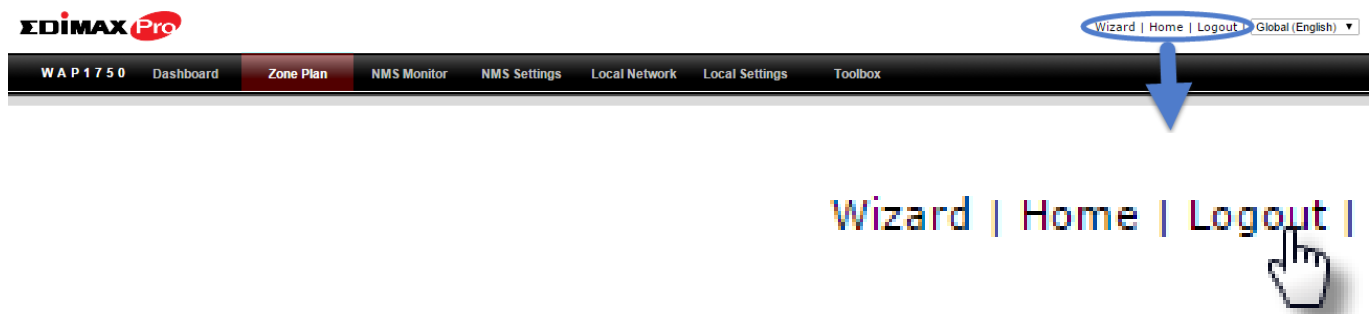


If using a DHCP server on the network, it is advised to use your DHCP server's settings to assign the AP Controller a static IP address.

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".

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



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



V-2. DASHBOARD

The dashboard displays an overview of your AP array:

Auto Refresh Time ● 1 minute ○ 30 seconds ○ Disable 56

System Information

Product Name	APC500
Host Name	AP00AABCCDD10
MAC Address	00-AA-BB-CC-DD:10
IP Address	192.168.2.1
Firmware Version	1.3.1
System Time	2015/11/06 15:39:15
Uptime	0 day 03:34:20
CPU Usage	3%
Memory Usage	9%

Managed AP

Search ☐ Match whole words

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74-DA-38-27-1B-54	AP74DA38271B54	CAP1200	192.168.2.124	11	36	0	●	
2	74-DA-38-03-23-9C	AP74DA3803239C	WAP1750	192.168.2.102	11	36	0	●	
3	74-DA-38-27-1B-48	AP74DA38271B48	CAP1200	192.168.2.120	11	36	0	●	
4	74-DA-38-27-1B-38	AP74DA38271B38	CAP1200	192.168.2.118	11	36	0	●	
5	74-DA-38-27-1B-3C	AP74DA38271B3C	CAP1200	192.168.2.110	11	36	0	●	
6	80-1F-02-CC-DD-10	AP801F02CCDD10	WAP1750	192.168.2.105	11	36	0	●	
7	74-DA-38-27-1B-46	AP74DA38271B46	CAP1200	192.168.2.121	11	36	0	●	
8	74-DA-38-27-1B-40	AP74DA38271B40	CAP1200	192.168.2.126	11	36	0	●	
9	74-DA-38-27-1B-44	AP74DA38271B44	CAP1200	192.168.2.127	11	36	0	●	
10	74-DA-38-27-1B-3E	AP74DA38271B3E	CAP1200	192.168.2.128	11	36	0	●	

Managed AP Group

Search ☐ Match whole words

Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (10)							
	74-DA-38-27-1B-54	AP74DA38271B54	CAP1200	192.168.2.124	0	●	
	74-DA-38-03-23-9C	AP74DA3803239C	WAP1750	192.168.2.102	0	●	
	74-DA-38-27-1B-48	AP74DA38271B48	CAP1200	192.168.2.120	0	●	
	74-DA-38-27-1B-38	AP74DA38271B38	CAP1200	192.168.2.118	0	●	
	74-DA-38-27-1B-3C	AP74DA38271B3C	CAP1200	192.168.2.110	0	●	
	80-1F-02-CC-DD-10	AP801F02CCDD10	WAP1750	192.168.2.105	0	●	
	74-DA-38-27-1B-46	AP74DA38271B46	CAP1200	192.168.2.121	0	●	
	74-DA-38-27-1B-40	AP74DA38271B40	CAP1200	192.168.2.126	0	●	
	74-DA-38-27-1B-44	AP74DA38271B44	CAP1200	192.168.2.127	0	●	
	74-DA-38-27-1B-3E	AP74DA38271B3E	CAP1200	192.168.2.128	0	●	

Active Clients

Search ☐ Match whole words

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

Active Users

Search ☐ Match whole words

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



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

Auto Refresh Time : ● 1 minute ○ 30 seconds ○ Disable 35

V-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), CPU Usage & Memory Usage.*

System Information 	
Product Name	APC500
Host Name	AP00AABBCCDD10
MAC Address	00:AA:BB:CC:DD:10
IP Address	192.168.2.1
Firmware Version	1.3.1
System Time	2015/11/06 15:44:04
Uptime	0 day 03:39:09
CPU Usage	4%
Memory Usage	9%

V-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	10
Client Devices	0
Rogue Devices	0

V-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:38:27:1B:54	AP74DA38271B54	CAP1200	192.168.2.124	11	36	0		
2	74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	192.168.2.102	11	36	0		
3	74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	192.168.2.120	11	36	0		
4	74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	192.168.2.118	11	36	0		
5	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	192.168.2.110	11	36	0		
6	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	192.168.2.105	11	36	0		
7	74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	192.168.2.121	11	36	0		
8	74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	192.168.2.126	11	36	0		
9	74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	192.168.2.127	11	36	0		
10	74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	192.168.2.128	11	36	0		

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

Search ☐ Match whole words

The **Status** icon displays *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 V-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.

V-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, 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 **V-5-1. Access Point**).

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74:DA:38:27:1B:54	AP74DA38271B54	CAP1200	192.168.2.124	11	36	0		
2	74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	192.168.2.102	11	36	0		
3	74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	192.168.2.120	11	36	0		
4	74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	192.168.2.118	11	36	0		
5	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	192.168.2.110	11	36	0		
6	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	192.168.2.105	11	36	0		
7	74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	192.168.2.121	11	36	0		
8	74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	192.168.2.126	11	36	0		
9	74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	192.168.2.127	11	36	0		
10	74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	192.168.2.128	11	36	0		

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

Search ☐ Match whole words

The **Status** icon displays *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 V-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.

V-2-5. Active Clients

Active Clients displays information about each client in the local network: *Index (reference number), Client MAC Address, AP MAC Address, WLAN, User Name, Radio (frequency), Signal Strength, Connected Time, Idle Time, Tx & Rx (data transmitted and received) and Vendor of the client device.*

Active Clients											
Search ☐ Match whole words											
Index	Client MAC Address	AP MAC Address	WLAN	User Name	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
1	B4:52:7E:84:DB:5B	74:DA:38:03:23:9C	Edimax 2.4GHz	N/A	2.4GHz	100	3 min 47 secs	0	1.604	14.53	Sony Mobile Communications AB
2	4C:7C:5F:3B:F1:89	74:DA:38:03:23:9C	Edimax 5GHz	N/A	5GHz	100	3 min 46 secs	0	5.066	602.327	Apple

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



V-2-6. Active Users

Active Users displays information about each user in the local network via guest portals: *Index (reference number), User Name, MAC Address, IP Address, SSID, Creator, Create Time, Expire Time, Usage Percentage, Vendor & Platform of the user device.*

Active Users


Search
☐ Match whole words

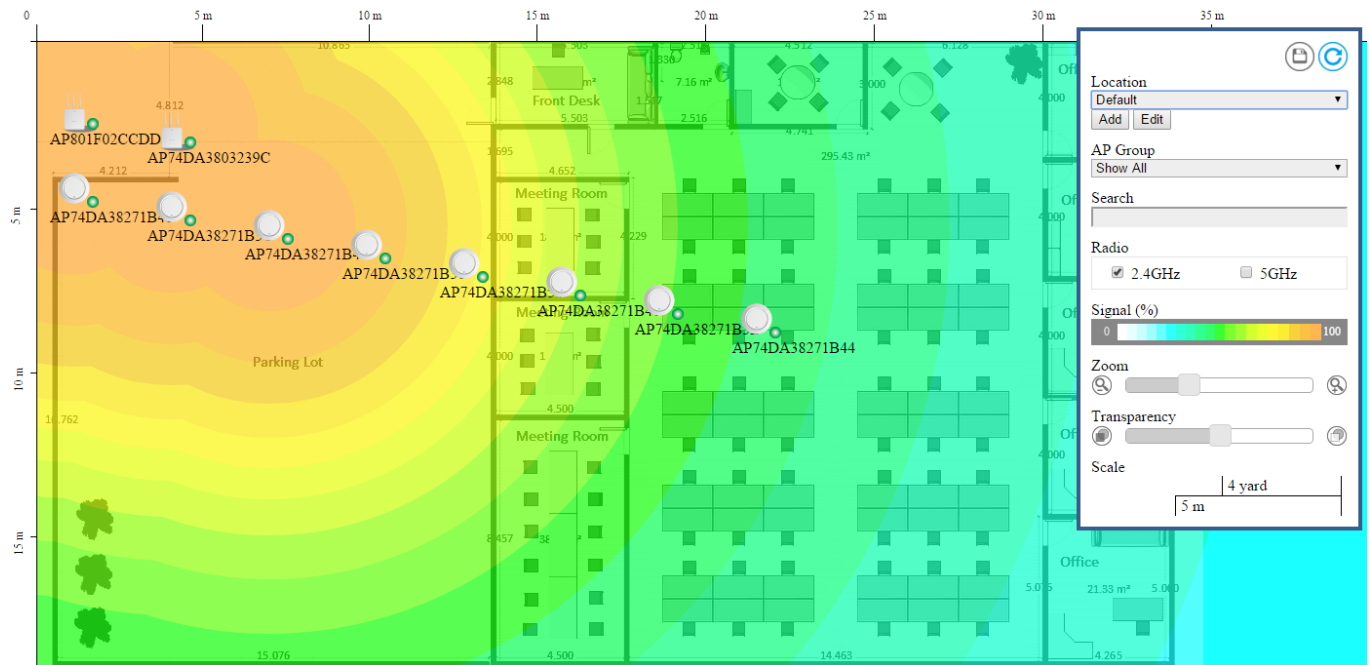
Index	User Name	MAC Address	IP Address	SSID	Creator	Create Time	Expire Time	Usage Percentage	Vendor	Platform	Action
Empty											

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

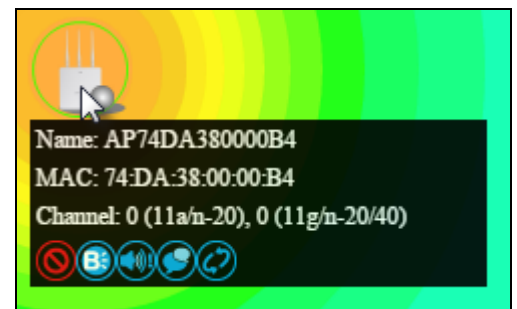
Search
☐ Match whole words

V-3. ZONE PLAN

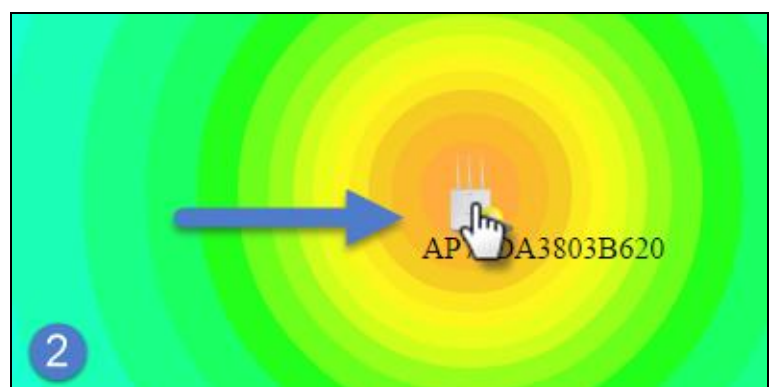
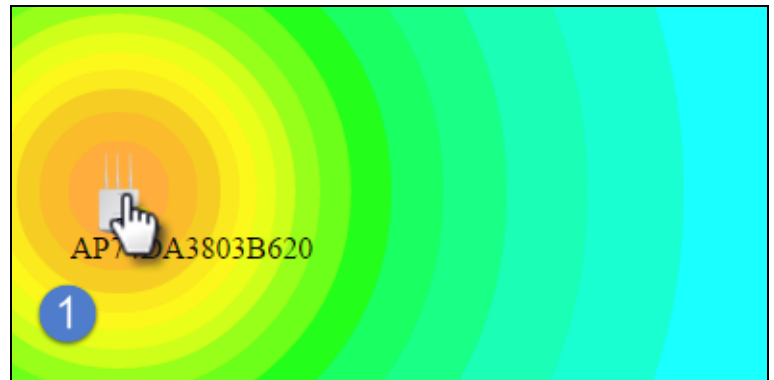
The Zone Plan can be fully customized to match your network environment. You can move the AP icons and select different location images (upload location images in **NMS Settings → Zone Edit**) to create a visual map of your AP array.



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



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



Location	Select a pre-defined location from the drop down menu. When you upload a location image in NMS Settings → Zone Edit , it will be available for selection here.
AP Group	You can select an AP Group to display in the zone map. Edit AP Groups in NMS Settings → Access Point .
Search	Use the search box to quickly locate an AP.
Radio	Use the checkboxes to display APs according to 2.4GHz or 5GHz wireless radio frequency.
Signal	Signal strength key for the signal strength display around each AP in the zone map.
Zoom	Use the slider to adjust the zoom level of the map.
Transparency	Use the slider to adjust the transparency of location images.
Scale	Zone map scale.
Device/Number	Displays number and type of devices in the zone map.

V-4. NMS MONITOR

V-4-1. Access Point

V-4-1-1. Managed AP

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

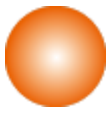
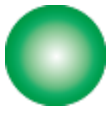
Managed AP ⌕									
Search		☐ Match whole words							
Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74:DA:38:27:1B:54	AP74DA38271B54	CAP1200	192.168.2.124	11	36	0		
2	74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	192.168.2.102	11	36	0		
3	74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	192.168.2.120	11	36	0		
4	74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	192.168.2.118	11	36	0		
5	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	192.168.2.110	11	36	0		
6	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	192.168.2.105	11	36	0		
7	74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	192.168.2.121	11	36	0		
8	74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	192.168.2.126	11	36	0		
9	74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	192.168.2.127	11	36	0		
10	74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	192.168.2.128	11	36	0		

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

Search ☐ Match whole words

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

Status Icons			
Icon	Color	Status	Definition
	Grey	Disconnected	Managed AP is disconnected. <i>Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.</i>
	Red	Authentication Failed	System security must be the same for all access points in the AP array. <i>Please check security settings (refer to V-5-12-1).</i>

		Or Incompatible NMS Version	System Security). Access points must use the same version of Edimax NMS: the managed AP will not be able to make configurations. <i>Please use the AP Controller's firmware upgrade function (refer to V-5-11. Firmware Upgrade).</i>
	Orange	Configuring or Upgrading	<i>Please wait while the Managed AP makes configurations or while the firmware is upgrading.</i>
	Yellow	Connecting	<i>Please wait while Managed AP is connecting.</i>
	Green	Connected	<i>Managed AP is connected.</i>
	Blue	Waiting for Approval	Managed AP is waiting for approval. Refer to V-5-1. Access Point: Auto Approval . Note: 200 Managed APs are supported. Additional APs will display this status until an existing Managed AP is removed.

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



1. Disallow

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

1. Edit

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

2. Blink LED

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

3. Buzzer

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

4. Network Connectivity

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

5. Restart

Restarts the Managed AP.

V-4-1-2. Managed AP Group

Managed APs can be grouped according to your requirements. 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).*

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

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74:DA:38:27:1B:54	AP74DA38271B54	CAP1200	192.168.2.124	11	36	0		
2	74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	192.168.2.102	11	36	0		
3	74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	192.168.2.120	11	36	0		
4	74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	192.168.2.118	11	36	0		
5	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	192.168.2.110	11	36	0		
6	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	192.168.2.105	11	36	0		
7	74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	192.168.2.121	11	36	0		
8	74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	192.168.2.126	11	36	0		
9	74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	192.168.2.127	11	36	0		
10	74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	192.168.2.128	11	36	0		

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

Search ☐ Match whole words

The **Status** icon displays *grey* (disconnected), *red* (authentication failed/incompatible NMS version), *orange* (upgrading firmware), *yellow*

(connecting), *green* (connected) or *blue* (waiting for approval) for each individual Managed AP. Refer to **V-4-1-1. Managed AP: Status Icons** for full descriptions.

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



2. Disallow

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

3. Edit

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

4. Blink LED

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

5. Buzzer

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

6. Network Connectivity

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

7. Restart

Restarts the Managed AP.

V-4-2. WLAN

V-4-2-1. Active WLAN

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

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

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

Search ☐ Match whole words

Active WLAN					
Search		☐ Match whole words			
Index	Name/SSID	VLAN ID	Authentication	Encryption	Additional Authentication
1	SSID_DEMO_01	1	OPEN	NONE	No additional authentication
2	SSID_DEMO_02	1	OPEN	NONE	No additional authentication

V-4-2-2. Active WLAN Group

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

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

Search ☐ Match whole words

Active WLAN Group					
Search ☐ Match whole words					
Group Name	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
Wizard WLAN 2.4G Group 1 (1)					
	Edimax 2.4GHz	1	WPA2PSK	AES	No additional authentication
Wizard WLAN 5G Group 2 (1)					
	Edimax 5GHz	1	WPA2PSK	AES	No additional authentication

V-4-3. Clients

V-4-3-1. Active Clients

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

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

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

Search ☐ Match whole words

Refresh time

Auto Refresh time

☒ 1 Minute
☐ 30 seconds
☐ Disable

Manual Refresh

Refresh

Active Clients											
Search			☐ Match whole words								
Index	Client MAC Address	AP MAC Address	WLAN	User Name	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
1	4C:7C:5F:3B:F1:89	74:DA:38:27:1B:46	Guest 2.4GHz	user002	2.4GHz	100	1 min 17 secs	0	455.182	42.152	Apple
2	B4:52:7E:84:DB:5B	74:DA:38:27:1B:48	Guest 2.4GHz	user001	2.4GHz	100	2 min 12 secs	31	1170.65	341.822	Sony Mobile Communications AB
3	4C:7C:5F:3B:F1:89	74:DA:38:27:1B:48	Guest 2.4GHz	user002	2.4GHz	100	1 min 44 secs	101	2.468	1.25	Apple

V-4-4. Users

V-4-4-1. Active Users

Displays information about each user in the local network via guest portals: *Index (reference number), User Name, MAC Address, IP Address, SSID, Creator, Create Time, Expire Time, Usage Percentage, Vendor & Platform of the user device.*

Active Users											
Search			☐ Match whole words								
Index	User Name	MAC Address	IP Address	SSID	Creator	Create Time	Expire Time	Usage Percentage	Vendor	Platform	Action
1	user001	B4:52:7E:84:DB:5B	192.168.2.141	Guest%202.4GHz	Admin	1970/01/01 00:11:41	forever	0%	Sony Mobile Communications AB	Android	
2	user002	4C:7C:5F:3B:F1:89	192.168.2.140	Guest%202.4GHz	Admin	1970/01/01 00:11:53	forever	0%	Apple	iPhone	

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

Search
☐ Match whole words

V-4-4-2. Users Log

Displays a detailed information log of users and activity on the network via guest portals: *ID, Date and Time of entry, Category of entry, Severity, Users, Event/Activities details.*

Users Log

Search

☐ Match whole words

ID	Date and Time	Category	Severity	Users	Events/Activities
2	2015/11/06 17:21:56	NMS	Low	guest	Static User[user002]'s device[4C:7C:5F:3B:F1:89] login successfully
1	2015/11/06 17:21:31	NMS	Low	guest	Static User[user001]'s device[B4:52:7E:84:DB:5B] login successfully

Refresh

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

Search ☐ Match whole words

V-4-5. Rogue Devices

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

Click “Start” to scan for rogue devices:



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

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

Search ☐ Match whole words

Rogue Devices

Unknown Rogue Devices

Search ☐ Match whole words

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

Known Rogue Devices

Search ☐ Match whole words

V-4-6. Information

V-4-6-1. All Events/Activities

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

Select AP:

```
2015/11/06 12:08:33: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) connect successfully
2015/11/06 12:11:56: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) connect successfully
2015/11/06 12:13:44: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) connect successfully
2015/11/06 12:20:39: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:23:34: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) connect successfully
2015/11/06 12:42:47: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:44:44: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:46:41: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:48:39: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:50:22: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:51:52: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:53:22: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 12:59:00: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 13:00:58: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 13:02:55: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
2015/11/06 13:04:52: [S3]: [admin]: Managed AP(74:DA:38:27:1B:54) was disconnected
```

V-4-6-2. Monitoring

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

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

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

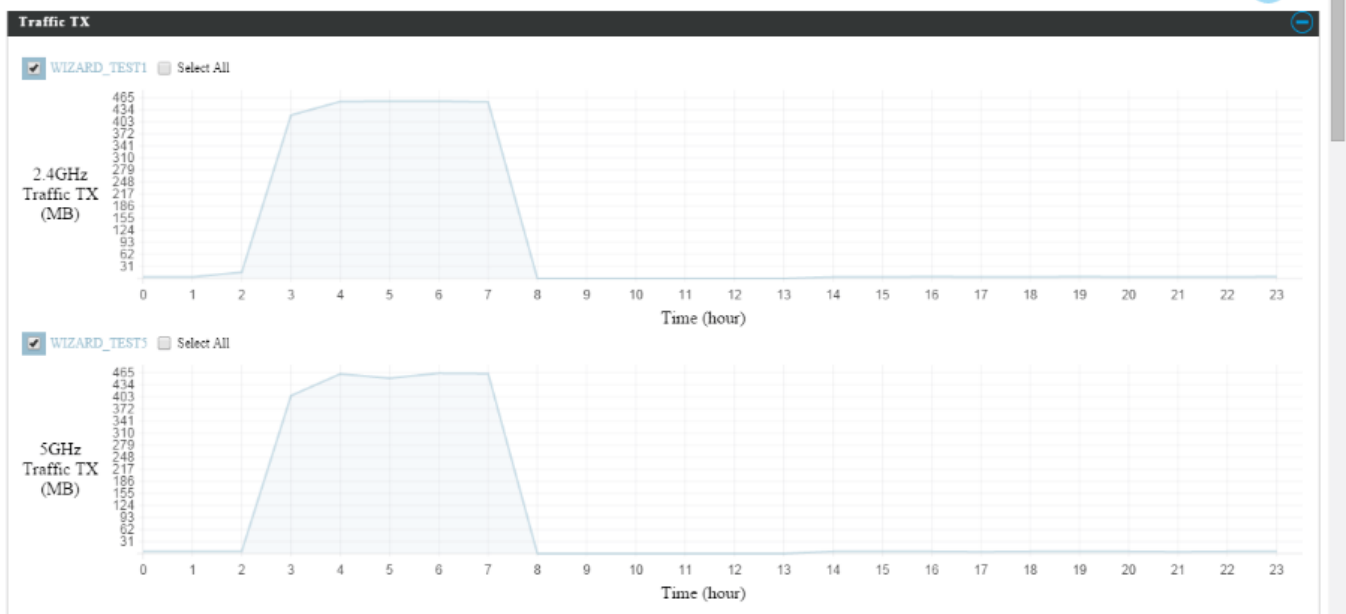
Auto Refresh Time : ☒ 1 minute ☐ 30 seconds ☐ Disable



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

Auto Refresh Time : ☒ 1 minute ☐ 30 seconds ☐ Disable

47



V-5. NMS Settings

V-5-1. Access Point

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

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



Access Point

Search
☐ Match whole words

☐	MAC Address	Device Name	Model	AP Group	2.4G Channel	5G Channel	2.4G Tx Power	5G Tx Power	Status	Action
☐	74:DA:38:27:1B:54	AP74DA38271B54	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	System Default	11	36	Full	Full		
☐	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	System Default	11	36	Full	Full		

Refresh
Edit
Delete Selected
Delete All

Access Point Group

Search
☐ Match whole words

☐	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
☐	System Default	10	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Add
Edit
Clone
Delete Selected
Delete All

Access Point Settings

Auto Approve
☒ Enable
☐ Disable

Apply

The **Status** icon displays *grey* (disconnected), *red* (authentication failed/incompatible NMS version), *orange* (upgrading firmware), *yellow* (connecting), *green* (connected) or *blue* (waiting for approval) for each individual Managed AP. Refer to **V-4-1-1. Managed AP: Status Icons** for full descriptions.

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

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



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

Access Point Settings

Auto Approve

☒ Enable
 ☐ Disable

Apply

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

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

Edit Access Point

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

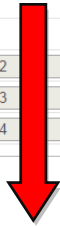
You can also use **Profile Settings** to assign the access point to WLAN, Guest Network, RADIUS and Access Control groups independently from Access Point Group settings.

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



Override Group Setting

Basic Settings	
Name	AP74DA3803B530
Description	
MAC Address	74:DA:38:03:B5:30
AP Group	System Default ▼
IP Address Assignment ☐ Override Group Setting Static IP Address ▼	
IP Address	192.168.222.101
Subnet Mask	255.255.255.0
Default Gateway	User-Defined ▼ 192.168.222.2
Primary DNS	User-Defined ▼ 192.168.222.3
Secondary DNS	User-Defined ▼ 192.168.222.4



IP Address Assignment	☒ Override Group Setting DHCP Client ▼
IP Address	192.168.222.101
Subnet Mask	255.255.255.0
Default Gateway	From DHCP ▼ 192.168.222.2
Primary DNS	From DHCP ▼ 192.168.222.3
Secondary DNS	From DHCP ▼ 192.168.222.4

Basic Settings	
Name	Edit the access point name. The default name is AP + MAC address.
Description	Enter a description of the access point for reference e.g. 2 nd Floor Office.
MAC Address	Displays MAC address.
AP Group	Use the drop down menu to assign the AP to an AP Group. You can edit AP Groups from the NMS Settings → Access Point page.
IP Address Assignment	Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server, or select “Static IP” to manually specify a static/fixed IP address for your access point (below). Check the box “Override Group Setting” if the AP is a member of an AP Group and you wish to use a different setting than the AP Group setting.
IP Address	Specify the IP address here. This IP address

	will be assigned to your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank.
Primary DNS	DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.
Secondary DNS	DHCP users can select “From DHCP” to get secondary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank.

VLAN Settings			
Wired LAN Port	VLAN Mode	VLAN ID	
Wired Port(#1)	☐ Override Default Setting Untagged Port ▼	☐ Override Default Setting	1
Wired Port(#2)	☐ Override Default Setting Untagged Port ▼	☐ Override Default Setting	1
Management VLAN ID		☐ Override Default Setting	1

VLAN Settings	
Wired LAN Port	Identifies LAN port 1 or 2.
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	Check ‘Override Default Setting’ to specify the VLAN ID of the management VLAN. Only the hosts belonging to the same VLAN can manage the device.

Radio Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Domain	CH1-13 (ETSI/MKK) ▼	W52,W53,W56 (MKK) ▼
Wireless	☐ Override Default Setting Disable ▼	☐ Override Default Setting Disable ▼
Band	☐ Override Default Setting 11b/g/n ▼	☐ Override Default Setting 11a/n ▼
Auto Pilot	☐ Override Default Setting Enable ▼ Please set AP position on the Zone Plan first.	☐ Override Default Setting Enable ▼ Please set AP position on the Zone Plan first.
Auto Pilot Sensitivity	☐ Override Default Setting Low ▼	☐ Override Default Setting Low ▼
Auto Pilot Range	☐ Override Default Setting Ch 1 - 11 ▼	☐ Override Default Setting Band 1 ▼
Auto Pilot Interval	☐ Override Default Setting One day ▼ ☐ Change channel even if clients are connected	☐ Override Default Setting One day ▼ ☐ Change channel even if clients are connected
Channel	☐ Override Default Setting Ch 11, 2462MHz ▼	☐ Override Default Setting Ch 36, 5.18GHz ▼
Channel Bandwidth	☐ Override Default Setting 20 MHz ▼	☐ Override Default Setting 20 MHz ▼
BSS BasicRateSet	☐ Override Default Setting 1,2,5,5,11 Mbps ▼	☐ Override Default Setting 6,12,24 Mbps ▼

Advanced Settings

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

Radio Settings

Domain	Set the regulatory domain for the access point's wireless channels for each frequency.
Wireless	Enable or disable the access point's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot Range	Select a range from which the auto channel

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

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



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

Advanced Settings	
Contention Slot	Select “Short” or “Long” – this value is used for contention windows.
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.

Profile Settings

	Radio B/G/N (2.4 GHz)	Radio A/N (5.0 GHz)
WLAN Group	☐ Override Group Setting WLAN Group 2 ▼	☐ Override Group Setting WLAN Group 3 ▼
Guest Network Group	☐ Override Group Setting Disable ▼	☐ Override Group Setting Disable ▼
RADIUS Group	☐ Override Group Setting ▼	
Access Control Group	☐ Override Group Setting Default ▼	

Profile Settings	
WLAN Group	Assign the access point's 2.4GHz or 5GHz SSID(s) to a WLAN Group. You can edit WLAN groups in NMS Settings → WLAN .
Guest Network Group	Assign the access point's 2.4GHz or 5GHz SSID(s) to a Guest Network Group. You can edit Guest Network groups in NMS Settings

	→ Guest Network.
RADIUS Group	Assign the access point's 2.4GHz SSID(s) to a RADIUS group. You can edit RADIUS groups in NMS Settings → RADIUS.
Access Control Group	Assign the access point's 2.4GHz SSID(s) to a RADIUS group. You can edit RADIUS groups in NMS Settings → Access Control

Add/Edit Access Point Group

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

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

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

Basic Group Settings	
Name	System Default
Description	System default group for APs

Basic Group Settings	
Name	Edit the access point group name.
Description	Enter a description of the access point group for reference e.g. 2 nd Floor Office Group.

VLAN Group Settings		
Wired LAN Port	VLAN Mode	VLAN ID
Wired Port(#1)	Untagged Port ▼	1
Wired Port(#2)	Untagged Port ▼	1
Management VLAN ID	1	

VLAN Group Settings	
Wired LAN Port	Identifies LAN port 1 or 2.
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	Check ‘Override Default Setting’ to specify the VLAN ID of the management VLAN. Only the hosts belonging to the same VLAN can manage the device.

Radio Group Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Domain	CH1-13 (ETSI/MKK) ▼	W52,W53,W56 (MKK) ▼
Wireless	Enable ▼	Enable ▼
Band	11b/g/n ▼	11a/n/ac ▼
Auto Pilot	Enable ▼ Please set AP position on the Zone Plan first.	Enable ▼ Please set AP position on the Zone Plan first.
Auto Pilot Sensitivity	Low ▼	Low ▼
Auto Pilot Range	Ch 1 - 11 ▼	Band 1 ▼
Auto Pilot Interval	Half day ▼ ☐ Change channel even if clients are connected	Half day ▼ ☐ Change channel even if clients are connected
Channel	Ch 11, 2462MHz ▼	Ch 36, 5.18GHz ▼
Channel Bandwidth	20 MHz ▼	20 MHz ▼
BSS BasicRateSet	all ▼	all ▼

Advanced Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Contention Slot	Short ▼	
Preamble Type	Short ▼	
Guard Interval	Short GI ▼	Short GI ▼
802.11n Protection	Enable ▼	Enable ▼
CE Adaptive	Disable ▼	
DTIM Period	255 (1-255)	255 (1-255)
RTS Threshold	2347 (1-2347)	2347 (1-2347)
Fragment Threshold	2346 (256-2346)	2346 (256-2346)
Multicast Rate	Auto ▼	Auto ▼
Tx Power	100% ▼	100% ▼
Beacon Interval	100 (40-1000 ms)	100 (40-1000 ms)
Station idle timeout	300 (30-65535 seconds)	300 (30-65535 seconds)

Radio Group Settings

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

	channel setting will check/reassign the wireless channel. Check/uncheck the “Change channel even if clients are connected” box according to your preference.
Channel Bandwidth	Set the channel bandwidth or use Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

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



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

Advanced Settings	
Contention Slot	Select “Short” or “Long” – this value is used for contention windows.
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.

Profile Group Settings		
	Radio B/G/N (2.4 GHz)	Radio A/N/A/C (5.0 GHz)
WLAN Group	☐ Override Default Setting Disable ▾	☐ Override Default Setting Disable ▾
Guest Network Group	☐ Override Default Setting Disable ▾	☐ Override Default Setting Disable ▾
RADIUS Group ☐ Override Default Setting Disable ▾ MAC Access Control Group ☐ Override Default Setting Disable ▾		

Group Settings		
Members	Search Group Name : MAC Address Device Name No Access Point	Search System Default ▾ MAC Address Device Name 80:1F:02:CC:DD:10 AP801F02CCDD10 74:DA:38:27:1B:48 AP74DA38271B48 74:DA:38:27:1B:3C AP74DA38271B3C 74:DA:38:03:23:9C AP74DA3803239C 74:DA:38:27:1B:46 AP74DA38271B46 74:DA:38:27:1B:38 AP74DA38271B38 74:DA:38:27:1B:54 AP74DA38271B54 74:DA:38:27:1B:40 AP74DA38271B40 74:DA:38:27:1B:3E AP74DA38271B3E 74:DA:38:27:1B:44 AP74DA38271B44
	<< >>	

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

V-5-2. WLAN

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

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

Search ☐ Match whole words

WLAN

Search ☐ Match whole words

☐	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
☐	SSID_DEMO_01	1	OPEN	NONE	No additional authentication
☐	SSID_DEMO_02	1	OPEN	NONE	No additional authentication

Add Edit Clone Delete Selected Delete All

WLAN Groups

Search ☐ Match whole words

☐	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
☐	Group_SSID_Demo	2	SSID_DEMO_01 SSID_DEMO_02		

Add Edit Clone Delete Selected Delete All

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



Add/Edit WLAN

WLAN Settings	
Name/SSID	edimax2.4
Description	
VLAN ID	1
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
Load Balancing	50 /50
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

WLAN Advanced Settings	
Smart Handover Settings	
Smart Handover	☐ Enable ☒ Disable
RSSI Threshold	-80 ▼ dB
Active WLAN Schedule Settings *This function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.	
Schedule Group	Disable ▼

WLAN Settings	
Name/SSID	Edit the WLAN name (SSID).
Description	Enter a description of the SSID for reference e.g. 2 nd Floor Office HR.
SSID	Select which SSID to configure security settings for.
VLAN ID	Specify the VLAN ID.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.

Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu.
Additional Authentication	Select an additional authentication method from the drop down menu.

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



It's essential to configure wireless security in order to prevent unauthorised access to your network.



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

Please refer to **V-5-2-1. No Authentication** and onwards below for more information on authentication and additional authentication types.

WLAN Advanced Settings	
Smart Handover	Enable or disable Smart Handover.
RSSI Threshold	Set a RSSI Threshold level.
Schedule Group	Assign to a specified schedule (schedule must be pre-configured in NMS Settings → Schedule.)

V-5-2-1. 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.

V-5-2-2. 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.

V-5-2-3. IEEE802.1x/EAP

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

V-5-2-4. 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.
-----------------------	--

V-5-2-5. WPA-EAP

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



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

V-5-2-6. Additional Authentication

Additional wireless authentication methods can also be used:

MAC Address Filter

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



See V-5-4. 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 V-5-3. RADIUS to configure RADIUS servers.

MAC RADIUS Password

☒ Use MAC address

☐ Use the following password

MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If
----------------------------	--

	you select “Use the following password”, enter the password in the field below. The password should match the “Shared Secret” used in V-5-3. RADIUS .
--	--

Add/Edit WLAN Group

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

WLAN Group Settings			
Name			
Description			
Members	Search		☐ Match whole words
	☐	Name/ESSID	VLAN ID
	☐	edimax2.4	Override 1
	☐	Override	Schedule Group
*Schedule Group function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.			

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

V-5-3. RADIUS

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

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

Search ☐ Match whole words

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



External RADIUS Server

Search ☐ Match whole words

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

Add Edit Clone Delete Selected Delete All

Internal RADIUS Server

Search ☐ Match whole words

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

Add Edit Clone Delete Selected Delete All

RADIUS Account

Search ☐ Match whole words

☐	Name	Password
Please add User Account		

Add Edit Delete Selected Delete All

RADIUS Group

Search ☐ Match whole words

☐	Name	2.4GHz	5GHz	RADIUS accounts
Please add RADIUS group setting				

Add Edit Clone Delete Selected Delete All

Add/Edit External RADIUS Server

External RADIUS Server	
Name	
Description	
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 Seconds
Accounting	☒ Enable ☐ Disable
Accounting Port	1813

Name	Enter a name for the RADIUS Server.
Description	Enter a description of the RADIUS Server for reference.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the password in RADIUS server's configuration.
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.

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

Internal RADIUS Server	
Name	
Description	
EAP Internal Authentication	PEAP(MS-PEAP) ▼
Shared Secret	
Session-Timeout	3600 Seconds
Termination-Action	☒ Reauthentication (RADIUS-Request) ☐ Not-Reauthentication (Default) ☐ Not-Send

Add/Edit Internal RADIUS Server

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

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

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

Add/Edit RADIUS Accounts

The internal RADIUS server can authenticate up to 512 user accounts. The “RADIUS Accounts” page allows you to configure and manage users.

RADIUS Accounts

User Name
 Example: USER1, USER2, USER3, USER4
 Enter username here

User Registration List

Select	User Name	Password	Customize
☐	Edimax	Not Configured	Edit



Edit User Registration List		
User Name	Edimax	(4-16characters)
Password		(6-32characters)

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

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

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

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

Add/Edit RADIUS Group

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

RADIUS Group Settings							
Group Name							
Description							
2.4GHz RADIUS	Primary : Disabled Secondary : Disabled						
5GHz RADIUS	Primary : Disabled Secondary : Disabled						
Members	Search ☐ Match whole words <table border="1"> <thead> <tr> <th>☐</th> <th>Username</th> <th>Password</th> </tr> </thead> <tbody> <tr> <td> Add </td> <td> </td> <td> </td> </tr> </tbody> </table>	☐	Username	Password	Add		
☐	Username	Password					
Add							

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

V-5-4. Access Control

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

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

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

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

Search ☐ Match whole words

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



MAC Access Control

Search

☐ Match whole words

☐

MAC Address

Description

Please add MAC Access Control setting

Add

Delete Selected

Delete All

Add/Edit MAC Access Control

MAC Access Control

Add MAC Address

Remain entries (256)

Add

Reset

MAC Access Control List

MAC Address	Description	Delete
Please add MAC Addresses		

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

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

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.

Add/Edit MAC Access Control Group

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

MAC Filter Group Settings

Group Name

Please enter a new group name

Description

Please enter a new group description

Action

Blacklist ▾

Search

☐ Match whole words

Members

☐

MAC Address

Description

No MAC Access Control Profile

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

V-5-5. Guest Network

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

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

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



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



Guest Network

Search ☐ Match whole words

☐	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
☐	Guest 2.4GHz	1	WPA2-PSK	AES	No additional authentication
☐	Guest 5GHz	1	WPA2-PSK	AES	No additional authentication

Guest Network Group

Search ☐ Match whole words

☐	Group Name	Guest Network members	Guest Network member list	Used AP	Used AP Group
☐	Wizard Guest 2.4G Group 1	1	Guest 2.4GHz	AP801F02CCDD10 AP74DA38271B48 AP74DA38271B3C AP74DA3803239C AP74DA38271B46	Wizard AP Group 2
☐	Wizard Guest 5G Group 2	1	Guest 5GHz	AP801F02CCDD10 AP74DA38271B48 AP74DA38271B3C AP74DA3803239C AP74DA38271B46	Wizard AP Group 2

Add/Edit Guest Network

Guest Network Settings	
Name/SSID	
Description	
VLAN ID	1
Broadcast SSID	Enable
Wireless Client Isolation	STA Separator
Load Balancing	50 /50
Authentication Method	No Authentication
Additional Authentication	No additional authentication

Guest Access Policy													
Guest Portal Settings													
Guest Portal	Disable												
Traffic Shaping Settings													
Traffic Shaping	Disable												
Downlink	50 Mbps												
Uplink	50 Mbps												
Filtering Settings													
IP Filtering	Disable												
Rules	<table border="1"> <thead> <tr> <th>☐</th> <th colspan="2">IP/Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>☐</td> <td>0.0.0.0</td> <td>/0.0.0.0</td> </tr> <tr> <td>☐</td> <td>0.0.0.0</td> <td>/0.0.0.0</td> </tr> <tr> <td>☐</td> <td>0.0.0.0</td> <td>/0.0.0.0</td> </tr> </tbody> </table>	☐	IP/Subnet Mask		☐	0.0.0.0	/0.0.0.0	☐	0.0.0.0	/0.0.0.0	☐	0.0.0.0	/0.0.0.0
☐	IP/Subnet Mask												
☐	0.0.0.0	/0.0.0.0											
☐	0.0.0.0	/0.0.0.0											
☐	0.0.0.0	/0.0.0.0											

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

Guest Network Settings	
Name/SSID	Edit the Guest Network name (SSID).
Description	Enter a description of the Guest Network for reference e.g. 2 nd Floor Office HR.
VLAN ID	Specify the VLAN ID.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client	Enable or disable wireless client isolation.

Isolation	Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu.
Additional Authentication	Select an additional authentication method from the drop down menu.

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



It's essential to configure wireless security in order to prevent unauthorised access to your network.



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

Please refer to **V-5-2-1.** for more information on authentication and additional authentication types.

Guest Access Policy	
Guest Portal	Select a guest portal to use for this guest SSID. Guest portals can be configured in NMS Settings → Guest Portal.
Traffic Shaping	Enable or disable traffic shaping for the guest network.
Downlink	Enter a downlink limit in MB.
Uplink	Enter an uplink limit in MB.
IP Filtering	Select "Deny" or "Allow" to deny or allow specified IP addresses to access the guest network. Select "Disable" to disable IP

	filtering.
Rules	Enter IP addresses to be filtered according to the Deny or Allow rule specified above and check the box for each IP address to be filtered.

Guest Network Advanced Settings	
Schedule Group	Assign guest SSID to a specified schedule (schedule must be pre-configured in NMS Settings → Schedule.)

Add/Edit Guest Network Group

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

Guest Group Settings

Name

Description

Search

Match whole words

Members

☐	Name/ESSID	VLAN ID	Schedule Group
☐	GuestPL	☐ Override 1	☐ Override Disable ▾

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

Guest Network Group Settings	
Group Name	Edit the Guest Network Group name.
Description	Enter a description of the Guest Network for reference.
Members	Add SSIDs to the Guest Network group. You can override individual VLAN ID & schedule settings and assign a different VLAN ID or schedule.

V-5-6. Users

User accounts can be created, monitored and managed for use with the controller's guest portal function. Guest portal settings can be found at **V-5-7. Guest Portal** (NMS Settings → Guest Portal).

When a guest portal is enabled, users who connect to the Guest SSID will automatically arrive at the customizable guest portal page. From there a user account login is required to access the network. These user accounts are created and grouped here, and then selected as the **Authentication User Group** at **NMS Settings → Guest Portal**.

The guest portal also generates a Front Desk URL which allows staff/admins to login and quickly create/manage user accounts and expiry times, and generate & print tickets with login credentials to give to guest users. These staff/admin accounts are created and grouped here, and selected as the **Front Desk User Group** at **NMS Settings → Guest Portal**.

Information on the users page is displayed about each user account and user account group.

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

Search ☐ Match whole words

Users						
Search		☐ Match whole words				
☐	Name	Create Time	Valid Period	Description	Status	Action
☐	user001	1970/01/01 00:11:41	Always			 
☐	user002	1970/01/01 00:11:53	Always			 
Add Edit Clone Delete Selected Delete All Upload List Download List						

User Group					
Search		☐ Match whole words			
☐	Group Name	User members	User member list	Description	Role Type
☐	Default	0			Default
☐	Group_Static_Users	2	user001 user002		Guest Portal user
Add Edit Clone Delete Selected Delete All					

The **Status** icon displays *grey* (logged out), *yellow* (expired), *red* (locked) or *green* (active) for each user.

The **Action** icons can lock/unlock or revive (an expired) user account.



Select a user or user group using the check-boxes and click “**Edit**” to make configurations, or click “**Add**” to add new users and groups:



You can download and upload user lists as .csv files for convenience.

Add/Edit User

User Settings	
Name	manager
Description	managerOfGuestPortalPL
Password	
Confirm Password	
User Group	managerPL ▼

User Settings	
Name	Edit the user account name.
Description	Enter a description of the user account name e.g. Guest Portal 1
Password	Specify a password for the account.
Confirm Password	Confirm the password for the account.
User Group	Assign the user account to a user group so it can be utilized by the guest portal.

Add/Edit User Group

User Group Settings												
Name	Group_Static_Users											
Description												
Role Type	Guest Portal user ▼											
Members	Search ☐ Match whole words											
	<table border="1"> <thead> <tr> <th>☐</th> <th>Name</th> <th>User Group</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>☒</td> <td>user001</td> <td>Group_Static_Users</td> <td></td> </tr> <tr> <td>☒</td> <td>user002</td> <td>Group_Static_Users</td> <td></td> </tr> </tbody> </table>	☐	Name	User Group	Description	☒	user001	Group_Static_Users		☒	user002	Group_Static_Users
☐	Name	User Group	Description									
☒	user001	Group_Static_Users										
☒	user002	Group_Static_Users										

User Group Settings	
Name	Edit the user group name.
Description	Enter a description of the user group name e.g. Front Desk or Guest Users.
Role Type	Select whether the group is for Guest Portal users or Front Desk managers.
Members	Select which user accounts to include in the group.

V-5-7. Guest Portal

Displays information about guest portals and allows you to edit guest portal settings. Guest portals require **users** to be created at **NMS Settings → Users**.

When a guest portal is enabled, users who connect to the Guest SSID will automatically arrive at the customizable guest portal page. From there a user account login is required to access the network. These user accounts are created and grouped at **NMS Settings → Users**, and then selected as the **Authentication User Group** here.

The guest portal also generates a Front Desk URL which allows staff/admins to login and quickly create/manage user accounts and expiry times, and generate & print tickets with login credentials to give to guest users. These staff/admin accounts are created and grouped at **NMS Settings → Users** and then selected as the **Front Desk User Group** here.

Guest Portal

Search ☐ Match whole words

☐	Name	Guest Portal Type	Used Guest Network
☐	Guest_Portal_Static_Users	Static Users	Guest 2.4GHz Guest 5GHz

Add Edit Delete Selected Delete All

Guest Portal Settings

Idle Timeout
5 minutes

Login Password Retry Lockout
5 (1-30 times)

Apply

Guest Portal Settings	
Idle Timeout	Specify a duration of idle time after which the guest portal will timeout.
Login Password Retry Lockout	Specify number of incorrect login attempts before the user account is locked.

V-5-7-1. Add/Edit Guest Portal

Add a guest portal or edit an existing guest portal for use with the guest network.

Guest Portal Settings	
Name	GuestPortalPL
Description	PLOfficeTestGuestPortal
Guest Portal Type	Dynamic Users ▼
Authentication Server	Local Database ▼
Front Desk User Group	managerPL ▼
Front Desk Generation URL	http://192.168.8.37/frontdesk.html
Front Desk Printout Message	Edit
Authentication User Group	guestGroupPL ▼
Landing Page	☐ Redirect to the original URL ☒ Promotion URL http:// ▼ www.edimax.pl

Guest Portal Settings	
Name	Edit the name of the guest portal for reference.
Description	Enter a description of the guest portal for reference.
Guest Portal Type	Select a guest portal type. Refer below for more information about available types.
Authentication Server	Select an authentication server: Local Database is the default setting.
Front Desk User Group	Select a user group for front desk access.
Front Desk Generation URL	Displays the URL of your Front Desk page. See below for more information.
Front Desk Printout Message	Edit the content of Front Desk printout ticket. Refer below for more information.
Authentication User Group	Select a user group for login to the guest network.
Landing Page	Specify a landing page for users after successful login.

V-5-7-1-1. Front Desk URL

Go to this URL in a web browser and members of the **Front Desk User Group** can login to create guest accounts, set expiry limits and printout tickets.



Guest Portal Type Dynamic must be selected to use Front Desk.

Guest Portal Settings	
Name	GuestPortalPL
Description	PLOfficeTestGuestPortal
Guest Portal Type	Dynamic Users ▼
Authentication Server	Local Database ▼
Front Desk User Group	managerPI ▼
Front Desk Generation URL	http://192.168.8.37/frontdesk.html
Front Desk Printout Message	Edit
Authentication User Group	guestGroupPL ▼
Landing Page	☐ Redirect to the original URL ☒ Promotion URL http:// ▼ www.edimax.pl

1. Login with an account from the **Front Desk User Group** (NMS Settings → Users).



Front Desk Login

Username

Password

2. The **Guest Account Wizard** allows you to setup a new user account and configure the valid period & SSID, or upload a bulk guest list in .csv format. Click **Next** to continue.



Logout | Global (English) ▼

Guest Account Wizard Guest Account Monitor

Generate Method ☒ Manual ☐ Profile

Valid Period Days ▼

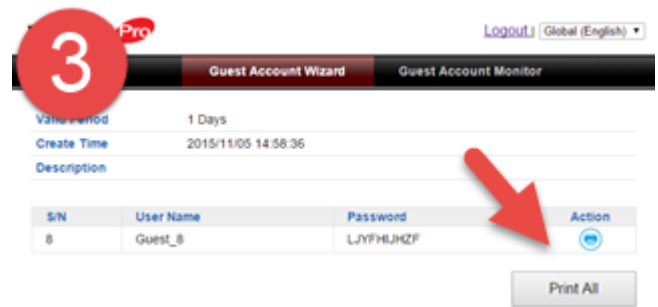
SSID

Account Number

Guest #1 Name Password

Description

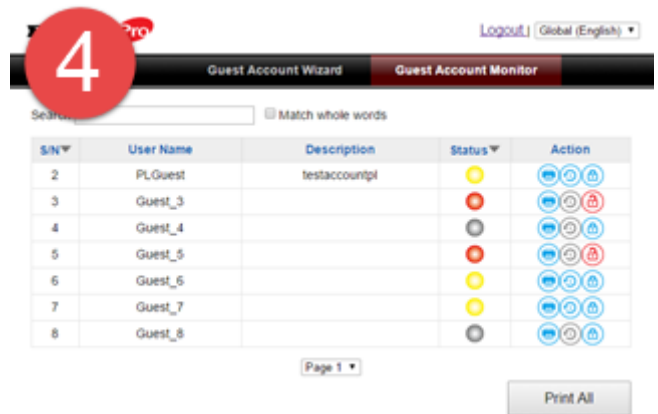
3. A summary of the new account(s) is displayed with quick links to print tickets for individual or all new accounts.



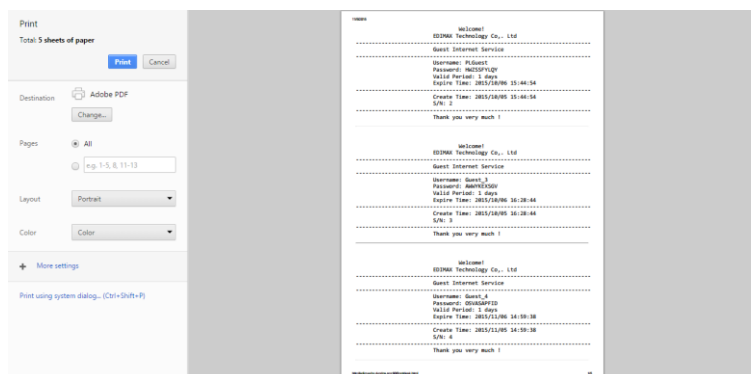
4. The **Guest Account Monitor** displays all guest accounts along with status and quick action icons to print, revive expired accounts or lock/unlock (disable/enable) accounts.

Yellow: Expired
Red: Locked
Grey: Logged out
Green: Active


Mouseover a status or action icon for a description, and use the arrows to reorder the list according to S/N or Status.



Anytime you choose to print account(s) your browser will open a print dialog box where you can select your print destination and configure print settings as usual:



V-5-7-1-2. Front Desk Printout

Edit and preview the content of the Front Desk printout in the text box using the variables listed in the Definition Table. E.g. (USERNAME) will display on the printout as the specified username.



Guest Portal Type Dynamic must be selected to use Front Desk.

Front Desk User Group	managerPL ▼
Front Desk Generation URL	http://192.168.8.37/frontdesk.html
Front Desk Printout Message	Edit
Authentication User Group	guest groupPL ▼
Landing Page	☐ Redirect to the original URL ☒ Promotion URL http:// ▼

Definition Table

Symbol	Description
{SSID}	Suggest SSID of Captive Portal user
{USERNAME}	Name of Captive Portal user
{PASSWORD}	Password of Captive Portal user
{PERIOD}	The valid access time of Network Service.
{EXPIRETIME}	The expire time of user account
{CREATETIME}	The create time of user account
{SN}	Serial number of user account

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

Printout Content

Welcome!
EDIMAX Technology Co., Ltd

Guest Internet Service

SSID: {SSID}
Username: {USERNAME}
Password: {PASSWORD}
Valid Period: {PERIOD}
Expire Time: {EXPIRETIME}

Create Time: {CREATETIME}
S/N: {SN}

Thank you very much !

V-5-7-1-3. Guest Portal Type

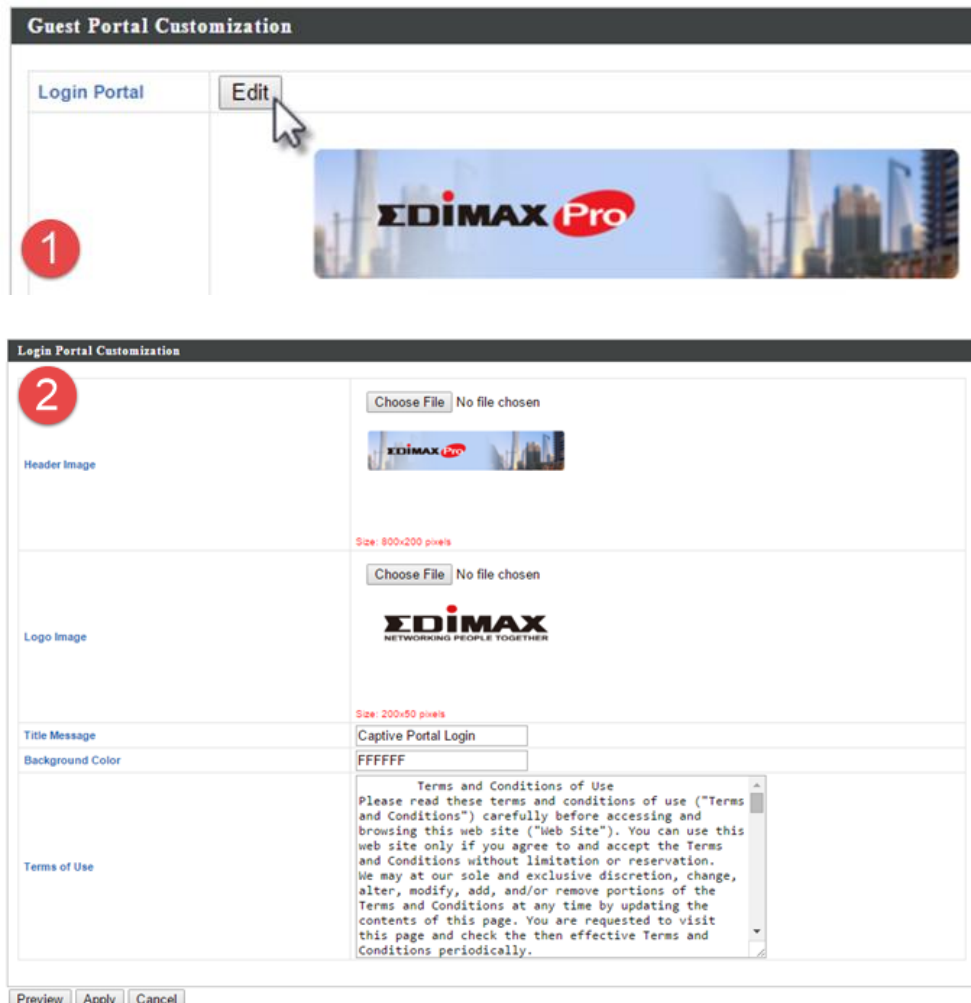
Four types of guest portal are available from the drop down menu:

Name	GuestPortalPL
Description	PLOfficeTestGuestPortal
Guest Portal Type	Dynamic Users ▼
Authentication Server	Free
Front Desk User Group	Service Level Agreement
Front Desk Generation URL	Static Users
	Dynamic Users

- | | |
|--------------------------------|--|
| Free | Redirects users to the specified landing page, with no user login required. |
| Service Level Agreement | Requires users to accept terms and conditions, with no user login required. |
| Static Users | Requires user login and accept terms and conditions. Users must be created in Edimax NMS at NMS Settings → Users . Front Desk is not used. |
| Dynamic Users | Requires user login and accept terms and conditions. Allows Front Desk to create user accounts in addition to Edimax NMS. |

V-5-7-1-4. Guest Portal Customization

Guest portal customization varies according to guest portal type. Click **Edit** to make changes.



Guest Portal Customization

Login Portal **Edit**

1

Login Portal Customization

2

Header Image

Choose File No file chosen

Size: 800x200 pixels

Logo Image

Choose File No file chosen

Size: 200x50 pixels

Title Message

Captive Portal Login

Background Color

FFFFFF

Terms of Use

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

Preview Apply Cancel

Login Portal Settings	
Header Image	Select an 800 x 200 header image.
Logo Image	Select a 200 x 50 logo image.
Title Message	Enter a title message for the guest portal page.
Background Color	Specify a background color as a HEX value.
Terms of Use	Enter your terms of use.

V-5-8. Zone Edit

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

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

Search ☐ Match whole words

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



Zone Edit

Search
☐ Match whole words

541674 bytes Available (655360 bytes Total)

☐	Name/Location	Map	Map Size	Number of APs
☐	Default		113686 bytes	10

Add Edit Clone Delete Selected Delete All

Add/Edit Zone

Upload Zone Image

Map Image File

選擇檔案 未選擇任何檔案

Upload



Member(s) Settings

Name/Location

Description

Member(s)

Search

☐ Match whole words

	MAC Address	Device Name	Model	Status
☐	System Default			
☐	74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	
☐	74:DA:38:27:1B:54	AP74DA38271B54	CAP1200	
☐	74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	
☐	74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	
☐	74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	
☐	Wizard AP Group 2			
☐	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	
☐	74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	
☐	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	
☐	74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	
☐	74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	

Upload Zone Image	
Choose File	Click to locate an image file to be displayed as a map in the Zone Plan feature. Typically a floor plan image is useful.
Zone Setting	
Name/Location	Enter a name of the zone/location.
Description	Enter a description of the zone/location for reference.
Members	Assign access points to the specified zone/location for use with the Zone Plan feature.

86

V-5-9. Schedule

You can define schedules according to day, start time and end time - and group multiple schedules together into schedule groups.

Schedule groups can be assigned to **WLANs**, **WLAN Groups** & **Guest Network** at **NMS Settings → WLAN** and **NMS Settings → Guest Network**.

Schedule

Search ☐ Match whole words

☐	Name	Day of week	Time
☐	Office	Mon,Tue,Wed,Thu,Fri,	08:30-19:30

Add Edit Delete Selected Delete All

Schedule Groups

Search ☐ Match whole words

☐	Group Name	Schedule members	Schedule member list
☐	Office	1	Office

Add Edit Delete Selected Delete All

Add/Edit Schedule

Use the checkboxes and drop-down menus to setup your schedule.

Schedule Settings

Name Office

Description Office HQ Mon - Fri

Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
☐	☒	☒	☒	☒	☒	☐

Start Time 08 : 30 End Time 19 : 30

Add/Edit Schedule Group

Schedule Group Settings					
Name	Office				
Description					
	Search ☐ Match whole words				
Members	<table border="1"> <thead> <tr> <th>☐</th> <th>Name</th> </tr> </thead> <tbody> <tr> <td>☒</td> <td>Office</td> </tr> </tbody> </table>	☐	Name	☒	Office
☐	Name				
☒	Office				

WLAN Group Settings	
Name	Edit the schedule group name.
Description	Enter a description of the schedule group for reference.
Members	Select individual schedules to include in the schedule group using the checkboxes.

V-5-10. Device Monitoring

Device monitoring enables you to specify and monitor the status any IP devices on the network such as IP cameras. The description and status of each device is displayed in the table.

Device Monitoring

Search

☐ Match whole words

☐	Device IP	Description	Status
☐	192.168.8.47	IR-113E	

Add

Edit

Delete Selected

Delete All

Add or **Edit** IP devices by entering the IP address.

Device Monitoring

Add IP Address

Add

Reset

Devices List

Device IP	Description	Delete
192.168.8.47	IR-113E	

V-5-11. Firmware Upgrade

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

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

Firmware Upgrade

Update firmware from

☒ Local
 ☐ External FTP Server

Firmware File

No file selected.

Timeout

Seconds

Firmware Name	Firmware Version	NMS Version	Model	Size (bytes)
[Local Firmware]	1.3.12	1.0.2.0	CAP1200	9076864

Access Point Group

	Group Name	MAC Address	Device Name	Model	IP Address	Status	Firmware Version	NMS Version	Progress
	System Default (10)								
☐		74:DA:38:27:1B:54	AP74DA38271B54	CAP1200	192.168.2.124		1.3.12	1.0.2.0	0%
☐		74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	192.168.2.102		1.3.11	1.0.2.0	0%
☐		74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	192.168.2.120		1.3.12	1.0.2.0	0%
☐		74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	192.168.2.118		1.3.12	1.0.2.0	0%
☐		74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	192.168.2.110		1.3.12	1.0.2.0	0%
☐		80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	192.168.2.105		1.3.11	1.0.2.0	0%
☐		74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	192.168.2.121		1.3.12	1.0.2.0	0%
☐		74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	192.168.2.126		1.3.12	1.0.2.0	0%
☐		74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	192.168.2.127		1.3.12	1.0.2.0	0%
☐		74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	192.168.2.128		1.3.12	1.0.2.0	0%

V-5-12. Advanced

V-5-12-1. System Security

Configure the NMS system name and security key for communication between AP Controller and Managed APs.

System Security	
NMS System Name	administrator
NMS Security Key	1234567890123456 (8~16 Characters)
Apply	

V-5-12-2. Date & Time

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

Date and Time Settings						
Local Time	2015	Year	Nov	Month	6	Day
	16	Hours	13	Minutes	23	Seconds
Acquire Current Time from Your PC						
NTP Time Server						
Use NTP	☐ Enable					
Server Name	User-Defined					
Update Interval	24 (Hours)					
Time Zone						
Time Zone	(GMT+08:00) Taipei, Taiwan					

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

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

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

V-6. Local Network

V-6-1. Network Settings

V-6-1-1. LAN-Side IP Address

The “LAN-side IP address” page allows you to configure your AP Controller on your Local Area Network (LAN). You can enable the access point to dynamically receive an IP address from your router’s DHCP server or you can specify a static IP address for your access point, as well as configure DNS servers. You can also set your AP Controller as a DHCP server to assign IP addresses to other devices on your LAN.



The AP Controller’s default IP address is 192.168.2.1



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

LAN-side IP Address	
IP Address Assignment	Static IP Address ▼
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.3
Primary DNS Address	8.8.8.8
Secondary DNS Address	0.0.0.0

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

Static IP Address	
IP Address	Specify the IP address here. This IP address will be assigned to your access point and will

	replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank.
Primary DNS Address	For static IP users, the default value is blank.
Secondary DNS Address	For static IP users, the default value is blank.

LAN-side IP Address

IP Address Assignment	DHCP Client
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	From DHCP 192.168.2.3
Primary DNS Address	From DHCP 8.8.8.8
Secondary DNS Address	From DHCP 0.0.0.0

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

LAN-side IP Address	
IP Address Assignment	DHCP Server
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
IP Address Range	192.168.2.120 ~ 192.168.2.240
Domain Name	APC500
Lease Time	One Hour
Default Gateway	192.168.2.3
Primary DNS Address	8.8.8.8
Secondary DNS Address	0.0.0.0

DHCP Server Static IP Address			
Index	MAC Address	IP Address	Action
1			Add

DHCP Client List			
Index	MAC Address	IP Address	Lease Time
No DHCP Client			

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

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

DHCP Server Static IP Address	
MAC Address	Enter the MAC address of the network device

	to be assigned a static IP address.
IP Address	Specify the IP address to assign the device.
Add	Click to assign the IP address to the device.

V-6-1-2. LAN Port Settings

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

Wired LAN Port Settings				
Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
LAN0	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼
LAN1	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼
LAN2	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼
LAN3	Enabled ▼	Auto ▼	Enabled ▼	Enabled ▼

Wired LAN Port	Identifies LAN port 0 - 4.
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.

V-6-1-3. VLAN

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



VLAN IDs in the range 1 – 4095 are supported.

VLAN Interface		
Wired LAN Port	VLAN Mode	VLAN ID
LAN0	Untagged Port ▼	1
LAN1	Untagged Port ▼	1
LAN2	Untagged Port ▼	1
LAN3	Untagged Port ▼	1

Management VLAN	
VLAN ID	1

VLAN Interface	
Wired LAN Port/Wireless	Identifies LAN port 1 or 2 and wireless SSIDs (2.4GHz or 5GHz).
VLAN Mode	Select “Tagged Port” or “Untagged Port” for specified 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.

V-7. Local Settings

V-7-1. System Settings

V-7-1-1. System Information

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

System		
Model	APC500	
Product Name	AP00AABCCDD10	
Uptime	0 day 04:11:39	
System Time	2015/11/06 16:16:35	
Boot from	Internal memory	
Firmware Version	1.3.1	
MAC Address	00:AA:BB:CC:DD:10	
Management VLAN ID	1	
IP Address	192.168.2.1	
Default Gateway	192.168.2.3	
DNS	---	
DHCP Server	---	
Internal Storage	Not detected	

Wired LAN Port Settings		
Wired LAN Port	Status	VLAN Mode/ID
LAN0	Disconnected (---)	Untagged Port / 1
LAN1	Disconnected (---)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1
LAN3	Connected (100 Mbps Full-Duplex)	Untagged Port / 1

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 V-6-1-3. VLAN

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

V-7-1-2. Log

This information is useful for network administrators. Displays a detailed information log of users and activity on the network: *ID, Date and Time of entry, Category of entry, Severity, Users, Event/Activities details.*



When the log is full, old entries are overwritten.

All Events/Activities

Search

☐ Match whole words

ID ▼	Date and Time	Category ▲	Severity ▲	Users ▲	Events/Activities
680	2015/11/06 15:22:57	NMS	Low	admin	Managed AP(74:DA:38:03:23:9C) connect successfully
679	2015/11/06 15:22:54	NMS	Low	admin	Managed AP(80:1F:02:CC:DD:10) connect successfully
678	2015/11/06 15:22:25	NMS	Low	admin	Managed AP(74:DA:38:03:23:9C) was disconnected
677	2015/11/06 15:22:22	NMS	Low	admin	Managed AP(80:1F:02:CC:DD:10) was disconnected
676	2015/11/06 15:21:50	NMS	Low	admin	Managed AP(74:DA:38:27:1B:54) connect successfully
675	2015/11/06 15:21:33	NMS	Low	admin	Managed AP(74:DA:38:31:27:B8) was disconnected
674	2015/11/06 15:21:30	NMS	Low	admin	Managed AP(74:DA:38:31:27:BA) was disconnected
673	2015/11/06 15:21:24	NMS	Low	admin	Managed AP(74:DA:38:31:27:BB) was disconnected
672	2015/11/06 15:20:42	NMS	Low	admin	Managed AP(80:1F:02:CC:DD:10) was disconnected
671	2015/11/06 15:19:36	NMS	Low	admin	Managed AP(74:DA:38:03:23:9C) was disconnected
670	2015/11/06 15:19:33	NMS	Low	admin	Managed AP(74:DA:38:27:1B:54) was disconnected
669	2015/11/06 15:19:21	NMS	Low	admin	Managed AP(00:AA:BB:CC:DD:30) was disconnected
668	2015/11/06 15:19:18	NMS	Low	admin	Managed AP(74:DA:38:27:1B:42) was disconnected
667	2015/11/06 15:19:12	NMS	Low	admin	Managed AP(00:AA:BB:CC:DD:70) was disconnected
666	2015/11/06 15:19:00	NMS	Low	admin	Managed AP(74:DA:38:00:00:24) was disconnected
665	2015/11/06 15:18:47	NMS	Low	admin	Managed AP(74:DA:38:03:23:9C) connect successfully
664	2015/11/06 15:18:46	NMS	Low	admin	Managed AP(00:AA:BB:CC:DD:30) connect successfully
663	2015/11/06 15:18:46	NMS	Low	admin	Managed AP(80:1F:02:CC:DD:10) connect successfully
662	2015/11/06 15:18:45	NMS	Low	admin	Managed AP(00:AA:BB:CC:DD:70) connect successfully
661	2015/11/06 15:18:15	NMS	Low	admin	Managed AP(74:DA:38:03:23:9C) was disconnected

Save

Clear

Refresh

< 680-661 >

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

V-7-2. Management

V-7-2-1. 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 V-7-3-4. Factory Default for how to reset the access point.

Account to Manage This Device	
Administrator Name	admin
Administrator Password	 (4-32Characters)
	 (Confirm)
Apply	

Advanced Settings	
Product Name	AP00AABBCCDD10
HTTP Port	80 (80, 1024-65535)
HTTPS Port	443 (443, 1024-65535)
Management Protocol	☒ HTTP ☒ HTTPS ☒ TELNET ☐ SSH ☐ SNMP
SNMP Version	v1/v2c ▼
SNMP Get Community	public
SNMP Set Community	private
SNMP Trap	Disabled ▼
SNMP Trap Community	public
SNMP Trap Manager	
Apply	

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.
HTTP Port	Specify a HTTP port for management.
HTTPS Port	Specify a HTTPS port for management.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below). When SNMP is enabled, complete the SNMP fields below.
SNMP Version	Select SNMP version appropriate for your SNMP manager.
SNMP Get Community	Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests.
SNMP Set Community	Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests.
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of network errors.
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (2-128 alphanumeric characters) of the SNMP manager.

HTTP

Internet browser HTTP protocol management interface

HTTPS

Internet browser HTTPS protocol management interface

TELNET

Client terminal with telnet protocol management interface

SSH

Client terminal with SSH protocol version 1 or 2 management interface

SNMP

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

V-7-2-2. Date and Time

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

Date and Time Settings						
Local Time	2015	Year	Nov	Month	6	Day
	16	Hours	17	Minutes	37	Seconds
Acquire Current Time from Your PC						

NTP Time Server	
Use NTP	☒ Enable
Server Name	
Update Interval	24 (Hours)

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

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

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

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

V-7-2-3. Syslog Server

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

Syslog Server Settings

Transfer Logs
☐ Enable Syslog Server

Syslog E-mail Settings

E-mail Logs

E-mail Subject

SMTP Server Address

SMTP Server Port

Sender E-mail

Receiver E-mail

Authentication

☐

Disable

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

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

	account name.
Password	When authentication is used above, enter the password.

V-7-2-4. I'm Here

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

Duration of Sound	
Duration of Sound	10 (1-300 seconds)



The buzzer is loud!

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

V-7-3. Advanced

V-7-3-1. LED Settings

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

LED Settings	
Power LED	☒ On ☐ Off
System LED	☒ On ☐ Off
USB LED	☒ On ☐ Off
LAN 0 LED	☒ On ☐ Off
LAN 1 LED	☒ On ☐ Off
LAN 2 LED	☒ On ☐ Off
LAN 3 LED	☒ On ☐ Off

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

V-7-3-2. 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.



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

Firmware Location	
Update firmware from	☒ a file on your PC

Update Firmware from PC	
Firmware Update File	Browse... No file selected.
Update	



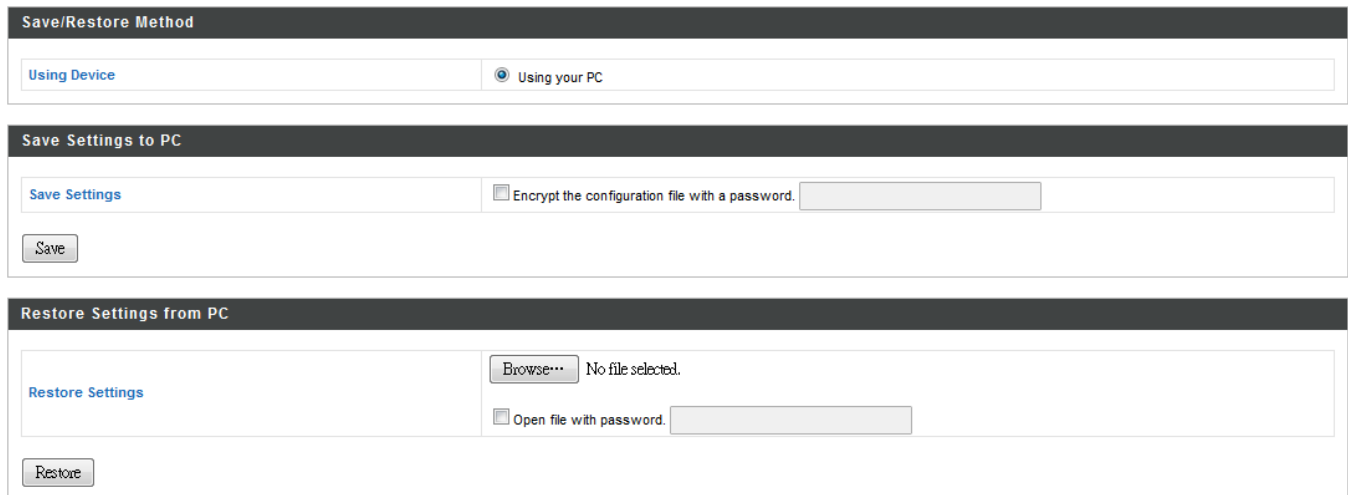
Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.

Update Firmware	Select “a file on your PC” to upload firmware
-----------------	---

From	from your local computer.
Firmware Update File	Click “Browse” to open a new window to locate and select the firmware file in your computer.
Update	Click “Update” to upload the specified firmware file to your access point.

V-7-3-3. 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.

V-7-3-4. Factory Default

If the access point malfunctions or is not responding, then it is recommended that you reboot the device (see **V-7-3-5.**) 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.

This will restore all settings to factory defaults.

Factory Default

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.

V-7-3-5. 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 **V-7-3-4.**). You can reboot the access point remotely using this feature.

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

Reboot

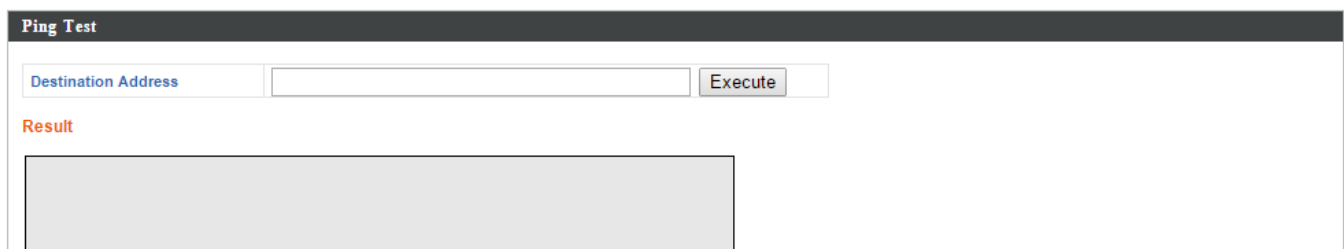
Reboot	Click "Reboot" to reboot the device. A countdown will indicate the progress of the reboot.
---------------	--

V-8. Toolbox

V-8-1. Network Connectivity

V-8-1-1. Ping

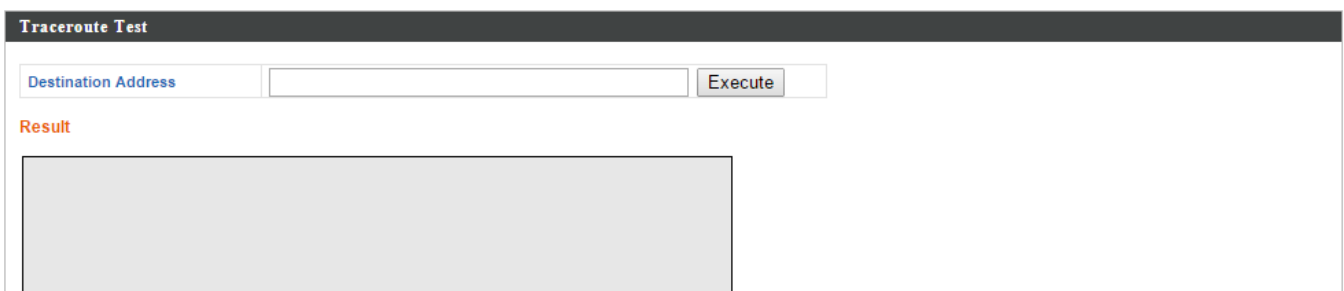
Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.



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

V-8-1-2. Trace Route

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



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

VI. Appendix

VI-1. Configuring your IP address

The AP Controller uses the default IP address **192.168.2.1**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254)**.

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

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



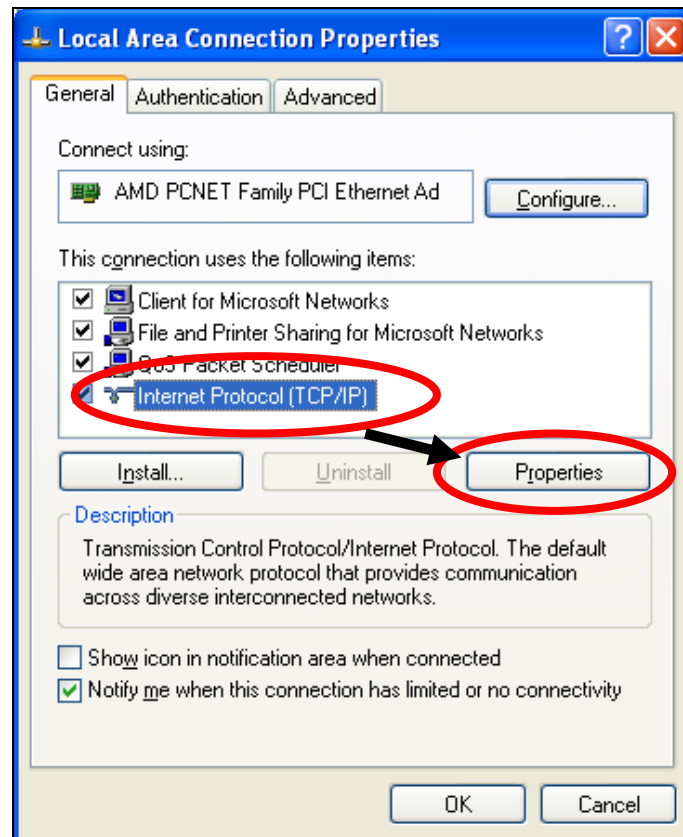
If you changed the AP Controller's IP address, or if your gateway/router uses a DHCP server, ensure you enter the correct IP address. Refer to your gateway/router's settings. Your computer's IP address must be in the same subnet as the AP Controller.



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

VI-1-1. Windows XP

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Double-click the “Network and Internet Connections” icon, click “Network Connections”, and then double-click “Local Area Connection”. The “Local Area Connection Status” window will then appear, click “Properties”.

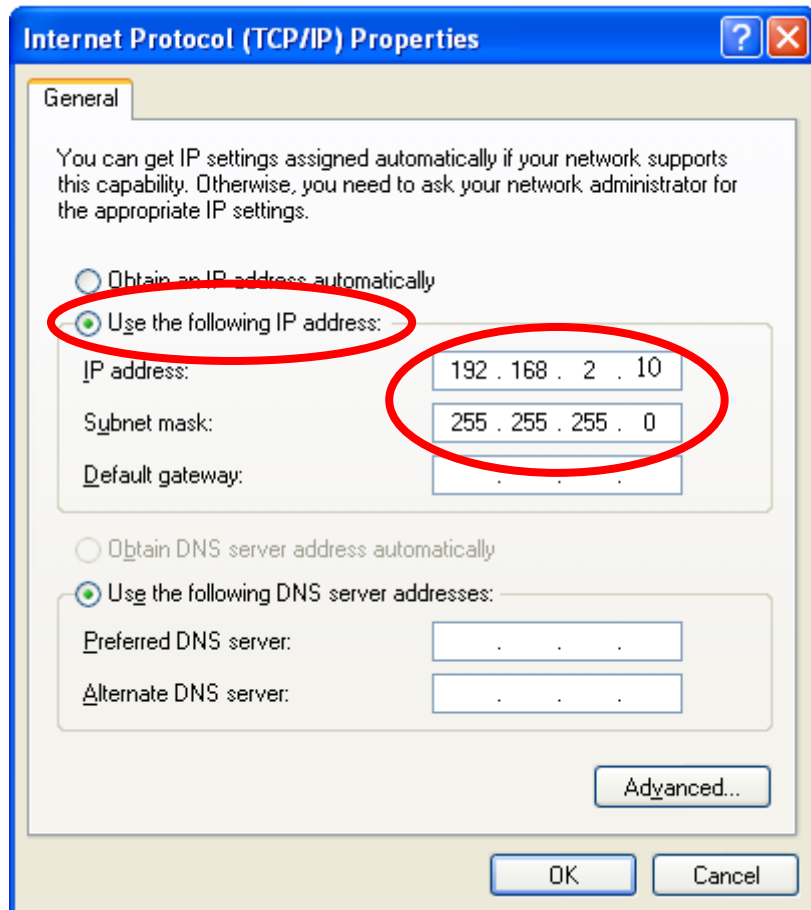


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

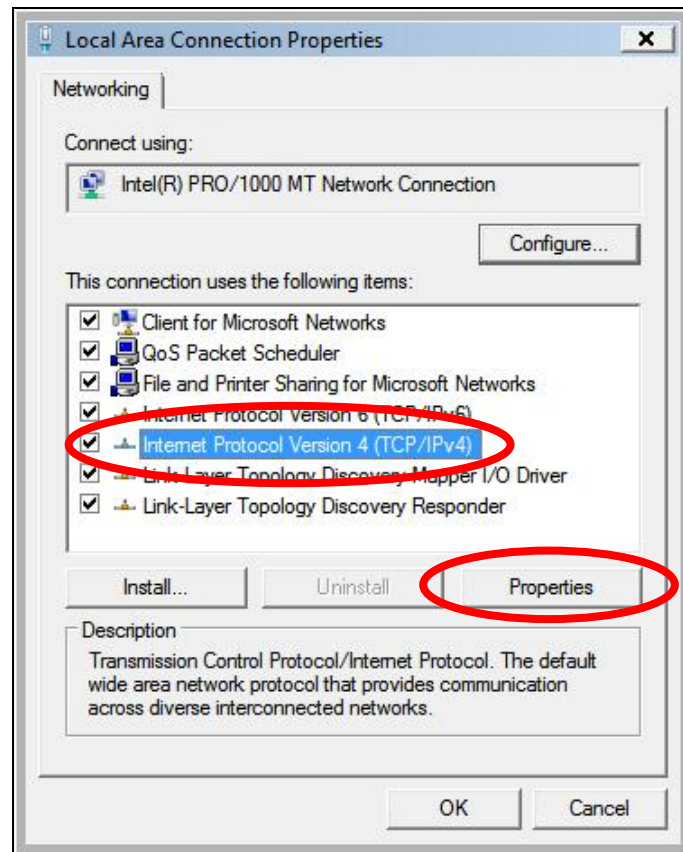
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



VI-1-2. Windows Vista

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

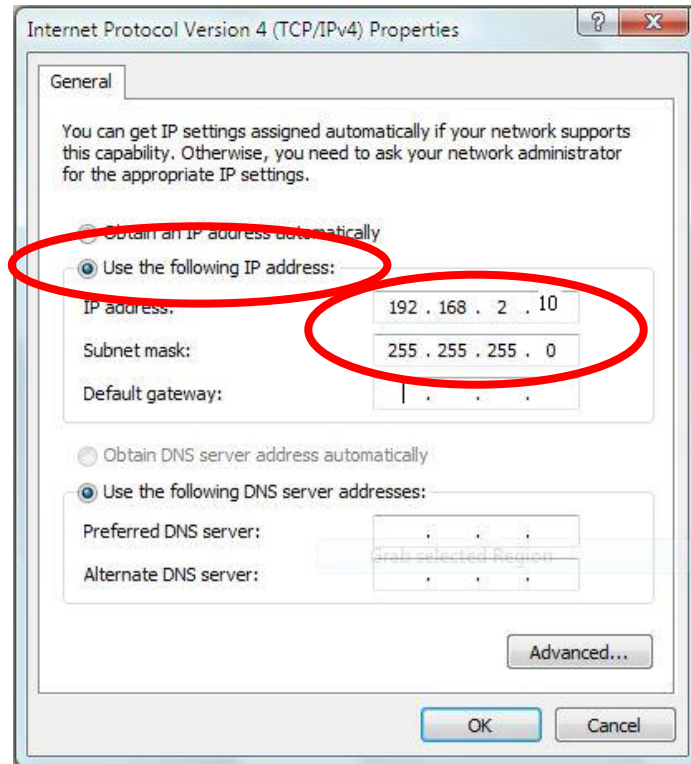


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

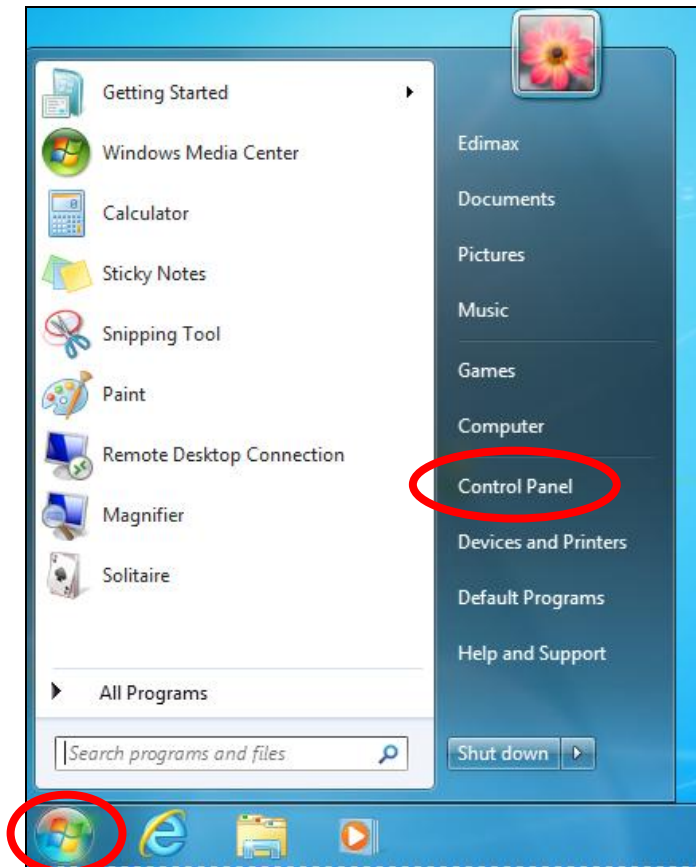
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

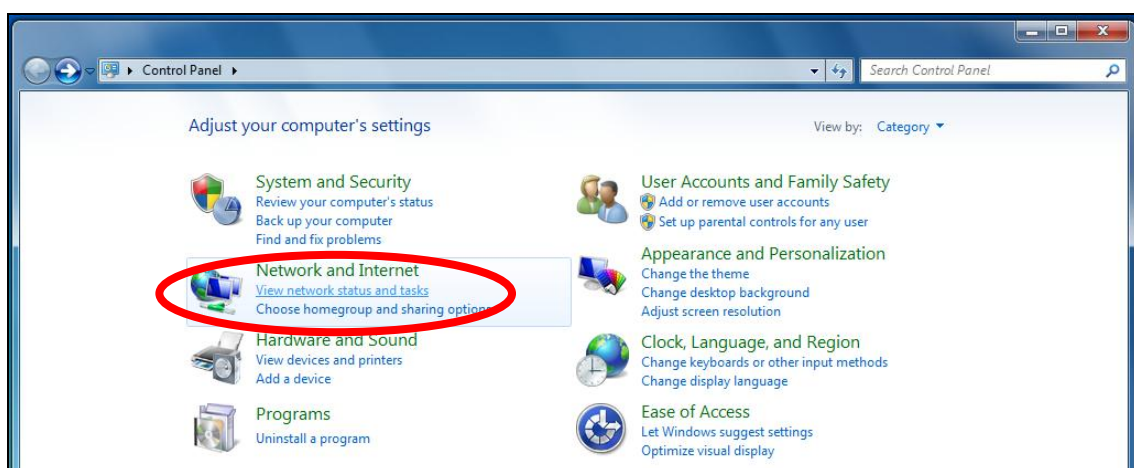


VI-1-3. Windows 7

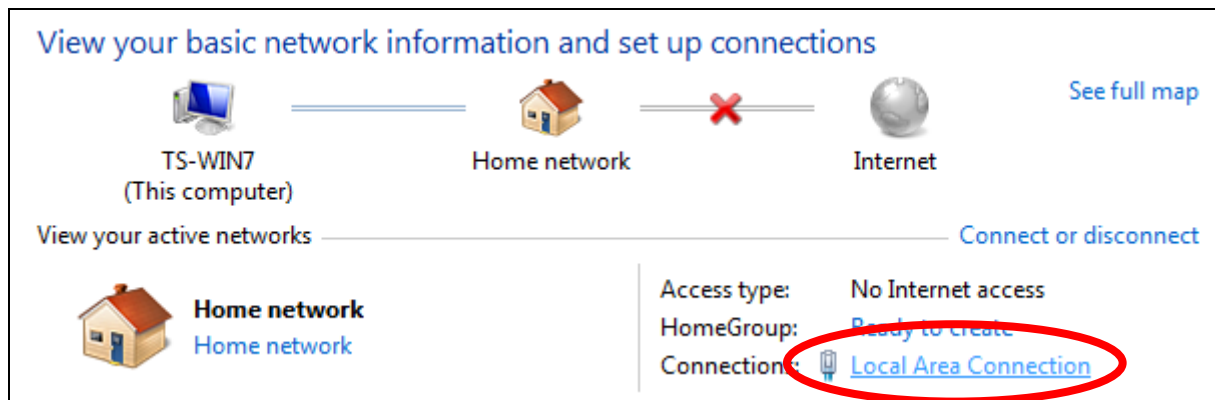
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



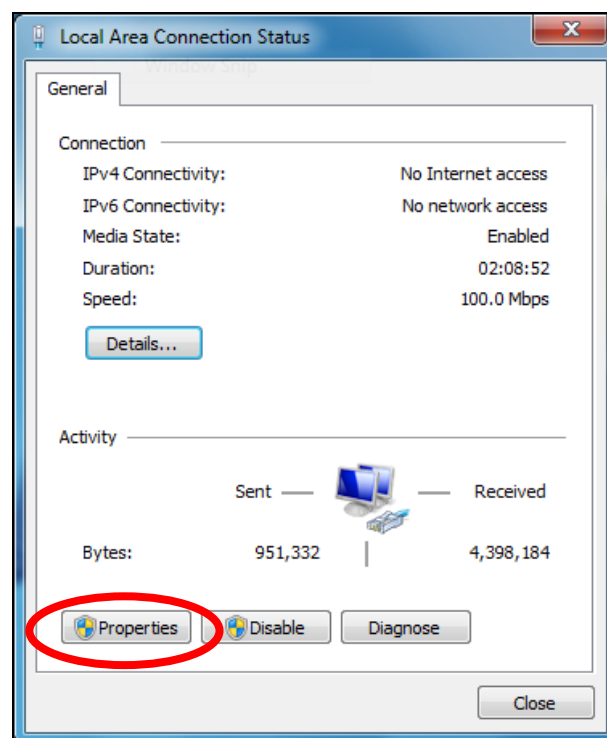
2. Under “Network and Internet” click “View network status and tasks”.



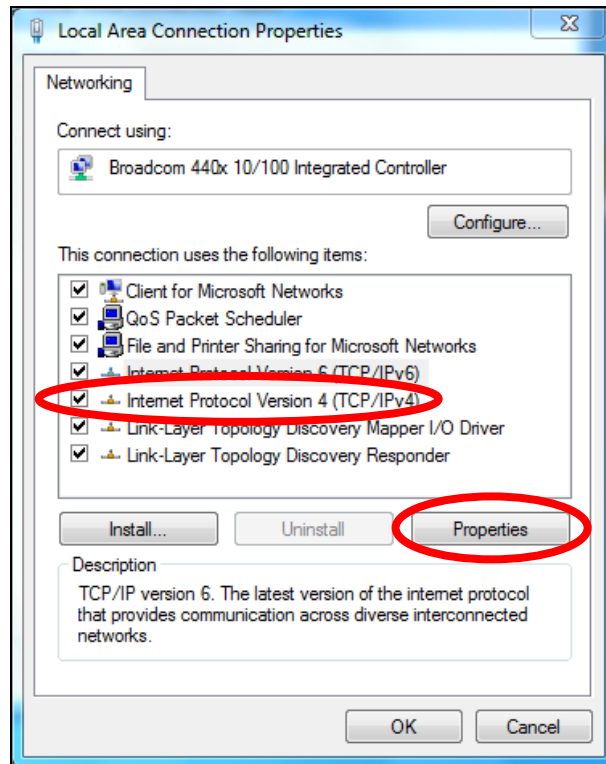
3. Click “Local Area Connection”.



4. Click “Properties”.



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

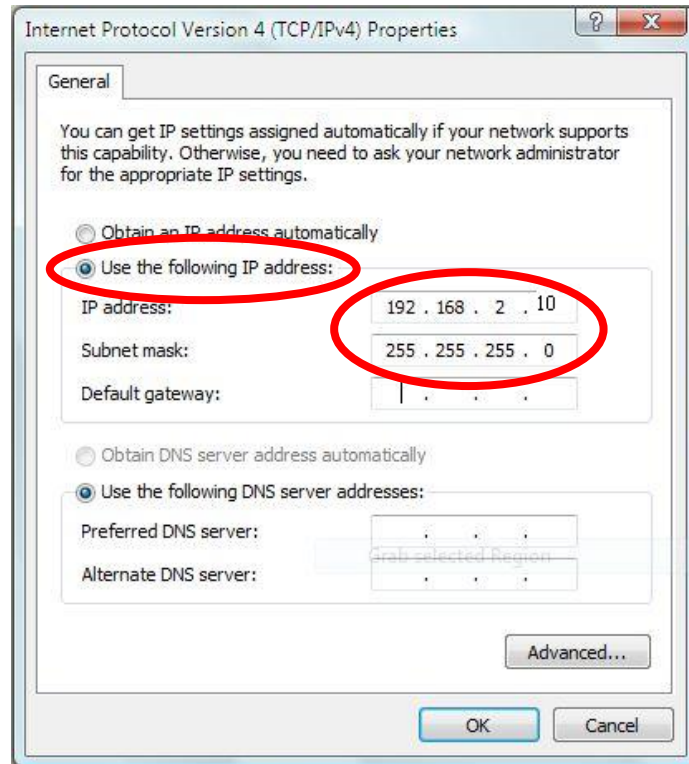


6. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

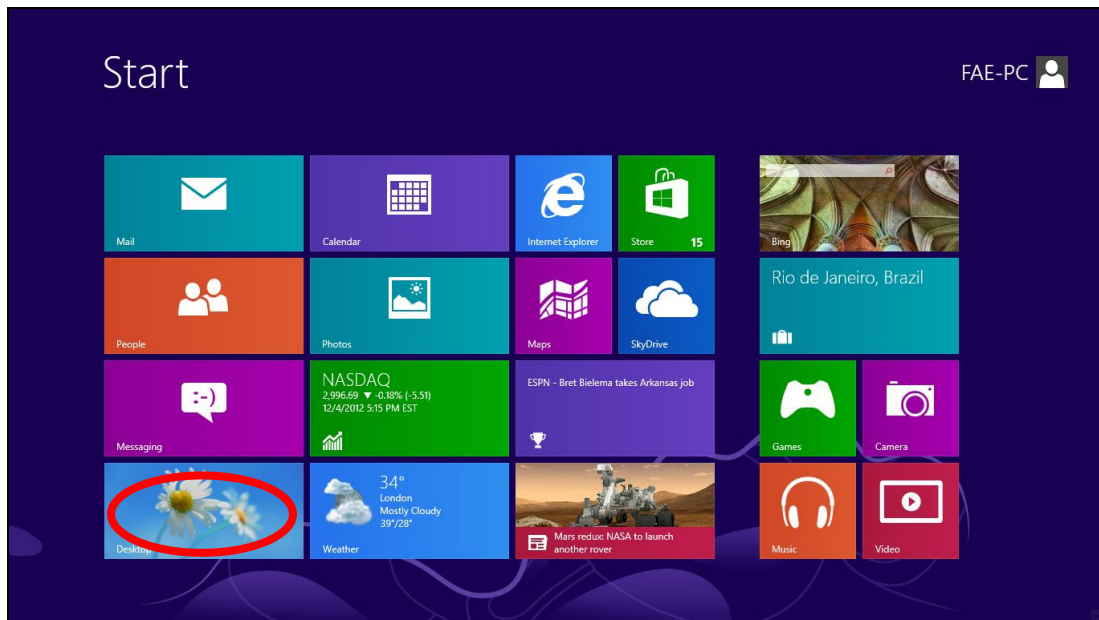
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

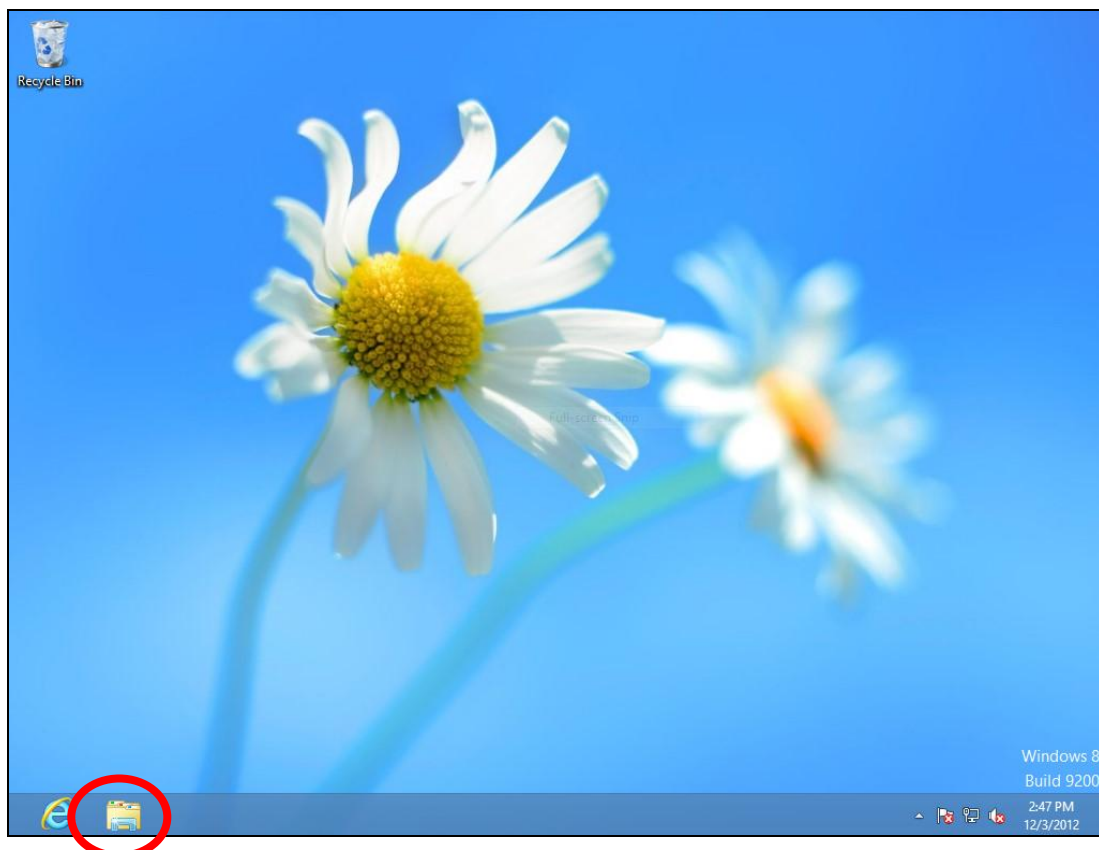


VI-1-4. Windows 8

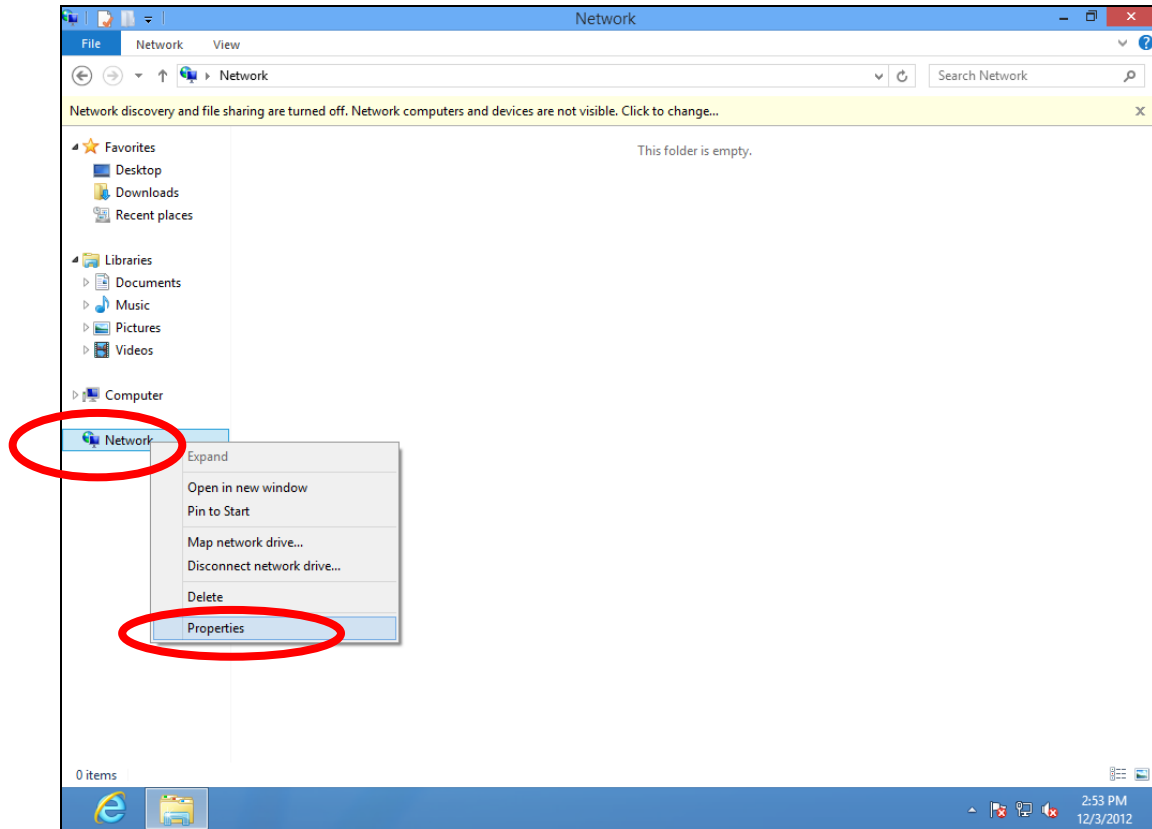
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your cursor to the bottom left of the screen and click.



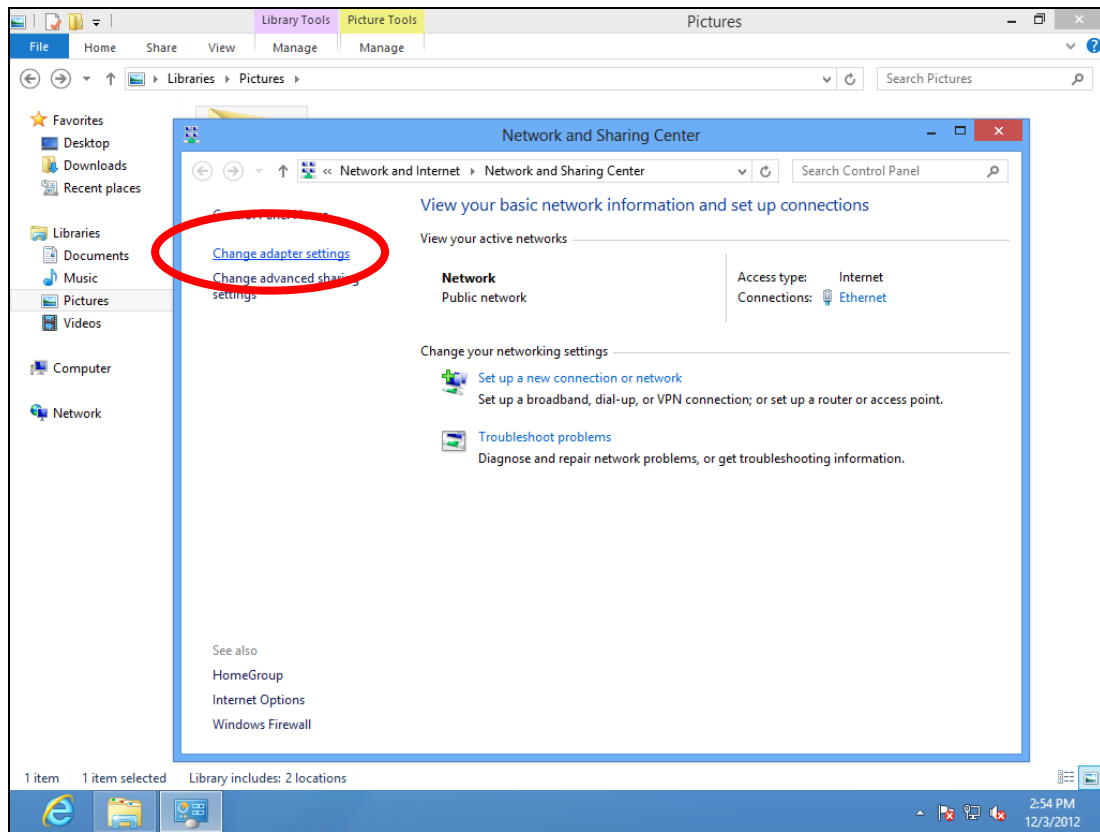
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



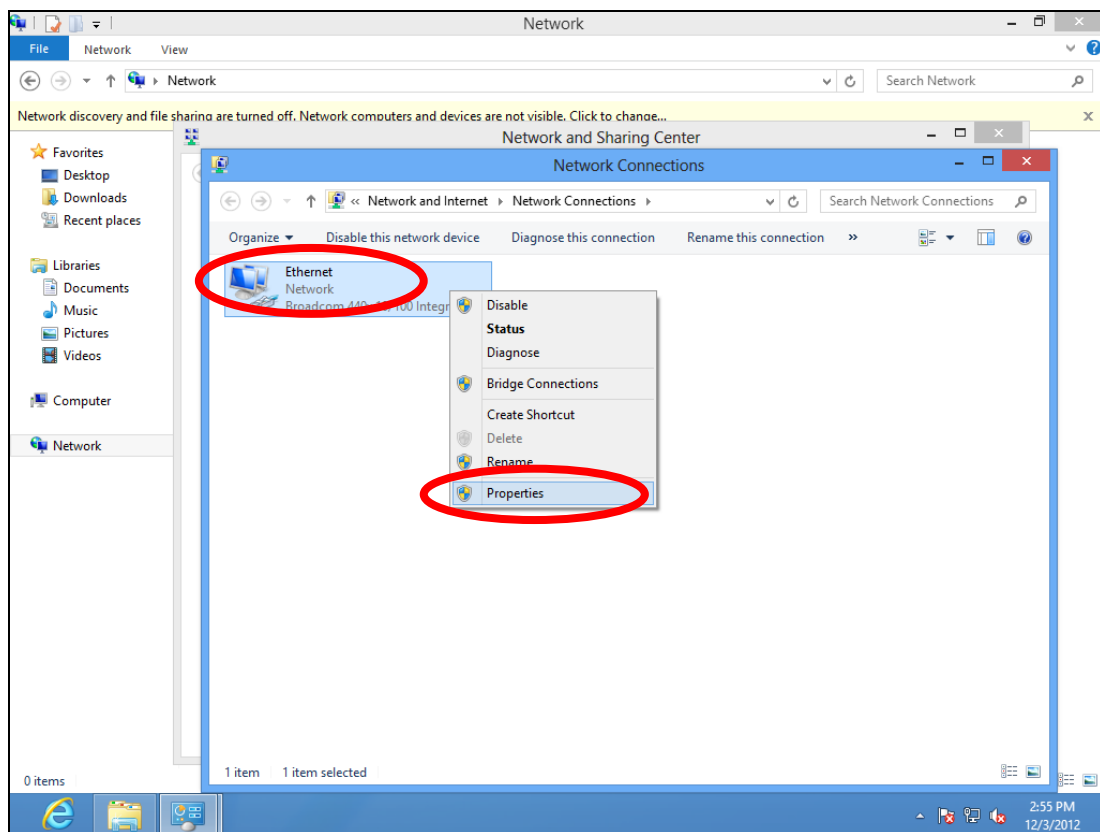
3. Right click “Network” and then select “Properties”.



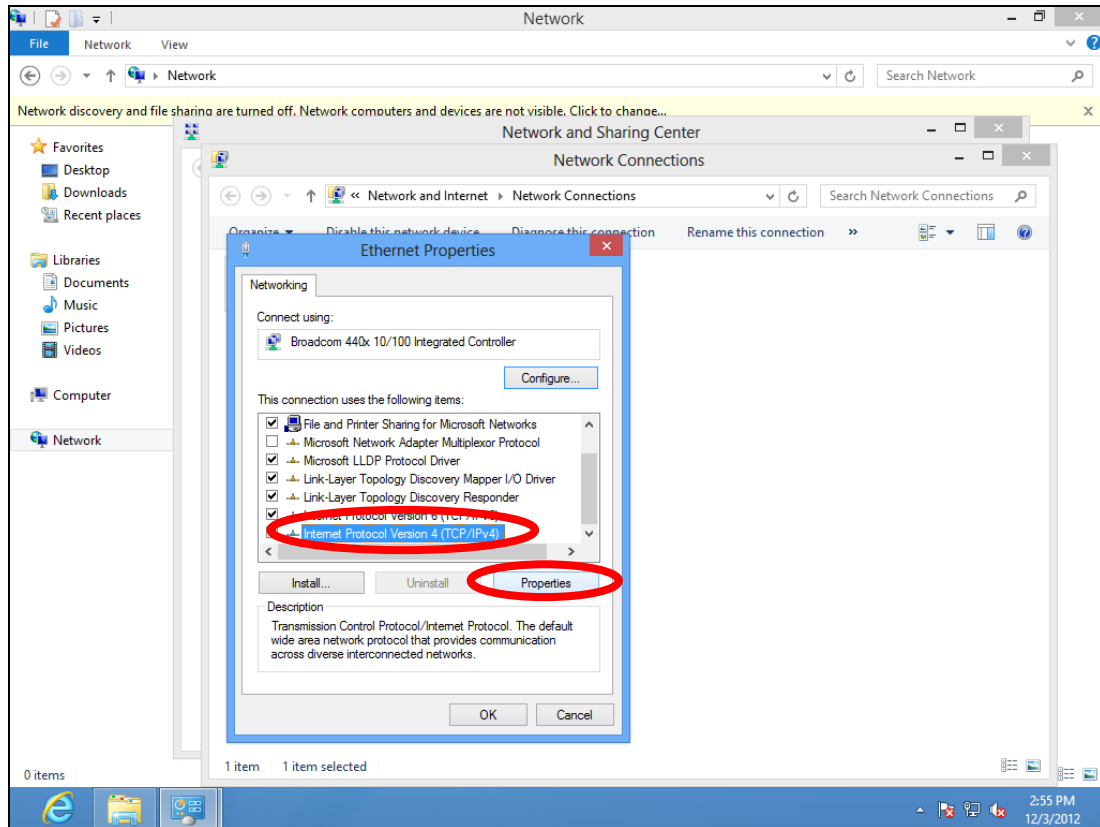
4. In the window that opens, select “Change adapter settings” from the left side.



5. Choose your connection and right click, then select “Properties”.



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



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

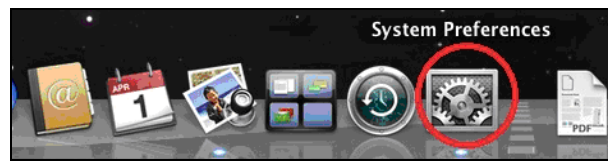
IP address: 192.168.2.10

Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

VI-1-5. Mac

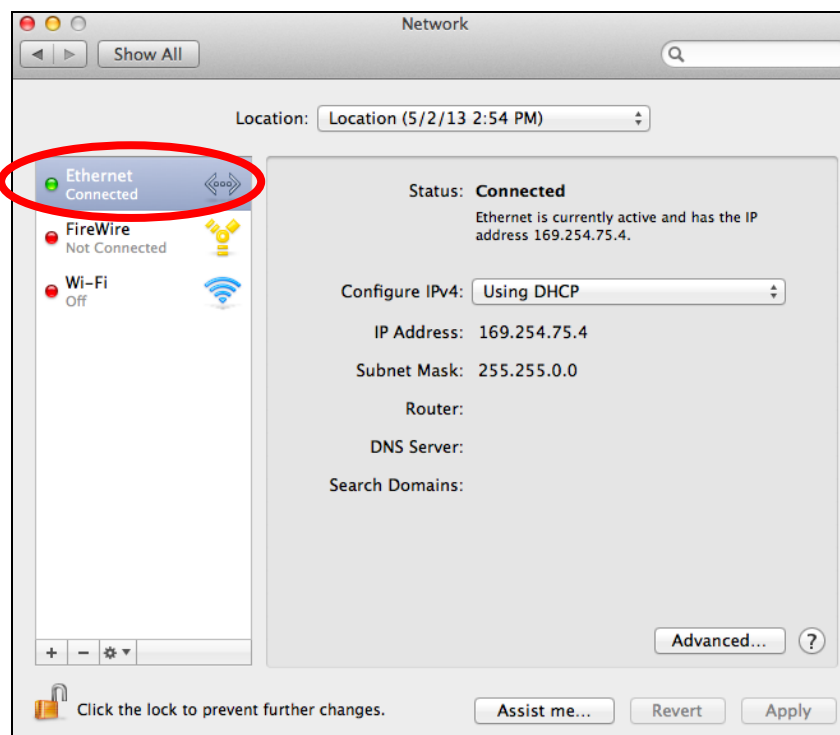
1. Have your Macintosh computer operate as usual, and click on “System Preferences”



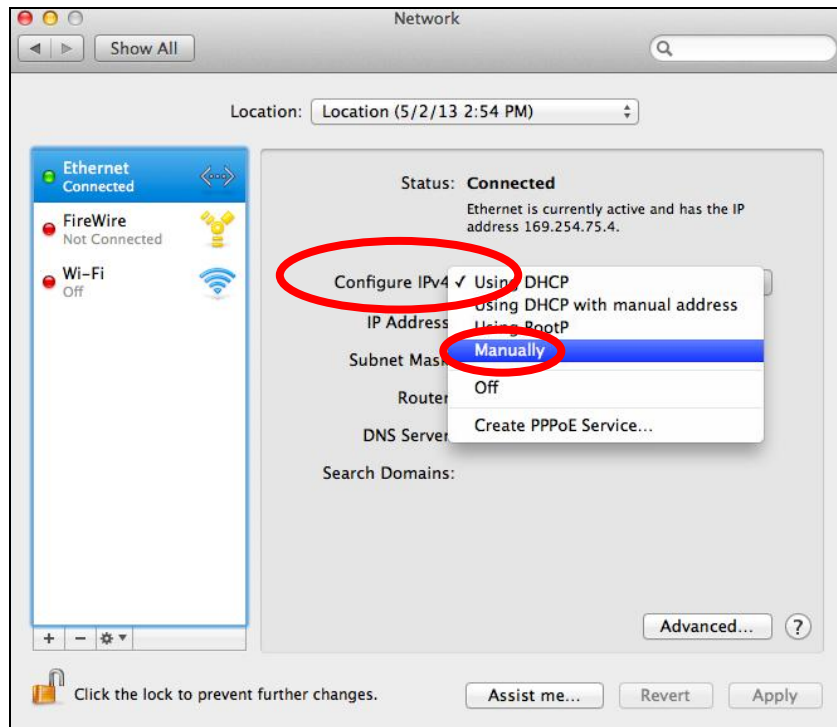
2. In System Preferences, click on “Network”.



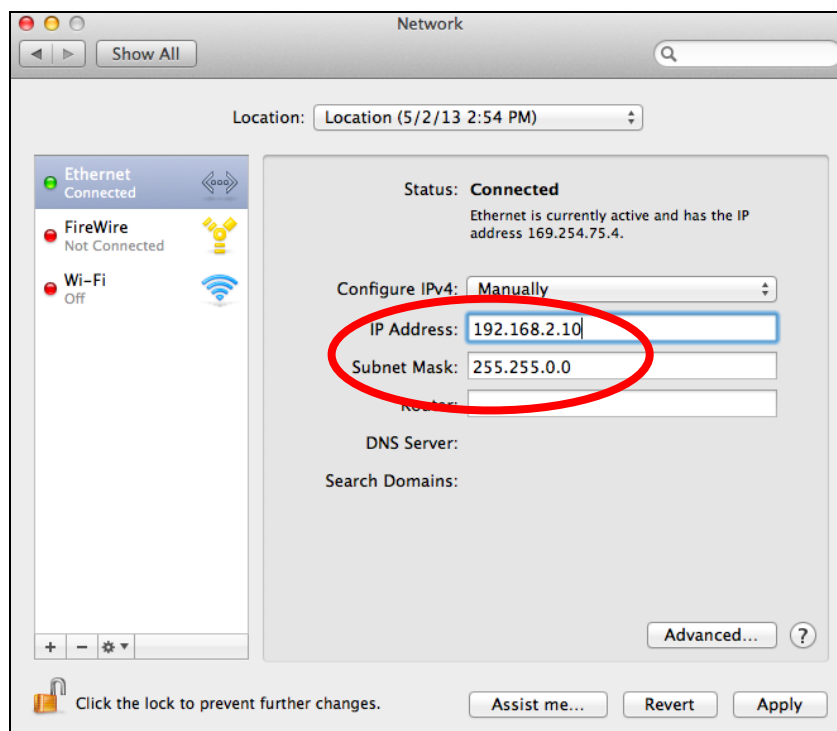
3. Click on “Ethernet” in the left panel.



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



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



VII. Best Practice

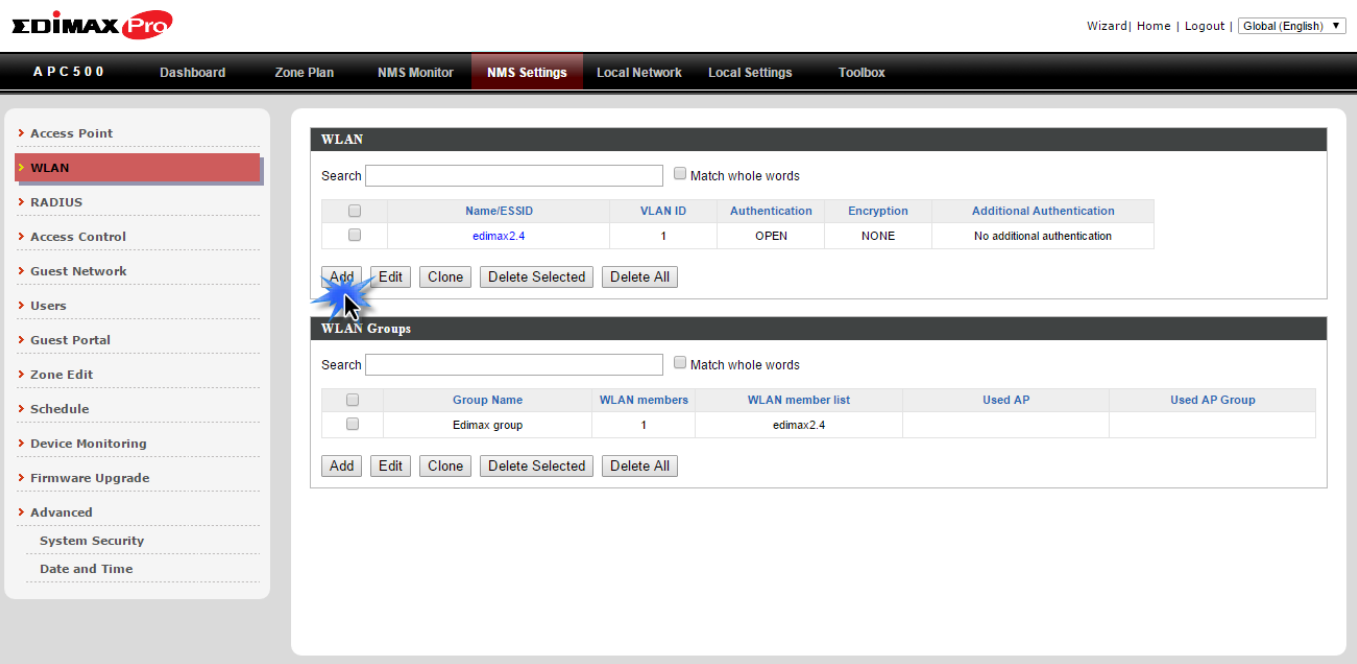
VII-1. How to Create and Link WLAN & Access Point Groups

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

Follow the example below to to:

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

- A.
1. Go to **NMS Settings** → **WLAN** and click “**Add**” in the **WLAN** panel:



2. Enter an SSID name and set authentication/encryption and click “Apply”:

EDIMAX Pro

Wizard | Home | Logout | Global (English) ▼

A P C 5 0 0 Dashboard Zone Plan NMS Monitor **NMS Settings** Local Network Local Settings Toolbox

Access Point
WLAN
RADIUS
Access Control
Guest Network
Users
Guest Portal
Zone Edit
Schedule
Device Monitoring
Firmware Upgrade
Advanced
System Security
Date and Time

WLAN Settings

Name/ESSID	Edimax SSID1
Description	
VLAN ID	1
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
Load Balancing	50 /50

Authentication Method	WPA-PSK ▼
WPA Type	WPA/WPA2 Mixed Mode-PSK ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase ▼
Pre-shared Key	12345678
Additional Authentication	No additional authentication ▼

WLAN Advanced Settings

Smart Handover Settings	
Smart Handover	☐ Enable ☒ Disable
RSSI Threshold	-80 dB

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

Schedule Group	Disable ▼
----------------	-----------

Apply Cancel

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

EDIMAX Pro

Wizard | Home | Logout | Global (English) ▼

A P C 5 0 0 Dashboard Zone Plan NMS Monitor **NMS Settings** Local Network Local Settings Toolbox

Access Point
WLAN
RADIUS
Access Control
Guest Network
Users
Guest Portal
Zone Edit
Schedule
Device Monitoring
Firmware Upgrade
Advanced
System Security
Date and Time

WLAN

Search ☐ Match whole words

☐	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
☐	edimax2.4	1	OPEN	NONE	No additional authentication
☐	Edimax SSID1	1	WPA1PSK/WPA2PSK	TKIP/AES	No additional authentication
☐	Edimax SSID2	1	WPA1PSK/WPA2PSK	TKIP/AES	No additional authentication

Add Edit Clone Delete Selected Delete All

WLAN Groups

Search ☐ Match whole words

☐	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
☐	Edimax group	1	edimax2.4		

Add Edit Clone Delete Selected Delete All

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

The screenshot shows the Edimax Pro NMS Settings page. The left sidebar contains a menu with options: Access Point, WLAN (selected), RADIUS, Access Control, Guest Network, Users, Guest Portal, Zone Edit, Schedule, Device Monitoring, Firmware Upgrade, and Advanced. The main content area is titled 'WLAN Group Settings'. It includes a form with fields for Name (Edimax SSID Group 1) and Description. Below these is a search bar and a checkbox for 'Match whole words'. A table lists members with columns: Name/ESSID, VLAN ID, and Schedule Group. The table has three rows: edimax2.4, Edimax SSID1, and Edimax SSID2. The first row is unchecked, while the other two are checked. Below the table is a red note: '*Schedule Group function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.' At the bottom are 'Apply' and 'Cancel' buttons.

Name/ESSID	VLAN ID	Schedule Group
☐ edimax2.4	1	☐ Override Disable
☒ Edimax SSID1	1	☐ Override Disable
☒ Edimax SSID2	1	☐ Override Disable

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

The screenshot shows the Edimax Pro NMS Settings page with the 'WLAN' and 'WLAN Groups' panels. The 'WLAN' panel has a search bar and a table with columns: Name/ESSID, VLAN ID, Authentication, Encryption, and Additional Authentication. It lists three entries: edimax2.4, Edimax SSID1, and Edimax SSID2. Below the table are buttons: Add, Edit, Clone, Delete Selected, and Delete All. The 'WLAN Groups' panel also has a search bar and a table with columns: Group Name, WLAN members, WLAN member list, Used AP, and Used AP Group. It lists three groups: Edimax group (1 member), Edimax SSID Group 1 (2 members), and Edimax SSID Group 2 (0 members). Below the table are buttons: Add, Edit, Clone, Delete Selected, and Delete All.

Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
☐ edimax2.4	1	OPEN	NONE	No additional authentication
☐ Edimax SSID1	1	WPA1PSK/WPA2PSK	TKIP/AES	No additional authentication
☐ Edimax SSID2	1	WPA1PSK/WPA2PSK	TKIP/AES	No additional authentication

Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
☐ Edimax group	1	edimax2.4		
☐ Edimax SSID Group 1	2	Edimax SSID1 Edimax SSID2		
☐ Edimax SSID Group 2	0			

B.

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

The screenshot displays the EDIMAX Pro NMS Settings interface. The top navigation bar includes links for Wizard, Home, Logout, and Global (English). The main menu on the left lists various settings categories, with 'Access Point' highlighted. The central panel is divided into three sections: 'Access Point', 'Access Point Group', and 'Access Point Settings'.

Access Point Section: This section contains a search bar and a table of access points. The table has columns for MAC Address, Device Name, Model, AP Group, 2.4G Channel, 5G Channel, 2.4G Tx Power, 5G Tx Power, Status, and Action. A blue arrow points to the 'Add' button below the table.

	MAC Address	Device Name	Model	AP Group	2.4G Channel	5G Channel	2.4G Tx Power	5G Tx Power	Status	Action
☐	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	System Default	N/A	N/A	Full	Full		
☐	74:DA:38:27:1B:48	AP74DA38271B48	CAP1200	System Default	N/A	N/A	Full	Full		
☐	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	System Default	N/A	N/A	Full	Full		
☐	74:DA:38:03:23:9C	AP74DA3803239C	WAP1750	System Default	N/A	N/A	Full	Full		
☐	74:DA:38:27:1B:46	AP74DA38271B46	CAP1200	System Default	N/A	N/A	Full	Full		
☐	74:DA:38:27:1B:38	AP74DA38271B38	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:54	AP74DA38271B54	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:40	AP74DA38271B40	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:3E	AP74DA38271B3E	CAP1200	System Default	11	36	Full	Full		
☐	74:DA:38:27:1B:44	AP74DA38271B44	CAP1200	System Default	11	36	Full	Full		

Access Point Group Section: This section contains a search bar and a table of access point groups. The table has columns for Group Name, AP Members, 2.4G WLAN Profile, 5G WLAN Profile, 2.4G Guest Network Profile, 5G Guest Network Profile, RADIUS Profile, and Access Control Profile.

	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
☐	System Default	10	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Access Point Settings Section: This section contains a radio button for 'Auto Approve' (set to 'Enable') and an 'Apply' button.

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

Group Settings

Search

Group Name : Edimax 5F

MAC Address

Device Name

74:DA:38:1E:54:30
74:DA:38:1E:54:3E
74:DA:38:64:CD:32

Members

Search

System Default

MAC Address

Device Name

74:DA:38:3E:79:10
74:DA:38:3E:78:C0
74:DA:38:40:E0:E4
74:DA:38:30:71:D8
74:DA:38:3E:7D:E8
74:DA:38:06:E1:AA
80:1F:02:F1:95:D2

Apply

Cancel

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

EDIMAX Pro

Wizard | Home | Logout | Global (English)

A P C 5 0 0

Dashboard

Zone Plan

NMS Monitor

NMS Settings

Local Network

Local Settings

Toolbox

Access Point

WLAN

RADIUS

Access Control

Guest Network

Users

Guest Portal

Zone Edit

Schedule

Device Monitoring

Firmware Upgrade

Advanced

System Security

Date and Time

Access Point

Search

Match whole words

	MAC Address	Device Name	Model	AP Group	2.4G Channel	5G Channel	2.4G Tx Power	5G Tx Power	Status	Action
☐	80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	System Default	N/A	N/A	Full	Full	●	⊗
☐	74:DA:33:27:1B:48	AP74DA38271B48	CAP1200	System Default	N/A	N/A	Full	Full	●	⊗
☐	74:DA:38:27:1B:3C	AP74DA38271B3C	CAP1200	System Default	N/A	N/A	Full	Full	●	⊗
☐	74:DA:33:03:23:9C	AP74DA3803239C	WAP1750	System Default	N/A	N/A	Full	Full	●	⊗
☐	74:DA:33:27:1B:46	AP74DA38271B46	CAP1200	System Default	N/A	N/A	Full	Full	●	⊗
☐	74:DA:33:27:1B:38	AP74DA38271B38	CAP1200	System Default	11	36	Full	Full	●	⊗
☐	74:DA:33:27:1B:54	AP74DA38271B54	CAP1200	System Default	11	36	Full	Full	●	⊗
☐	74:DA:33:27:1B:40	AP74DA38271B40	CAP1200	System Default	11	36	Full	Full	●	⊗
☐	74:DA:33:27:1B:3E	AP74DA38271B3E	CAP1200	System Default	11	36	Full	Full	●	⊗
☐	74:DA:33:27:1B:44	AP74DA38271B44	CAP1200	System Default	11	36	Full	Full	●	⊗

Refresh Edit Delete Selected Delete All

Access Point Group

Search

Match whole words

	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
☐	System Default	7	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☐	Edimax 5F	3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Add Edit Clone Delete Selected Delete All

Access Point Settings

Auto Approve ☒ Enable ☐ Disable

Apply

C.

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

The screenshot shows the EDIMAX Pro NMS Settings interface. The 'Access Point' tab is selected. The 'Access Point Group' table lists several groups, with 'Edimax 5F' selected. The 'Edit' button is highlighted with a blue star. The 'Access Point Settings' panel is visible below the table.

MAC Address	Device Name	Model	AP Group	2.4G Channel	5G Channel	2.4G Tx Power	5G Tx Power	Status	Action
80:1F:02:CC:DD:10	AP801F02CCDD10	WAP1750	System Default	N/A	N/A	Full	Full	●	⊗
74 DA 38 27 1B 48	AP74DA38271B48	CAP1200	System Default	N/A	N/A	Full	Full	●	⊗
74 DA 38 27 1B 3C	AP74DA38271B3C	CAP1200	System Default	N/A	N/A	Full	Full	●	⊗
74 DA 38 03 23 9C	AP74DA3803239C	WAP1750	System Default	N/A	N/A	Full	Full	●	⊗
74 DA 38 27 1B 46	AP74DA38271B46	CAP1200	System Default	N/A	N/A	Full	Full	●	⊗
74 DA 38 27 1B 38	AP74DA38271B38	CAP1200	System Default	11	36	Full	Full	●	⊗
74 DA 38 27 1B 54	AP74DA38271B54	CAP1200	System Default	11	36	Full	Full	●	⊗
74 DA 38 27 1B 40	AP74DA38271B40	CAP1200	System Default	11	36	Full	Full	●	⊗
74 DA 38 27 1B 3E	AP74DA38271B3E	CAP1200	System Default	11	36	Full	Full	●	⊗
74 DA 38 27 1B 44	AP74DA38271B44	CAP1200	System Default	11	36	Full	Full	●	⊗

Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
System Default	7	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
☒ Edimax 5F	3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

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

The screenshot shows the 'Profile Group Settings' panel. The 'WLAN Group' is selected in the drop-down menu. The 'Override Default Setting' checkbox is checked. The 'Apply' button is visible.

Group	Override Default Setting	Setting
WLAN Group	☒	Disable
Guest Network Group	☐	Disable
RADIUS Group	☐	Disable
MAC Access Control Group	☐	Disable

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

COPYRIGHT

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

Edimax Technology Co., Ltd. makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability, or fitness for any particular purpose. Any software described in this manual is sold or licensed as is. Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Edimax Technology Co., Ltd. reserves the right to revise this publication and to make changes from time to time in the contents hereof without the obligation to notify any person of such revision or changes.

The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. The software and specifications are subject to change without notice. Please visit our website www.edimax.com for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such as PDAs or lap pads is not authorized. This transmitter is restricted for use with the specific antenna tested in the application for certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

EU Declaration of Conformity

- English:** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/30/EU.
- Français:** Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/30/EU.
- Čeština:** Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/30/EU.
- Polski:** Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/30/EU.
- Română:** Acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/30/EU.
- Русский:** Это оборудование соответствует основным требованиям и положениям Директивы 2014/30/EU.
- Magyar:** Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/30/EU).
- Türkçe:** Bu cihaz 2014/30/EU. direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.
- Українська:** Обладнання відповідає вимогам і умовам директиви 2014/30/EU.
- Slovenčina:** Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/30/EU.
- Deutsch:** Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/30/EU.
- Español:** El presente equipo cumple los requisitos esenciales de la Directiva 2014/30/EU.
- Italiano:** Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/30/EU.
- Nederlands:** Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/30/EU.
- Português:** Este equipamento cumpre os requisitos essenciais da Directiva 2014/30/EU.
- Norsk:** Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/30/EU.
- Svenska:** Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/30/EU.
- Dansk:** Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/30/EU.
- suomen kieli:** Tämä laite täyttää direktiivien 2014/30/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN



WEEE Directive & Product Disposal



At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European R&TTE directives.

Equipment: AP Controller

Model No.: APC500

The following European standards for essential requirements have been followed:

Directives 2004/108/EC

EMC : EN 55022:2010+AC:2011 Class B
EN 55024:2010
EN 61000-3-2:2014 Class A
EN 61000-3-3:2013

Safety (LVD) : IEC 62368-1:2014 (2nd Edition) and/or EN 62368-1:2014+A11:2017

Edimax Technology Europe B.V.
Fijenhof 2,
5652 AE Eindhoven,
The Netherlands

Printed Name: David Huang

Title: Director

Edimax Technology Europe B.V.

a company of:

Edimax Technology Co., Ltd.
No. 278, Xinhua 1st Rd.,
Neihu Dist., Taipei City,
Taiwan



Date of Signature: Nov. , 2020

Signature:

A handwritten signature in black ink, appearing to read 'Albert Chang'.

Printed Name:

Albert Chang

Title:

Director

Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.