

Office 1-2-3

User Manual

11-2020 / 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

3444 De La Cruz Blvd., Santa Clara, CA 95054, USA

Live Tech Support: 1(800) 652-6776

Email: support@edimax.com

CONTENTS

OVERVIEW	1
<i>I Quick Summary & Reminder</i>	2
<i>II Product Information</i>	5
II-1 Package Contents.....	5
II-2 System Requirements.....	6
II-3 Hardware Overview	6
II-4 LED Status	7
II-5 Reset	7
<i>III Quick Setup</i>	8
III-1 Initial Setup – Computer.....	8
III-2 Initial Setup – Mobile Device.....	12
III-3 Setup Wizard.....	15
<i>IV Further Expansion</i>	21
<i>V Hardware Installation / Deployment</i>	22
V-1 Office 1-2-3 Deployment	22
V-2 Mounting	24
V-2-1 Wooden Ceiling	24
V-2-2 Other Ceiling.....	26
V-2-3 T-Rail Mount.....	28
<i>VI Replacing Master AP</i>	30
<i>VII Office 1-2-3 Interface.....</i>	37

VII-1	IP Finder	37
VII-2	Home.....	39
VII-3	Wizard	41
VII-4	Navigation.....	41
VII-5	Network Settings	42
VII-5-1	Manage AP	43
VII-5-1-1	Edit Managed AP.....	46
VII-5-1-1-1	Basic Settings.....	46
VII-5-1-1-2	Radio Settings.....	48
VII-5-1-1-3	Bandsteering	49
VII-5-1-1-4	Airtime Fairness	49
VII-5-1-2	Group Edit Managed AP.....	51
VII-5-1-2-1	Basic Settings.....	51
VII-5-1-2-2	Radio Settings.....	52
VII-5-1-2-3	Bandsteering	52
VII-5-1-2-4	Airtime Fairness	53
VII-5-2	Office Network.....	54
VII-5-3	Device Network.....	56
VII-5-4	Wireless Schedule	59
VII-5-5	Guest Network.....	61
VII-6	Guest Accounts	64
VII-6-1	Manage User Account.....	65
VII-6-2	Generate Printed Ticket	67
VII-6-3	Captive Portal.....	69
VII-6-4	SMS Service.....	72
VII-7	Office Accounts	74
VII-7-1	RADIUS Authentication for Office Network under Win 7	76
VII-8	System Settings.....	80
VII-8-1	LAN IP Address	81
VII-8-2	System Settings.....	83
VII-8-3	Management VLAN ID.....	86
VII-8-4	Save Settings to PC.....	86
VII-8-5	Restore Settings from PC	87

VII-8-6	Master AP Firmware Upgrade	87
VII-8-7	Slave AP Firmware Upgrade.....	88
VII-8-8	Firmware Upgrade (Slave-Only Interface)	88
VII-9	E-MAPs.....	89
VII-9-1	Add / Edit Zone	90
VII-9-2	Delete Zone.....	92
VII-9-3	Show Map	92
VII-10	System Status.....	98
VII-11	Advance Settings.....	104
VIII	<i>Advanced Settings</i>	106
VIII-1	Dashboard.....	106
VIII-1-1	System Information	107
VIII-1-2	Devices Information.....	107
VIII-1-3	Managed AP	108
VIII-1-4	Managed AP Group.....	110
VIII-1-5	Active Clients	112
VIII-1-6	Active Users	112
VIII-2	Zone Plan	112
VIII-2-1	Menu.....	114
VIII-2-2	Control	117
VIII-3	NMS Monitor	119
VIII-3-1	Access Point	119
VIII-3-1-1	Managed AP	119
VIII-3-1-2	Managed AP Group.....	121
VIII-3-2	WLAN	124
VIII-3-2-1	Active WLAN.....	124
VIII-3-2-2	Active WLAN Group	125
VIII-3-3	Clients	126
VIII-3-3-1	Active Clients.....	126
VIII-3-4	Users	127
VIII-3-4-1	Active Users.....	127
VIII-3-4-2	Users Log	127
VIII-3-5	Rogue Devices	128
VIII-3-6	Information	129

VIII-3-6-1	All Events/Activities	129
VIII-3-6-2	AP Monitoring	130
VIII-3-6-3	SSID Overview	132
VIII-4	NMS Settings.....	133
VIII-4-1	Access Point	134
VIII-4-1-1	Edit Access Point	135
VIII-4-1-1-1	Edit Basic Settings	136
VIII-4-1-1-2	Edit Web Account Settings.....	137
VIII-4-1-1-3	Edit VLAN Settings.....	138
VIII-4-1-1-4	Edit Radio Settings	139
VIII-4-1-1-5	Edit WMM-EDCA Settings	142
VIII-4-1-1-6	Edit BandSteering Settings.....	142
VIII-4-1-1-7	Edit Profile Settings	143
VIII-4-1-1-8	Events.....	144
VIII-4-1-2	Add/Edit Access Point Group.....	145
VIII-4-1-2-1	Edit Basic Group Settings	145
VIII-4-1-2-2	Edit Web Account Group Settings.....	146
VIII-4-1-2-3	Edit VLAN Group Settings	146
VIII-4-1-2-4	Edit Radio Group Settings	146
VIII-4-1-2-5	Edit WMM-EDCA Settings	149
VIII-4-1-2-6	Edit BandSteering Settings.....	149
VIII-4-1-2-7	Edit Profile Settings	149
VIII-4-1-2-8	Edit Group Settings.....	150
VIII-4-2	WLAN	151
VIII-4-2-1	Add/Edit WLAN	152
VIII-4-2-2	Add/Edit WLAN Group.....	155
VIII-4-3	RADIUS	156
VIII-4-3-1	Add/Edit External RADIUS Server.....	157
VIII-4-3-2	Add/Edit Internal RADIUS Server	158
VIII-4-3-3	Add/Edit/Import/Export RADIUS Accounts.....	159
VIII-4-3-4	Add/Edit RADIUS Group	162
VIII-4-4	Access Control.....	163
VIII-4-4-1	Add/Edit MAC Access Control	164
VIII-4-4-2	Add/Edit/Clone MAC Access Control Group.....	165
VIII-4-5	Guest Network.....	166
VIII-4-5-1	Add/Edit Guest Network	167
VIII-4-5-2	Add/Edit Guest Network Group	170
VIII-4-6	Users	171
VIII-4-7	Guest Portal	173
VIII-4-7-1	Free Guest Portal Type.....	174

VIII-4-7-2	User Level Agreement Guest Portal Type	175
VIII-4-7-3	Static Users Guest Portal Type	176
VIII-4-7-4	Dynamic Users Guest Portal Type	177
VIII-4-7-5	External Captive Portal Guest Portal Type	179
VIII-4-7-6	Editing "Login Portal"	180
VIII-4-8	Zone Edit	182
VIII-4-9	Schedule	184
VIII-4-10	Smart Roaming	185
VIII-4-11	Device Monitoring	187
VIII-4-12	Firmware Upgrade	188
VIII-4-13	Advanced	189
VIII-4-13-1	System Security	189
VIII-4-13-2	Date & Time	189
VIII-4-13-3	Google Maps	191
VIII-4-13-4	SMS	192
VIII-5	Local Network	194
VIII-6	Local Settings	195
VIII-6-1	Operation Mode	195
VIII-6-2	Network Settings	197
VIII-6-2-1	System Information	197
VIII-6-2-2	Wireless Clients	200
VIII-6-2-3	Wireless Monitor	201
VIII-6-2-4	Log	202
VIII-6-3	Management	204
VIII-6-3-1	Admin	204
VIII-6-3-2	Date and Time	206
VIII-6-3-3	Syslog Server Settings	208
VIII-6-3-4	Syslog E-mail Settings	209
VIII-6-3-5	I'm Here	210
VIII-6-4	Advanced	211
VIII-6-4-1	LED Settings	211
VIII-6-4-2	Update Firmware	212
VIII-6-4-3	Save/Restore Settings	213
VIII-6-4-4	Factory Default	214
VIII-6-4-5	Reboot	215
VIII-7	Toolbox	216
VIII-7-1	Network Connectivity	217
VIII-7-1-1	Ping	217

VIII-7-1-2	Trace Route	218
VIII-7-1-3	IP Scan.....	219
IX	Appendix	220
IX-1	Configuring your IP address.....	220
IX-1-1	Windows XP.....	221
IX-1-2	Windows Vista	223
IX-1-3	Windows 7.....	225
IX-1-4	Windows 8.....	229
IX-1-5	Mac	233
X	FAQ	235

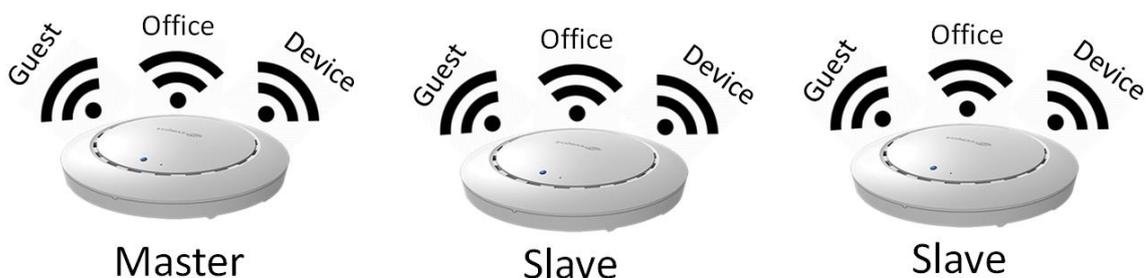
OVERVIEW

The Edimax Office 1-2-3 is a complete and expandable Wi-Fi system designed to meet the needs of small to medium offices. With easy setup, friendly operation user interface, super-fast wireless speed, an extensive feature set and a practical, ceiling-mount design, it is ideal for modern business environments – in working areas, meeting rooms, lobby, or open spaces.

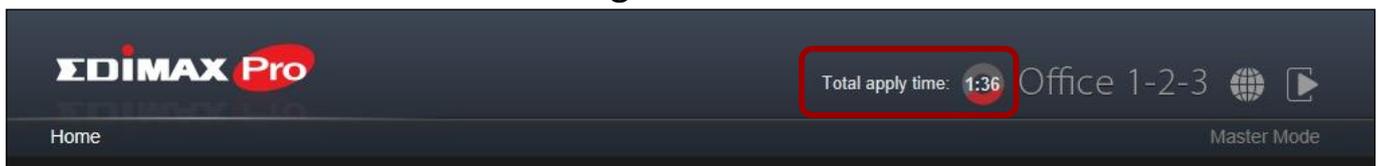
Office 1-2-3 kit includes 3 pre-configured Access Points (expandable with Office +1 AP to up to a total of 8 APs), each allowing a capacity of up to 100 simultaneous users. The kit can setup multiple SSIDs (up to 32) to suit different user environments such as departmental groups or user groups. A built-in RADIUS server provides additional verification with a scalable AP array architecture, as well as a centralized management system for multiple access points. Power over Ethernet (PoE) support allows for deployment flexibility and extensive network options for company MIS departments and network administrators.

I Quick Summary & Reminder

1. You can find all supporting documents, video, and programs, we advise you to upgrade to the latest firmware first:
<http://office123.edimax.com>
2. This is a Quick Install Guide. For complete user manual or QIG in other languages, please check the included CD or visit the link below:
www.edimax.com/edimax_pro/download/Office1-2-3
3. During the initial power up, please wait 10 minutes for APs to communicate with each other.
4. Download our **IP Finder** from the link below to search and find the master AP for configurations.
www.edimax.com/edimax_pro/download/IPfinder
5. To setup Office 1-2-3 using a mobile device, **IP Finder** mobile app can be downloaded and used. Please see **III-2 Initial Setup – Mobile Device** below.
6. If you are unable to load IP Finder: **Right-click** on the IP Finder and choose “Property”. Click **Unblock** on the bottom selection and click “OK”.
7. The Office 1-2-3 will create 3 wireless network initially for each AP.



8. The default *username* and *password* are **admin** and **1234** respectively. Changing password on the Master AP will also change the password of the Slave APs.
9. It is recommended that you use the default settings whenever possible. Refer to later sections of this manual for more information on the settings
10. It is recommended to use **import** and **export list** for simple management of guest and office accounts.
11. When configuring, please check for a “Progress Circle” on the upper right hand side of the page. Please wait until the progress circle is finished before further configurations.



12. The RADIUS function used by Office network works directly with most OS except Windows versions older than Win 8.0. For instructions on setting up RADIUS function, please refer to 1) VII-7-1 **RADIUS Authentication for Office Network under Win 7** on page 76; 2) the included A4 Sheet; or 3) download “RADIUS Authentication for Office Network” from the link:
www.edimax.com/edimax_pro/download/Office1-2-3
13. This product supports multiple devices per login account.
14. Clicking **Apply** during any of the configuration will **reboot** the AP, which takes time, it is recommended that you use **Apply** only after changing all settings.
15. Should you connect to the guest network, **open a browser** to trigger the login page. If no login page is shown, try entering www.edimax.com.

- 16.** A maximum of 128 Guest accounts and 256 Office accounts are supported. Multiple logins (of the same account/password) are accounted as using multiple accounts.
- 17.** The **frontdesk account** is for **creation of guest accounts** only. It cannot make changes to other settings.
- 18.** To connect Office 1-2-3 to your VLAN Network, Management VLAN ID (under System Settings) must be configured to be the same as the one on your switch. All the wireless SSID and LAN can only share one VLAN ID. It is recommended to put the AP on the VLAN that can access both LAN and Internet network. The Guest network in Office 1-2-3 can prohibit guest accessing the Intranet network by IP filtering.
- 19.** If you wish to add more APs to **expand** your office coverage, please consult your representative and refer to the “**Office +1 AP**” package.

Attention / Beachtung / Atención / Attention / Attenzione / Attentie

English: The socket-outlet/power adapter shall be installed near the equipment and shall be easily accessible.

Deutsch: Die Steckdose/das Netzteil muss in der Nähe des Geräts installiert werden und leicht zugänglich sein.

Español: La toma de corriente/adaptador debe estar ubicado cerca del equipo y ser de fácil acceso.

Français: La prise de courant/l'adaptateur doit être situé près de l'équipement et facilement accessible.

Italiano: La presa/adattatore di alimentazione deve essere posizionata vicino all'apparecchiatura ed essere facilmente accessibile.

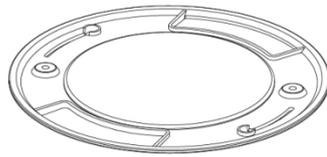
Nederlands: Het stopcontact/stroomadapter moet in de buurt van de apparatuur worden geïnstalleerd en moet gemakkelijk toegankelijk zijn.

II Product Information

II-1 Package Contents



1



2



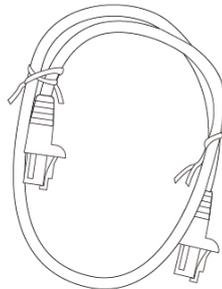
3



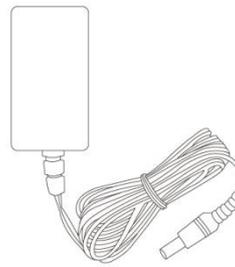
4



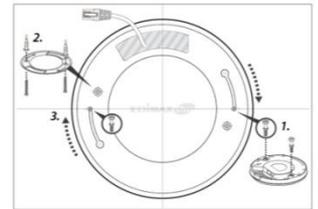
5



6



7



8

1. Office 1-2-3 Access Point x 3
(1 Master, 2 Slaves)
2. Ceiling Mount Bracket x 3
3. T-Rail Mounting Kit & Screws
x 3
4. CD

5. Quick Installation Guide
6. Ethernet Cable x 3
7. Power Adapter
8. Ceiling Mount Screw Template
x 3

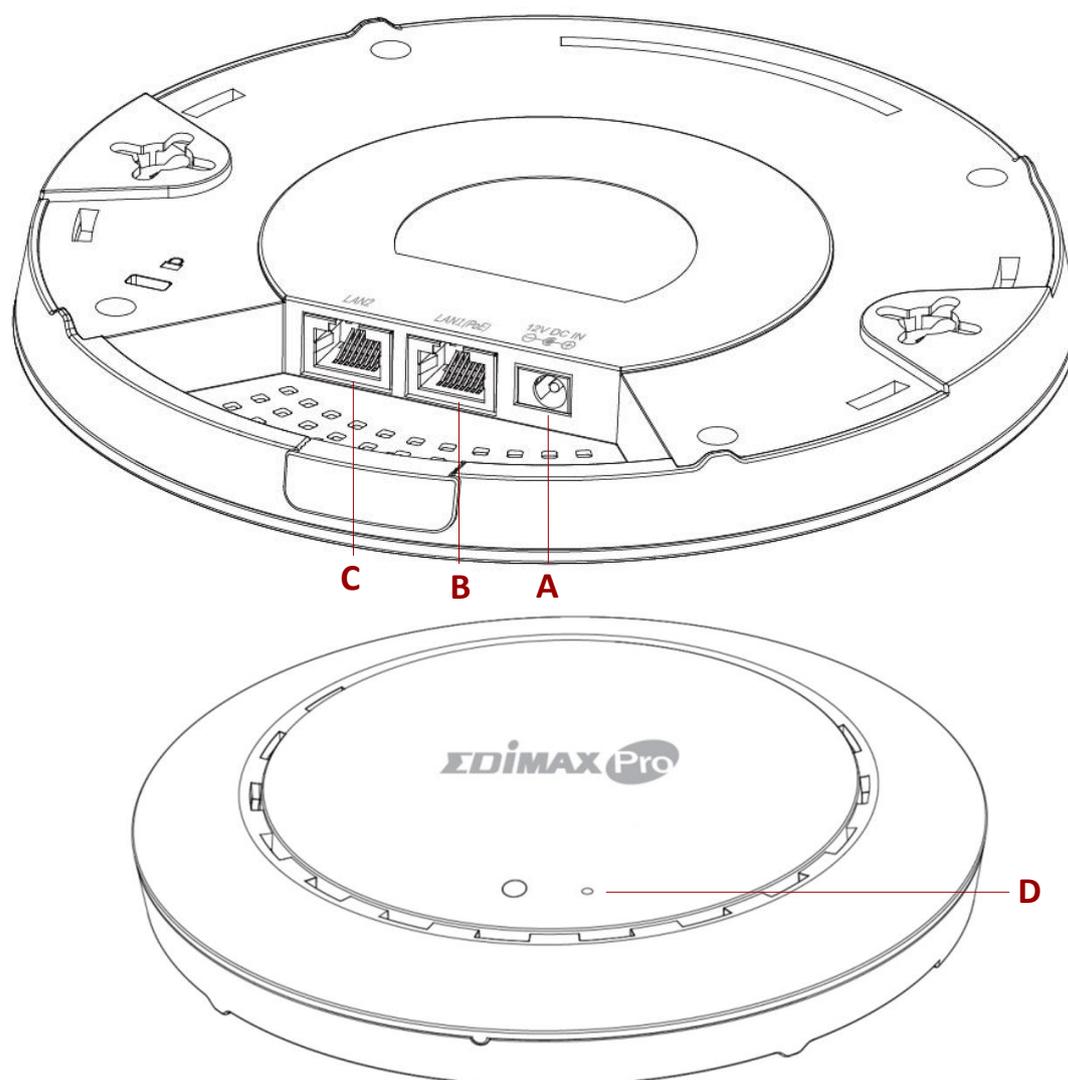


NOTE: One of the APs has a **Master** sticker while the other two have **Slave** stickers, indicating their relationships.

II-2 System Requirements

- Existing cable/DSL modem & router.
- Existing PoE Switch connected to the router
- Computer with web browser for access point configuration

II-3 Hardware Overview



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

II-4 LED Status

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

II-5 Reset

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

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



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



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

III Quick Setup

This quick setup is a guide to setting up your Office 1-2-3 high speed Wi-Fi network. Please note that these sections can be revisited later on for further configurations, but will serve as the basics of the system.

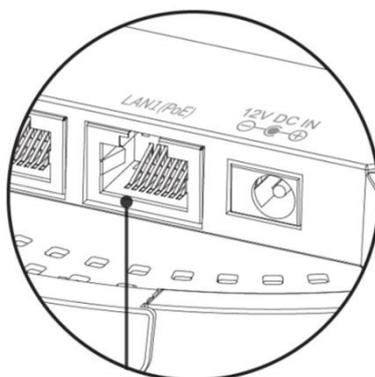
III-1 Initial Setup – Computer

The computer initial setup is a simple step-by-step process to start up the web user interface. Please follow the steps below:

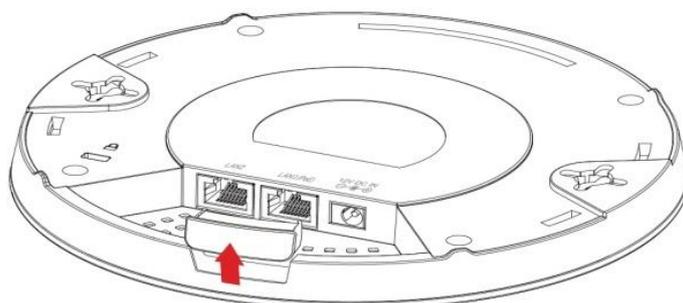
1. Connect your computer to the PoE Switch using an Ethernet cable.
2. Connect the 3 access points to the PoE Switch using Ethernet cables. Please make sure the Ethernet cable is connected to the PoE port of the access point as shown below:



NOTE: One of the APs has a **Master** sticker while the other two have **Slave** stickers, indicating their relationships.



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

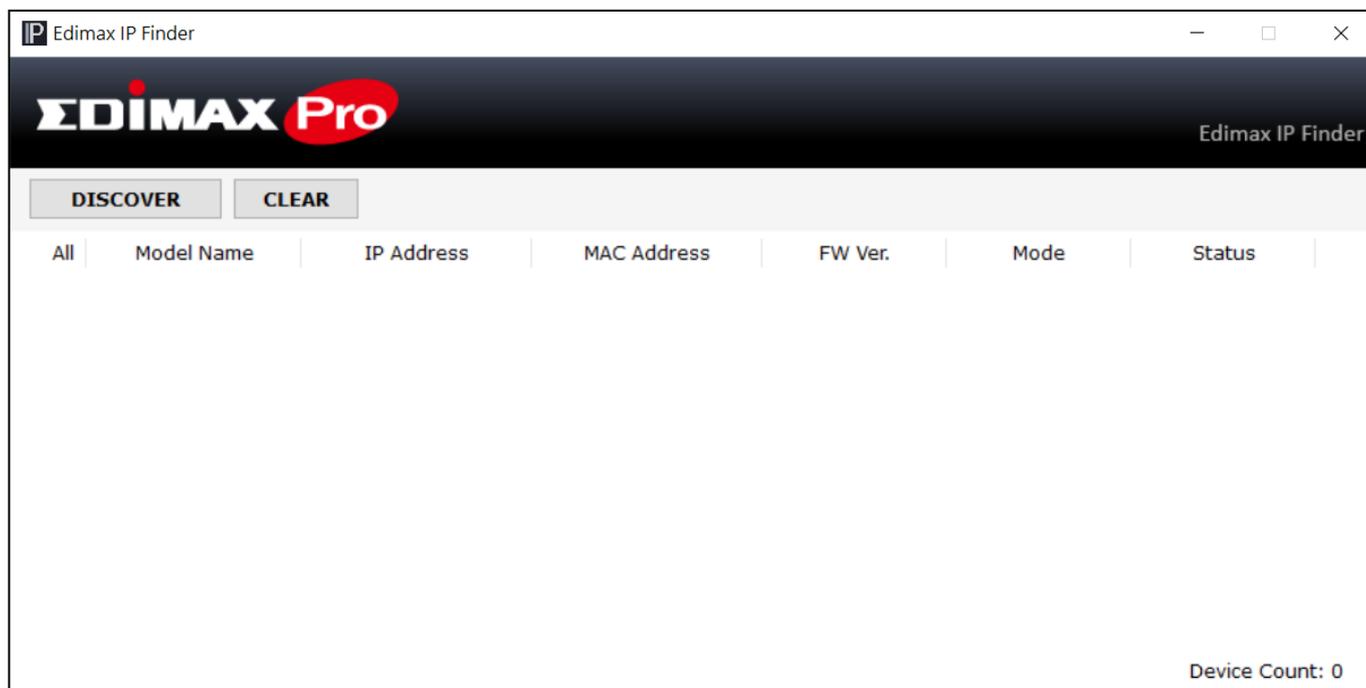


3. Please wait for 10 minutes for the APs to communicate between themselves.
4. Download and Install the Edimax Cloud Discovery Tool (IP Finder) on your computer from the link below:

www.edimax.com/edimax_pro/download/IPfinder



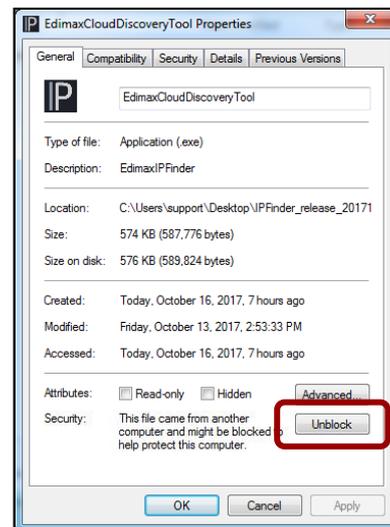
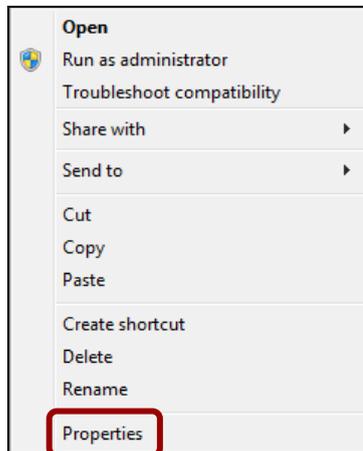
5. Open the “EdimaxCloudDiscoveryTool”:



Unable to open IP Finder Tool

If you were unable to open the IP Finder Tool, it may be because the antivirus on your system is blocking it. To unblock, please see below:

1. Right-click on the IP Finder tool and click “Properties”
2. Locate “Security” at the bottom of the window. Click the **Unblock** button.



6. Locate your master access point by clicking “Discover”  on the IP finder.

All	Model Name	IP Address	MAC Address	FW Ver.	Mode	Status
1		192.168.2.107	74:DA:38:D3:6B:60	1.0.0	Master	Ready
2		192.168.2.105	74:DA:38:D3:6B:4A	1.0.0	Slave	Ready
3		192.168.2.108	74:DA:38:D3:6B:43	1.0.0	Slave	Ready

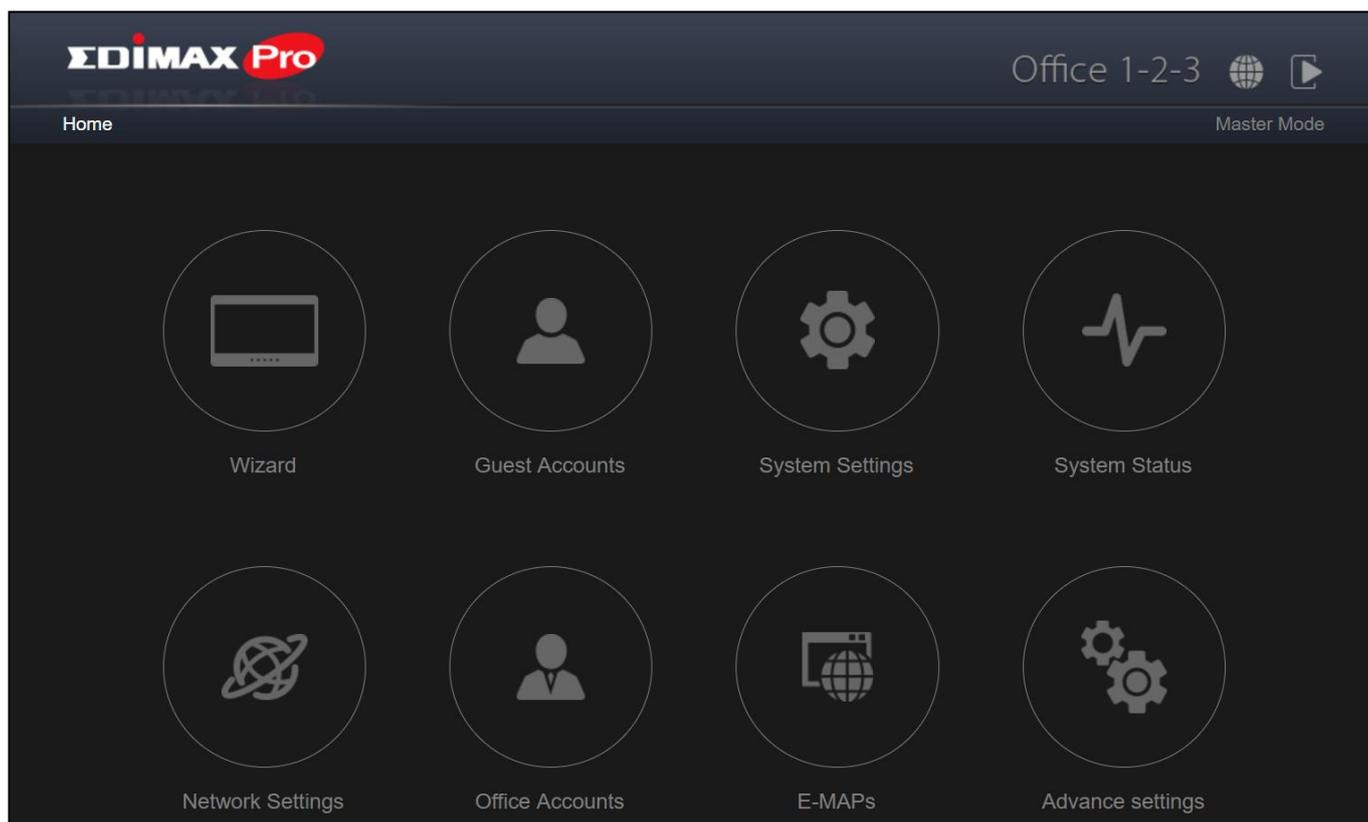
7. Click the IP address of the master access point to go into the web user interface.

All	Model Name	IP Address	MAC Address	FW Ver.	Mode	Status
1		192.168.2.107	74:DA:38:D3:6B:60	1.0.0	Master	Ready
2		192.168.2.105	74:DA:38:D3:6B:4A	1.0.0	Slave	Ready
3		192.168.2.108	74:DA:38:D3:6B:43	1.0.0	Slave	Ready

Upon entering the webpage, you should be prompted to enter the username and password, enter them (default username: **admin**, password: **1234**) to proceed:



The web user interface is shown below:



8. Click “Wizard” and go to the next section to go through the setup wizard.

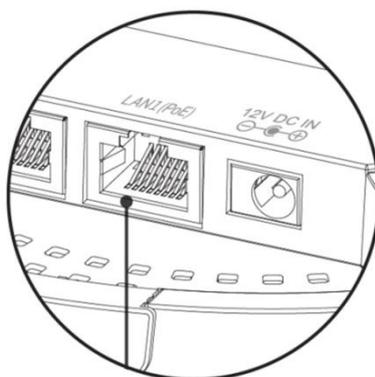
III-2 Initial Setup – Mobile Device

The initial setup for mobile device is a simple step-by-step process to start up the mobile web user interface.

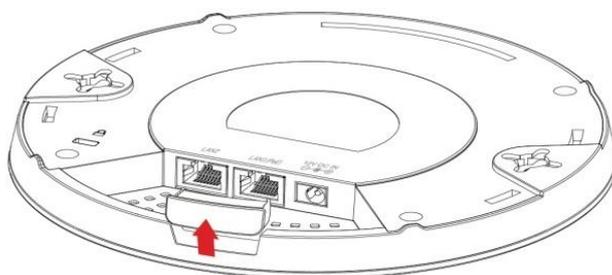
1. Connect the 3 access points to the PoE Switch using Ethernet cables. Please make sure the Ethernet cable is connected to the PoE port of the access point as shown below:



NOTE: One of the APs has a **Master** sticker while the other two have **Slave** stickers, indicating their relationships.



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



2. Please wait for 10 minutes for the APs to communicate between themselves.
3. Please scan the QR Code below to download the mobile app “Office123”.

iOS



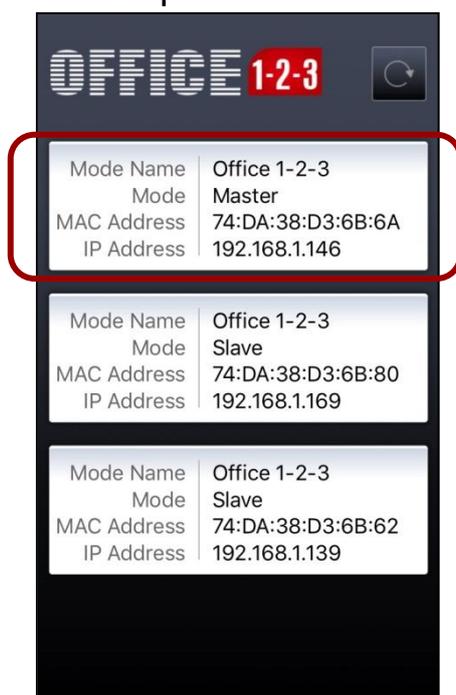
Android



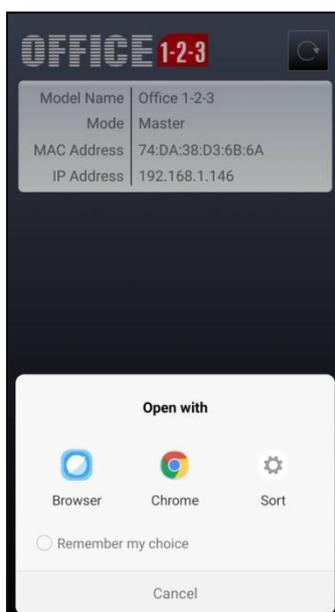
4. On your mobile device, connect to the device network. The device network SSID is “device”.
5. Open the “Office123” app.



6. Locate the Master AP and tap it.



The system may prompt you to select a desired browser as shown below:

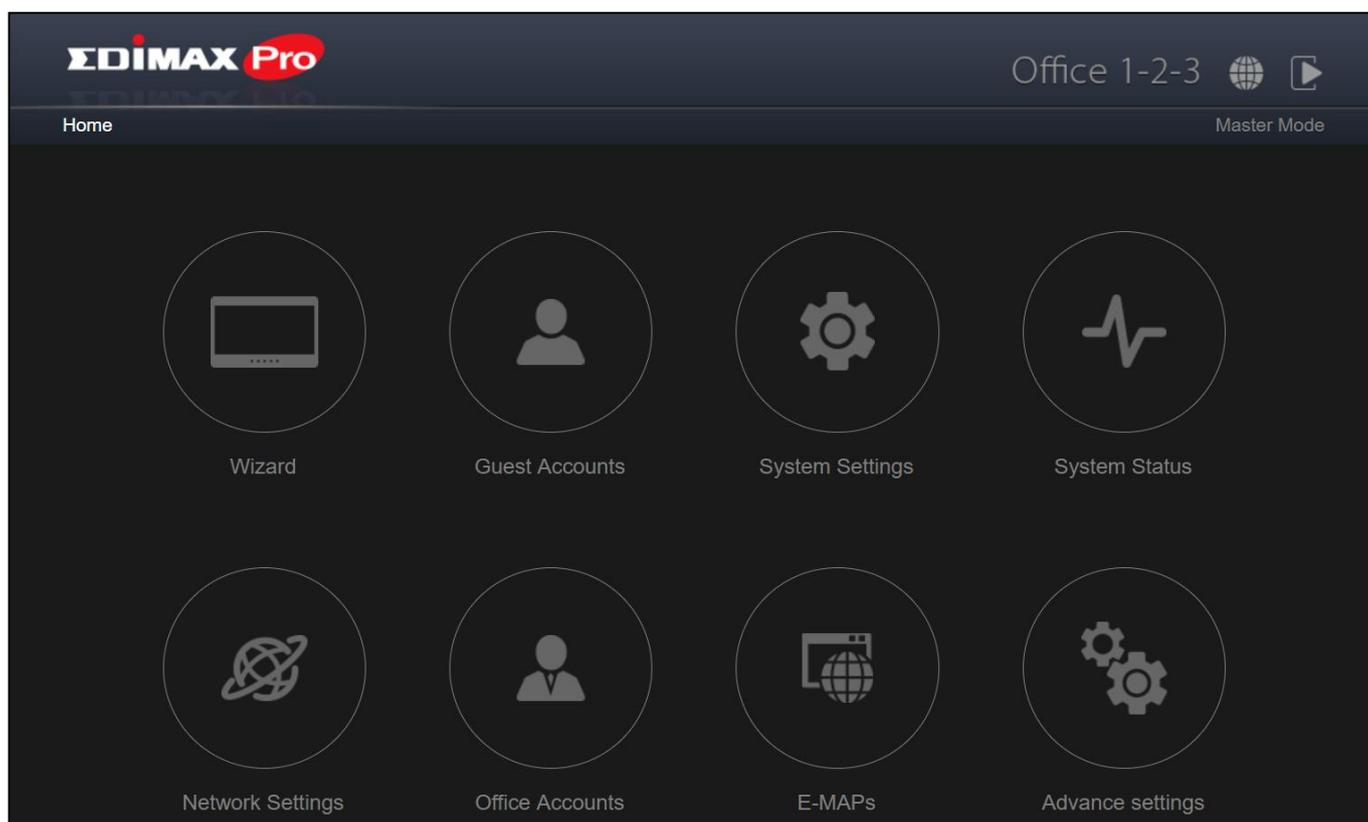


7. The browser will be at the login page of Office 1-2-3.

Upon entering the webpage, you should be prompted to enter the username and password, enter them (default username: **admin**, password: **1234**) to proceed:



The web user interface is shown below:



8. Tap “Wizard” and go to the next section to go through the setup wizard.



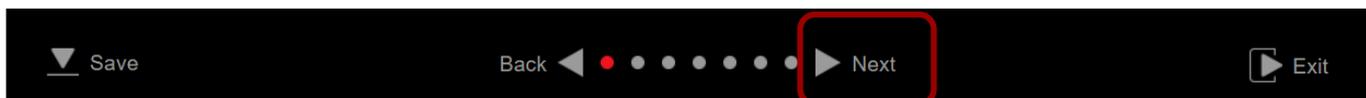
NOTE: Please remember to assign a WPA-PSK2 password to the Device Network later to prevent others from accessing the network freely.

III-3 Setup Wizard

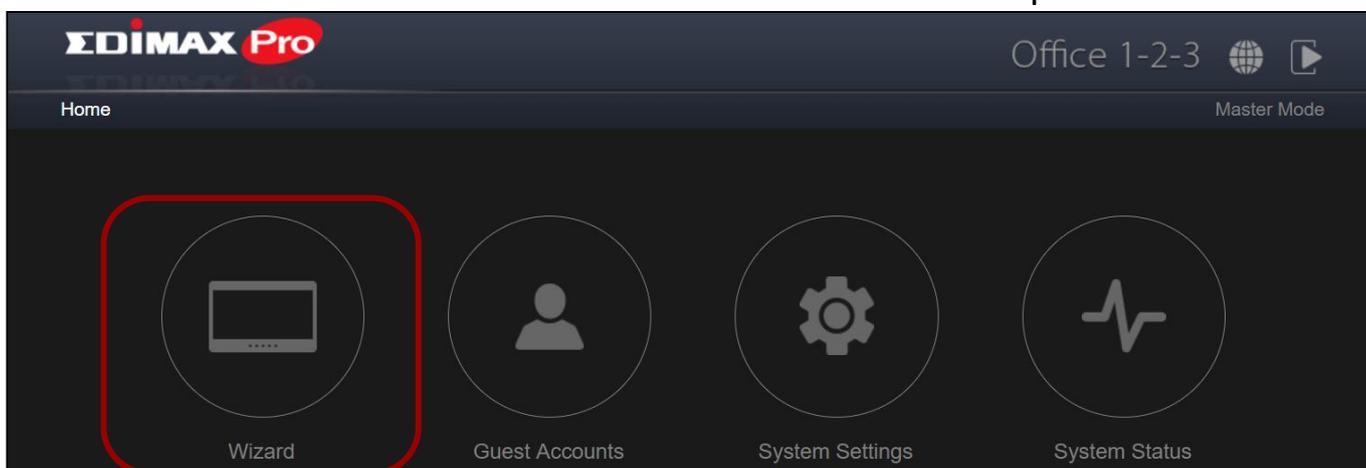
The wizard aims to help you with setting the basic settings of the Office 1-2-3 network including **Office Accounts**, **Guest Accounts** and **Device Network**, etc.



NOTE: In most cases, simply go through the steps below by clicking “Next”, although adding / editing password, Wi-Fi-key, and accounts are recommended.



1. Click “Wizard” on the web interface to start the setup wizard:



2. Change the password for Administrator and Frontdesk account.

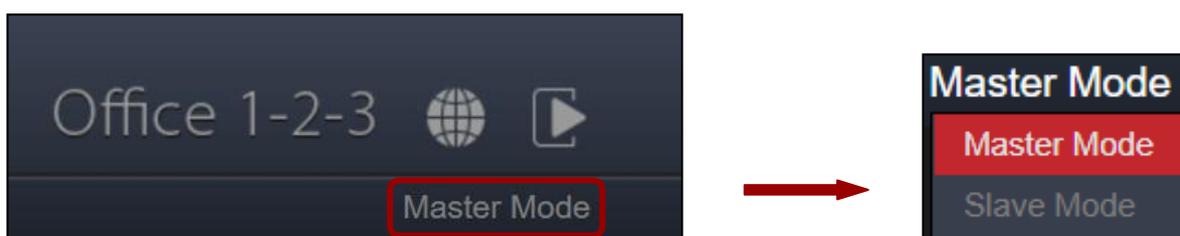


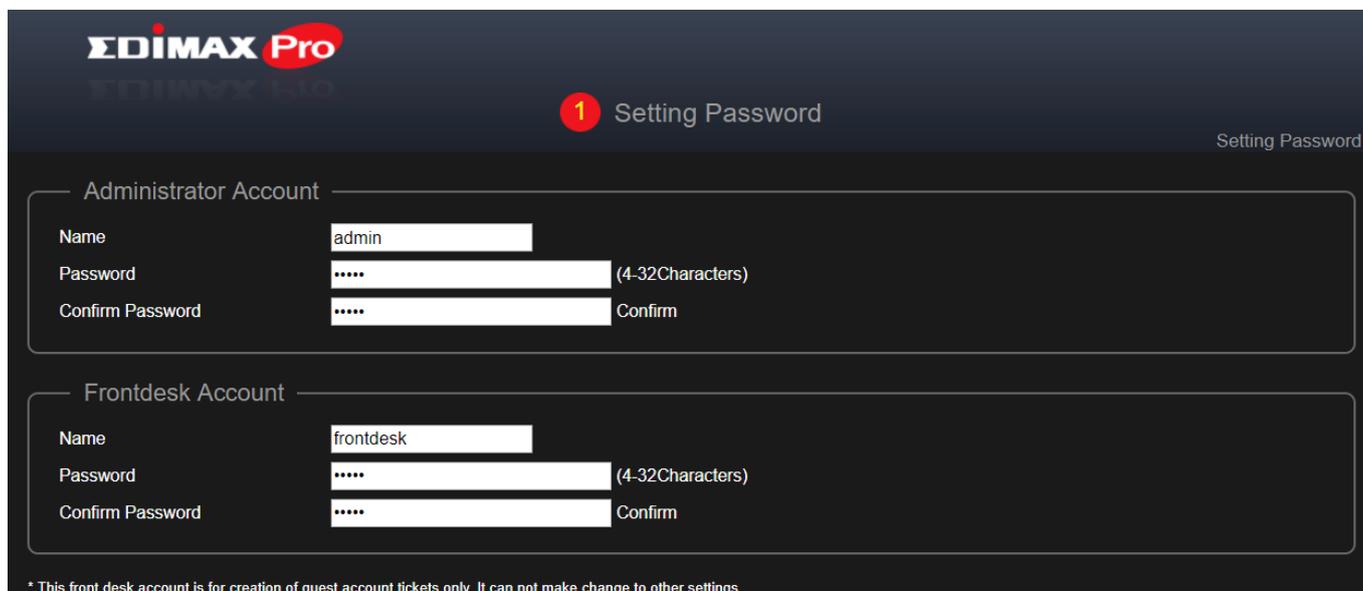
NOTE: The Frontdesk account is for creating guest accounts and ticket printing only.

Once the change is made on the master, the slave’s username and password will be changed also.



NOTE: You can change between master and slave modes at will by clicking the current mode (outlined area below). It is, however, not recommended except for the recovery of master AP.





EDIMAX Pro

1 Setting Password

Setting Password

Administrator Account

Name: admin

Password: (4-32Characters)

Confirm Password: Confirm

Frontdesk Account

Name: frontdesk

Password: (4-32Characters)

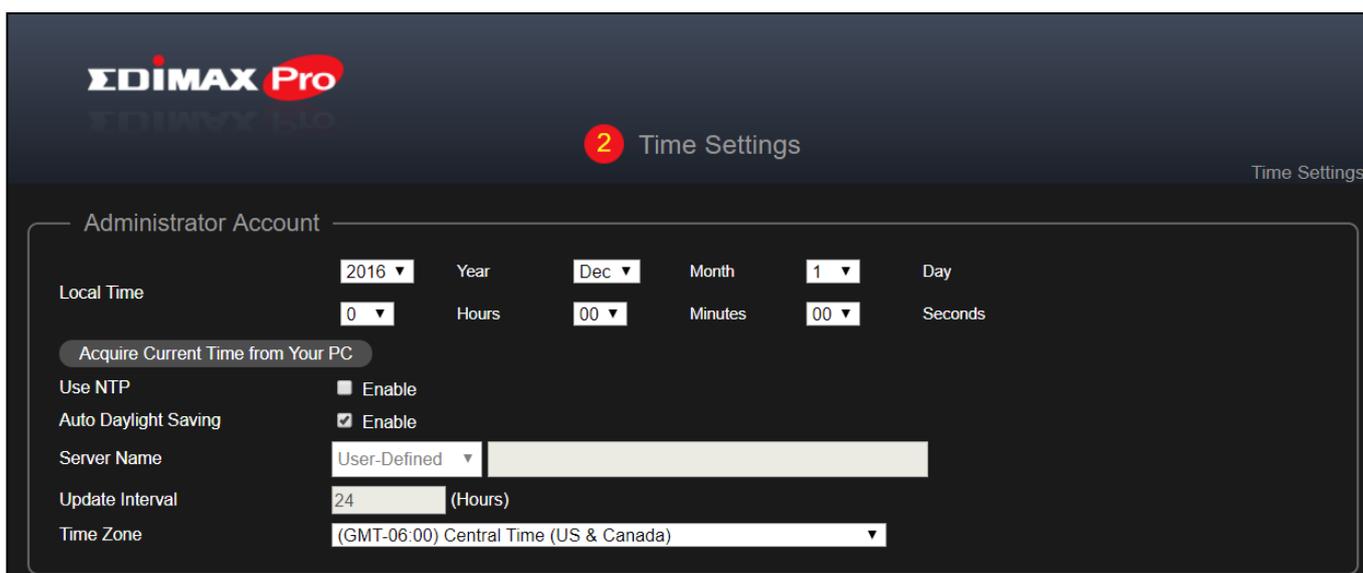
Confirm Password: Confirm

* This front desk account is for creation of guest account tickets only. It can not make change to other settings.

3. Time Settings: Set the time of your access point.



NOTE: It is highly recommended to turn on the NTP server so the device can remain on time even after power recycling. Choose an NTP server that is close to your country.



EDIMAX Pro

2 Time Settings

Time Settings

Administrator Account

Local Time: 2016 Year, Dec Month, 1 Day

0 Hours, 00 Minutes, 00 Seconds

Acquire Current Time from Your PC

Use NTP: Enable

Auto Daylight Saving: Enable

Server Name: User-Defined

Update Interval: 24 (Hours)

Time Zone: (GMT-06:00) Central Time (US & Canada)

Date and Time Settings	
Local Time	Set the system's date and time manually using the drop down menus.
Acquire Current Time from your PC	Click to acquire time and date automatically from your PC.
Use NTP	Check to enable automatic time and date sync to an NTP server.

Auto Daylight Saving	Check / uncheck to enable / disable daylight saving function.
Server Name	Use the drop down menu to select a region. A server will be shown after selecting the region. Choose the region according to your location.
Update Interval	Specify how often (in hours) the access point synchronizes with the NTP server.
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.

4. Guest Network: Configure the guest network settings

EDIMAX Pro

3 Guest Network

Guest Network

Guest Network

Same settings for both Radios

SSID	guest123
Hide SSID	Disable
Encryption	None
Type	TKIP/AES
WiFi Password	

Bandwidth limit

Bandwidth limit

Disable

Access

Access

Internet Only

Type	IP Address	Subnet Mask
Gateway	192.168.2.250	255.255.255.0

Device Name	IP Address	Subnet Mask	Action
	192.168.2.250	255.255.255.0	Disable
	192.168.2.101	255.255.255.0	Disable
	192.168.2.102	255.255.255.0	Disable

Additional Access IP

Back Next Exit

For more information on the settings, please refer to VII-5-5 **Guest Network** on page 61.

Press "Next" to continue.

5. Office Network: Configure the office network settings.



NOTE: It is recommended to leave the settings as it is (default values).

Office Network	
Same settings for both Radios ▼	
SSID	office123
Hide SSID	Disable ▼

For more information on the settings, please refer to VII-5-2 **Office Network** on page 54.

Press “Next” to continue.

6. Device Network: Configure the device network settings.



NOTE: It is recommended to only change the Wi-Fi password.

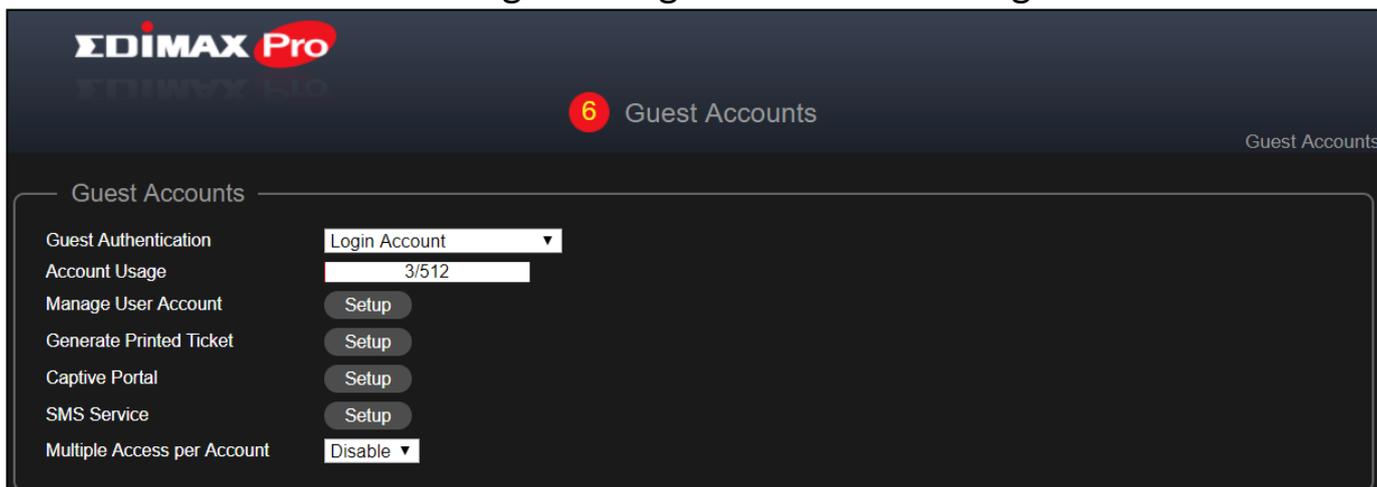
Device Network		
Same settings for both Radios ▼		
SSID	device	
Hide SSID	Disable ▼	
Encryption	WPA/WPA2-PSK ▼	
Type	TKIP/AES ▼	
WiFi Password	12345678	
Bandwidth limit		
Bandwidth limit	Disable ▼	
MAC Address Controls		
MAC Address Controls	Allow List ▼	
Device Name	MAC Address	Action
		Add
		Import List Export List

Select WPA-PSK2 for encryption field and enter a Wi-Fi Password.

For more information on the settings, please refer to VII-5-3 **Device Network** on page 56.

Press “Next” to continue.

7. Guest Accounts: Configure the guest account settings.



EDIMAX Pro

6 Guest Accounts

Guest Accounts

Guest Accounts

Guest Authentication: Login Account

Account Usage: 3/512

Manage User Account: Setup

Generate Printed Ticket: Setup

Captive Portal: Setup

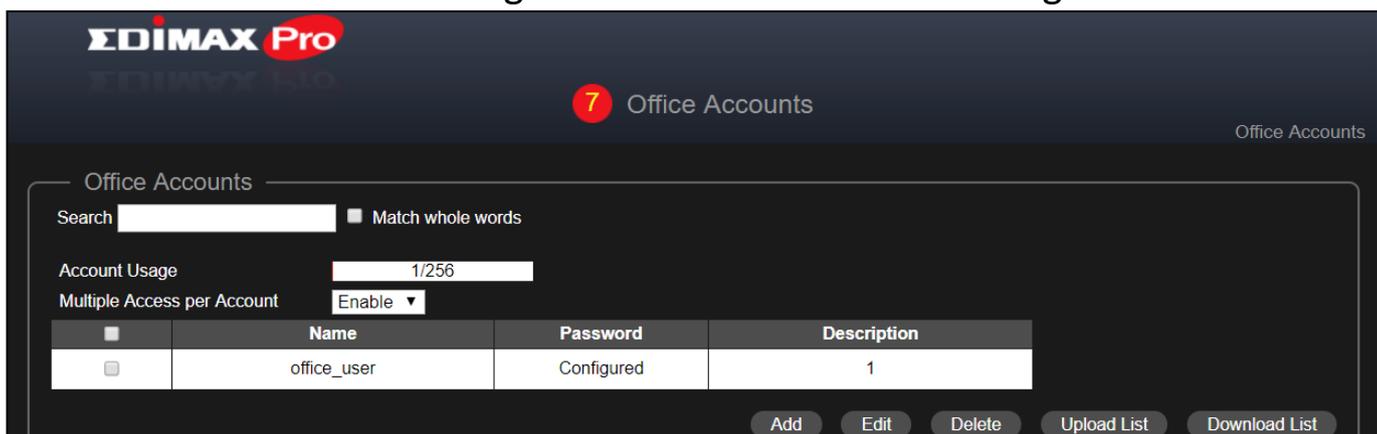
SMS Service: Setup

Multiple Access per Account: Disable

For more information on the settings, please refer to VII-6 **Guest Accounts** on page 64.

Press “Next” to continue.

8. Office Accounts: Configure the Office Accounts settings.



EDIMAX Pro

7 Office Accounts

Office Accounts

Office Accounts

Search: Match whole words

Account Usage: 1/256

Multiple Access per Account: Enable

	Name	Password	Description
<input type="checkbox"/>	office_user	Configured	1

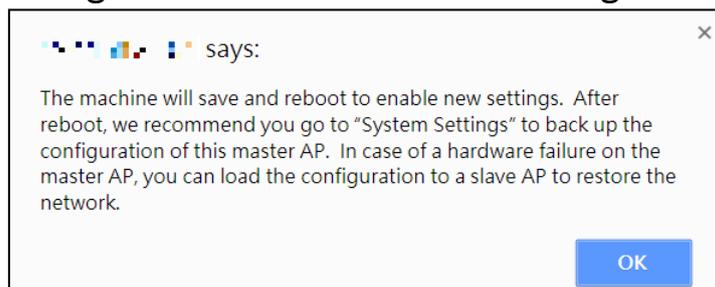
Add Edit Delete Upload List Download List

For more information on the settings, please refer to VII-7 **Office Accounts** on page 74.

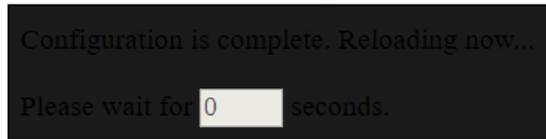
Press “Next” to continue.

9. Click “Save & Exit” to complete the wizard.

An advice message will be shown before saving and rebooting:



Click "OK" to continue (with message shown below):



- 10.** Please wait for ~10 minutes to apply the settings to the Slave APs.

IV Further Expansion

The Office 1-2-3 comes with 3 Office 1-2-3 Access Points that are pre-configured. Expansion is very easy with additional Office 1-2-3 Access Points (available as Office +1 AP) of up to 8 access points in total. An example is shown below:

The master Office 1-2-3 AP is designated as the Master ap to manage other connected Office 1-2-3 APs as they are automatically designated as Managed APs (slaves).

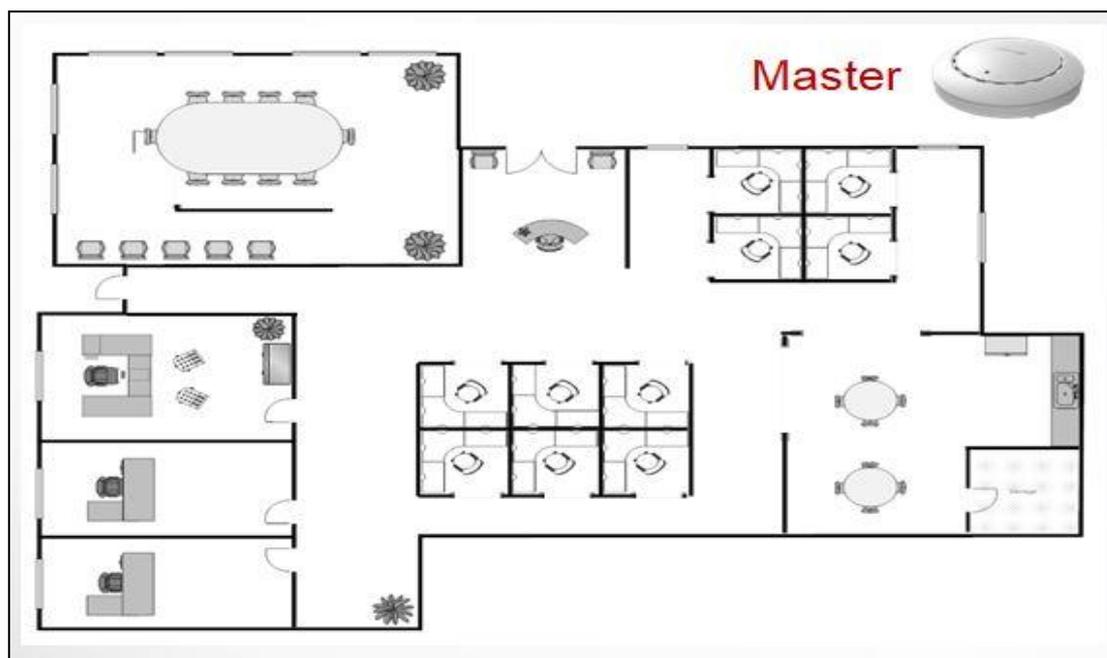
V Hardware Installation / Deployment

Once you have completed the setup wizard outlined in Quick Setup, you will have to determine how you will deploy your Office 1-2-3 Access Points.

V-1 Office 1-2-3 Deployment

1. Install the Master AP in a less crowded area.

This will reduce the loading of the Master AP. Due to the fact that the Master AP being the controller of the network, having a reduced loading will benefit. For example, you can install the Master AP in a corner of your office, where there will be less users attempting to connect to it.



2. Install the slave APs in more crowded areas.

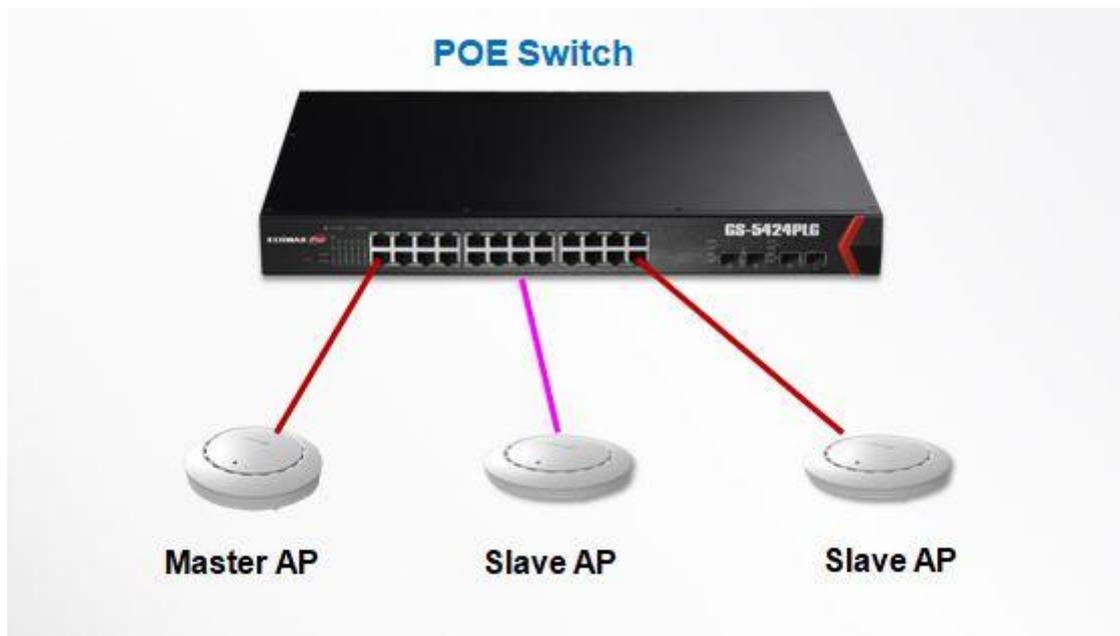
Since the APs will only be extending the Wi-Fi signals (no need to manage the network), they can be installed where connections are in greater demand.

The distance between the Master AP and the Slave APs is recommended to be between 20-25 meters.



3. Install Master/Slave AP Hardware on the POE switch.

Connect a PoE switch to the Master and Slave AP's **LAN 1** (PoE) port using an Ethernet cable.

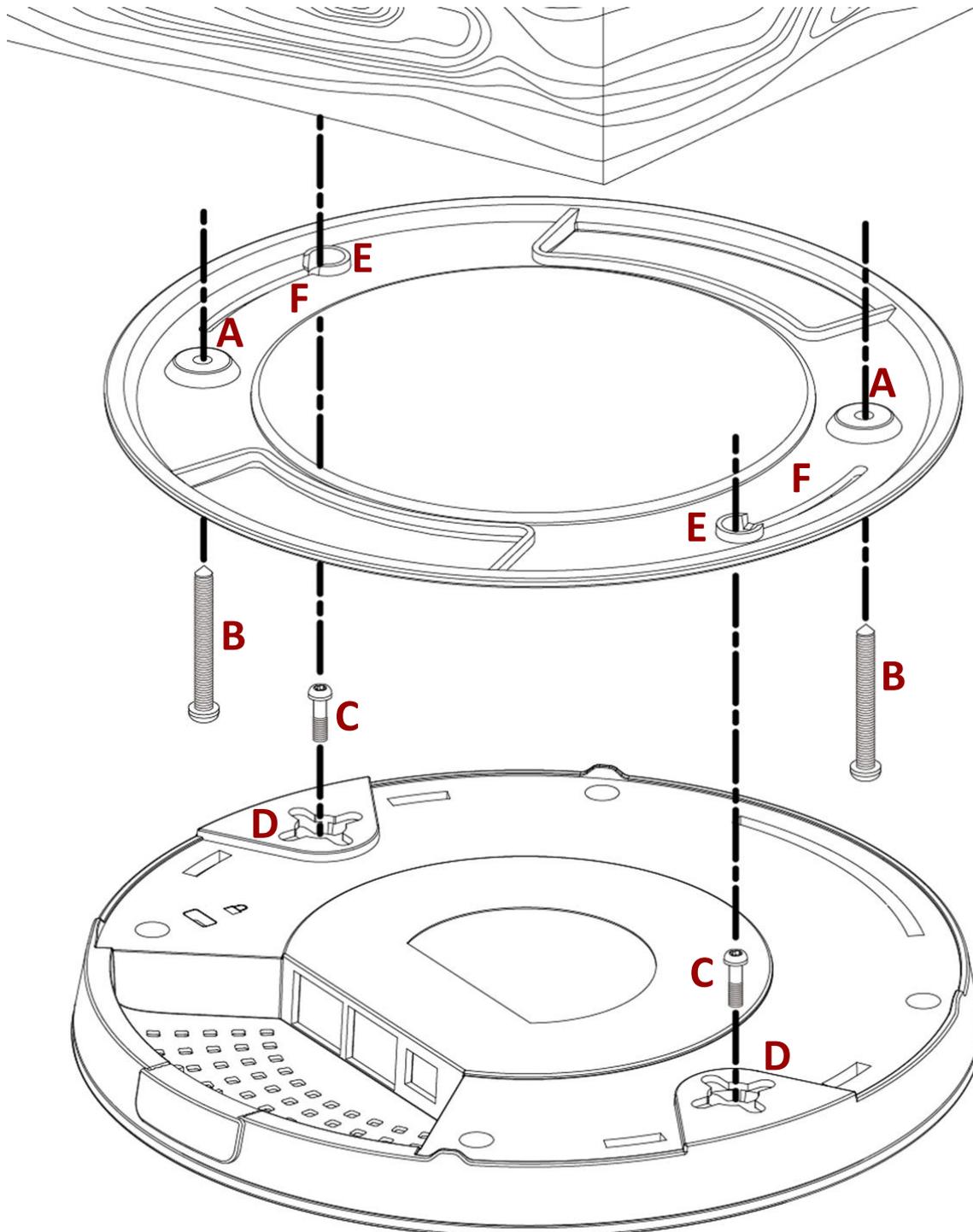


V-2 Mounting

When deployment plan is sorted, please refer to the instructions below on how to mount each of your Office 1-2-3 Access Points to a ceiling.

V-2-1 Wooden Ceiling

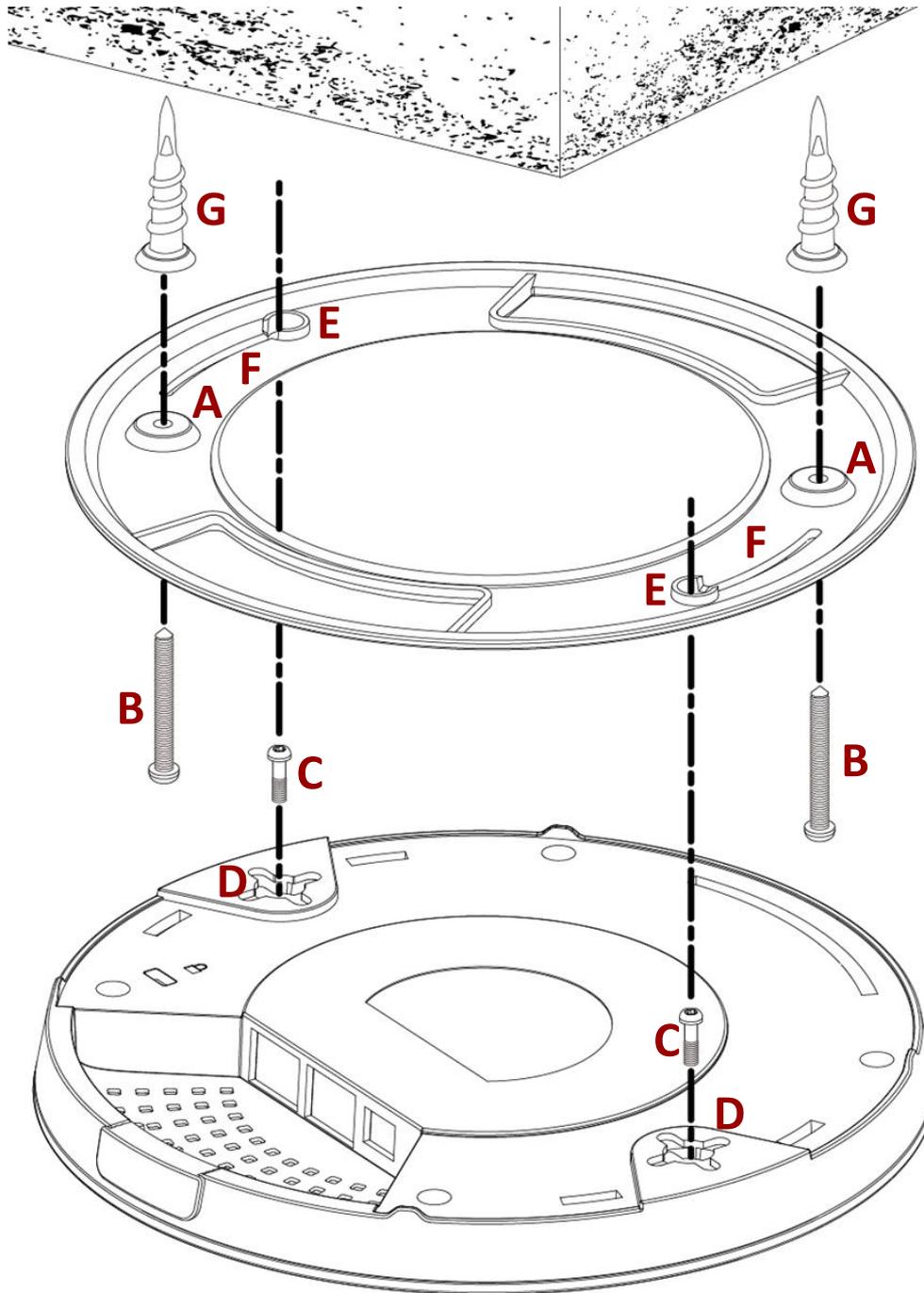
Please refer to the figure below:



- 1.** By using the holes **A** on the ceiling bracket, identify and mark correct screw positions of the desired mounting location.
- 2.** Where necessary, drill a hole (of radius smaller than the radius of the provided screws) on each of the marked screw positions.
- 3.** Fix the ceiling mount bracket to the desired location by inserting the ceiling fixing screws **B** through the bracket ceiling holes **A**. Tighten the ceiling fixing screws **B** to the marked screw position using a screw driver to fix the bracket in place.
- 4.** Fix the bracket rail screws **C** into the holes **D** on the device using a screw driver. The cap of the screws should be protruding outwardly from the holes **D**.
- 5.** Insert the bracket rail screws **C** into the device fixing holes **E**.
- 6.** Twist the device as the bracket rail screws **C** slide through the bracket rail **F**.
Twist the device all the way until you feel that it is fixed in position.

V-2-2 Other Ceiling

Please refer to the figure below:

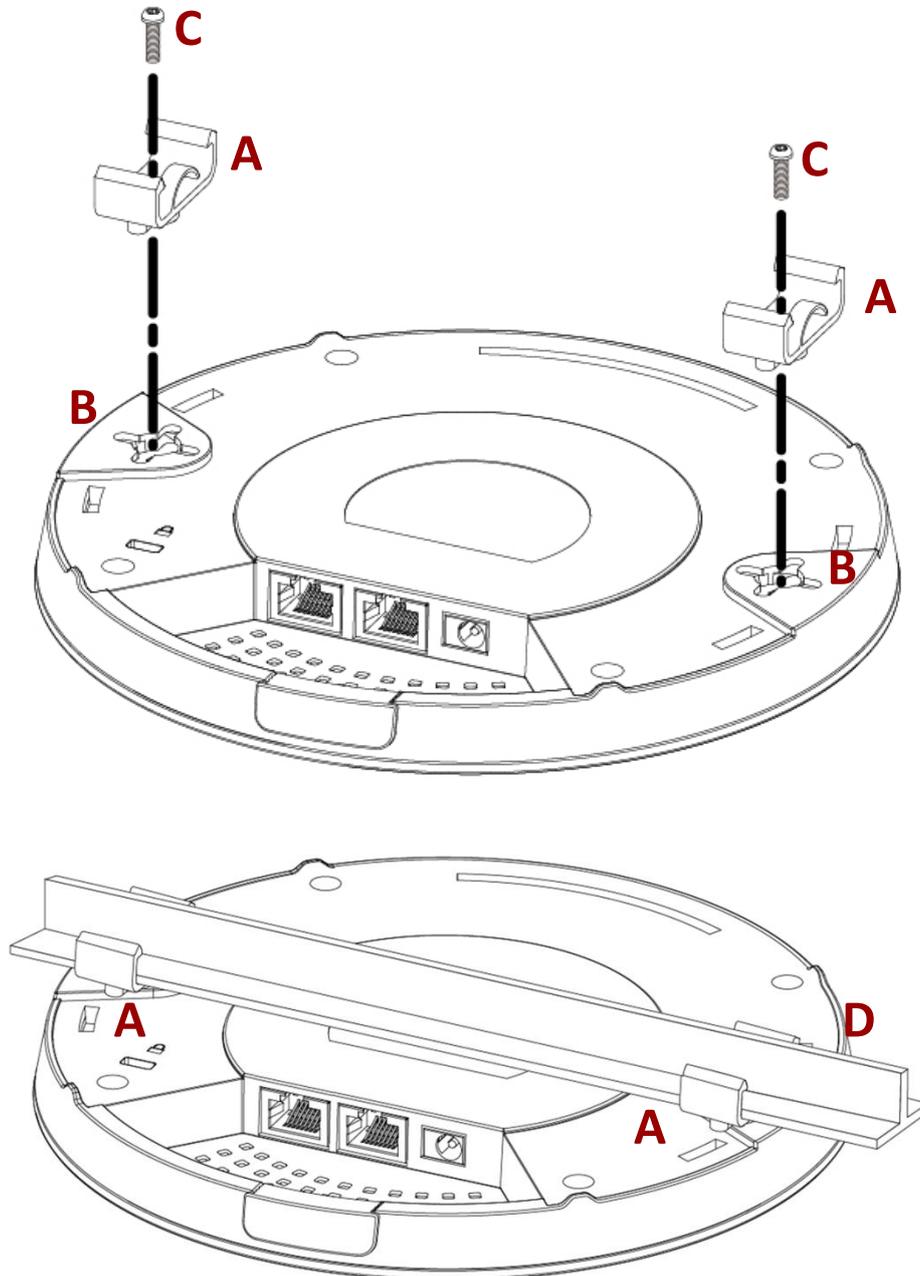


1. By using the holes **A** on the ceiling bracket, identify and mark correct screw positions of the desired mounting location.
2. Where necessary, drill a hole on each of the marked screw positions.

- 3.** Insert the anchors **G** into the holes (use a screw driver where necessary) at the marked screw positions.
- 4.** Fix the ceiling mount bracket to the desired location by inserting the ceiling fixing screws **B** through the bracket ceiling holes **A**. Tighten the ceiling fixing screws **B** onto the anchors **G** using a screw driver to fix the bracket to the ceiling.
- 5.** Fix the bracket rail screws **C** into the holes **D** on the device using a screw driver. The cap of the screws should be protruding outwardly from the holes **D**.
- 6.** Insert the bracket rail screws **C** into the device fixing holes **E**.
- 7.** Twist the device as the bracket rail screws **C** slide through the bracket rail **F**.
Twist the device all the way until you feel that it is fixed in position.

V-2-3 T-Rail Mount

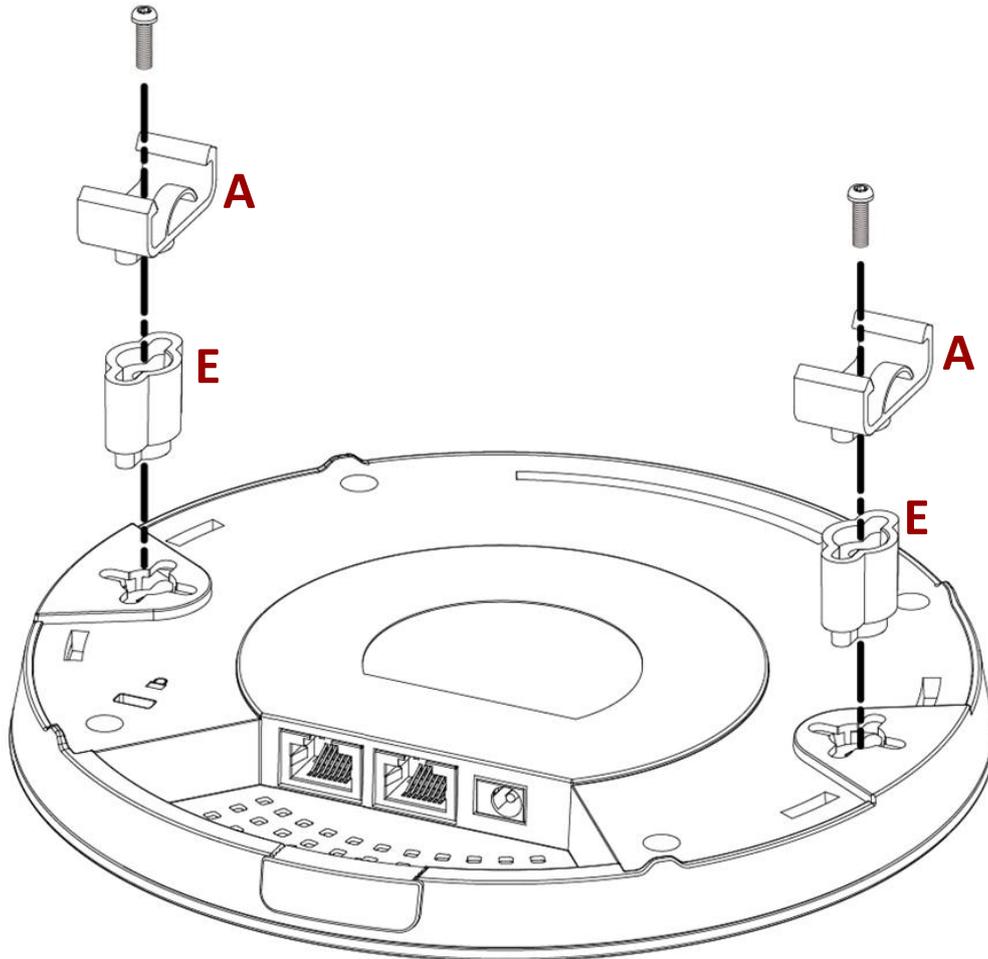
To mount the device to a T-Rail, please follow the instructions below and refer to the diagrams below.



1. Select the correct size T-Rail bracket included in the package contents.
2. Attach the selected T-Rail brackets **A** to holes **B** using bracket fixing screws **C**.

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

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



VI Replacing Master AP



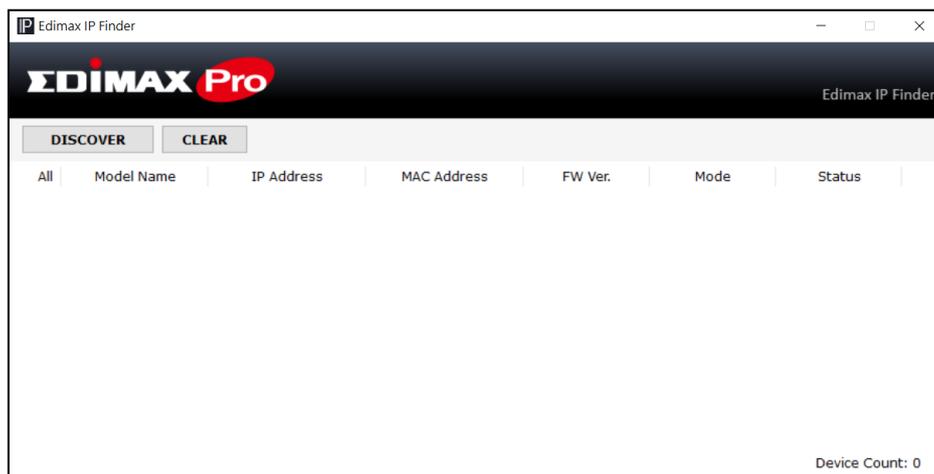
NOTE: there can only be **ONE** Master AP inside your network. Use this procedure only if your master AP is down and need a replacement.

This section will be a step-by-step procedure guiding you through replacing the original Master AP, where you will be upgrading to the Master AP's firmware, followed by recovering previously saved system settings.

Please make sure you have:

- **The Master AP firmware (downloadable from Edimax website)**
- **The Master AP's settings (backed up from the system on a regular basis)**

1. Open the "EdimaxCloudDiscoveryTool":



Reminder:

Download and Install the Edimax Cloud Discovery Tool (IP Finder) on your computer from the link below:

www.edimax.com/edimax_pro/download/IPfinder



If you are unable to open the IP Finder Tool, please refer to the included IP Finder document in the Office 1-2-3 Kit Box or III-1 **Initial Setup – Computer**.

2. Locate your Office +1 AP by clicking “Discover”  on the IP finder.

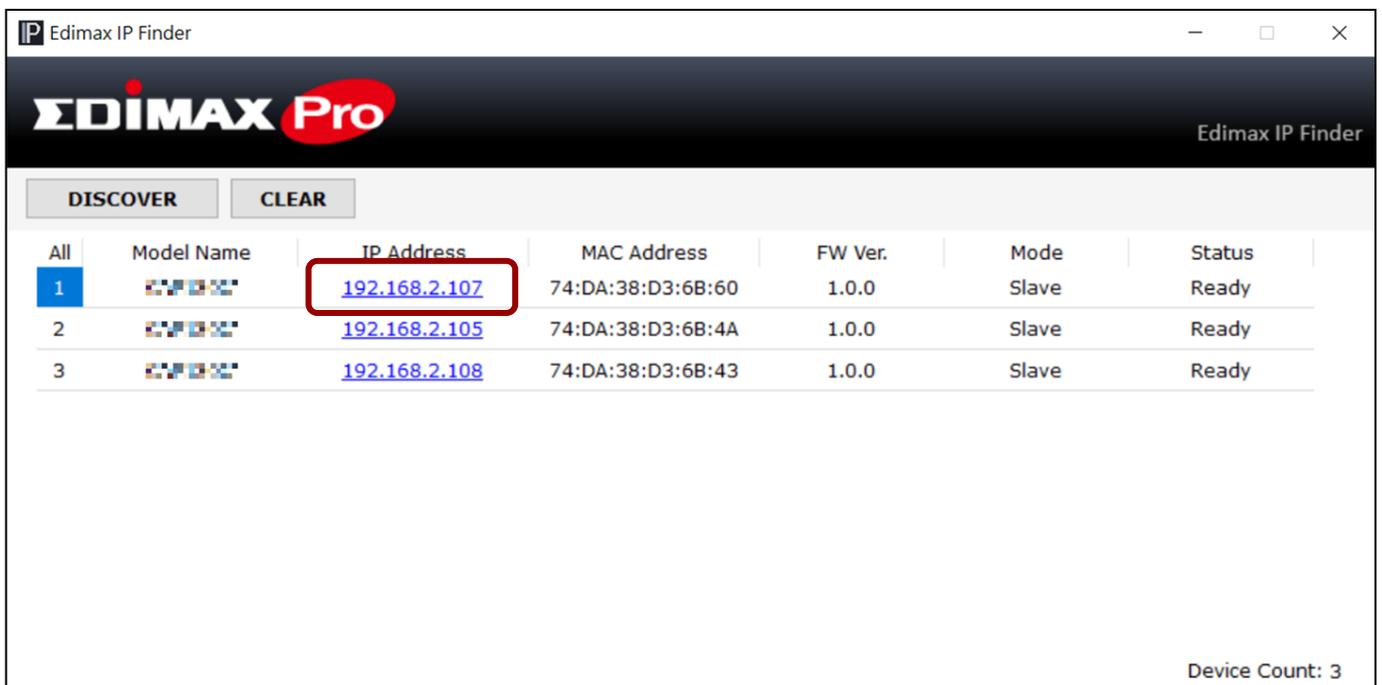


The screenshot shows the Edimax IP Finder application window. At the top, there is a header with the Edimax Pro logo and the text "Edimax IP Finder". Below the header, there are two buttons: "DISCOVER" and "CLEAR". A table displays the results of the discovery process. The table has seven columns: "All", "Model Name", "IP Address", "MAC Address", "FW Ver.", "Mode", and "Status". Three rows of data are shown, with the first row highlighted by a red border. The "All" column for the first row contains the number "1".

All	Model Name	IP Address	MAC Address	FW Ver.	Mode	Status
1	EW7220	192.168.2.107	74:DA:38:D3:6B:60	1.0.0	Slave	Ready
2	EW7220	192.168.2.105	74:DA:38:D3:6B:4A	1.0.0	Slave	Ready
3	EW7220	192.168.2.108	74:DA:38:D3:6B:43	1.0.0	Slave	Ready

Device Count: 3

3. Click the IP address of the access point designated to be the master AP and go into the web user interface.



This screenshot is identical to the previous one, showing the Edimax IP Finder application window with the same table of discovered devices. In this view, the IP address "192.168.2.107" in the first row of the table is highlighted with a red box.

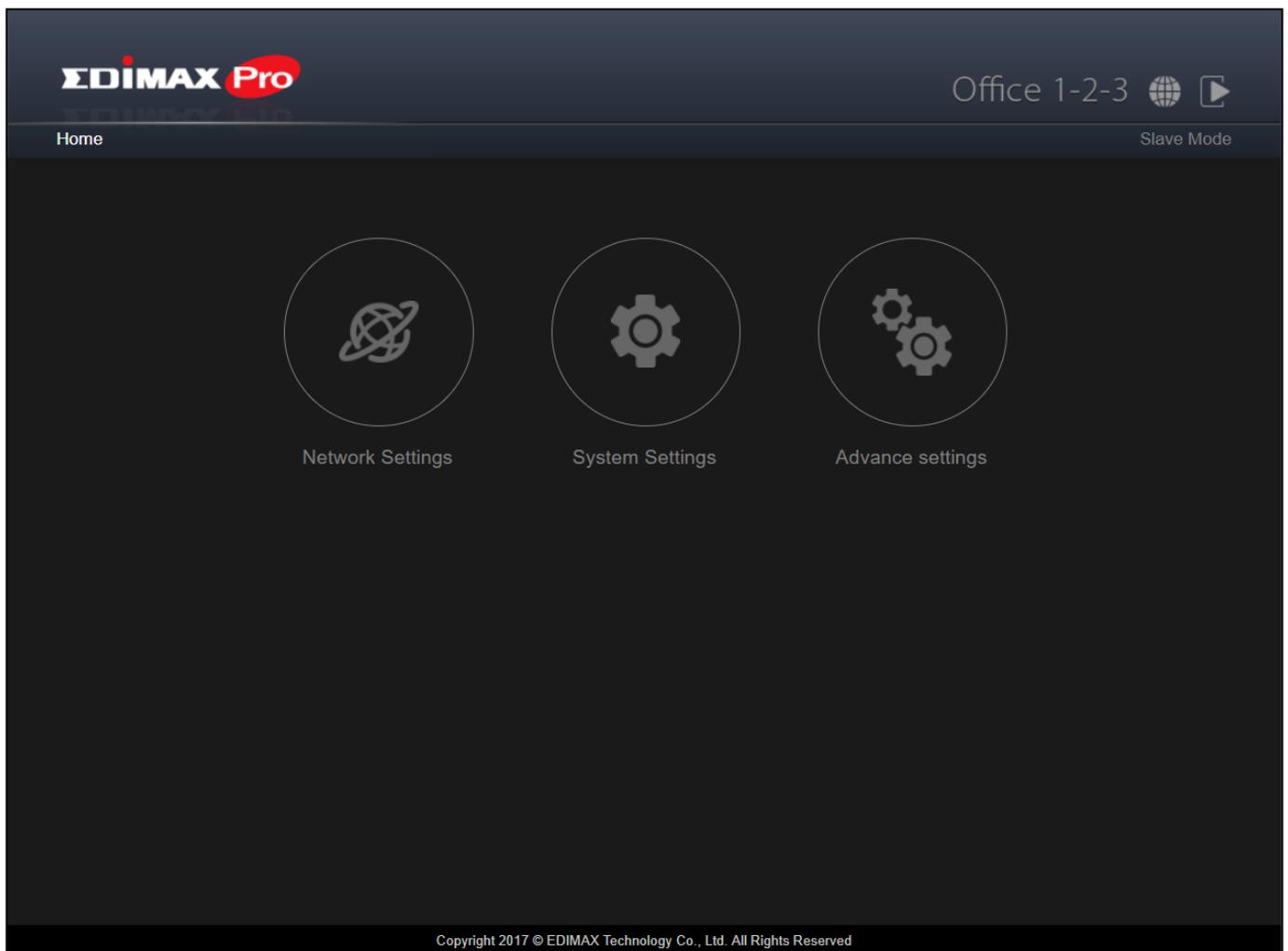
All	Model Name	IP Address	MAC Address	FW Ver.	Mode	Status
1	EW7220	192.168.2.107	74:DA:38:D3:6B:60	1.0.0	Slave	Ready
2	EW7220	192.168.2.105	74:DA:38:D3:6B:4A	1.0.0	Slave	Ready
3	EW7220	192.168.2.108	74:DA:38:D3:6B:43	1.0.0	Slave	Ready

Device Count: 3

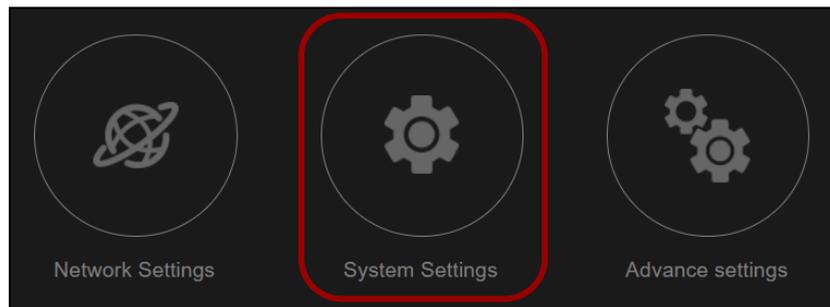
Upon entering the webpage, you should be prompted to enter the username and password, enter them (default username: **admin**, password: **1234**) to proceed:



The web user interface is shown below:

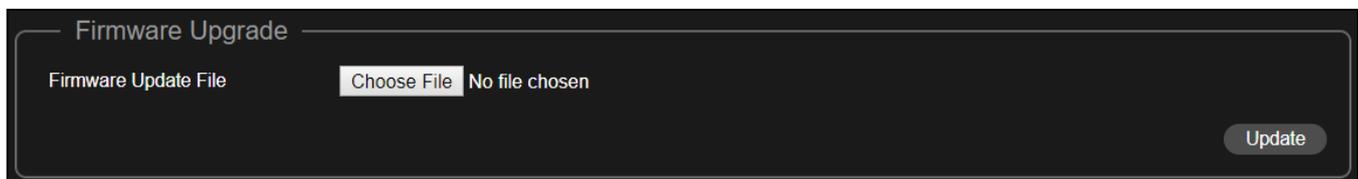


- Click on “System Settings” icon.



Upgrading Firmware

- Scroll down to the bottom of the page to find “Firmware Upgrade”.

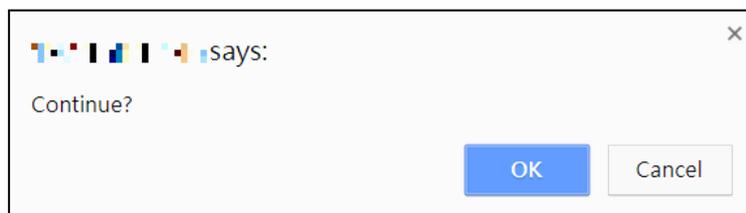


If you haven't already, please go to the URL link below to download the newest Master firmware:

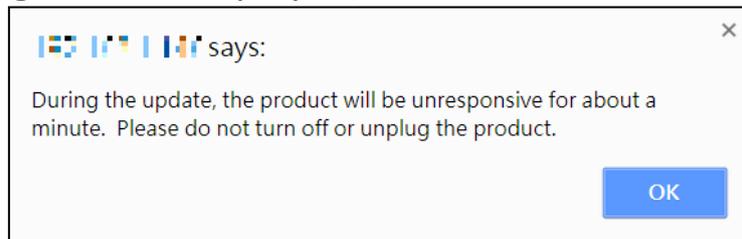
www.edimax.com/edimax_pro/download/Office1-2-3

Locate the Master firmware and click on the download icon to download.

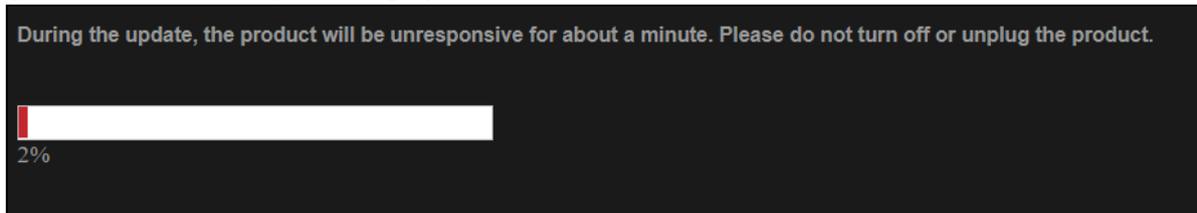
- Click “Choose File” to select the master firmware file.
- Click “Update” to update the unit to the master firmware version. The system will ask you whether to continue, click “OK”.



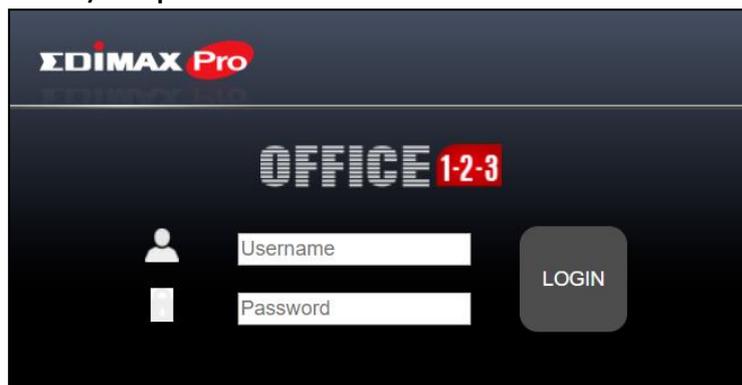
A reminder message will be displayed, click “OK” to continue.



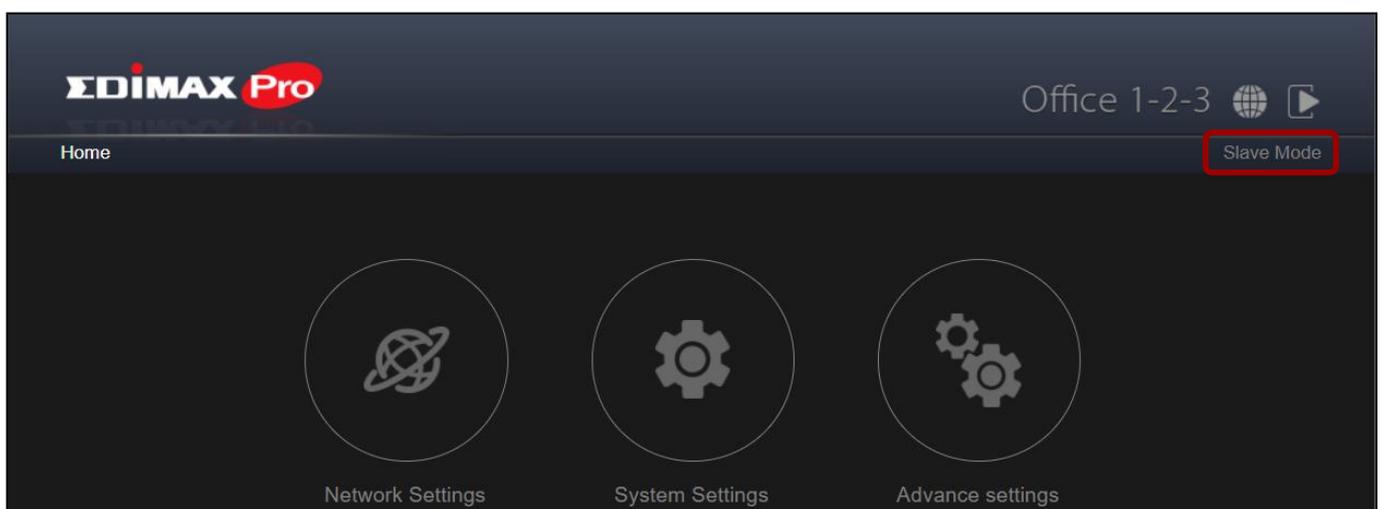
The system will be updating, please wait...



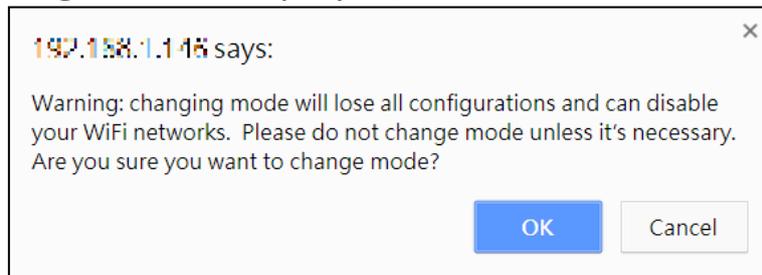
8. After the firmware upgrade, the system will prompt you to enter the username and password, enter them (default username: **admin**, password: **1234**) to proceed:



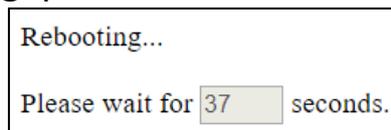
9. The system is still in slave mode, click on the outlined “Slave Mode” icon and click “Master Mode”:



More system message will be displayed, click “OK” to continue”



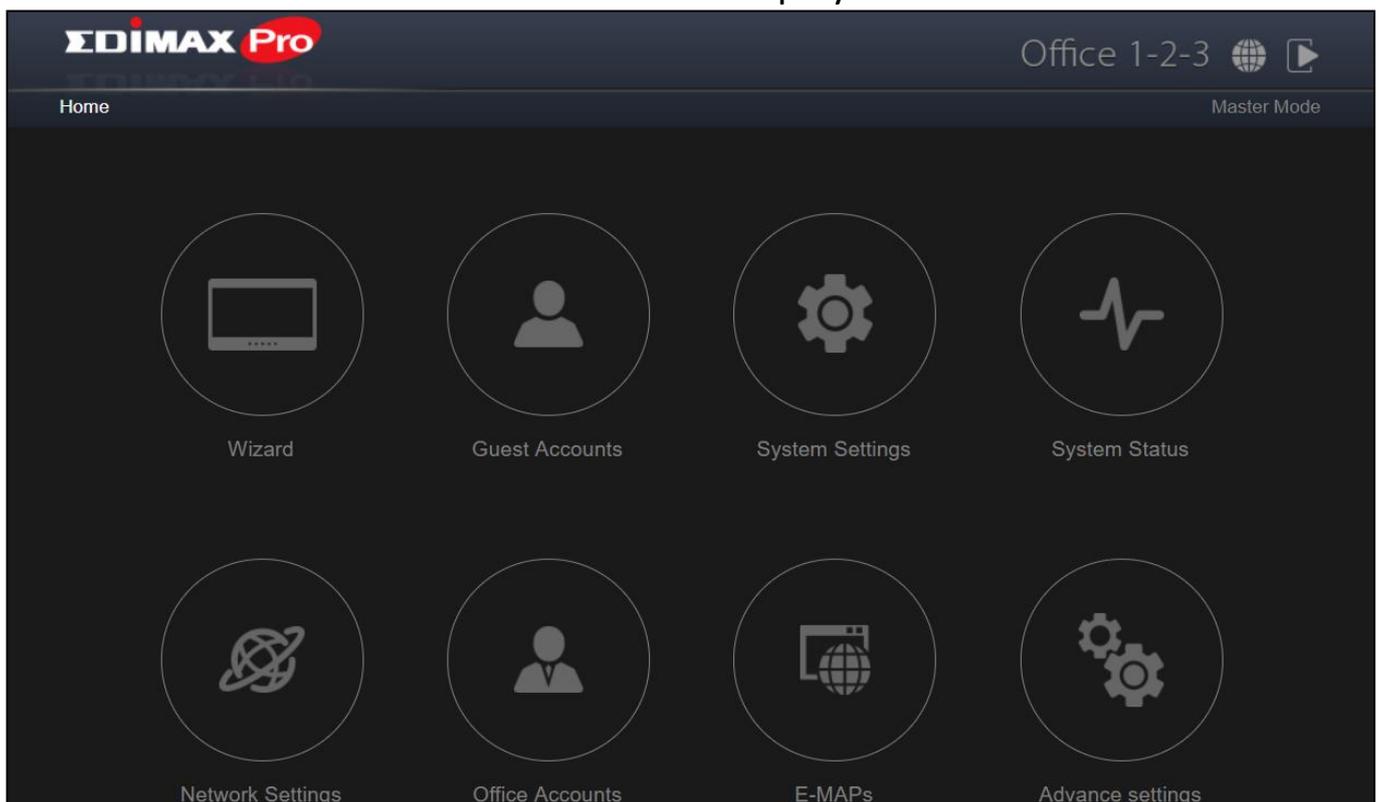
The system is now rebooting, please wait...



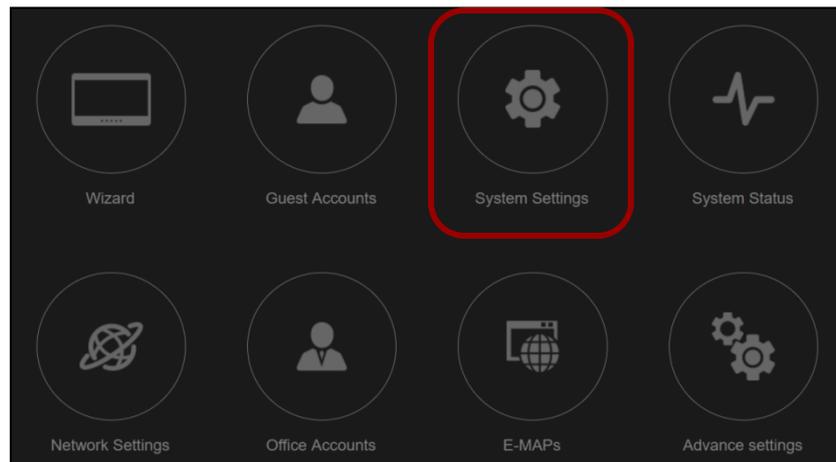
- 10.** After the firmware upgrade, the system will prompt you to enter the username and password again, enter them (default username: **admin**, password: **1234**) to proceed:



The Master AP web user interface will be displayed:

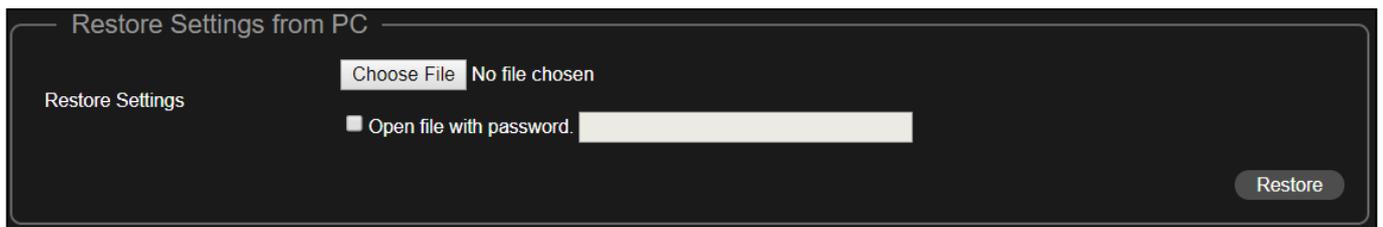


11. Click on “System Settings” icon.



Restore Previous Settings

12. Scroll down to find “Firmware Upgrade”.

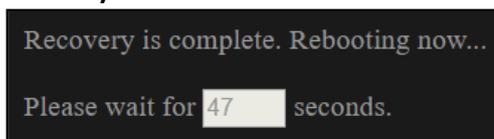


13. Click the “Choose File” button to find a previously saved settings file on your computer.

14. 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 following field.

The system will show that restoring the settings is complete and is rebooting:



Congratulations! You have successfully replaced the previous Master AP!

VII Office 1-2-3 Interface

Office 1-2-3 offers friendly interface that are easy to use and intuitive for administrators.

VII-1 IP Finder

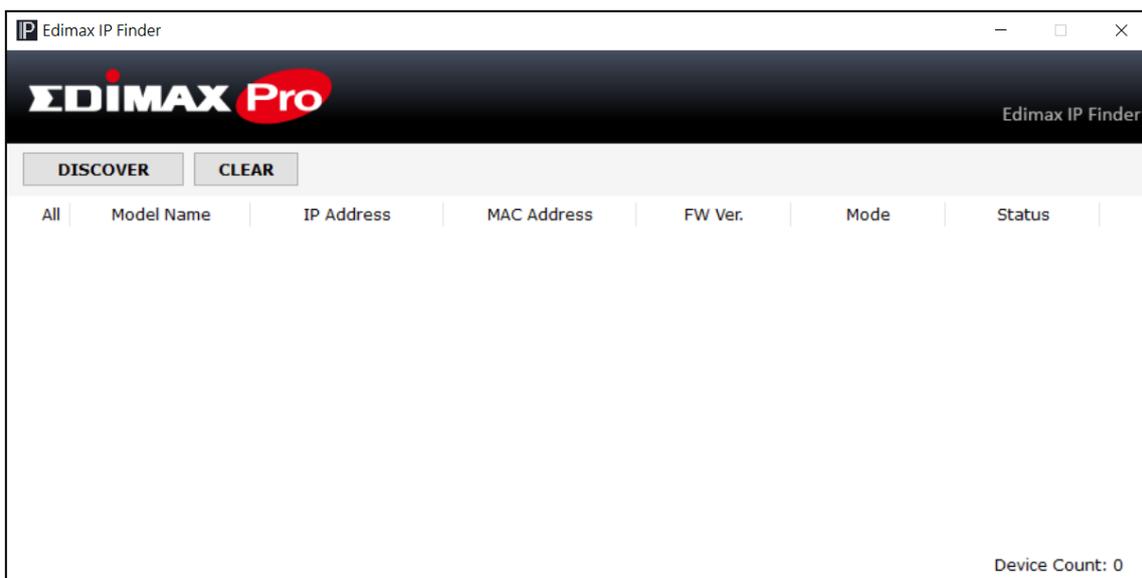
IP Finder is a tool to help you discover Office 1-2-3 Access Points currently connected to your network. It will display the Access Points' *IP Addresses*, *MAC Addresses*, *Firmware Version*, *Current Mode* and *Current Status*.

- Download and Install the Edimax Cloud Discovery Tool (IP Finder) on your computer from the link below:

www.edimax.com/edimax_pro/download/IPfinder



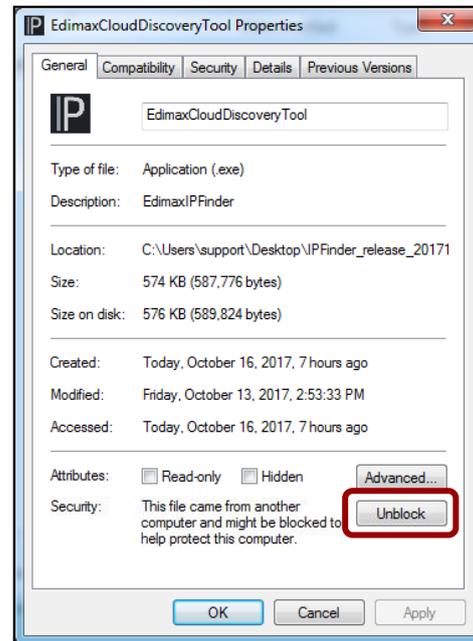
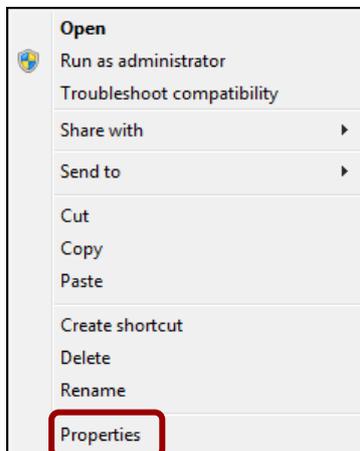
- Once downloaded, double-click the file to open the tool. The finder interface is as shown below:



Unable to open IP Finder Tool

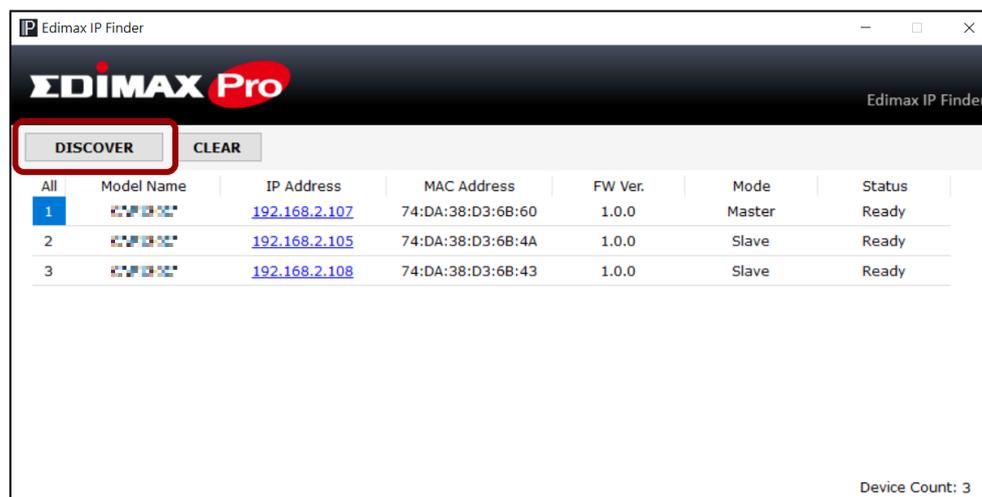
If you were unable to open the IP Finder Tool, it may be because the antivirus on your system is blocking it. To unblock, please see below:

1. Right-click on the IP Finder tool and click "Properties"
2. Locate "Security" at the bottom of the window. Click the **Unblock** button.



Discover

Clicking the  button will display all Access Points in your network.



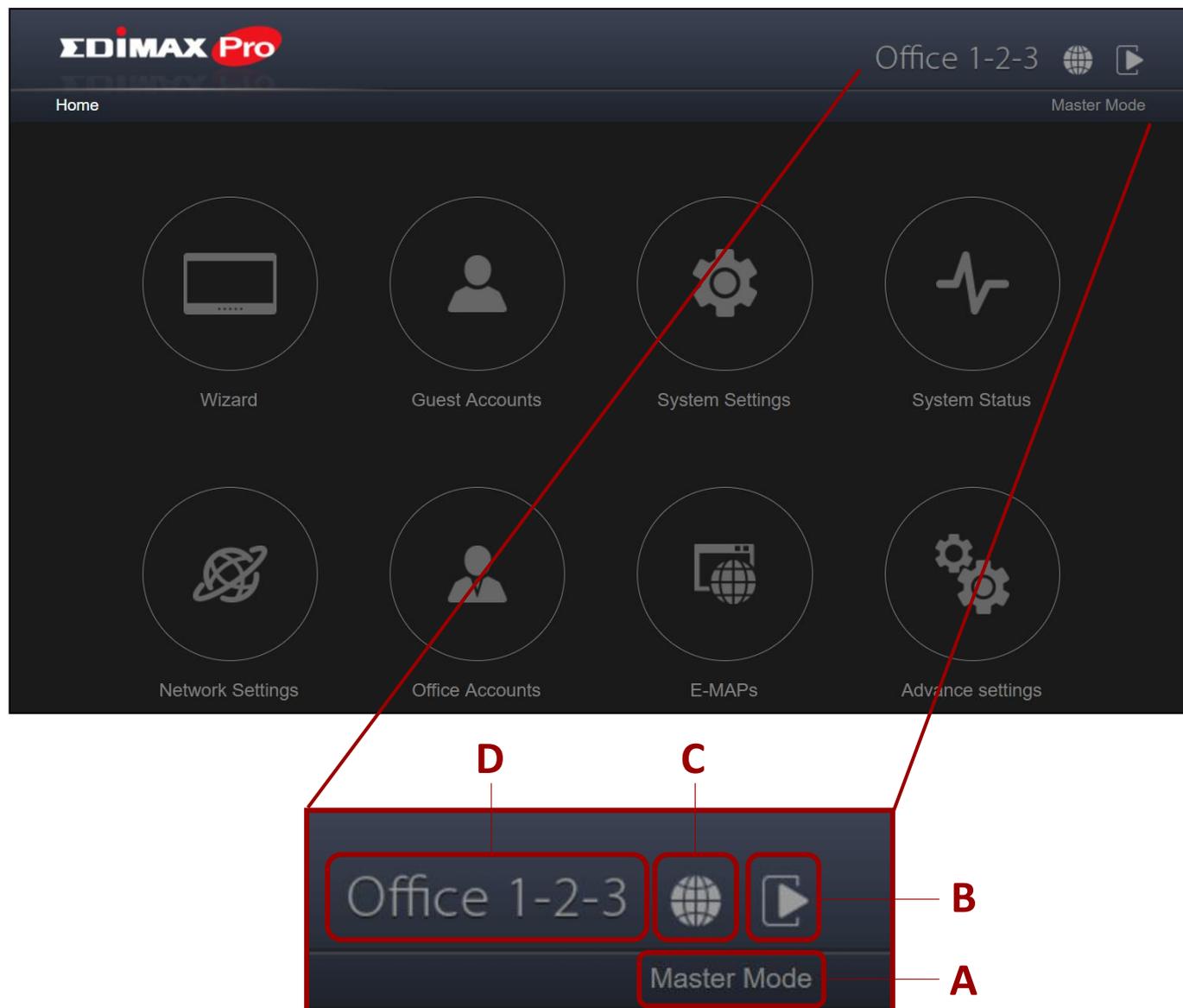
Enter Office 1-2-3 Setup Page

Clicking on the IP Address of an Access Point allows you to go into its setup page.

All	Model Name	IP Address	MAC Address	FW Ver.	Mode	Status
1		192.168.2.107	74:DA:38:D3:6B:60	1.0.0	Master	Ready
2		192.168.2.105	74:DA:38:D3:6B:4A	1.0.0	Slave	Ready
3		192.168.2.108	74:DA:38:D3:6B:43	1.0.0	Slave	Ready

VII-2 Home

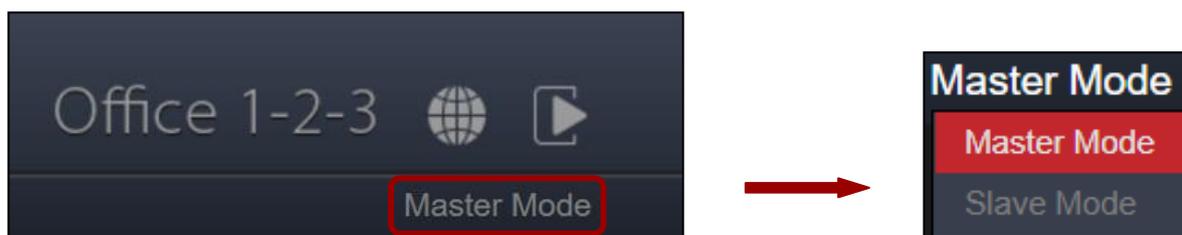
This is the dashboard or home of the Office 1-2-3 interface.



To **select the mode** of the access point, click **A** and select the mode:

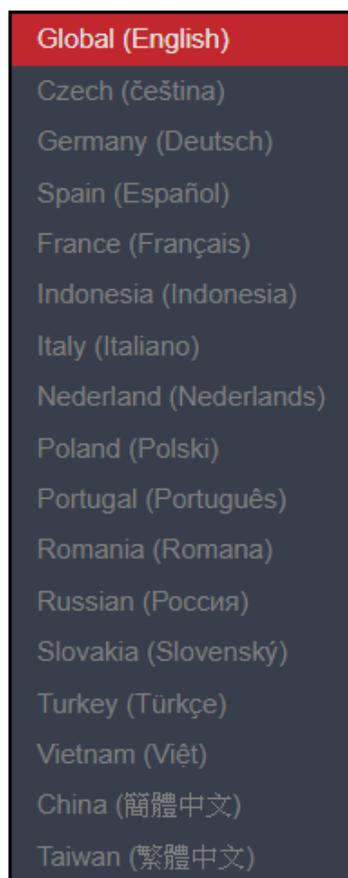


NOTE: You can change between master and slave modes at will by clicking the current mode (outlined area below). It is, however, not recommended except for the recovery of master AP.



To **log out** of the web user interface, click  (or **B**).

To select a different **language**, click  (or **C**) and select the language of the interface:



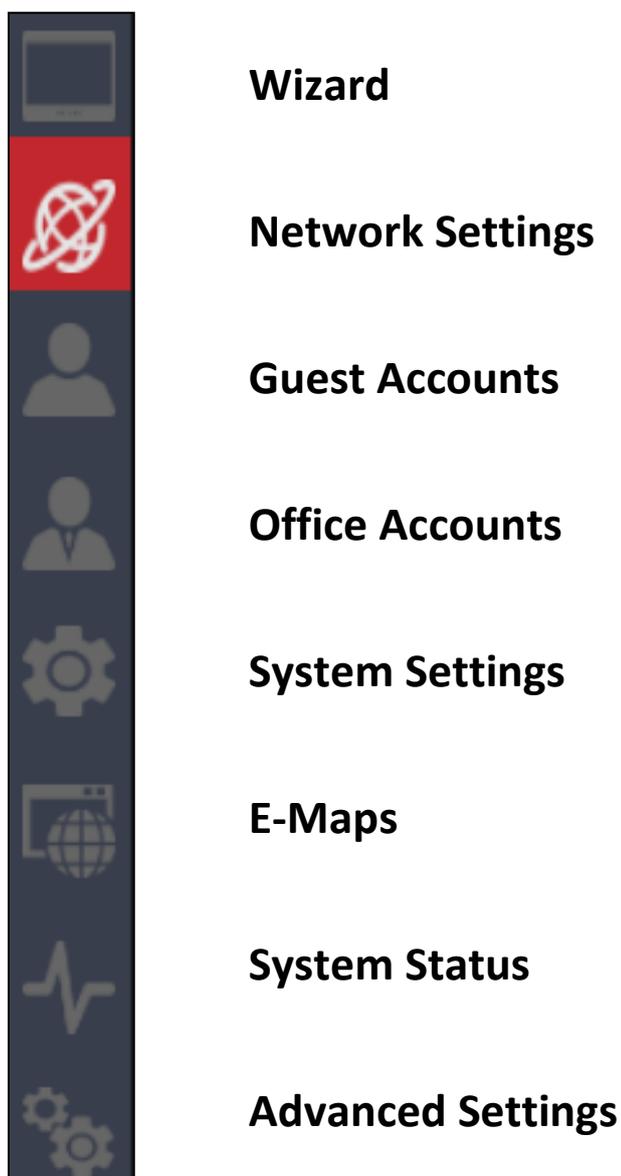
If you wish to return to this home page during any of the navigation through the interface, click  (or **D**) to **return home**.

VII-3 Wizard

Click the “Wizard” icon to go through the setup wizard of office 1-2-3. Refer to III-3 *Setup Wizard* on the setup process.

VII-4 Navigation

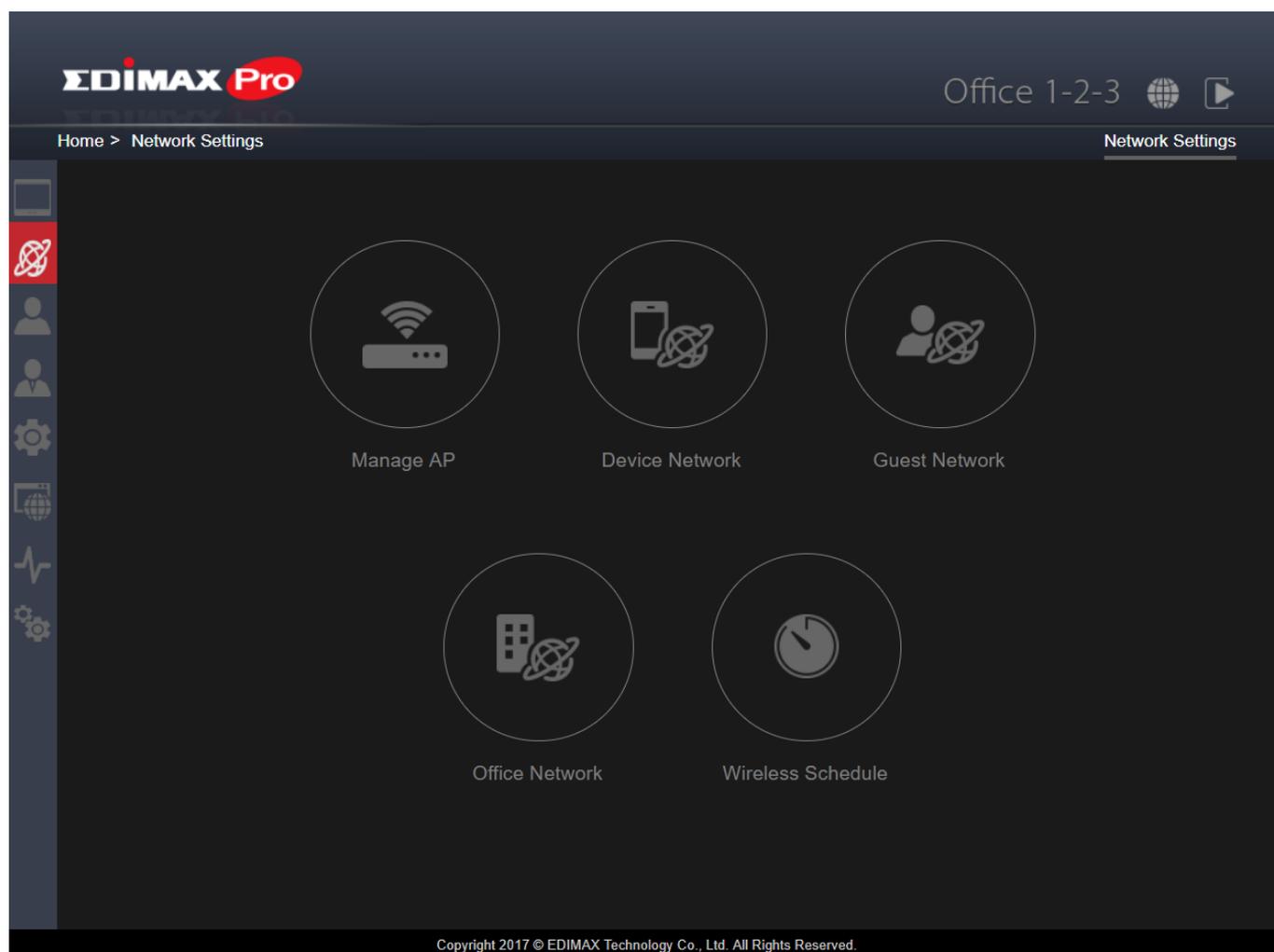
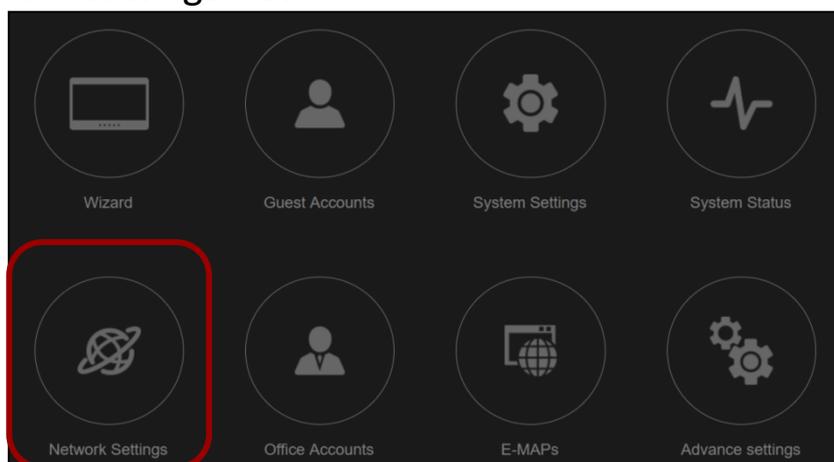
When using the user interface, navigation can also be achieved by selecting the navigation icons on the left, as demonstrated below:



VII-5 Network Settings

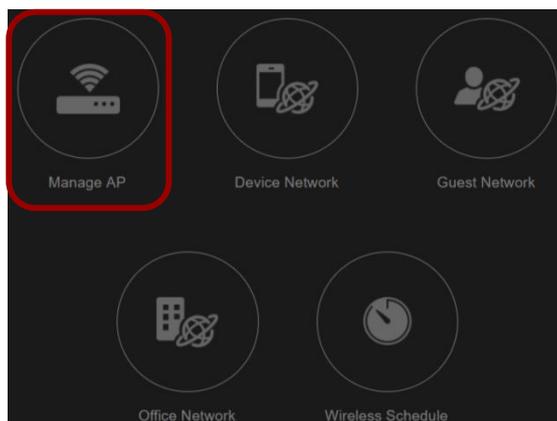
This is the general **network** settings of your Office 1-2-3 system. You can *Manage APs*, *Manage AP group*, configure *Office Network*, *Device Network*, *Guest Network* and setup a *Wireless Schedule* for your system.

Click the “Network Settings” icon.



VII-5-1 Manage AP

Click the “Manage AP” icon.



EDIMAX Pro Office 1-2-3

Home > Network Settings > Manage AP

Manage AP

Managed AP

Index	Mode	Device Name	Model	IP Address	Clients	Status	Action
1	Master	AP74DA38D36B60		192.168.2.107	1	●	[Icons]
2	Slave	AP74DA38D36B4A		192.168.2.105	0	●	[Icons]
3	Slave	AP74DA38D36B30		192.168.2.108	0	●	[Icons]

Refresh Edit Group Edit Delete

Unmanaged AP

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

Add Back

Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved.

This page displays information about each Managed AP in the local network: *Index (reference number), Mode, Device Name (MAC Address), Model, IP Address, No. of Clients connected to each access point, Status, and Actions.*

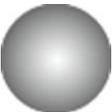
Click the “Refresh” button to refresh the managed AP list.

Click the “Edit” button to edit the checked AP’s settings (see **Edit** below).

Click the “Group Edit” button to edit the group settings (see **Group Edit** below).

Click the “Delete” button to delete the checked AP(s).

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 Master AP.</i>
	Red	Authentication Failed Or Incompatible AP Version	System security must be the same for all access points in the AP array. <i>Please check security settings.</i> All access points must have the same firmware version. <i>Please use the Master AP’s firmware upgrade function.</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 the Managed AP is connecting.</i>
	Green	Connected	<i>Managed AP is connected.</i>
	Blue	Waiting for Approval	Managed AP is waiting for approval. <i>Note: Up to 7 Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.</i>

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 (see **Edit** below).
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.

VII-5-1-1 Edit Managed AP

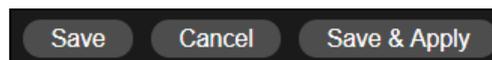
To Edit a managed AP, either **1)** check the checkbox of said AP, and click the “Edit” button;

<input type="checkbox"/>	Index	Mode	Device Name	Model	IP Address	Clients	Status	Action
<input type="checkbox"/>	1	Master	AP74DA38D36B60		192.168.2.107	1	●	
<input type="checkbox"/>	2	Slave	AP74DA38D36B4A		192.168.2.105	0	●	
<input type="checkbox"/>	3	Slave	AP74DA38D36B30		192.168.2.108	0	●	

Refresh Edit Group Edit Delete

Or **2)** click the  Edit icon.

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



VII-5-1-1-1 Basic Settings

If the AP is a member of an AP Group and you wish to use a different setting than the AP Group setting, check “**Override Group Setting**” for the options / fields to turn white to allow adjustments.



Basic Settings

Name: AP74DA38D36B4A

Description:

MAC Address: 74:DA:38:D3:6B:4A

IP Address Assignment: Override Group Setting DHCP Client

IP Address: 192.168.2.105

Subnet Mask: 255.255.255.0

Default Gateway: From DHCP 0.0.0.0

Primary DNS: User-Defined

Secondary DNS: User-Defined

IGMP Snooping: Override Group Setting Disable

LAN Port1 VLAN: Override Group Setting Untagged Port VID 1

LAN Port2 VLAN: Override Group Setting Untagged Port VID 1

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.
IP Address Assignment	<p>“DHCP Client” or “Static IP Address” are the two options. Select “DHCP Client” for automatic assignment of a dynamic IP address from your router’s DHCP server.</p> <p>Select “Static IP Address” to manually specify a static/fixed IP address for your access point.</p>
IP Address	<p>If “Static IP Address” is selected in the option above, specify an IP address in the field. This IP address will be assigned to your access point and will replace the default IP address.</p> <p>If “DHCP Client” is selected, no entry will be required.</p>
Subnet Mask	<p>If “Static IP Address” is selected in the option above, specify a subnet mask. The default value is 255.255.255.0.</p> <p>If “DHCP Client” is selected, no entry will be required.</p>
Default Gateway	<p>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.</p> <p>DHCP users can select “From DHCP” to get default gateway from DHCP. No entry will be required.</p> <p>Select “User-Defined” to manually enter a value.</p> <p>If “Static IP Address” is selected in the option above, enter a value in the field that follows.</p>
Primary DNS	<p>DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP. No entry will be required.</p> <p>Select “User-Defined” to manually enter a value.</p> <p>If “Static IP Address” is selected in the option above, enter a value in the field that follows.</p>
Secondary DNS	<p>DHCP users can select “From DHCP” to get secondary DNS server’s IP address from DHCP. No entry will be required.</p> <p>Select “User-Defined” to manually enter a value.</p> <p>If “Static IP Address” is selected in the option above, enter a value in the field that follows.</p>

IGMP Snooping	Enable / Disable the IGMP Snooping function. IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic.
----------------------	---

VII-5-1-1-2 Radio Settings

Check “**Override Group Setting**” for options/fields to turn white to allow adjustments.

Override Group Setting

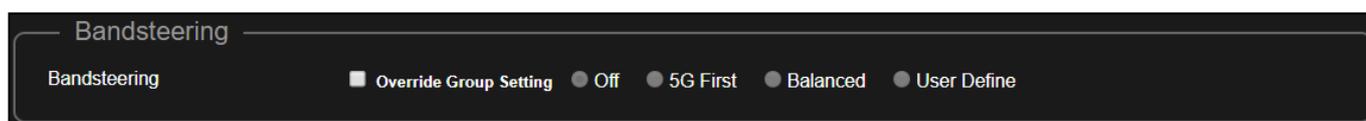
Radio Settings		
	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Wireless	<input type="checkbox"/> Override Group Setting Enable ▾	<input type="checkbox"/> Override Group Setting Enable ▾
Channel	<input type="checkbox"/> Override Group Setting Ch 11, 2462MHz ▾	<input type="checkbox"/> Override Group Setting Ch 36, 5.18GHz ▾
Channel Bandwidth	<input type="checkbox"/> Override Group Setting 20 MHz ▾	<input type="checkbox"/> Override Group Setting 20 MHz ▾
Tx Power	<input type="checkbox"/> Override Group Setting 100% ▾	<input type="checkbox"/> Override Group Setting 100% ▾

Radio Settings	
Wireless	Enable or disable the access point’s 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Channel	Select a channel manually.
Channel Bandwidth	Select a channel bandwidth.
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.

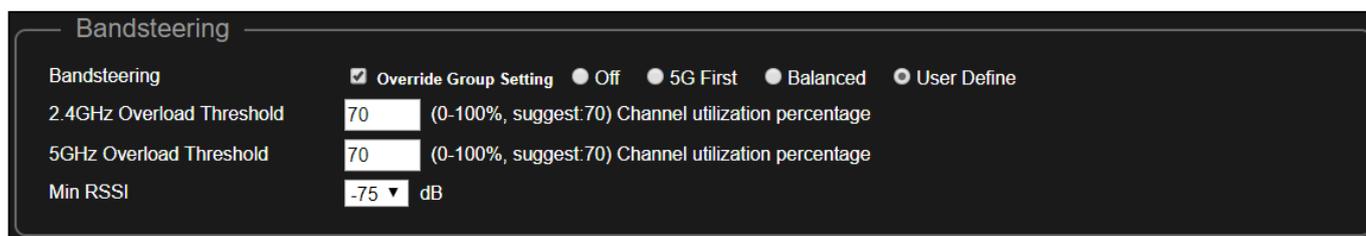
VII-5-1-1-3 Bandsteering

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

Check “**Override Group Setting**” for options/fields to turn white to allow adjustments.

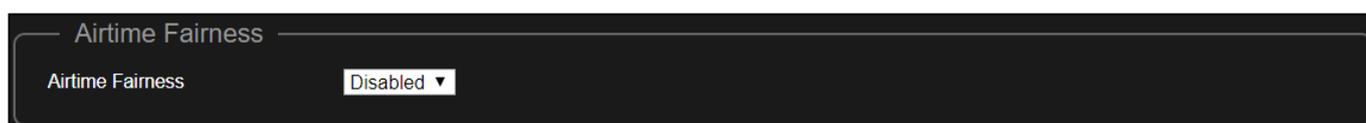


If user defined is selected, enter the threshold values and RSSI as desired.



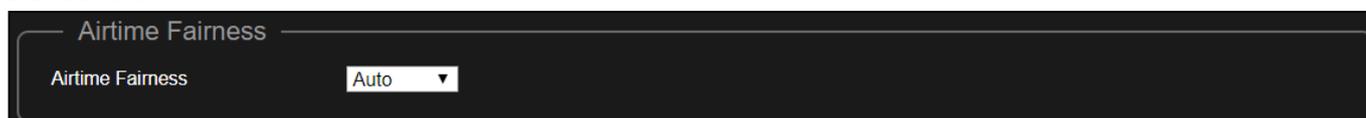
VII-5-1-1-4 Airtime Fairness

Enable / Disable this function by using the drop down menu.



Enable - Auto

The shared rate is automatically chosen by the system when “Auto” is selected.



Enable - Static

When "Static" is selected, enter the shared rates of the networks.

Airtime Fairness			
Airtime Fairness	Static		
Shared Rate	Device Network	0	%
	Office Network	0	%
	Guest Network	0	%

VII-5-1-2 Group Edit Managed AP

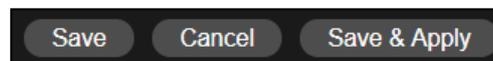
Click the “Group Edit” button to manage the AP group.

The screenshot shows the 'Managed AP' interface. It contains a table with the following data:

Index	Mode	Device Name	Model	IP Address	Clients	Status	Action
1	Master	AP74DA38D36B60	[Model Icon]	192.168.2.107	1	●	[Action Icons]
2	Slave	AP74DA38D36B4A	[Model Icon]	192.168.2.105	0	●	[Action Icons]
3	Slave	AP74DA38D36B30	[Model Icon]	192.168.2.108	0	●	[Action Icons]

Below the table are buttons for 'Refresh', 'Edit', 'Group Edit' (highlighted with a red box), and 'Delete'.

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



VII-5-1-2-1 Basic Settings

The screenshot shows the 'Basic Settings' interface with the following fields:

- Default Gateway: [Text Input]
- Primary DNS: [Text Input]
- Secondary DNS: [Text Input]
- IGMP Snooping: [Disable ▼]
- LAN Port1 VLAN: [Untagged Port ▼] VID [1]
- LAN Port2 VLAN: [Untagged Port ▼] VID [1]

Default Gateway, Primary DNS and Secondary DNS will be assigned by the DHCP Server.

Basic Settings	
IGMP Snooping	Enable / Disable the IGMP Snooping function. IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic.

VII-5-1-2-2 Radio Settings

Radio Settings		
	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Wireless	Enable ▼	Enable ▼
Channel	Ch 11, 2462MHz ▼	Ch 36, 5.18GHz ▼
Channel Bandwidth	20 MHz ▼	20 MHz ▼
Tx Power	100% ▼	100% ▼

Radio Settings	
Wireless	Enable or disable the access point's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Channel	Select a channel manually.
Channel Bandwidth	Select a channel bandwidth.
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.

VII-5-1-2-3 Bandsteering

Band steering detects clients capable of 5GHz operation and steers them there to make the more crowded 2.4 GHz band available for clients only capable of connecting to 2.4GHz band.

Bandsteering	
Bandsteering	<input type="radio"/> Off <input type="radio"/> 5G First <input type="radio"/> Balanced <input type="radio"/> User Define

If "User Defined" is selected, enter the threshold values and RSSI as desired.

Bandsteering	
Bandsteering	<input type="radio"/> Off <input type="radio"/> 5G First <input type="radio"/> Balanced <input checked="" type="radio"/> User Define
2.4GHz Overload Threshold	70 (0-100%, suggest:70) Channel utilization percentage
5GHz Overload Threshold	70 (0-100%, suggest:70) Channel utilization percentage
Min RSSI	-75 dB

VII-5-1-2-4 Airtime Fairness

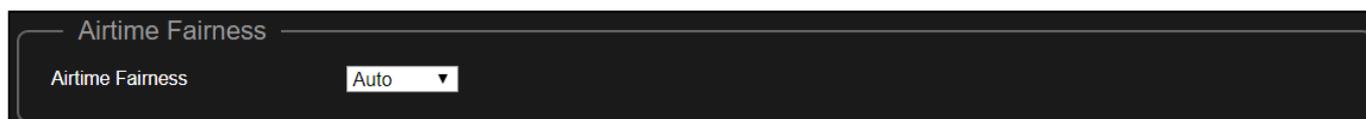
Enable / Disable this function by using the drop down menu.



A screenshot of a control panel titled "Airtime Fairness". It features a label "Airtime Fairness" and a dropdown menu currently set to "Disabled".

Enable - Auto

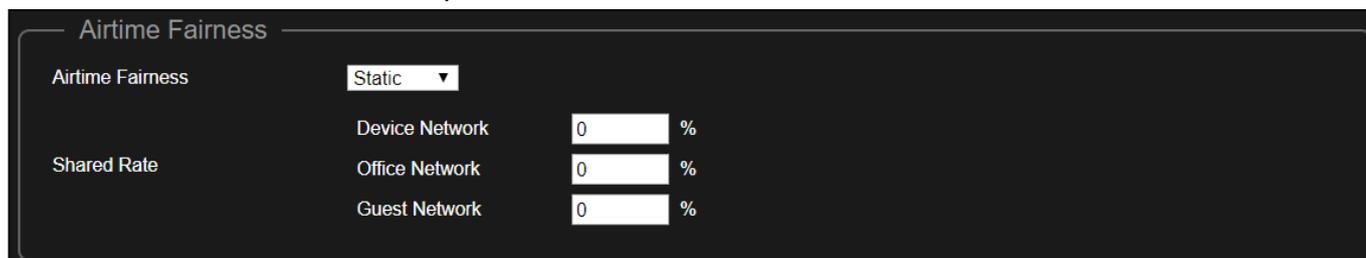
The shared rate is automatically chosen by the system when "Auto" is selected.



A screenshot of a control panel titled "Airtime Fairness". It features a label "Airtime Fairness" and a dropdown menu currently set to "Auto".

Enable - Static

When "Static" is selected, enter the shared rates of the networks.

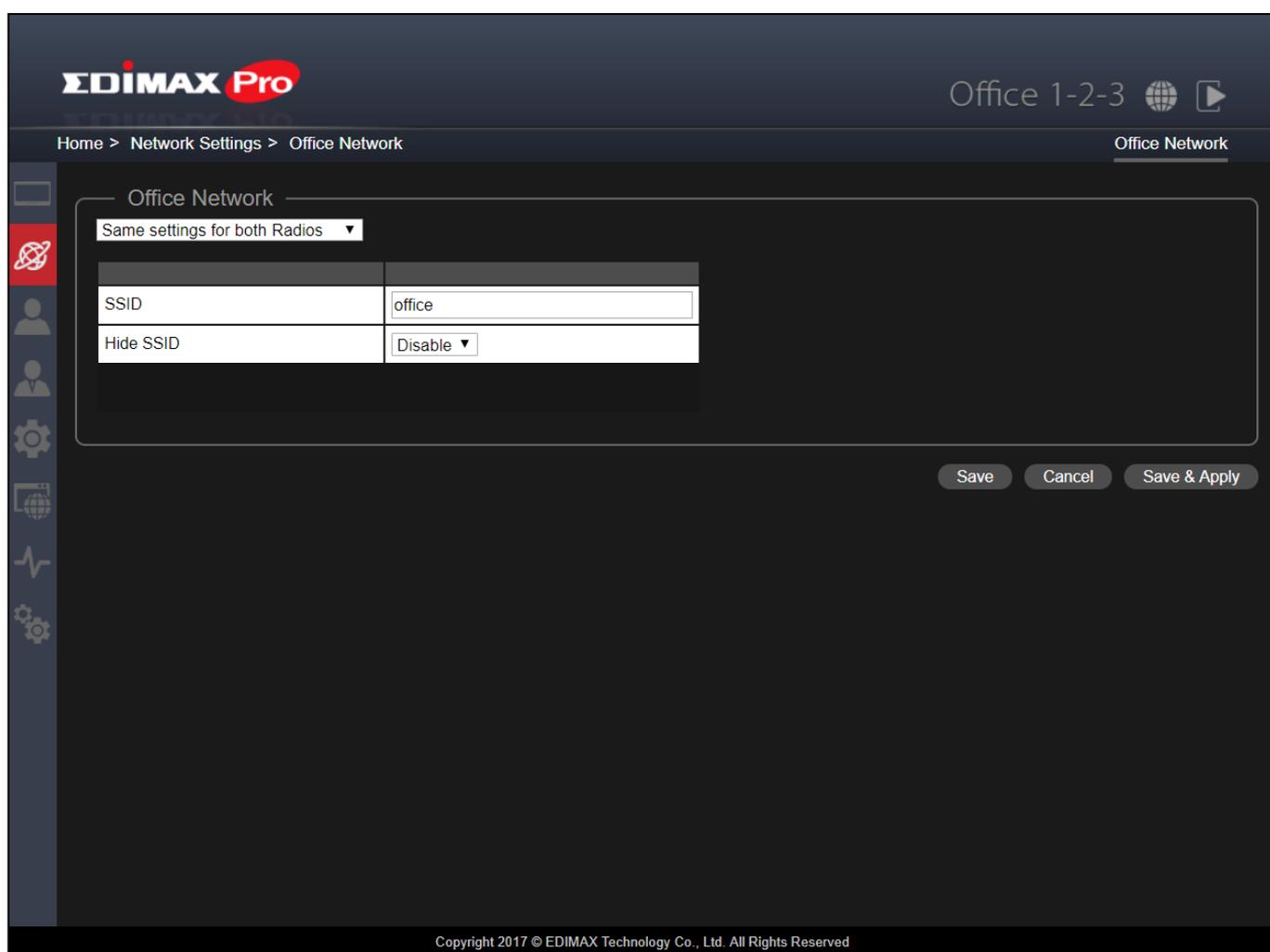
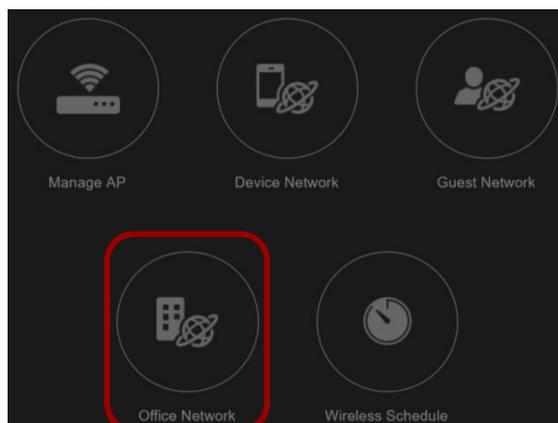


A screenshot of a control panel titled "Airtime Fairness". It features a label "Airtime Fairness" and a dropdown menu currently set to "Static". Below the dropdown, there are three rows of input fields under the heading "Shared Rate":

Network	Shared Rate (%)
Device Network	0
Office Network	0
Guest Network	0

VII-5-2 Office Network

Click the “Office Network” icon.



EDIMAX Pro

Office 1-2-3

Home > Network Settings > Office Network

Office Network

Office Network

Same settings for both Radios

SSID	office
Hide SSID	Disable

Save Cancel Save & Apply

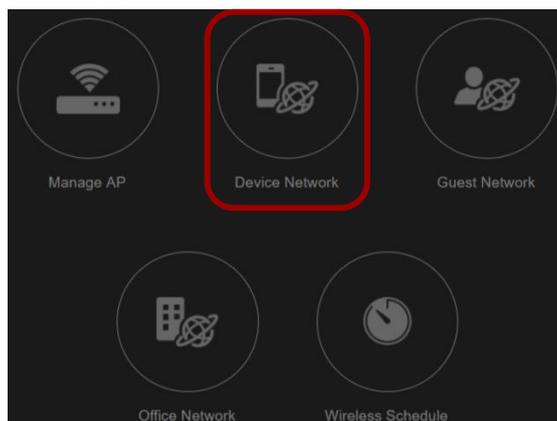
Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

Use the drop down menu to select whether you want “Same settings for both Radios” or “Different settings for each Radio” (“Different settings for each Radio” is displayed).

SSID	Enter an SSID name for the guest network.
Hide SSID	Enable: the SSID will be hidden. Clients must manually enter the SSID in order to connect. Disable: the SSID will be visible (default)

VII-5-3 Device Network

Click the “Device Network” icon.



EDIMAX Pro Office 1-2-3

Home > Network Settings > Device Network Device Network

Device Network

Same settings for both Radios ▾

SSID	device
Hide SSID	Disable ▾
Encryption	None ▾
Type	TKIP/AES ▾
WiFi Password	

Bandwidth limit

Bandwidth limit Disable ▾

MAC Address Controls

MAC Address Controls Disable ▾

Save Cancel Save & Apply

Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

Use the drop down menu to select whether you want “Same settings for both Radios” or “Different settings for each Radio” (“Different settings for each Radio” is displayed).

SSID	Enter an SSID name for the Device network.
Hide SSID	Enable: the SSID will be hidden. Clients must manually enter the SSID in order to connect. Disable: the SSID will be visible (default)
Encryption	Select from WPA/WPA2-PSK, WPA2-PSK, WPA-PSK or None.
Type	Select “TKIP/AES”, “TKIP” or “AES” encryption type. The “TKIP/AES” is the default encryption type.
WiFi Password	Please enter a Wi-Fi password.

Bandwidth Limit

This function limits the aggregated speed of the entire SSID.

When enabled, Downlink and Uplink fields will become available. Enter a value for each field.

MAC Address Controls

Select “Allow List” from the drop down menu to have an “Allow List”.

Enter the Device Name, MAC Address and click “Add” to add the device into the allow list.

Import List

If you have a previously saved Allow List, click “Import List” to enter the page below:

Click “Choose File”, select the list file (*.csv document format) and click “Upload”.



NOTE: Please wait for a few seconds for the upload task.



NOTE: Uploading a new list *will replace* the current list. If you wish to keep all listed details, please download your current list, add it to the desired list and upload.

Click “Cancel” to cancel the actions and return to the previous page.

Export List

If you wish to save your current Allow List, click “Export List”. Your browser should prompt you download the list in *.csv document format.

An example is shown below:



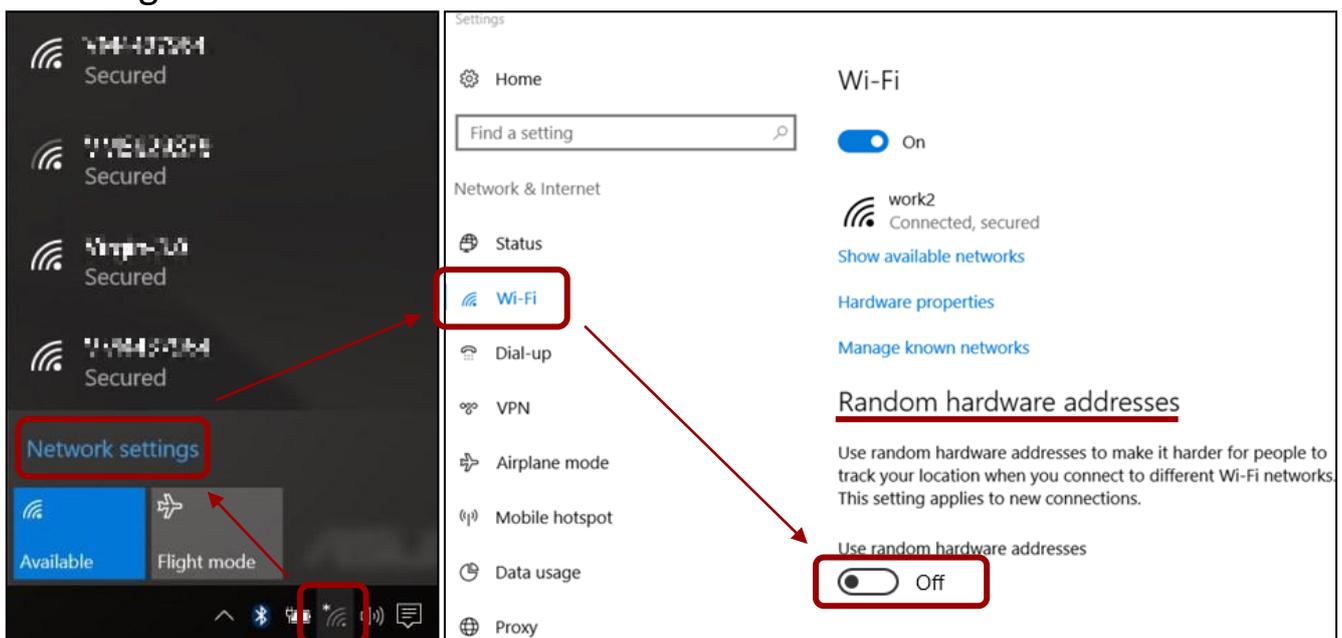
Click “Save” to save the settings. Click “Cancel” to forfeit the changes. Click “Save and Apply” to save and apply the settings to the system.



Random Hardware Addresses

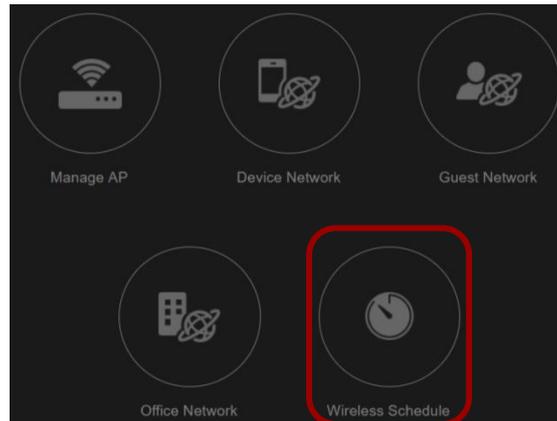
For Win 10 users, if you have trouble staying connected to the Device Network, please **Disable** the “Random Hardware Addresses” function. Follow the instructions below:

1. Click on the network icon  and click “Network Settings”
2. Click “Wi-Fi” on the left-side panel.
3. Locate “Random hardware addresses” and click the enable / disable icon. Make sure it is “Off”.



VII-5-4 Wireless Schedule

Click the “Device Network” icon.



EDIMAX Pro Office 1-2-3

Home > Network Settings > Wireless Schedule Wireless Schedule

Schedule Settings

Network: Device Network

Scheduling: Disable

Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
<input type="checkbox"/>						

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

Save Cancel Save & Apply

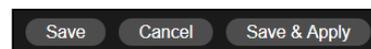
Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

The schedule feature allows you to automate the wireless network for the specified time ranges. Wireless scheduling can save energy and increase the security of your network.

To schedule:

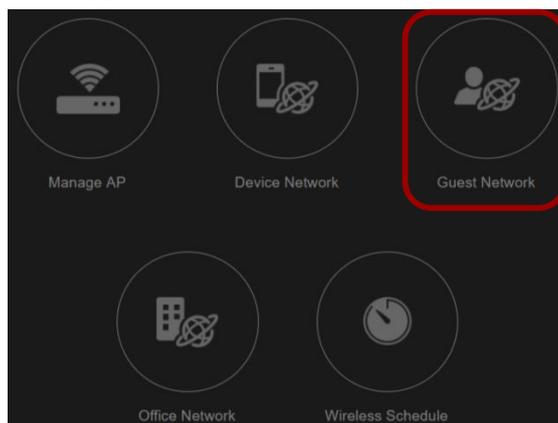
- 1.** Select the network (**Device**, **Office** or **Guest**) to be scheduled by using the drop down menu.
- 2.** Select enable by using the drop down menu.
- 3.** Select the day(s) you wish to put a schedule to by checking the checkbox of the day(s).
- 4.** Select the “Start Time” and “End Time” using the drop down menus.

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



VII-5-5 Guest Network

Click the “Guest Network” icon.



EDIMAX Pro Office 1-2-3  

Home > Network Settings > Guest Network Guest Network

Guest Network

Same settings for both Radios ▾

SSID	guest
Hide SSID	Disable ▾
Encryption	None ▾
Type	TKIP/AES ▾
WiFi Password	

Bandwidth limit

Bandwidth limit Disable ▾

Access

Access Internet Only ▾

Type	IP Address	Subnet Mask
Gateway	192.168.2.250	255.255.255.0
Primary DNS	192.168.2.250	
Secondary DNS	8.8.8.8	

Device Name	IP Address	Subnet Mask	Action
	0.0.0.0	0.0.0.0	Disable ▾
	0.0.0.0	0.0.0.0	Disable ▾
	0.0.0.0	0.0.0.0	Disable ▾
	0.0.0.0	0.0.0.0	Disable ▾
	0.0.0.0	0.0.0.0	Disable ▾

Additional Access IP

Save Cancel Save & Apply

Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

Use the drop down menu to select whether you want “Same settings for both Radios” or “Different settings for each Radio” (“Different settings for each Radio” is displayed).

SSID	Enter an SSID name for the guest network.
Hide SSID	Enable: the SSID will be hidden. Clients must manually enter the SSID in order to connect. Disable: the SSID will be visible (default)
Encryption	Select from WPA/WPA2-PSK, WPA2-PSK, WPA-PSK or None.
Type	Select “TKIP/AES”, “TKIP” or “AES” encryption type. The “TKIP/AES” is the default encryption type.
WiFi Password	Please enter a Wi-Fi password.

Bandwidth Limit

This function limits the aggregated speed of the entire SSID.

When enabled, Downlink and Uplink fields will become available. Enter a value for each field.

Bandwidth limit

Bandwidth limit

Downlink (1 - 10,000) Kbps

Uplink (1 - 10,000) Kbps

Guest Access

Access

Access

Type	IP Address	Subnet Mask
Gateway	<input type="text" value="192.168.2.250"/>	<input type="text" value="255.255.255.0"/>
Primary DNS	<input type="text" value="192.168.2.250"/>	
Secondary DNS	<input type="text" value="8.8.8.8"/>	

Device Name	IP Address	Subnet Mask	Action
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Disable"/>
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Disable"/>
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Disable"/>
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Disable"/>
<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="Disable"/>

Additional Access IP

Access:

Internet Only	Guests have Internet access only (Default Setting).
Full Access	Guests have full access to your network.

Access	
Gateway	Your router's IP address and subnet mask.
Primary DNS	The Primary DNS Server
Secondary DNS	The Secondary DNS Value.

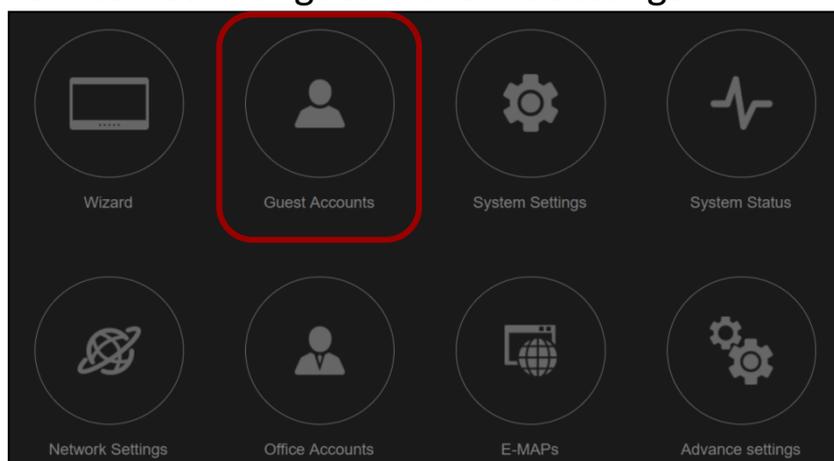
Office 1-2-3 will automatically get the Gateway and DNS data from the router.

Additional Access IP	
Additional Access IP	If you have devices (e.g. printer, scanner, etc.) that are within the network and wish these to be made available to the guests, select Allow in the "Action" column. Enter <i>Device Names, IP Addresses</i> and <i>Subnet Masks</i> .

VII-6 Guest Accounts

This section allows you to configure settings related to Guest Accounts. You can determine *Guest Authentication Method*, view *Account Usage*, *Manage User Account*, configure *Generate Printed Ticket*, *Captive Portal*, and *SMS Service* settings.

Click “Guest Accounts” icon for guest account settings.



EDIMAX Pro
Office 1-2-3

Home > Guest Accounts
Guest Accounts

Guest Accounts

Login Account ▼

Account Usage	2/512
Manage User Account	Setup
Generate Printed Ticket	Setup
Captive Portal	Setup
SMS Service	Setup
Multiple Access per Account	Enable ▼

[Apply](#)

Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

Guest Authentication	<p>You have 4 choices for Guest Authentication:</p> <ul style="list-style-type: none"> ● Free: Guests can access your network freely without an account. ● Service Level Agreement: Guests need to read a disclaimer and click okay in order to access the network. ● Login Account (Default): Guests need to enter username and password for access. ● Login Account+SMS: Guests can enter their phone number and the system will send the account information to their mobile phone via SMS.
Multiple Access per Account	<p>Enable to allow the use of one account information on multiple devices.</p>

VII-6-1 Manage User Account

Click “Setup” Manage User Account Setup for the page options below:

Users

Search Match whole words

☐	Name	Create Time	Valid Period	Description	Status	Action
☐	test1	2017/10/24 17:59:24	Always		●	
☐	test2	2017/10/24 17:59:39	Always		●	

Add
Edit
Delete
Delete All Expired Users
Upload List
Download List

Back

Add or Edit

Click “Add” to add a new user, or “Edit” to edit an existing user:

User Settings

Name

Description

Password

Confirm Password

Valid Time Days ▼

Apply
Cancel

Name	Enter a user name.
Description	Enter a description for possible future reference
Password	Enter a password
Confirm Password	Enter the same password as above
Valid Time	Select a valid time in days or hours. Or you can select “Always” to always allow this account’s access to the network.

Delete or Delete All Expired Users

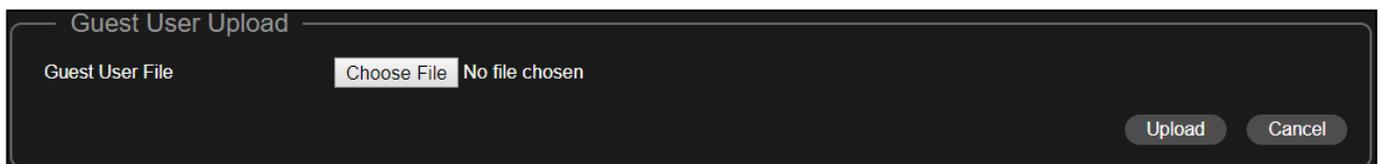
If you wish to delete certain users, check the user entries and click “Delete”. If you wish to delete expired users, click “Delete All Expired Users”.

Upload List or Download List

You can upload or down list of user accounts. The list is in .CSV format so you can edit it using a spread sheet program such as Microsoft Excel.

Import List

If you have a previously saved User List, click “Import List” to enter the page below:



Click “Choose File”, select the list file (*.csv document format) and click “Upload”.

Click “Cancel” to cancel the actions.

Export List

If you wish to save your current User List, click “Export List”. Your browser should prompt you download the list in *.csv document format.

An example is shown below:



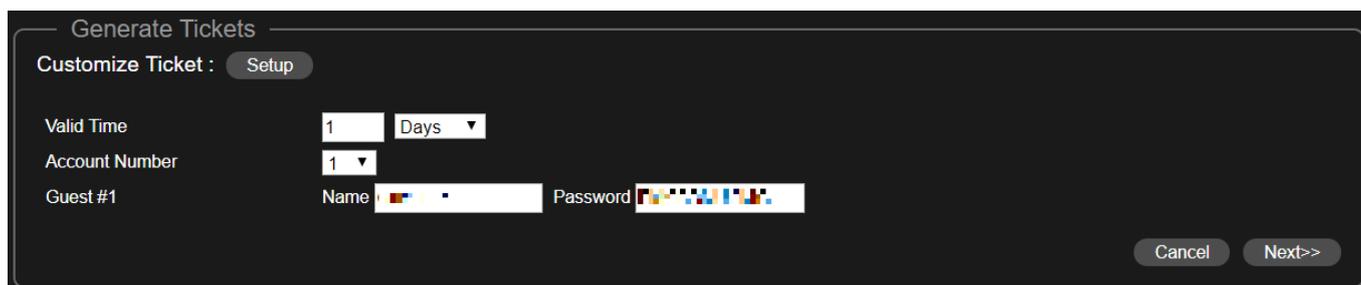
Click “Save” to save the settings. Click “Cancel” to forfeit the changes. Click “Save and Apply” to save and apply the settings.



VII-6-2 Generate Printed Ticket

This section configures the information required to generate random accounts to be printed out. The print out is the easiest way to create account for your guests on demand.

Click “Setup”   for the page options below:



Generate Tickets

Customize Ticket : 

Valid Time Days

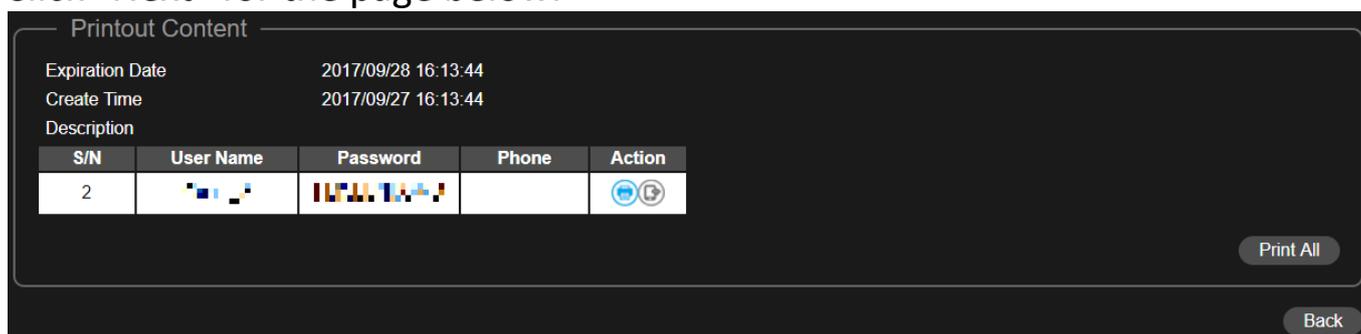
Account Number

Guest #1 Name Password

Valid Time	Select a valid time in days or hours. Or you can select “Always” to always allow this account’s access to the network.
Account Number	Select a number from the drop down menu for the number of guest accounts to generate.
Guest #1-10	Depends on the “Account Number” above, name(s) and password(s) of the Guest will be displayed. You can edit the fields available.

Click “Next” for the page below:



Printout Content

Expiration Date 2017/09/28 16:13:44

Create Time 2017/09/27 16:13:44

Description

S/N	User Name	Password	Phone	Action
2	<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value=""/>	

Click “Print All” to print all available tickets out, or click “Back” to go back to the previous page for more configuration.

Customized Ticket

Click “Setup” **Customize Ticket : Setup** to see / configure the content of the printed ticket.

Definition Table

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

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

Printout Content

Welcome!
EDIMAX Technology Co., Ltd

Guest Internet Service

SSID: {SSID}
Username: {USERNAME}
Password: {PASSWORD}
Expire Time: {EXPIRETIME}

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

Thank you very much !

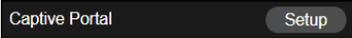
Preview Confirm Cancel

In the “Printout Content” section, enter / edit your desired messages.

You can preview the message by clicking the “Preview” button. A window will pop up with the preview. An example is shown below:

Welcome! EDIMAX Technology Co., Ltd
Guest Internet Service
SSID: Guest_ssid Username: Guest_1 Password: URSFKWPGMT Expire Time: 2012/01/03 21:41:00
Create Time: 2012/01/01 21:41:00 S/N: 16
Thank you very much !

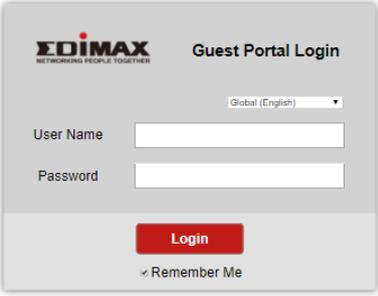
VII-6-3 Captive Portal

Click “Setup”  for the page options below:

Guest Portal

Login Portal Edit





Login page preview

Landing Page Redirect to the original URL

Default Language

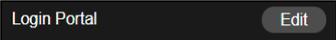
Idle Timeout minutes

Login Password Retry Lockout (1-30 times)

Apply Cancel

Landing Page	Check either “Redirect to the original URL” or the http:// field. If http:// field is checked, enter a website such as your company’s website.
Default Language	Choose a default language.
Idle Timeout	Select an idle timeout time from the drop down menu.
Login Password Retry Lockout	Enter a number (between 1 and 30) for the number of login password retry. If login password has been entered incorrectly for the number entered here, it will be locked.

Customize Login Portal

Click “Edit”  for the page below:

Customize Login Portal

Choose File No file chosen

Header Image 

Size: 800x200 pixels

Choose File No file chosen

Logo Image 

Size: 200x50 pixels

Title Message

Background Color

Accept by Default

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.

Limitation of Use

All materials on this Web Site are protected by copyright laws, and other applicable laws of each country throughout the world and treaty provisions. Except for personal or non-commercial internal use, you are prohibited to use (including, without limitation, copying, modifying, reproducing in whole or in part, uploading, transmitting, distributing, licensing, selling and publishing) any of the materials, without obtaining prior written permission. Each software that is made available from this Web Site ("Software") is

Header Image	Click “Choose File” to select a file as the header image.
Logo Image	Click “Choose File” to select a file as the logo image.
Title Message	Enter / edit a title message.
Background Color	Click on the field where color selection will be available. Select a desired color. 

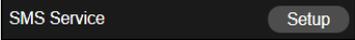
Accept by Default	Check / uncheck to enable / disable auto-accepting terms of use agreement.
Terms of use	Enter / edit the terms of use message

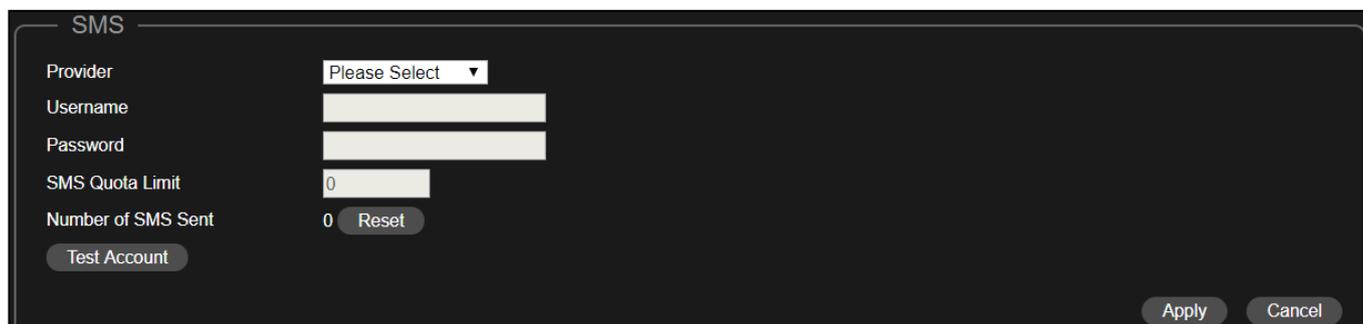
Click “Preview” for captive portal preview in another page (example below).

The screenshot shows a captive portal login page for EDIMAX Pro. At the top, there is a banner with the EDIMAX Pro logo and a cityscape background. Below the banner, the page title is "EDIMAX NETWORKING PEOPLE TOGETHER" and "Captive Portal Login". A language dropdown menu is set to "Global (English)". There are two input fields: "User Name" and "Password". A red "Login" button is located below the password field. Below the button is a checked checkbox for "Remember Me". At the bottom, there is an unchecked checkbox for "Accept [Terms of use](#)".

If you are sure of the content, click “Confirm” to confirm customization of the captive portal, or “Cancel” to forfeit the changes.

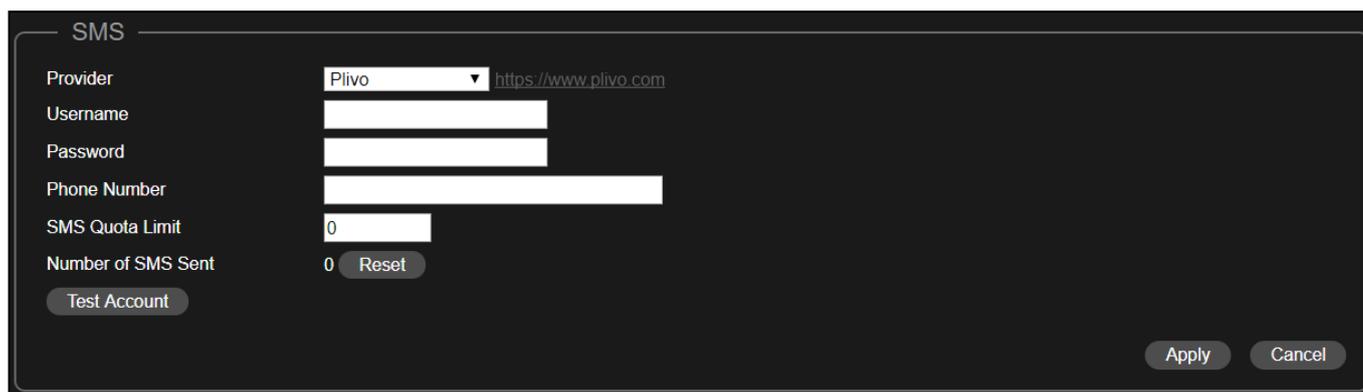
VII-6-4 SMS Service

Click “Setup”  for the page options below:



Provider	Select a service provider from the drop down menu. Plivo and Stream Telecom are the available options.
-----------------	--

Pilivo:



Username	Enter the username for the service provider.
Password	Enter the password for the service provider.
Phone Number	Enter the phone number.
SMS Quota Limit	Enter a number for SMS quota limit.
Number of SMS Sent	This keeps track of the number of sent SMS. Click “Reset” to restart the sent SMS count.

Click “Test Account” to test the validity of the above-entered fields.

Stream Telecom:

The screenshot shows a configuration window titled 'SMS'. It contains the following elements:

- Provider:** A dropdown menu set to 'Stream Telecom' with a link 'https://web.szkk-info.ru'.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Sender Name:** An empty text input field.
- SMS Quota Limit:** A text input field containing the number '0'.
- Number of SMS Sent:** A text input field containing '0' and a 'Reset' button next to it.
- Buttons:** 'Test Account', 'Apply', and 'Cancel' buttons are located at the bottom of the window.

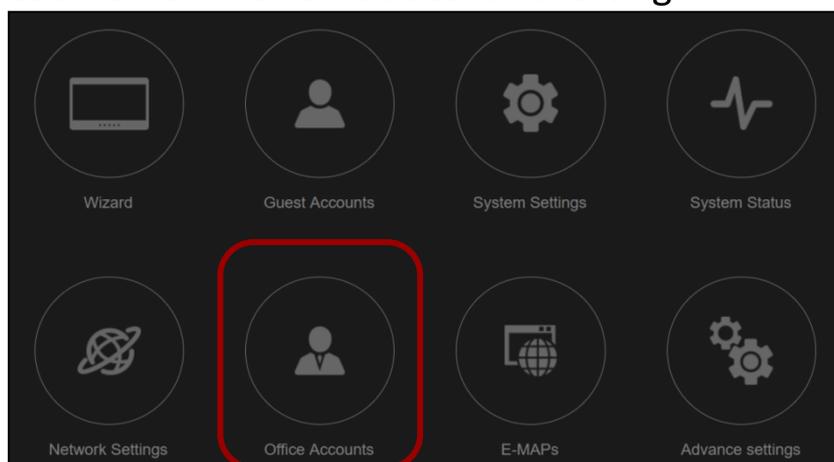
Username	Enter the username for the service provider.
Password	Enter the password for the service provider.
Sender Name	Enter the sender's name.
SMS Quota Limit	Enter a number for SMS quota limit.
Number of SMS Sent	This keeps track of the number of sent SMS. Click "Reset" to restart the sent SMS count.

Click "Test Account" to test the validity of the above-entered fields.
Click "Apply" to apply the settings, or "Cancel" to forfeit the changes.

VII-7 Office Accounts

This section allows you to configure settings related to Office Accounts. You can determine add / edit / delete *Office Accounts* and its settings, *Upload* and *Download* account list.

Click “Office Accounts” icon for office account settings.



ΣDIMAX Pro Office 1-2-3

Home > Office Accounts Office Accounts

Office Accounts

Search Match whole words

Account Usage

Multiple Access per Account

<input type="checkbox"/>	Name	Password	Description
<input type="checkbox"/>	albert	Configured	
<input type="checkbox"/>	office1	Configured	
<input type="checkbox"/>	office2	Configured	

Add Apply Edit Delete Upload List Download List

Users can **connect to the office accounts** using the account information created in this section.

It is recommended to use **Upload List** and / or **Download List** for simple management of office accounts. The list is in .CSV format so you can edit it using a spread sheet program such as Microsoft Excel.

Add or Edit User

Add or edit an user account for the office network. Click “Add” to add a new user or “Edit” to edit an existing user.

The screenshot shows the 'Office User Settings' page in the EDIMAX Pro interface. The page has a dark theme. At the top left is the EDIMAX Pro logo. At the top right, it says 'Office 1-2-3' with a globe icon and a play button icon. Below the logo is a breadcrumb trail: 'Home > Office Accounts > Office User Settings'. On the right side, there is a tab labeled 'Office User Settings'. The main content area is titled 'User Settings' and contains four input fields: 'Name' (with the value 'office_user'), 'Description', 'Password', and 'Confirm Password'. At the bottom right of the form are two buttons: 'Save' and 'Cancel'. On the left side of the page, there is a vertical sidebar with several icons, including a person icon which is highlighted in red.

Enter / edit the fields and click “Save” to save the settings, or “Cancel” to forfeit. Once you have created all the accounts, please remember to “**Apply**” for the new accounts to take effect. Otherwise, the setting will not take effect.

Apply

Please remember to click on Apply once you have created and saved your accounts.

Delete

If you wish to delete certain users, check the user entries and click “Delete” (multiple selections possible).

Upload List

Click “Upload List” to enter the page below:

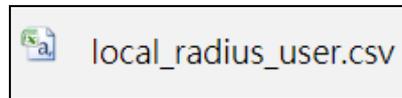
The screenshot shows the 'Office User Upload' page. The page title is 'Office User Upload'. Below the title, there is a section for file selection. It includes the text 'Office User File', a 'Choose File' button, and 'No file chosen' text. At the bottom right of the page are two buttons: 'Upload' and 'Cancel'.

Click “Choose File”, select the list file (*.csv document format) and click “Upload”.

Click “Cancel” to cancel the actions.

Download List

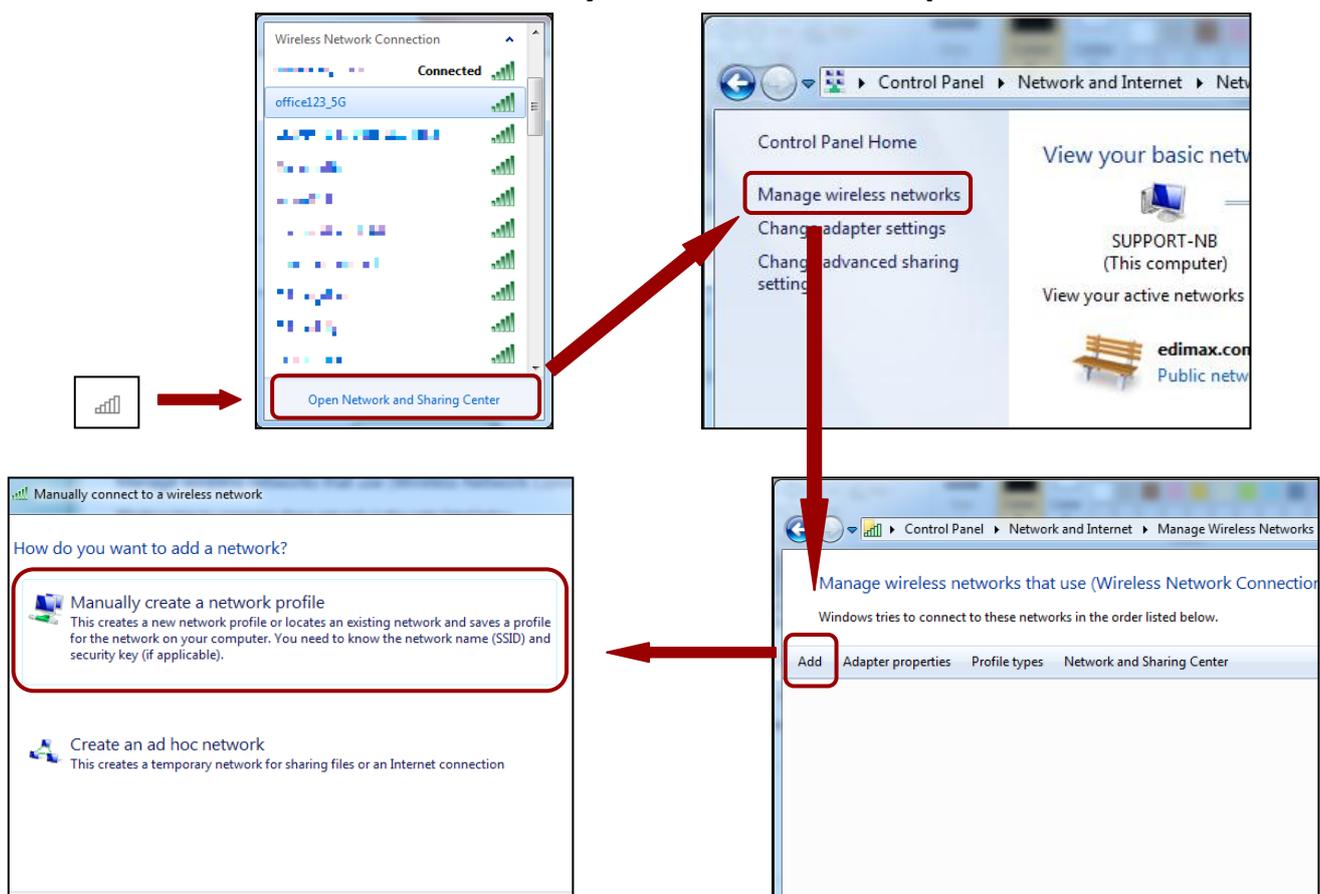
If you wish to save your current User List, click “Download List”. Your browser should prompt you download the list. The list is in *.csv document format. An example is shown:



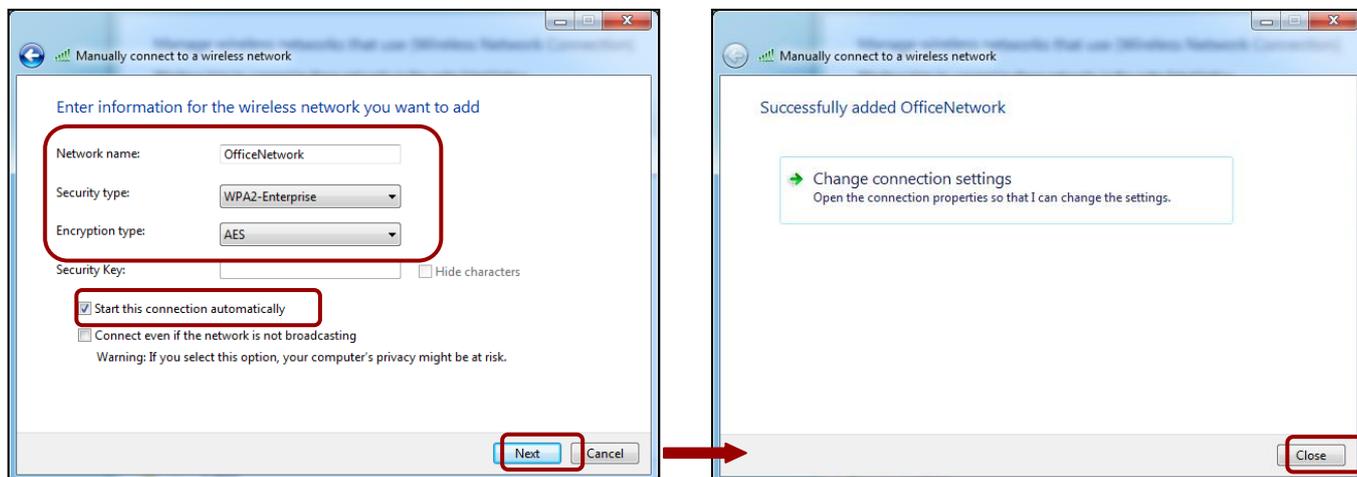
VII-7-1 RADIUS Authentication for Office Network under Win 7

The Office 1-2-3 uses RADIUS authentication for Office Network. For Win 7, Vista or OS version before, specific configuration is mandatory to enable radius login. Please follow the instructions below:

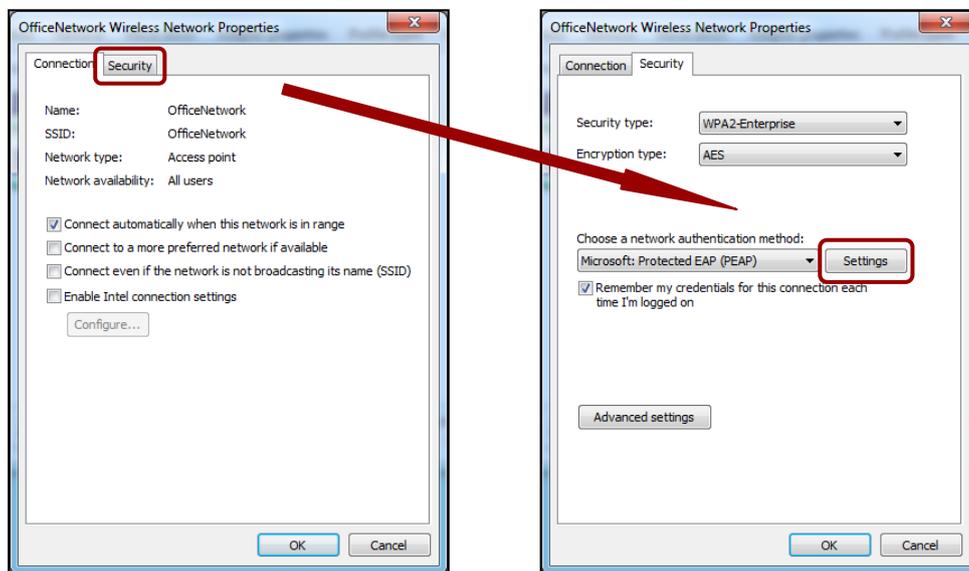
1. Find and click the network icon on the bottom right of the desktop and click **Open Network and Sharing Center**. Click **Manage wireless networks** → **Add** → **Manually create a network profile**.



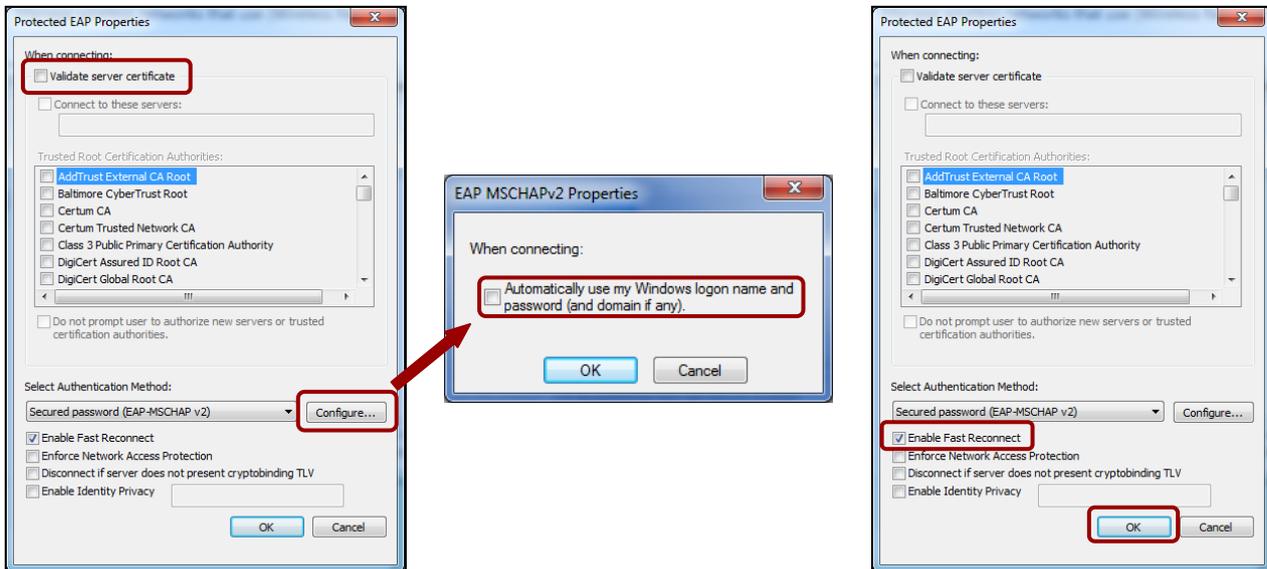
2. Enter a network name in the field after “Network name”, select **WPA2-Enterprise** for “Security type”, select **AES** for “Encryption type”, and make sure to check the “Start this connection automatically” checkbox. Click “Next” for a successfully added network message and click “Close” to close the window.



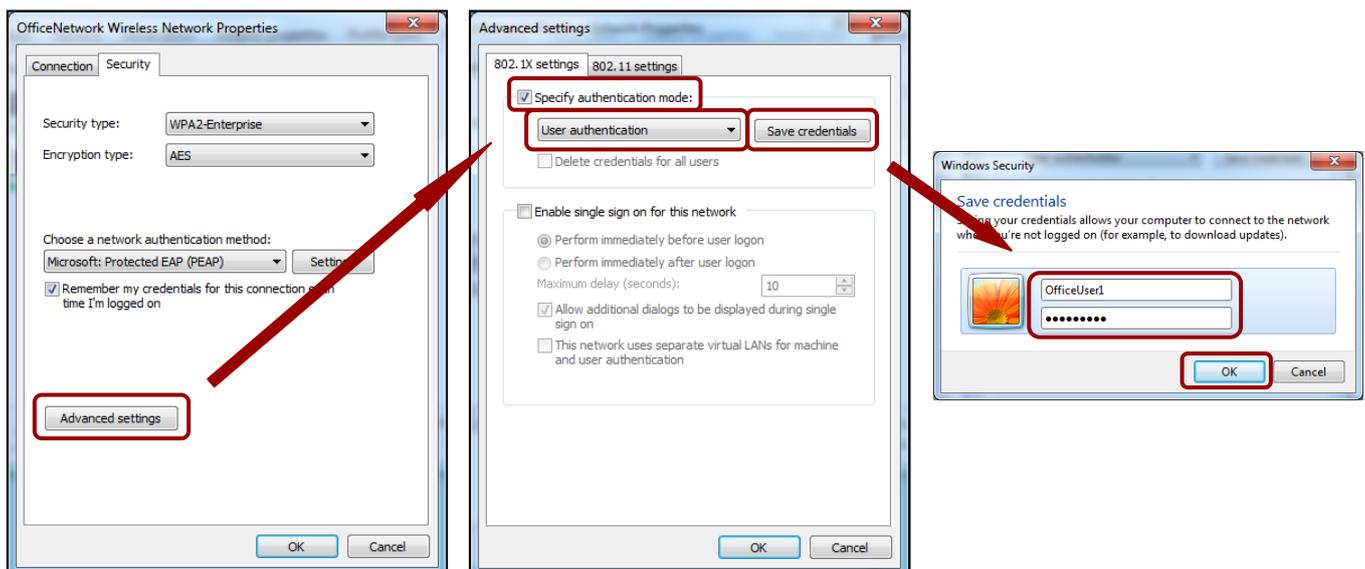
3. Double-click the newly created network to “Properties” page. Click **Security** → **Settings**.



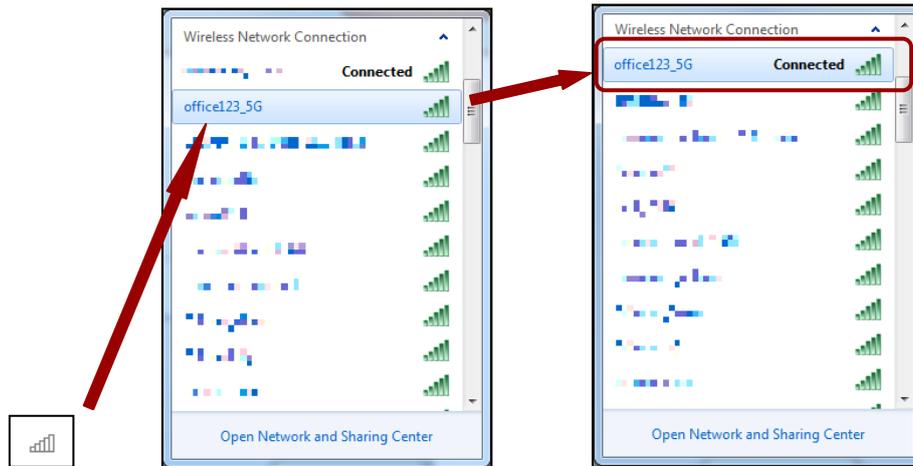
4. Uncheck “Validate server certificate” and click “Configure”. Make sure “Automatically use ...” is unchecked and click “OK”. Check “Enable Fast Reconnect” (if unchecked) and click “OK” to return to the “Security” tab.



5. Click “Advanced settings”. Check “Specify authentication mode”, select User authentication from the dropdown menu and click “Save credentials”. Enter an office account username and password. Confirm the newly created network by clicking “OK” until returning to the “Managed Wireless Network” page.



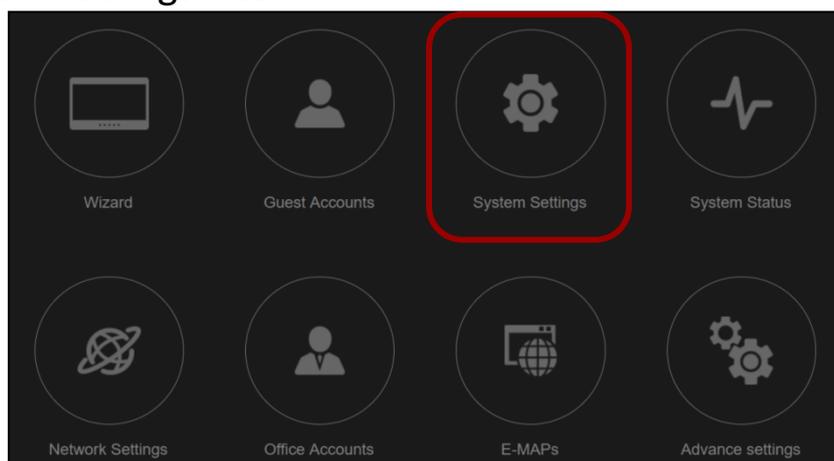
6. Find and click the network icon on the bottom right of the desktop. Select the office network of your Office 1-2-3 and connect to it.



VII-8 System Settings

This section allows you to configure the system settings. These settings include *LAN IP Address*, *Management Account*, *Frontdesk Account*, *Advanced Settings*, *Date & Time*, *System Logs / Log Server*, *VLAN Management*, *Save / Restore Settings from PC*, and *Master / Slave Firmware Upgrade*.

Click the “System Settings” icon.




Total apply time: 2:28
Office 1-2-3



Home > System Settings
System Settings









LAN IP Address

IP Address Assignment	<input type="text" value="DHCP Client"/>
IP Address	<input type="text" value="192.168.2.2"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="From DHCP"/> <input type="text"/>
Primary DNS Address	<input type="text" value="From DHCP"/> <input type="text" value="0.0.0.0"/>
Secondary DNS Address	<input type="text" value="From DHCP"/> <input type="text" value="0.0.0.0"/>

System Settings

Account to Manage This Device

Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/> (4-32Characters)
Confirm Password	<input type="password" value="....."/> Confirm
Management IP Lock	<input type="text" value="Disable"/>

Front Desktop Account

Name	<input type="text" value="frontdesk"/>
Password	<input type="password" value="....."/> (4-32Characters)
Confirm Password	<input type="password" value="....."/> Confirm

Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

VII-8-1 LAN IP Address

Enable the access point to dynamically receive an IP address from your router's DHCP server or specify a static IP address, as well as configure DNS servers.

DHCP Client

The access point will be assigned a dynamic IP address from the DHCP server of your network.

LAN IP Address

IP Address Assignment:

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS Address:

Secondary DNS Address:

DHCP Client	
IP Address	This field cannot be modified if "DHCP Client" is selected.
Subnet Mask	This field cannot be modified if "DHCP Client" is selected.
Default Gateway	This field cannot be modified if "From DHCP" is selected. Select "User-Defined" and enter a default gateway.
Primary DNS Address	This field cannot be modified if "From DHCP" is selected. Select "User-Defined" and enter a primary DNS address.
Secondary DNS Address	This field cannot be modified if "From DHCP" is selected. Select "User-Defined" and enter a secondary DNS address.

Static IP Address

Manually specify a static/fixed IP address for your access point.



NOTE: If **Static IP Address** is selected, system settings of all APs of Office 1-2-3 must also be configured.

LAN IP Address

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

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.

Click “Apply” to apply the changes.

VII-8-2 System Settings

System Settings

Account to Manage This Device

Name

Password (4-32Characters)

Confirm Password Confirm

Management IP Lock

Front Desktop Account

Name

Password (4-32Characters)

Confirm Password Confirm

Advanced Settings

HTTP Port (80, 1024-65535)

HTTPS Port (443, 1024-65535)

Management Protocol

- HTTP
- HTTPS
- TELNET
- SSH

Login Timeout (mins)

Date and Time Settings

Local Time

Year Month Day

Hours Minutes Seconds

Use NTP Enable

Auto Daylight Saving Enable

Server Name

Update Interval (Hours)

Time Zone

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

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).															
Management IP Lock	<p>This feature allows you to determine who is able to manage the whole system.</p> <p>Disable (Default): All that have the administrator name and password can manage the system.</p> <p>Enable: Up to 3 computers / devices can manage the system. The 3 computers / devices are allocated according to the settings shown below:</p> <table border="1" data-bbox="564 846 1318 1084"> <thead> <tr> <th colspan="2">Management IP Lock</th> <th>Enable ▾</th> </tr> <tr> <th>IP Address</th> <th>Subnet Mask</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>0.0.0.0</td> <td>0.0.0.0</td> <td>Disable ▾</td> </tr> <tr> <td>0.0.0.0</td> <td>0.0.0.0</td> <td>Disable ▾</td> </tr> <tr> <td>0.0.0.0</td> <td>0.0.0.0</td> <td>Disable ▾</td> </tr> </tbody> </table> <p>Use the drop down menu in the Action column to enable / disable the IP addresses. When Enable is selected, enter the IP Address and Subnet Mask.</p>	Management IP Lock		Enable ▾	IP Address	Subnet Mask	Action	0.0.0.0	0.0.0.0	Disable ▾	0.0.0.0	0.0.0.0	Disable ▾	0.0.0.0	0.0.0.0	Disable ▾
Management IP Lock		Enable ▾														
IP Address	Subnet Mask	Action														
0.0.0.0	0.0.0.0	Disable ▾														
0.0.0.0	0.0.0.0	Disable ▾														
0.0.0.0	0.0.0.0	Disable ▾														

The Frontdesk account is for creating guest accounts and ticket printing only.

Front Desktop Account	
Name	Set the system's front desktop account name.
Password	Set the system's front desktop account password.

Advanced Settings	
HTTP Port	Specify an HTTP Port
HTTPS Port	Specify an HTTPS Port
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below).
Login Timeout	Specify the idle time (in minutes) before being kicked from the server.

HTTP

Internet browser HTTP protocol management interface

TELNET

Client terminal with telnet protocol management interface

Date and Time Settings	
Local Time	Set the system's date and time manually using the drop down menus.
Acquire Current Time from your PC	Click to acquire time and date automatically from your PC.
Use NTP	Check to enable automatic time and date sync to an NTP server.
Auto Daylight Saving	Check / uncheck to enable / disable daylight saving function.
Server Name	Use the drop down menu to select a region. A server will be shown after selecting the region. Choose the region according to your location.
Update Interval	Specify how often (in hours) the access point synchronizes with the NTP server.
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.

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

Syslog E-mail Settings	
E-mail Logs	Check the box to enable/disable e-mail logs.
E-mail Subject	Specify the subject line of log emails.
SMTP Server Address	Specify the SMTP server address used to send log emails.
SMTP Server Port	Specify the SMTP server port used to send log emails.
Sender E-mail	Specify the sender email address.
Receiver	Specify the email to receive log emails.

E-mail	
Authentication	Disable or select authentication type: SSL or TLS. When using SSL or TLS, enter the username and password.

Click “Apply” to apply the changes.

VII-8-3 Management VLAN ID

To connect Office 1-2-3 to your VLAN Network, Management VLAN ID (under System Settings) must be configured to be the same as the one on your switch. All the wireless SSID and LAN can only share one VLAN ID. It is recommended to put the AP on the VLAN that can access both LAN and Internet network. The Guest network in Office 1-2-3 can prohibit guest accessing the Intranet network by IP filtering.

Click “Apply” to apply the changes.

VII-8-4 Save Settings to PC

This section enables you to save / backup the device’s current settings as a file to your local computer.

Click “Save” to save current settings.

Encryption: If you wish to encrypt the configuration file with a password, check the “Encrypt the configuration file with a password” box and enter a password.

VII-8-5 Restore Settings from PC

This section enables you to restore the device's current settings from a file in your local computer.

Click the “Choose File” button to find a previously saved settings file on your computer.

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 following field.

VII-8-6 Master AP Firmware Upgrade

This section allows you to update the firmware of the Master AP. Updated firmware versions often offer increased performance and security, as well as bug fixes. Download the latest firmware from the Edimax website.

Click “Choose File” to upload firmware from your local computer and click “Update” to start firmware upgrade.



NOTE: Please upgrade the firmware of the slave APs before the master AP. See next section.

VII-8-7 Slave AP Firmware Upgrade

This section allows you to update the firmware of the Slave AP using the master AP's interface. Updated firmware versions often offer increased performance and security, as well as bug fixes. Download the latest firmware from the Edimax website.

Slave AP Firmware Upgrade

Firmware Update File No file chosen

Firmware Name	Firmware Version	NMS Version	Model	Size (bytes)

Select Slave AP

☐	Index	MAC Address	Device Name	IP Address	Firmware Version	Progress
<input type="checkbox"/>	1	74:DA:38:D3:6B:4A	AP74DA38D36B4A	192.168.2.102	1.0.0	0%
<input type="checkbox"/>	2	74:DA:38:D3:6B:6A	AP74DA38D36B6A	192.168.2.103	1.0.0	0%

Click “Choose File” to upload firmware from your local computer and click “Upload” to upload the firmware to the interface.

Check the checkbox of the slave AP you want to upgrade and click “Update Selected” to start firmware upgrade.

VII-8-8 Firmware Upgrade (Slave-Only Interface)

This section allows you to update the firmware of the Access Point. Updated firmware versions often offer increased performance and security, as well as bug fixes. Download the latest firmware from the Edimax website.

Firmware Upgrade

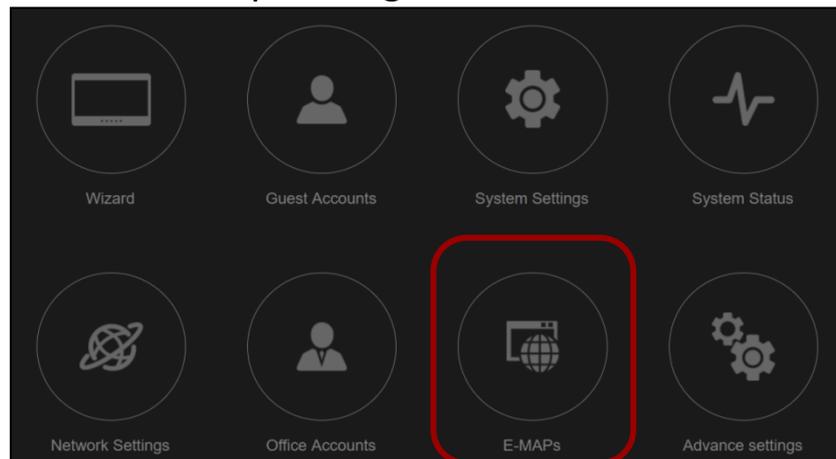
Firmware Update File No file chosen

Click “Choose File” to upload firmware from your local computer and click “Update” to start firmware upgrade.

VII-9 E-MAPS

This section allows you to simulate how you would deploy the Office 1-2-3 APs and provides a pictorial presentation of various information for each AP. For a general rule of deployment, please also refer to v-1 **Office 1-2-3 Deployment**.

Click “E-MAPS” icon for E-Map settings.



The screenshot displays the EDIMAX Pro Office 1-2-3 interface. The breadcrumb navigation shows 'Home > E-MAPS'. The page title is 'Edit Map'. In the top right corner, it indicates '655360 bytes Available (655360 bytes Total)'. Below this is a table with the following structure:

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

At the bottom right of the table area, there are four buttons: 'Add', 'Edit', 'Delete', and 'Show Map'. The left sidebar contains various navigation icons, with the 'E-MAPS' icon highlighted in red.

Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

VII-9-1 Add / Edit Zone

Click “Add” for the page shown below:

Upload Map Image

Map Image File Choose File No file chosen

Upload

Member(s) Settings

Name/Location

Description

Search Match whole words

Select AP

	MAC Address	Device Name	Model	Status
<input type="checkbox"/>	74:DA:38:D3:6B:60	AP74DA38D36B60	Office 1-2-3	●
<input type="checkbox"/>	74:DA:38:D3:6B:4A	AP74DA38D36B4A	Office 1-2-3	●
<input type="checkbox"/>	74:DA:38:D3:6B:74	AP74DA38D36B74	Office 1-2-3	●

Apply Cancel

Upload Map Image

Upload Zone Image

Choose File

Click to locate an image file to be displayed as a map. Typically a floor plan image is useful.

Click “Upload” to upload the image.

An example of an image being uploaded is shown below:

Upload Map Image

Map Image File Choose File No file chosen



Upload

Member(s) Settings

Member(s) Settings

Name/Location:

Description:

Search: Match whole words

Select AP

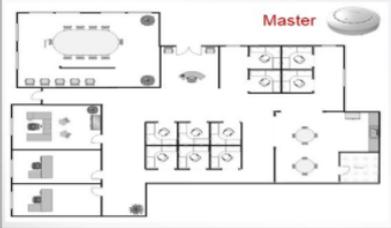
	MAC Address	Device Name	Model	Status
<input type="checkbox"/>	74:DA:38:D3:6B:60	AP74DA38D36B60	Office 1-2-3	●
<input type="checkbox"/>	74:DA:38:D3:6B:4A	AP74DA38D36B4A	Office 1-2-3	●
<input type="checkbox"/>	74:DA:38:D3:6B:74	AP74DA38D36B74	Office 1-2-3	●

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

Click “Apply” to complete your zone addition. An example of adding the zone is shown below:

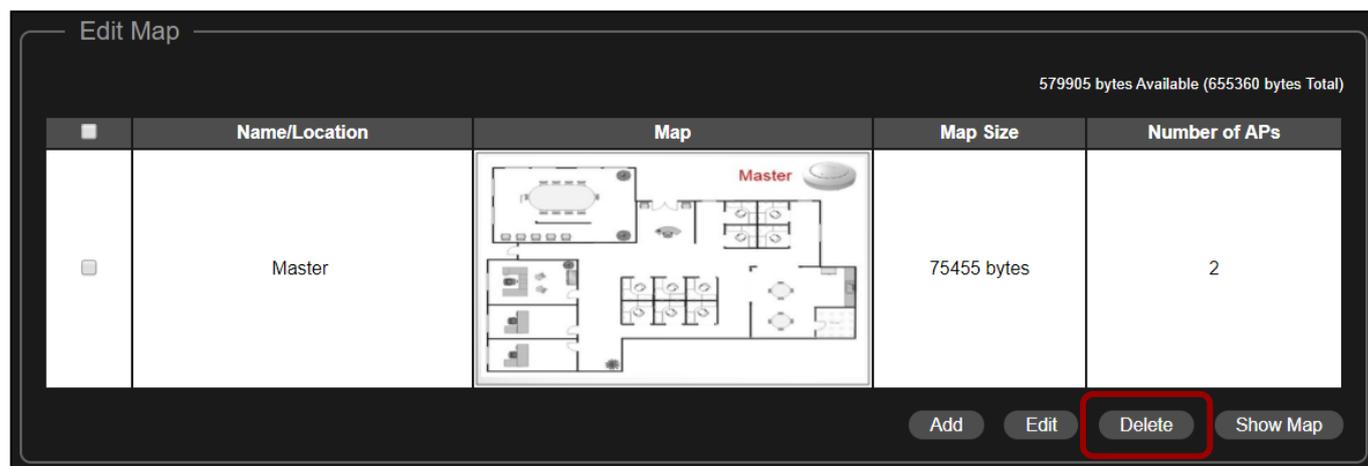
Edit Map

579905 bytes Available (655360 bytes Total)

<input type="checkbox"/>	Name/Location	Map	Map Size	Number of APs
<input type="checkbox"/>	Master		75455 bytes	2

VII-9-2 Delete Zone

Check the checkbox of the zone you wish to delete and click “Delete” to delete the zone.



VII-9-3 Show Map

When “Show Map” is clicked, the uploaded map image will be displayed. An example is shown below:

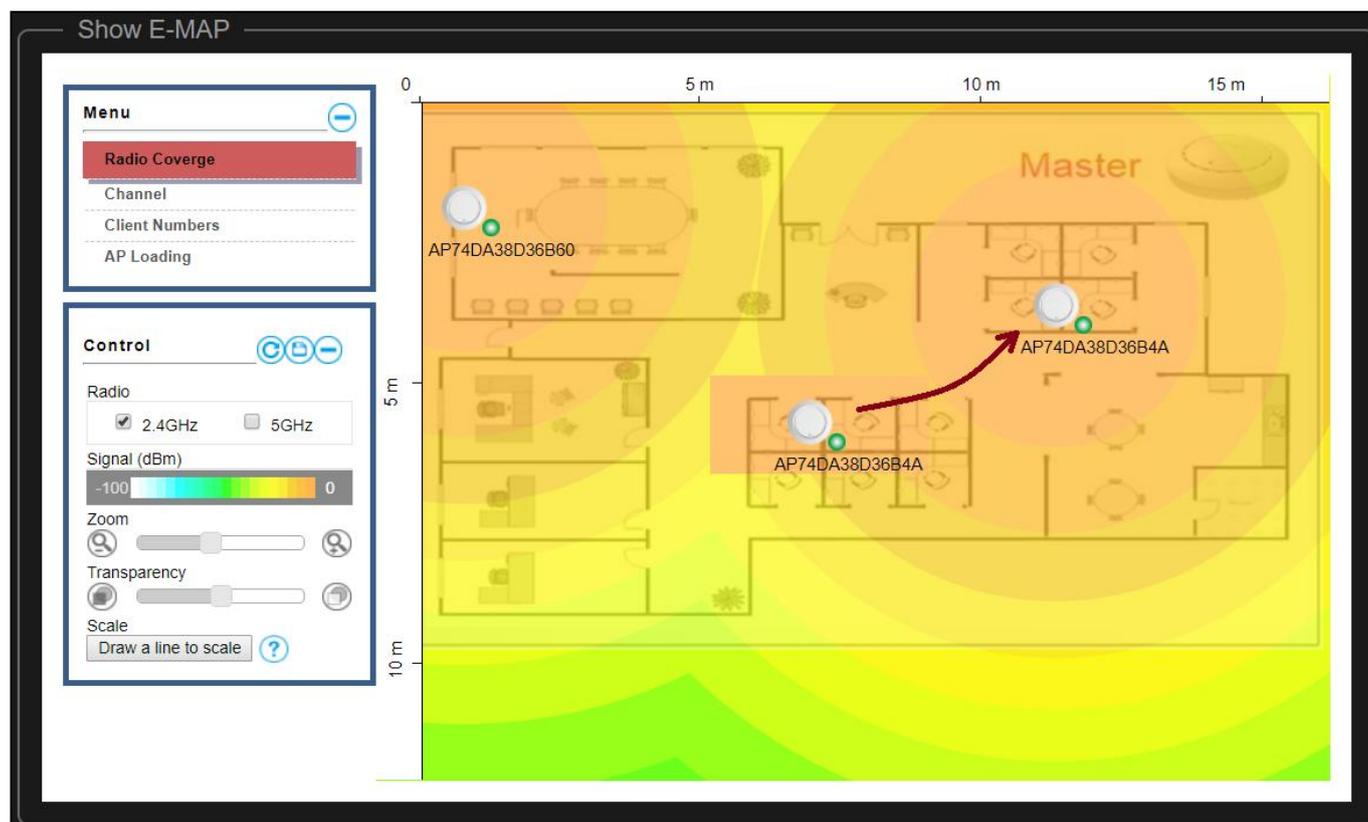


Move the cursor over an Access Point will display certain information.

Simulate Floor Plan

Moving the Access Point

On this page, the system planner can move the Access Points around to simulate the floor plan. Simply click the AP and drag it along. An example is shown:



Radio Coverage

Information such as radio coverage (in both 2.4GHz and 5GHz) can be displayed to allow the planner to plan where to put the access points.



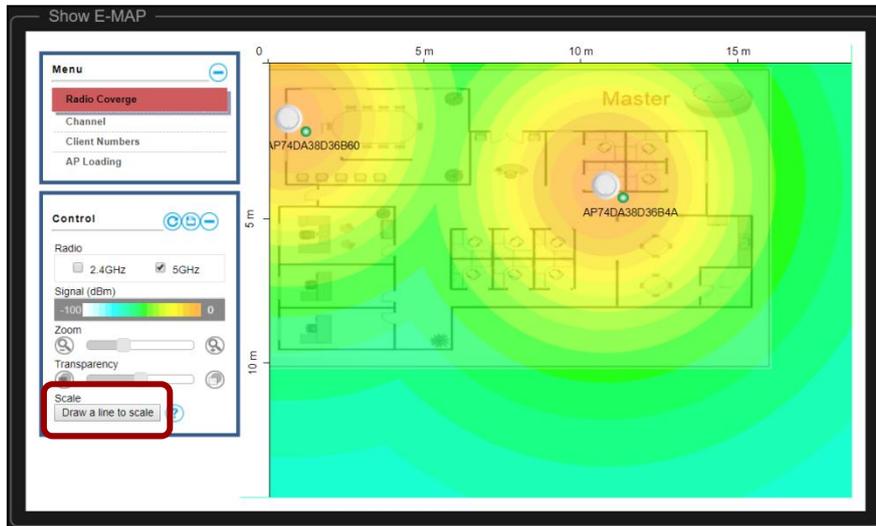
2.4GHz Radio Coverage

5GHz Radio Coverage

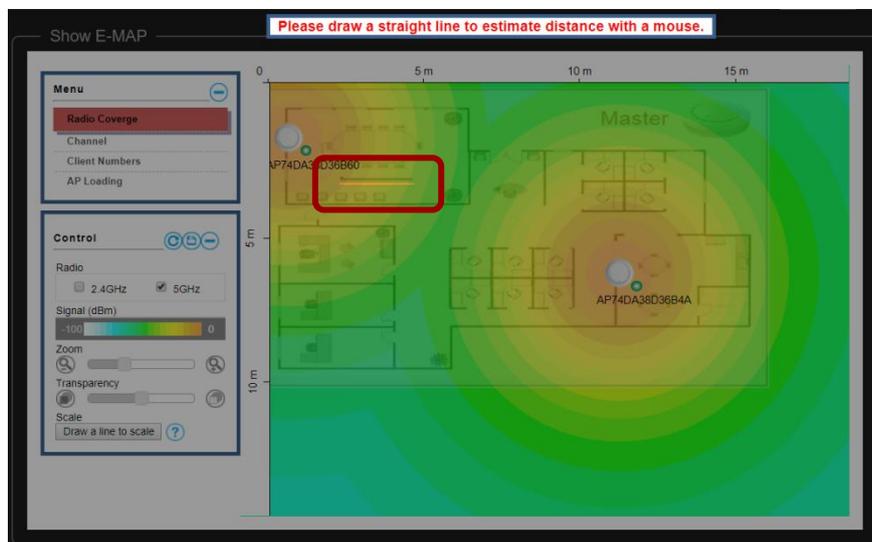
Draw to Scale

Actual scale of the floor plan can also be drawn on this page to have a much more relative, and thus more accurate, signal distribution and planning.

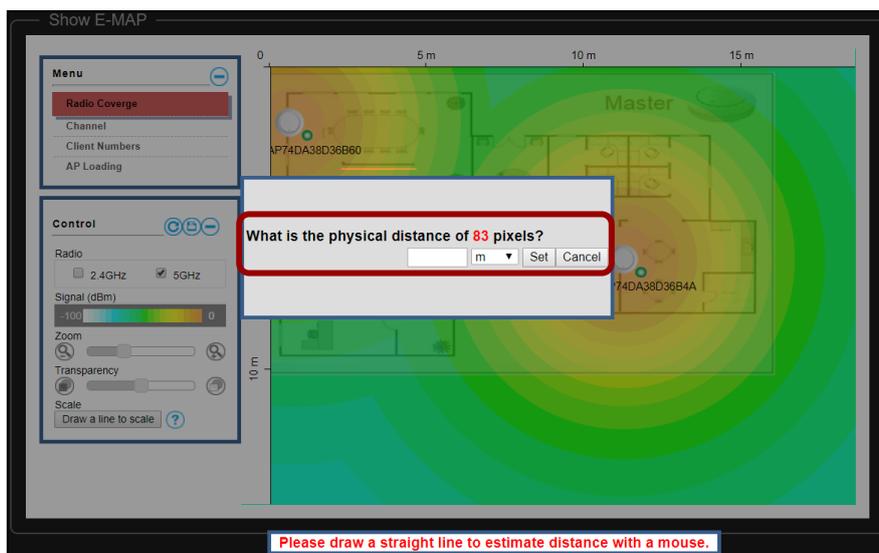
1. Click on “Draw a line to scale” button.



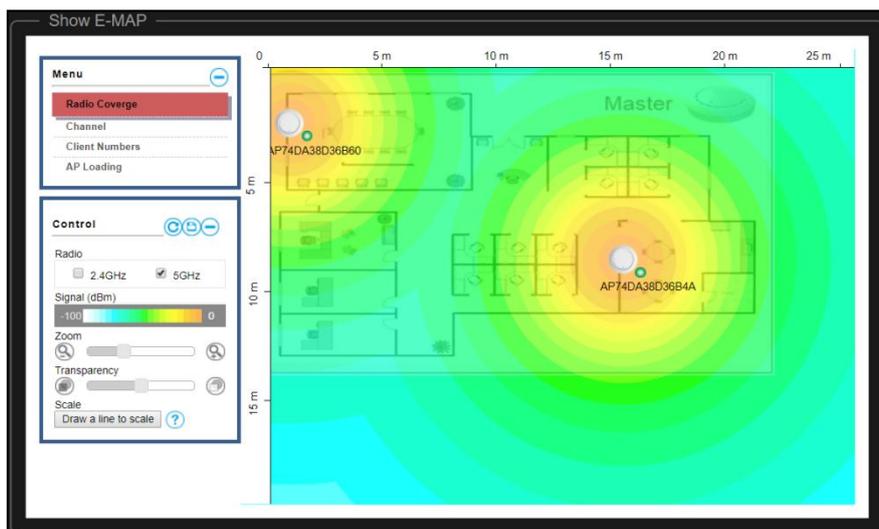
2. Draw a line on the map.



3. Enter the physical distance. Use the drop down menu to select the unit. Click “Set” after confirming the entry / selection.



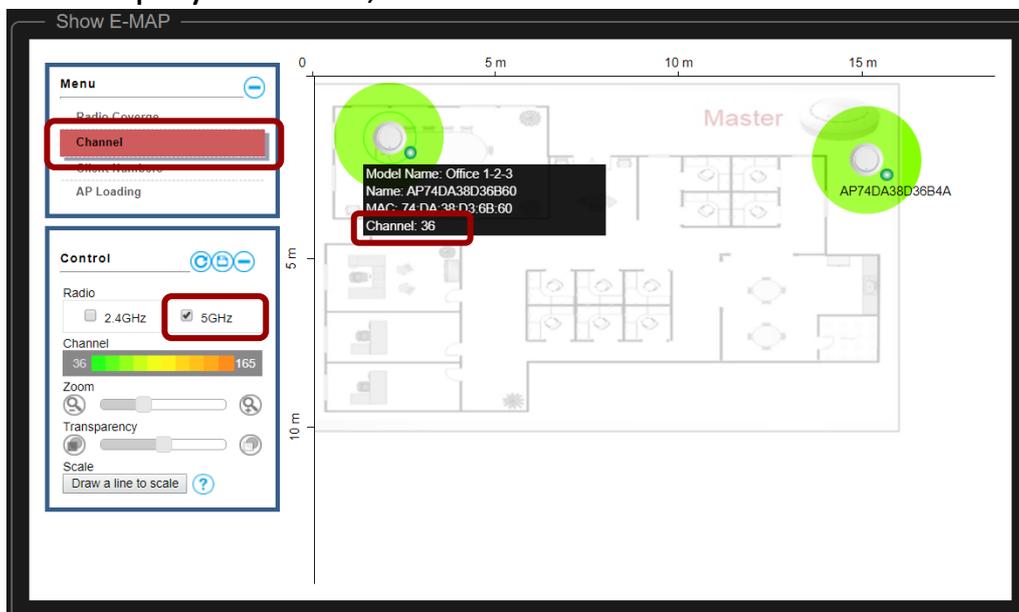
The scale will change in response to the entered scale. An example is below, as the scale differs from the previous pictures



Channel

When “Channel” is selected, the cursor will also display the channel of the radio network.

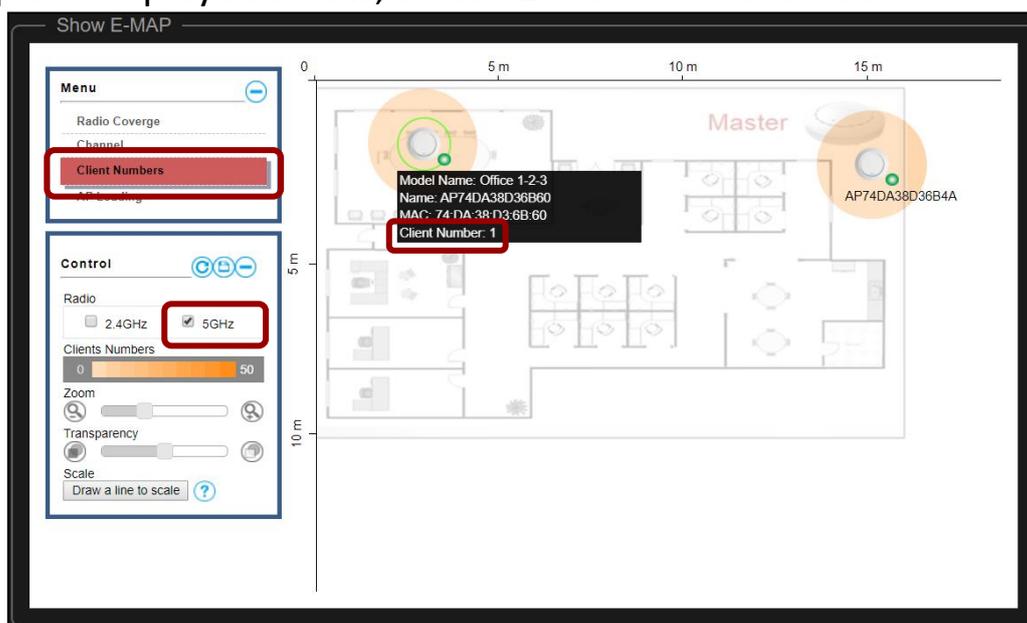
An example is displayed below, where the 5GHz network is on channel 36.



Client Numbers

When “Client Number” is selected, the cursor will display the client number.

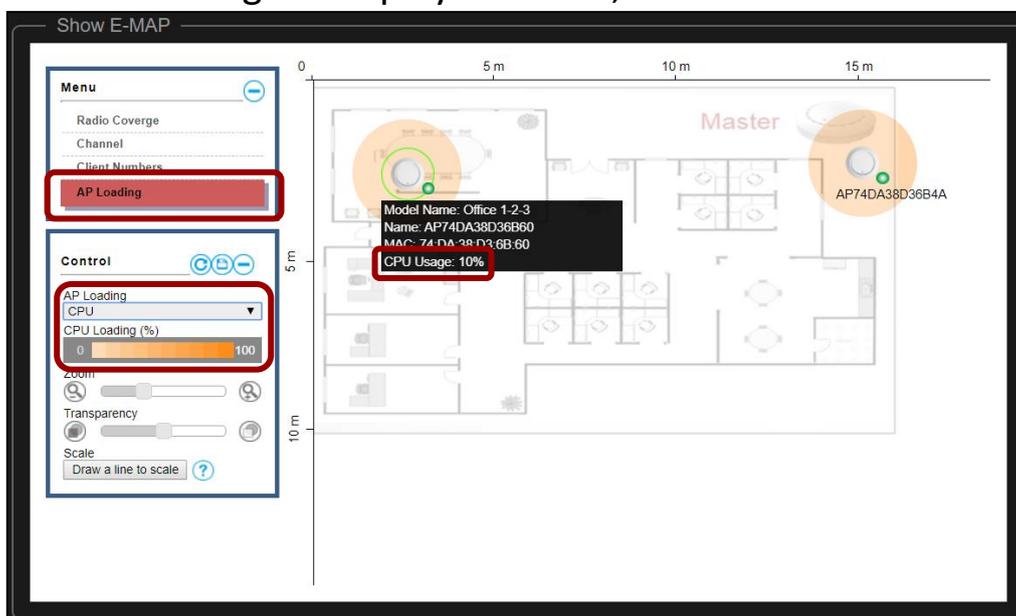
An example is displayed below, where 1 client is connected.



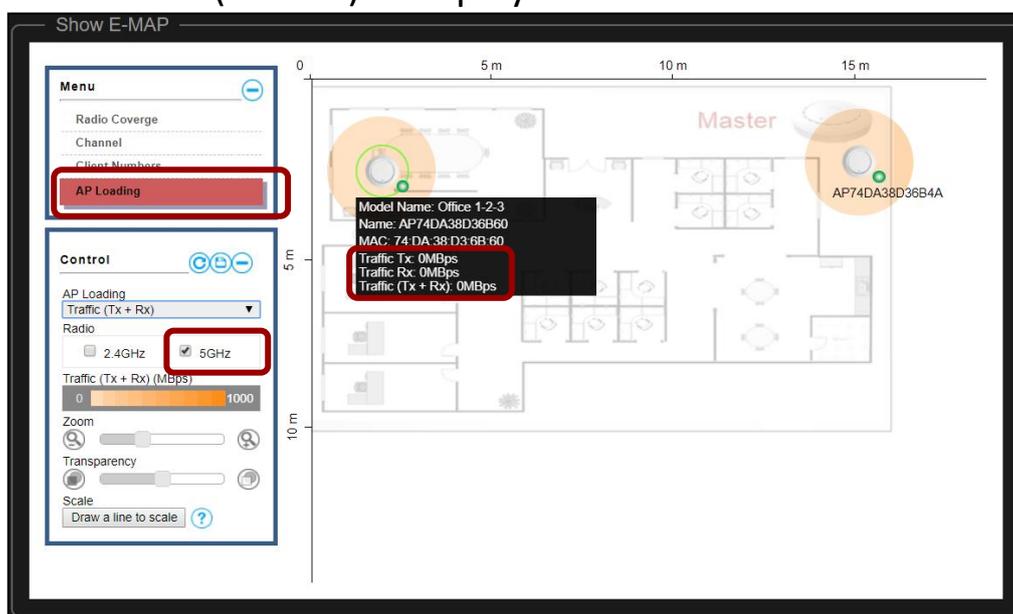
AP Loading

When “AP Loading” is selected, the cursor will display the either CPU Usage as a percentage, or Traffic (Tx + Rx).

An example of CPU Usage is displayed below, where 10% of CPU is used.



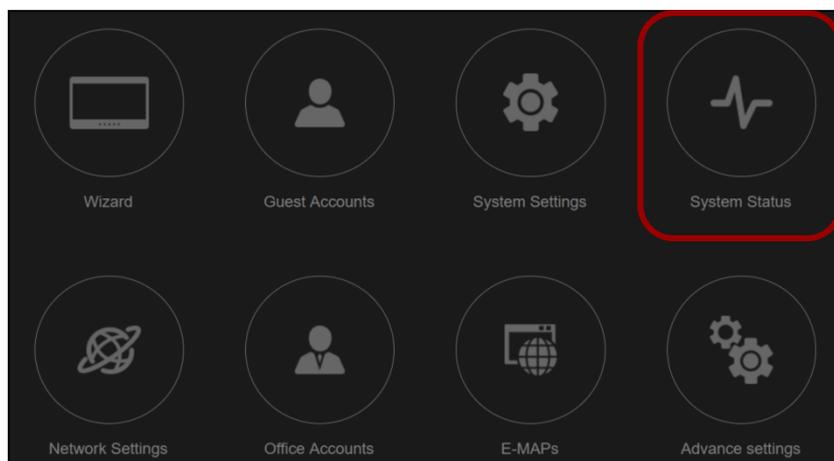
An example of Traffic (Tx + Rx) is displayed below.



VII-10 System Status

This section allows you to check information related to *Managed APs*, *Wireless Client*, *Guests*, *System Logs*, *Office Workers*, and *User Logs*.

Click the “System Status” icon.



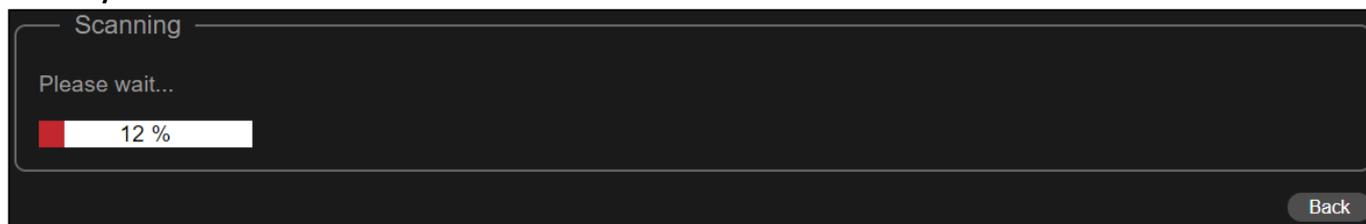
The screenshot shows the EDIMAX Pro interface. The top left features the EDIMAX Pro logo. The top right shows the location "Office 1-2-3" with a globe icon and a play button. Below the logo, the breadcrumb "Home > System Status" is visible, and "System Status" is underlined in the top right corner. A vertical sidebar on the left contains icons for various system functions, with the "System Status" icon (heartbeat line) highlighted in red. The main content area displays six circular status cards with the following data:

Category	Count
Managed APs	2
Guests	0
Office Workers	0
Wireless Client	3
System Logs	153
User logs	0

At the bottom of the page, the copyright notice reads: "Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved".

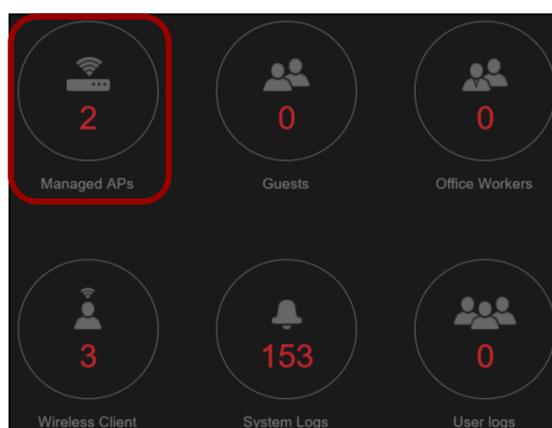
Click an icon for the information you want.

The system will scan the detailed information when an icon is clicked:



Managed APs

If you wish to know the current status of the APs, click the “Managed APs” icon.



Information of the APs will be shown. An example is displayed below:

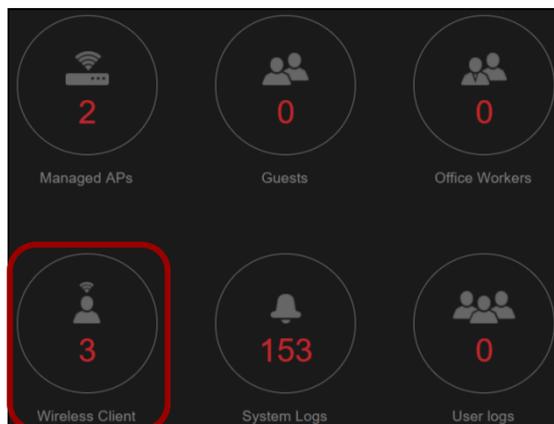
Home > System Status > APs Status APs Status

Master AP		Slave AP#1	
Product Name	AP74DA38D36B60	Product Name	AP74DA38D36B4A
Model	Office 1-2-3	Model	Office 1-2-3
Wireless Clients 2.4GHz	0	Wireless Clients 2.4GHz	0
Wireless Clients 5GHz	2	Wireless Clients 5GHz	0
2.4GHz Channel	11	2.4GHz Channel	11
5GHz Channel	36	5GHz Channel	36
Uptime	0 day 20:47:18	Uptime	0 day 00:36:35
System Time	2017/10/27 06:38:22	System Time	2017/10/27 06:38:22
MAC Address	74:DA:38:D3:6B:60	MAC Address	74:DA:38:D3:6B:4A
Management VLAN ID	1	Management VLAN ID	1
IP Address	192.168.2.101	IP Address	192.168.2.102
Default Gateway	192.168.2.250	Default Gateway	192.168.2.250
DNS	192.168.2.250,8.8.8.8	DNS	192.168.2.250,8.8.8.8

Back

Wireless Client

If you wish to know the information on the wireless clients, click the “Wireless Client” icon.



Home > System Status > Wireless Clients Status Wireless Clients Status

Master AP: AP74DA38D36B60

Client MAC Address	Signal	band(GHz)
28:56:5A:6B:2C:93	94%	5GHz

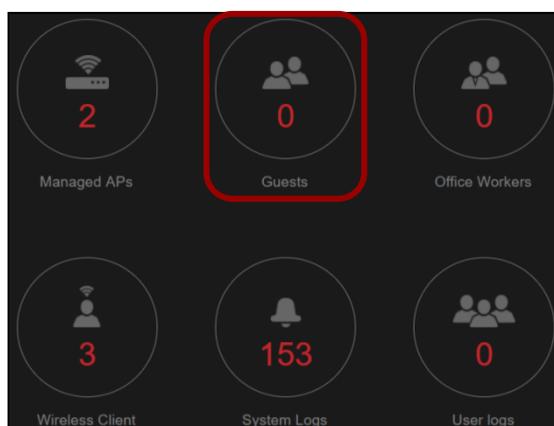
Slave AP#1: AP74DA38D36B4A

Client MAC Address	Signal	band(GHz)
D0:C5:F3:65:87:B3	100%	5GHz

Back

Guests

If you wish to know the information of the guests connected to the network, click the “Guests” icon.



Home > System Status > Guests Status Guests Status

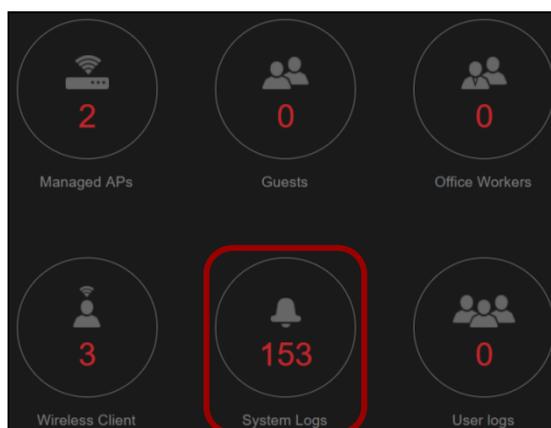
Guests Status

Index	User Name	MAC Address	Create Time	Expire Time	Usage Percentage	Vendor	Platform	Action
1	guest_test	B4:CE:F6:A7:73:6D	2017/10/27-07:16:10	forever	0%	HTC Corporation	Android	

[Back](#)

System Logs

If you wish to view the system logs of the network, click the “System Logs” icon.



Home > System Status > System Logs System Logs

System Logs

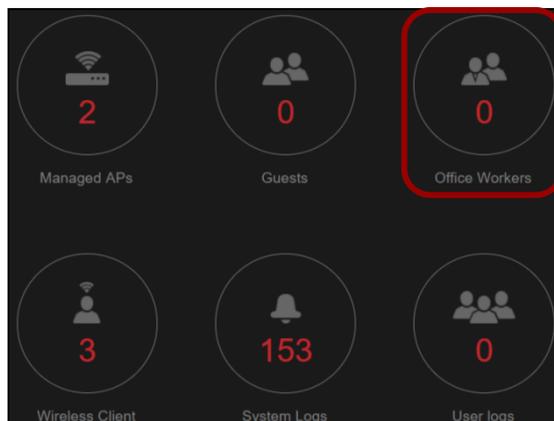
Search Match whole words

ID	Date and Time	Category	Severity	Users	Events/Activities
172	2017/10/27 07:41:51	NMS	Info	guest	User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] was logout automatically
171	2017/10/27 07:33:20	DHCP	Low	admin	DHCP Client, Lease obtained: 192.168.2.101; lease time 3600
170	2017/10/27 07:28:39	NMS	Low	guest	Static User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] login successfully
169	2017/10/27 07:27:33	WLAN	Low	admin	Wireless 2.4G (SSID3), STA(b4:ce:f6:a7:73:6d) : disassociated
168	2017/10/27 07:27:18	NMS	Info	guest	User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] was logout automatically
167	2017/10/27 07:26:47	WLAN	Low	admin	Wireless 2.4G (SSID3), STA(b4:ce:f6:a7:73:6d) : associated
166	2017/10/27 07:26:07	WLAN	Low	admin	Wireless 2.4G (SSID3), STA(b4:ce:f6:a7:73:6d) : disassociated
165	2017/10/27 07:25:32	WLAN	Low	admin	Wireless 2.4G (SSID3), STA(b4:ce:f6:a7:73:6d) : associated
164	2017/10/27 07:24:25	WLAN	Low	admin	Wireless 2.4G (SSID3), STA(b4:ce:f6:a7:73:6d) : disassociated
163	2017/10/27 07:19:53	WLAN	Low	admin	Wireless 5G (SSID3), STA(d0:c5:f3:65:87:b3) : disassociated
162	2017/10/27 07:18:24	NMS	Low	guest	Static User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] login successfully
161	2017/10/27 07:17:20	WLAN	Low	admin	Wireless 2.4G (SSID3), STA(b4:ce:f6:a7:73:6d) : associated
160	2017/10/27 07:03:20	DHCP	Low	admin	DHCP Client, Lease obtained: 192.168.2.101; lease time 3600
159	2017/10/27 07:01:37	WLAN	Low	admin	Wireless 5G (SSID2), STA(28:56:5a:6b:2c:93) : disassociated
158	2017/10/27 07:01:37	WLAN	Low	admin	Wireless 5G (SSID2), STA(28:56:5a:6b:2c:93) : deauthenticated due to session timeout
157	2017/10/27 06:52:16	WLAN	Low	admin	Wireless 5G (SSID2), STA(28:56:5a:6b:2c:93) : group key handshake completed (RSN)

Copyright 2017 © EDIMAX Technology Co., Ltd. All Rights Reserved

Office Workers

If you wish to view the information of the office workers connected to the network, click the “Office Workers” icon.



Home > System Status > Office Workers Status Office Workers Status

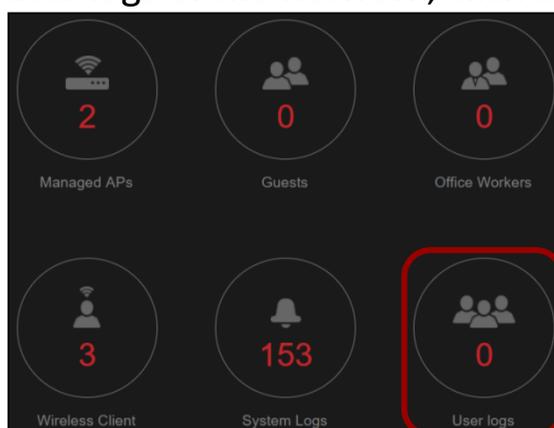
Office Workers Status

Index	Client MAC Address	AP MAC Address	WLAN	Radio	Signal	Connected Time	Idle Time	Tx	Rx	Vendor
1	28:56:5A:6B:2C:93	74:DA:38:D3:6B:4A	office123_5G	5GHz	95	52 min 30 secs	0	56671.107	15895.926	NULL

Back

User Logs

If you wish to view the user logs of the network, click the “User logs” icon.



These logs include the login / logout actions.

Users Log

Search

 Match whole words

ID	Date and Time	Category	Severity	Users	Events/Activities
4	2017/10/27 07:41:51	NMS	Info	guest	User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] was logout automatically
3	2017/10/27 07:28:39	NMS	Low	guest	Static User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] login successfully
2	2017/10/27 07:27:18	NMS	Info	guest	User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] was logout automatically
1	2017/10/27 07:18:24	NMS	Low	guest	Static User:[guest_test]'s device:[B4:CE:F6:A7:73:6D] login successfully

Refresh

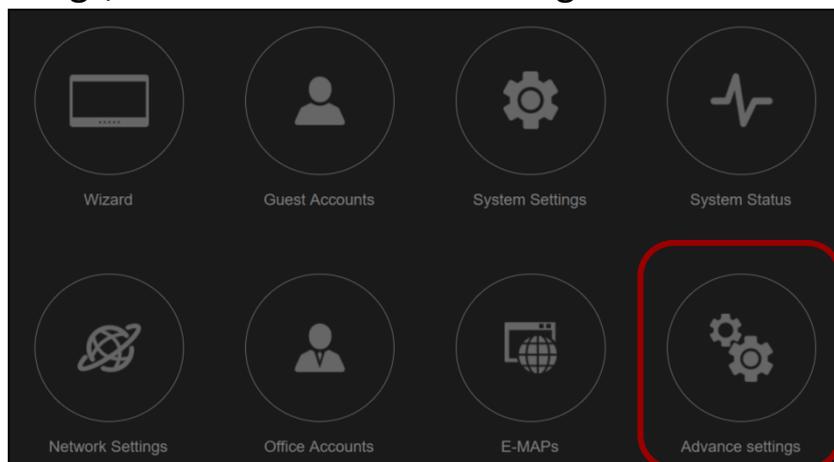
Back

VII-11 Advance Settings

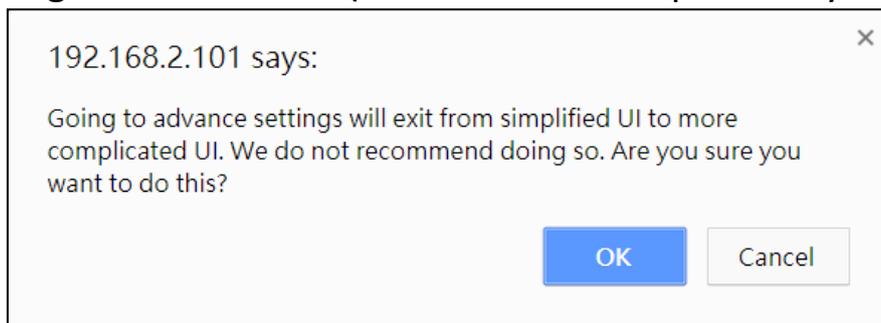


NOTE: It is NOT recommended to go to advance settings as the UI is a bit more complicated (although more detailed).

For Advance settings, click the “Advance settings” icon.



A pop-up message will be shown (the format will depend on your browser):



Refer to the next section on the advance settings and its options.

VIII Advanced Settings



NOTE: It is NOT recommended to go to advance settings as the UI is a bit more complicated (although more detailed).

The advanced settings include the top panel menu. When a category is selected, a left panel will appear for detailed configurations.

The top panel menu includes: *Dashboard*, *Zone Plan*, *NMS Monitor*, *NMS Settings*, *Local Network*, *Local Settings* & *Toolbox*.



VIII-1 Dashboard

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

The dashboard displays an overview of your AP array:

The dashboard interface includes the following sections:

- APs Information:** Shows 2 Managed, 2 Active, and 0 Offline APs. A 'Discovered' section shows 0 items.
- System Information:**
 - Product Name: Office 1-2-3
 - Host Name: AP74DA38D36B60
 - MAC Address: 74-DA-38-D3-6B-60
 - IP Address: 192.168.2.101
 - Firmware Version: 1.0.0
 - System Time: 2017/10/27 10:27:41
 - Uptime: 1 day 00:36:41
 - CPU Usage: 11%
 - Memory / Cache Usage: 53%
- Managed AP:** Searchable table with columns: Index, MAC Address, Device Name, Model, IP Address, 2.4G Channel, 5G Channel, Clients, 2.4G Domain, 5G Domain, Status, and Action.

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	2.4G Domain	5G Domain	Status	Action
1	74-DA-38-D3-6B-60	AP74DA38D36B60	Office 1-2-3	192.168.2.101	11	36	2	FCC	FCC+DFS	Green	[Refresh] [Refresh] [Refresh] [Refresh] [Refresh] [Refresh]
2	74-DA-38-D3-6B-4A	AP74DA38D36B4A	Office 1-2-3	192.168.2.102	11	36	2	FCC	FCC+DFS	Green	[Refresh] [Refresh] [Refresh] [Refresh] [Refresh] [Refresh]
- Managed AP Group:** Searchable table with columns: Group Name, MAC Address, Device Name, Model, IP Address, Clients, Status, and Action.

Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (0)							[Refresh]
ap_group (2)							[Refresh]
- Active Clients:** Searchable table with columns: Index, Client MAC Address, AP MAC Address, WLAN, User Name, Radio, Signal(%), Connected Time, Idle Time, Tx(KB), Rx(KB), and Vendor.

Index	Client MAC Address	AP MAC Address	WLAN	User Name	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
1	28:56:5A:6B:2C:93	74-DA-38-D3-6B-60	office123_5G	N/A	5GHz	91	23 min 39 secs	3	1246.907	940.528	NULL
2	CC:2F:71:CA:3B:4F	74-DA-38-D3-6B-60	office123_5G	N/A	5GHz	100	8 min 13 secs	2	2698.69	467.644	NULL
3	80:00:0B:3F:87:75	74-DA-38-D3-6B-4A	office123_5G	N/A	5GHz	98	40 min 37 secs	0	2521.627	764.594	Intel Corporate
4	D0:C5:F3:65:07:B3	74-DA-38-D3-6B-4A	guest123_5G	N/A	5GHz	97	43 min 19 secs	19	404.313	568.232	NULL

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:



VIII-1-1 System Information

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

System Information  	
Product Name	Office 1-2-3
Host Name	AP74DA38D36B60
MAC Address	74:DA:38:D3:6B:60
IP Address	192.168.2.101
Firmware Version	1.0.0
System Time	2017/10/27 10:27:41
Uptime	1 day 00:36:41
CPU Usage	<div style="width: 11%; background-color: #0070C0; height: 10px;"></div> 11%
Memory / Cache Usage	<div style="width: 53%; background-color: #0070C0; height: 10px;"></div> 53%

VIII-1-2 Devices Information

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

Devices Information  	
Device	Number
Access Points	1
Client Devices	0
Rogue Devices	0

VIII-1-3 Managed AP

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

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	2.4G Domain	5G Domain	Status	Action
1	74-DA-38-D3-6B-60	AP74DA38D36B60	Office 1-2-3	192.168.2.101	11	36	2	FCC	FCC+DFS		
2	74-DA-38-D3-6B-4A	AP74DA38D36B4A	Office 1-2-3	192.168.2.102	11	36	2	FCC	FCC+DFS		

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.

3. Blink LED

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

4. Buzzer

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

5. Network Connectivity

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

6. Restart

Restarts the Managed AP.

Status Icons			
Icon	Color	Status	Definition
	Grey	Disconnected	Managed AP is disconnected. <i>Please check the network connection and ensure the Managed AP is in the same IP subnet as the Master AP.</i>
	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all access points in the AP array. <i>Please check security settings.</i> All access points must have the same firmware version. <i>Please use the Master AP's firmware upgrade function.</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. <i>Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.</i>

VIII-1-4 Managed AP Group

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

To edit Managed AP Groups go to **NMS Settings → Access Point**.

Managed AP Group							
Search <input type="text"/> <input type="checkbox"/> Match whole words							
Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (0)							
Empty							
Wizard AP Group 2 (1)							

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

Search <input type="text"/>	<input type="checkbox"/> Match whole words
-----------------------------	--

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

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



1. Disallow

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

2. Edit

Edit various settings for the Managed AP Group.

3. Blink LED

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

4. Buzzer

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

5. Network Connectivity

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

6. Restart

Restarts all Managed APs in the group.

Status Icons			
Icon	Color	Status	Definition
	Grey	Disconnected	Managed AP group is disconnected. <i>Please check the network connection and ensure the group is in the same IP subnet as the Master AP.</i>
	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all access points in the AP array. <i>Please check security settings.</i> All access points must have the same firmware version. <i>Please use the Master AP's firmware upgrade function.</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. <i>Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.</i>

VIII-1-5 Active Clients

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

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

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

Search <input type="text"/>	<input type="checkbox"/> Match whole words
-----------------------------	--

VIII-1-6 Active Users

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

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

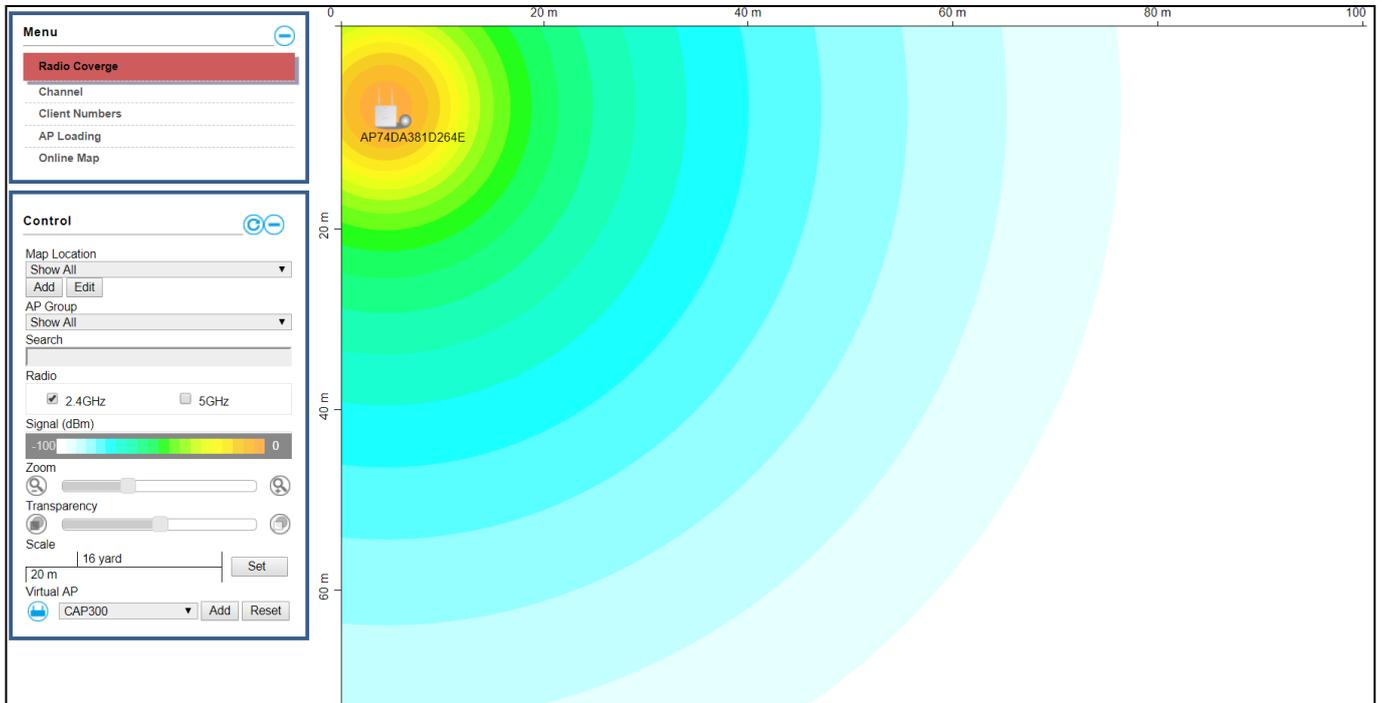
The search function can be used to locate a specific user. Type in the search box and the list will update:

Search <input type="text"/>	<input type="checkbox"/> Match whole words
-----------------------------	--

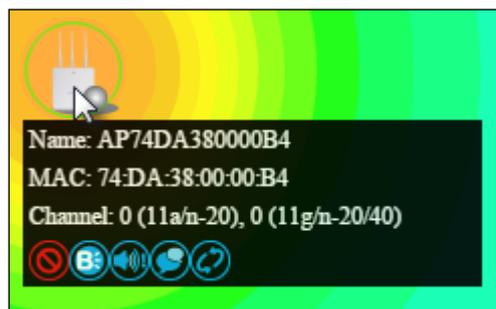
VIII-2 Zone Plan

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.



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



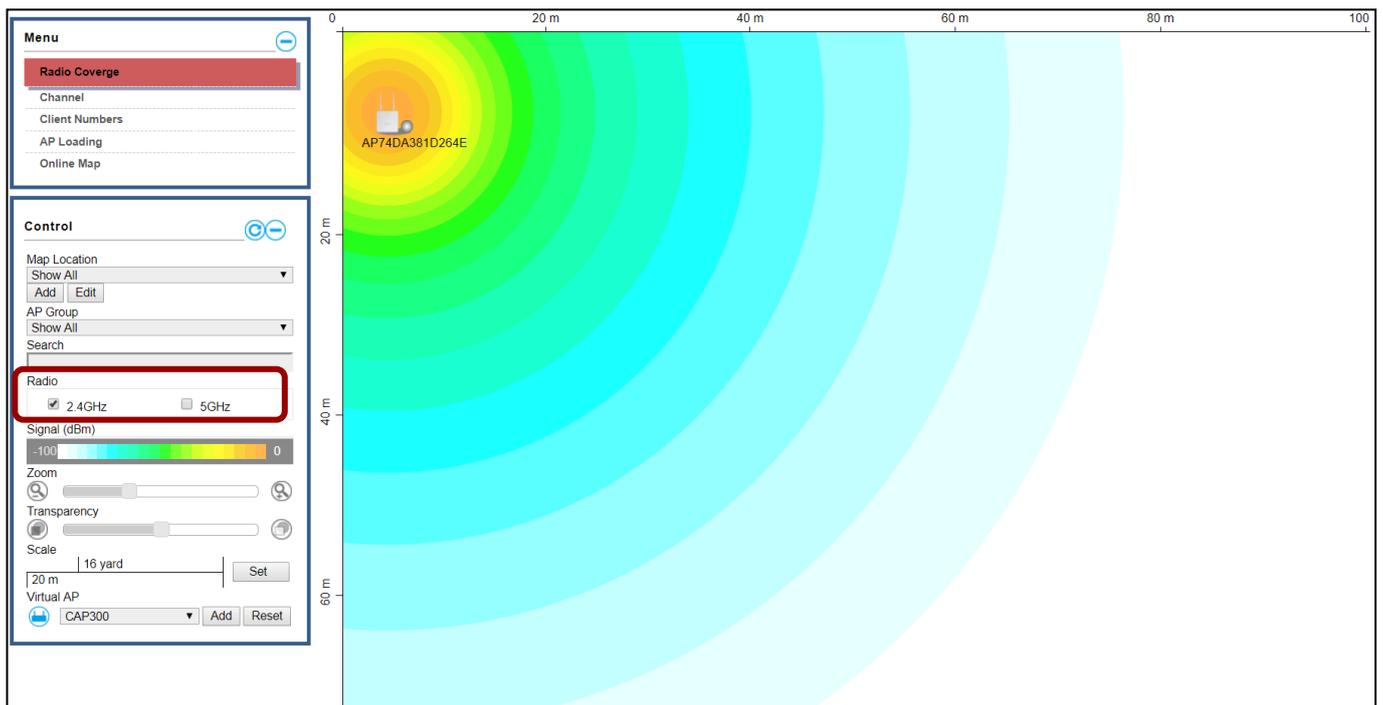
VIII-2-1 Menu

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



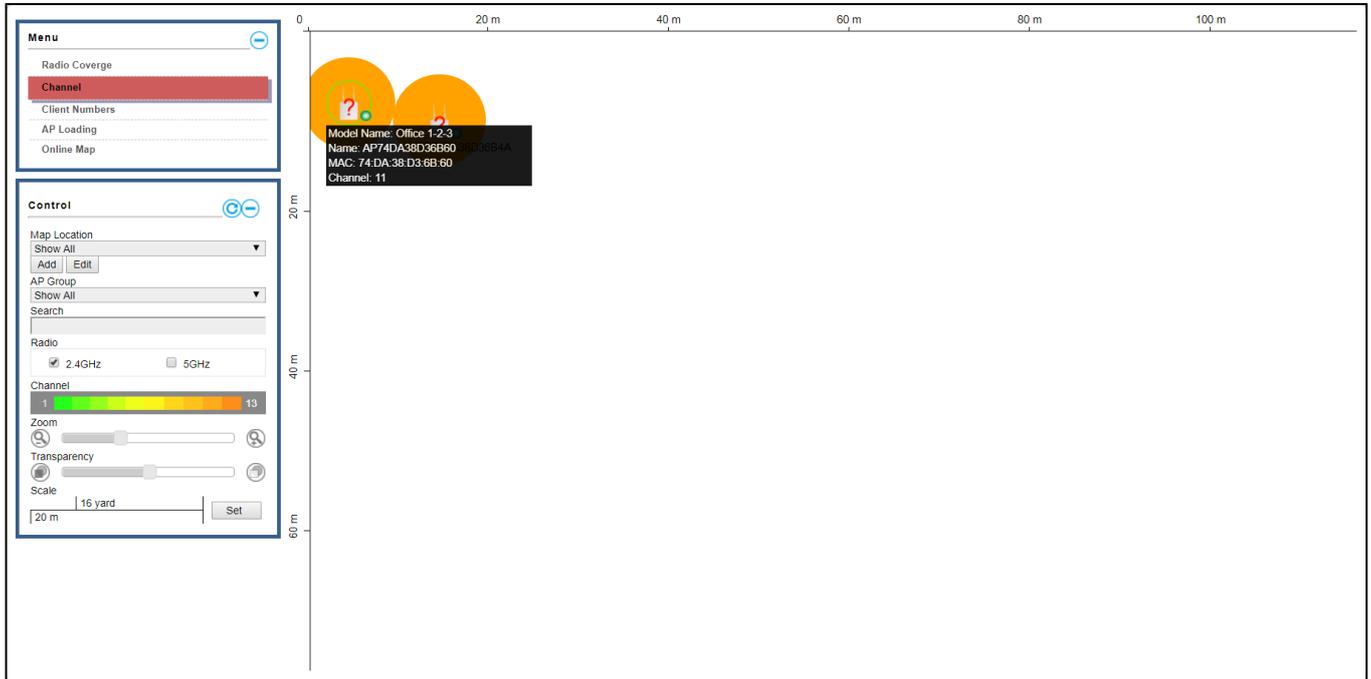
Radio Coverage

Information such as radio coverage (in both 2.4GHz and 5GHz) can be displayed to allow the planner to plan where to put the access points. Select 2.4GHz or 5GHz as outlined below:



Channel

When “Channel” is selected, the cursor will also display the channel of the radio network.



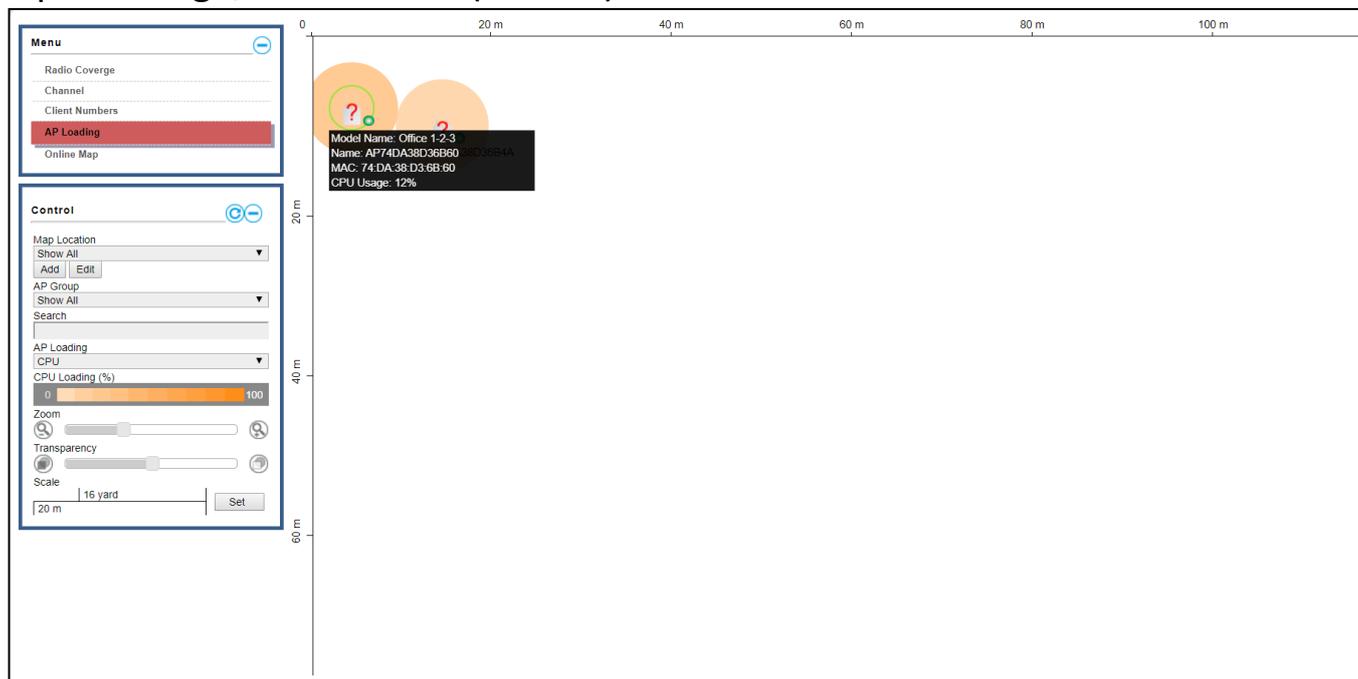
Client Numbers

When “Client Number” is selected, the cursor will display the client number.



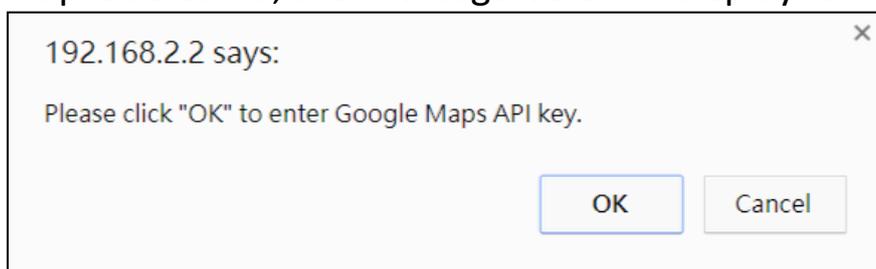
AP Loading

When “AP Loading” is selected, the cursor will display the either CPU Usage as a percentage, or or Traffic (Tx + Rx).

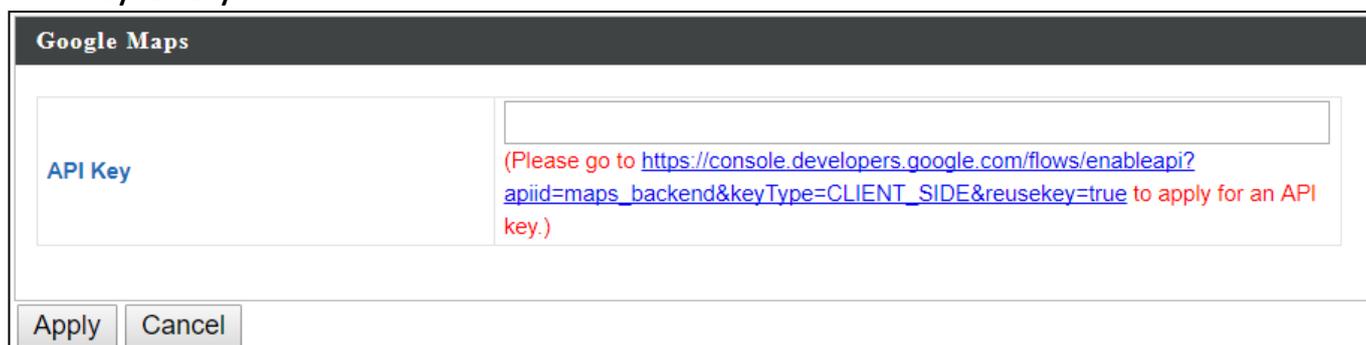


Online Map

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



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

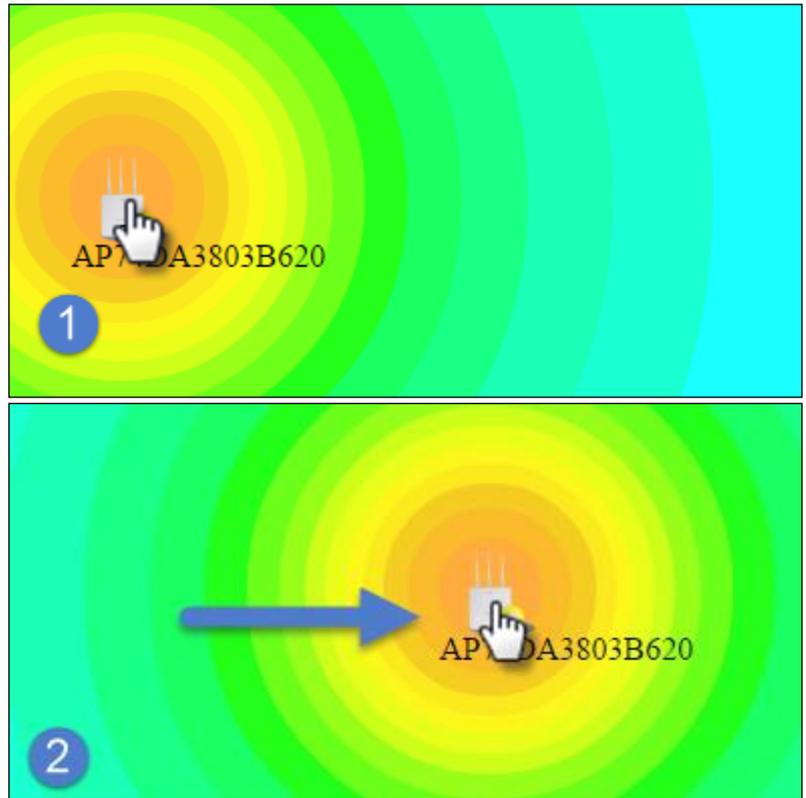


VIII-2-2 Control

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

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

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



VIII-3 NMS Monitor

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

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	74:DA:38:D3:6B:60	AP74DA38D36B60	Office 1-2-3	192.168.2.101	11	36	2	Connected	[Action icons]
2	74:DA:38:D3:6B:4A	AP74DA38D36B4A	Office 1-2-3	192.168.2.102	11	36	1	Connected	[Action icons]

VIII-3-1 Access Point

VIII-3-1-1 Managed AP

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

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	2.4G Domain	5G Domain	Status	Action
1	74:DA:38:D3:6B:60	AP74DA38D36B60	Office 1-2-3	192.168.2.101	11	36	2	FCC	FCC+DFS	Connected	[Action icons]
2	74:DA:38:D3:6B:4A	AP74DA38D36B4A	Office 1-2-3	192.168.2.102	11	36	2	FCC	FCC+DFS	Connected	[Action icons]

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

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

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



1. Disallow

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

2. Edit

Edit various settings for the Managed AP.

3. Blink LED

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

4. Buzzer

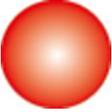
The Managed AP’s buzzer will sound temporarily to help identify/locate the access point.

5. Network Connectivity

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

6. Restart

Restarts the Managed AP.

Status Icons			
Icon	Color	Status	Definition
	Grey	Disconnected	Managed AP is disconnected. <i>Please check the network connection and ensure the Managed AP is in the same IP subnet as the Master AP.</i>
	Red	Authentication Failed Or	System security must be the same for all access points in the AP array. <i>Please check security settings.</i> All access points must have the same

		Incompatible NMS Version	firmware version. <i>Please use the Master AP's firmware upgrade function.</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. <i>Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.</i>

VIII-3-1-2 Managed AP Group

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

To edit Managed AP Groups go to **NMS Settings → Access Point**.

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

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

Search <input type="text"/>	<input type="checkbox"/> Match whole words
-----------------------------	--

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

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



1. Disallow

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

2. Edit

Edit various settings for the Managed AP Group.

3. Blink LED

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

4. Buzzer

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

5. Network Connectivity

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

6. Restart

Restarts all Managed APs in the group.

Status Icons			
Icon	Color	Status	Definition
	Grey	Disconnected	Managed AP group is disconnected. <i>Please check the network connection and ensure the group is in the same IP subnet as the Master AP.</i>
	Red	Authentication Failed Or Incompatible	System security must be the same for all access points in the AP array. <i>Please check security settings.</i> All access points must have the same firmware version. <i>Please use the Master</i>

		NMS Version	<i>AP's firmware upgrade function.</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	<i>Managed AP is waiting for approval. Note: Up to sixteen Managed APs are supported. Additional APs will have this status until an existing Managed AP is removed.</i>

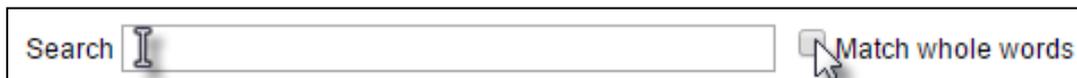
VIII-3-2 WLAN

VIII-3-2-1 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					
Index	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
1	wap1750	1	WPA2PSK	AES	No additional authentication

VIII-3-2-2 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	<input type="text"/>	<input type="checkbox"/> Match whole words			
Group Name	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
Wizard WLAN 2.4G Group 1 (1)	wap1750	1	WPA2PSK	AES	No additional authentication
Wizard WLAN 5G Group 2 (1)	wap1750	1	WPA2PSK	AES	No additional authentication

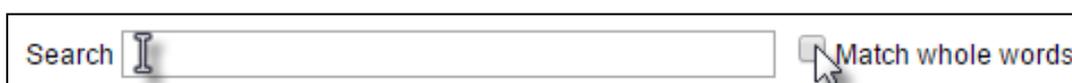
VIII-3-3 Clients

VIII-3-3-1 Active Clients

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

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

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



A search input field with the placeholder text "Search" and a cursor. To the right of the input field is a checkbox labeled "Match whole words".



The screenshot shows the "Clients" interface. At the top, there is a "Manual Refresh" button and a "Refresh" button. Below this is the "Active Clients" section, which includes a search input field and a "Match whole words" checkbox. A table header is visible with columns: Index, Client MAC Address, AP MAC Address, WLAN, User Name, Radio, Signal(%), Connected Time, Idle Time, Tx(KB), Rx(KB), and Vendor. The table content is currently empty.

VIII-3-4 Users

VIII-3-4-1 Active Users

Displays information about users currently connected.

Active Users											
Search <input type="text"/> <input type="checkbox"/> Match whole words											
Index	User Name	MAC Address	IP Address	SSID	Creator	Create Time	Expire Time	Usage Percentage	Traffic progress	Vendor	Platform Action
Empty											

VIII-3-4-2 Users Log

Displays the log information about users currently connected.

Search <input type="text"/> <input type="checkbox"/> Match whole words
--

Users Log						
Search <input type="text"/> <input type="checkbox"/> Match whole words						
ID ▾	Date and Time	Category	Severity ▲	Users	Events/Activities	
Refresh						

VIII-3-5 Rogue Devices

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

Click “Start” to scan for rogue devices:



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

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

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

VIII-3-6 Information

VIII-3-6-1 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: ▼

All Events/Activities

- 74:DA:38:1D:26:4E
- 74:DA:38:1D:26:5A

Select AP: ▼

All Events/Activities

Search Match whole words

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

VIII-3-6-2 AP Monitoring

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

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

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

Auto Refresh Time : 1 minute 30 seconds Disable



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

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

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

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

Tx Power

CPU Usage

Memory / Cache Usage

Collapse

Managed AP Information  Traffic

WLAN Information  **Expand**

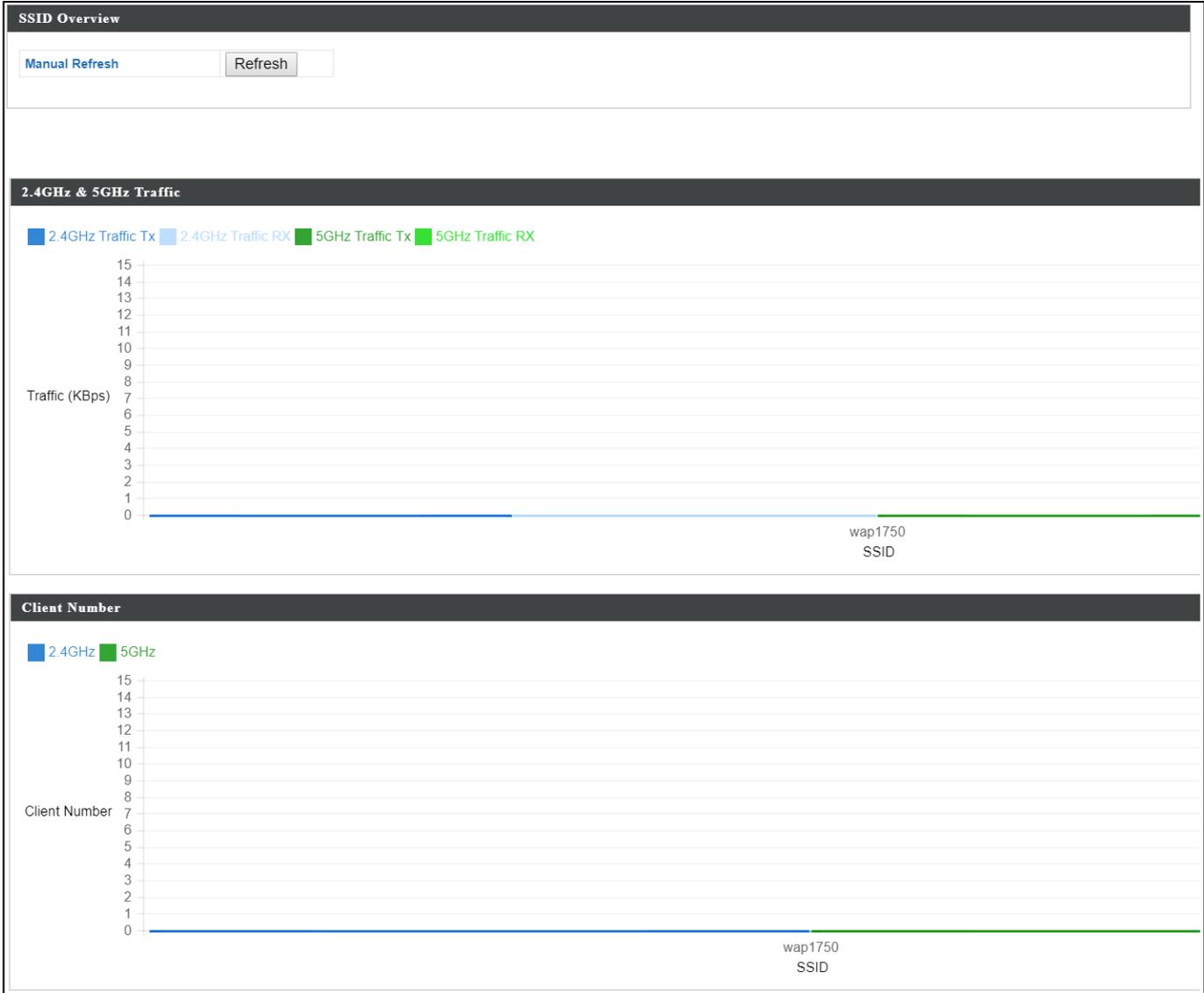
Select AP: 74:DA:38:1D:26:4E 

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

Managed AP Information 	Traffic Tx 												
<table border="1"><tr><td>Model Name</td><td>WAP1200</td></tr><tr><td>Model Image</td><td></td></tr><tr><td>Host Name</td><td>AP74DA381D264E</td></tr><tr><td>MAC Address</td><td>74:DA:38:1D:26:4E</td></tr><tr><td>IP Address</td><td>192.168.2.101</td></tr><tr><td>Firmware Version</td><td>1.8.1</td></tr></table>	Model Name	WAP1200	Model Image		Host Name	AP74DA381D264E	MAC Address	74:DA:38:1D:26:4E	IP Address	192.168.2.101	Firmware Version	1.8.1	Traffic RX 
Model Name	WAP1200												
Model Image													
Host Name	AP74DA381D264E												
MAC Address	74:DA:38:1D:26:4E												
IP Address	192.168.2.101												
Firmware Version	1.8.1												
WLAN Information 	Client Number 												
<table border="1"><tr><td colspan="2">2.4G</td></tr><tr><td>WLAN Groups</td><td>Wizard WLAN 2.4G Group 1</td></tr><tr><td>WLAN member list</td><td>wap1750</td></tr><tr><td colspan="2">5G</td></tr><tr><td>WLAN Groups</td><td>Wizard WLAN 5G Group 2</td></tr><tr><td>WLAN member list</td><td>wap1750</td></tr></table>	2.4G		WLAN Groups	Wizard WLAN 2.4G Group 1	WLAN member list	wap1750	5G		WLAN Groups	Wizard WLAN 5G Group 2	WLAN member list	wap1750	Channel 
2.4G													
WLAN Groups	Wizard WLAN 2.4G Group 1												
WLAN member list	wap1750												
5G													
WLAN Groups	Wizard WLAN 5G Group 2												
WLAN member list	wap1750												
	Tx Power 												
	CPU Usage 												
	Memory / Cache Usage 												

VIII-3-6-3 SSID Overview

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



VIII-4 NMS Settings

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

Access Point

- WLAN
- RADIUS
- Access Control
- Guest Network
- Users
- Guest Portal
- Zone Edit
- Schedule
- Smart Roaming
- Device Monitoring
- Firmware Upgrade
- Advanced
 - System Security
 - Date and Time
 - Google Maps

Access Point

Search Match whole words

<input type="checkbox"/>	Index ▲	MAC Address ▲	Device Name ▲	Model ▲	AP Group ▲	2.4G Channel ▲	5G Channel ▲	2.4G Tx Power ▲	5G Tx Power ▲	Status ▲	Action
<input type="checkbox"/>	1	74-DA-38-1D-26-4E	AP74DA381D264E	WAP1200	Wizard AP Group 2	N/A	N/A	N/A	N/A	●	

Refresh Edit Delete Selected Delete All

Access Point Group

Search Match whole words

<input type="checkbox"/>	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
<input type="checkbox"/>	System Default	0	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	Wizard AP Group 2	1	Wizard WLAN 2.4G Group 1	Wizard WLAN 5G Group 2	Disabled	Disabled	Disabled	Disabled

Add Edit Clone Delete Selected Delete All

Access Point Settings

Auto Approve Enable Disable

Apply

VIII-4-1 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:

Match whole words

Access Point

Match whole words

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

Access Point Group

Match whole words

<input type="checkbox"/>	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
<input type="checkbox"/>	System Default	1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
<input type="checkbox"/>	Wizard AP Group 2	1	Wizard WLAN 2.4G Group 1	Wizard WLAN 5G Group 2	Disabled	Disabled	Disabled	Disabled

Access Point Settings

Auto Approve Enable Disable

The **Status** icon displays *grey* (disconnected), *red* (authentication failed/incompatible NMS version), *orange* (upgrading firmware), *yellow* (connecting), *green* (connected) or *blue* (waiting for approval) for each individual Managed AP. Refer to the *Status Icons in VIII-1-3 Managed AP* for full descriptions.

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

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



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 Master AP. When disabled, Managed APs must be manually approved to join the AP Array with the Master 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:

VIII-4-1-1 Edit Access Point

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

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

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



VIII-4-1-1-1 Edit Basic Settings

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

Override Group Setting

Basic Settings	
Name	AP74DA381D264E
Description	
MAC Address	74:DA:38:1D:26:4E
AP Group	Wizard AP Group 2 ▼
IP Address Assignment	<input type="checkbox"/> Override Group Setting DHCP Client ▼
IP Address	192.168.2.101
Subnet Mask	255.255.255.0
Default Gateway	From DHCP ▼ 0.0.0.0
Primary DNS	User-Defined ▼
Secondary DNS	User-Defined ▼
IGMP Snooping	<input type="checkbox"/> Override Group Setting Disable ▼
Location Type	Indoor ▼

IP Address Assignment	<input checked="" type="checkbox"/> Override Group Setting DHCP Client ▼
IP Address	192.168.2.101
Subnet Mask	255.255.255.0
Default Gateway	From DHCP ▼ 0.0.0.0
Primary DNS	User-Defined ▼
Secondary DNS	User-Defined ▼
IGMP Snooping	<input checked="" type="checkbox"/> Override Group Setting Disable ▼
Location Type	Indoor ▼

Basic Settings	
Name	Edit the access point name. The default name is AP + MAC address.
Description	Enter a description of the access point for reference e.g. 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.
IGMP Snooping	Enable / Disable the IGMP Snooping function. IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic.
Location Type	Select the location of the AP (indoor or outdoor).

VIII-4-1-1-2 Edit Web Account Settings

Web Account Settings

Override Group Setting

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

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

Override Group Setting

VIII-4-1-1-3 Edit VLAN Settings

VLAN Settings			
Wired LAN Port	VLAN Mode		VLAN ID
Wired Port(#1)	<input type="checkbox"/> Override Group Setting	Untagged Port ▾	<input type="checkbox"/> Override Group Setting 1
Wired Port(#2)	<input type="checkbox"/> Override Group Setting	Untagged Port ▾	<input type="checkbox"/> Override Group Setting 1
Management VLAN ID	<input type="checkbox"/> Override Group Setting	1	

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

Override Group Setting

VIII-4-1-1-4 Edit Radio Settings

Radio Settings		Radio B/G/N (2.4 GHz)	Radio A/N/A/C (5.0 GHz)
Wireless	<input type="checkbox"/> Override Group Setting	Enable	Enable
Band	<input type="checkbox"/> Override Group Setting	11b/g/n	11a/n/ac
Auto Pilot	<input type="checkbox"/> Override Group Setting	Disable <small>Please set AP position on the Zone Plan first.</small>	Disable <small>Please set AP position on the Zone Plan first.</small>
Auto Pilot Sensitivity	<input type="checkbox"/> Override Group Setting	Low	Low
Auto Pilot Range	<input type="checkbox"/> Override Group Setting	Ch 1 - 11	Band 1
Auto Pilot Interval	<input type="checkbox"/> Override Group Setting	Half day	Half day
	<input type="checkbox"/> Change channel even if clients are connected		
Channel	<input type="checkbox"/> Override Group Setting	Ch 11, 2462MHz	Ch 36, 5.18GHz
Channel Bandwidth	<input type="checkbox"/> Override Group Setting	20 MHz	20 MHz
BSS BasicRateSet	<input type="checkbox"/> Override Group Setting	all	all
⊖ Advanced Settings			
		Radio B/G/N (2.4 GHz)	Radio A/N/A/C (5.0 GHz)
Contention Slot	<input type="checkbox"/> Override Group Setting	Short	
Preamble Type	<input type="checkbox"/> Override Group Setting	Short	
Guard Interval	<input type="checkbox"/> Override Group Setting	Short GI	<input type="checkbox"/> Override Group Setting Short GI
802.11n Protection	<input type="checkbox"/> Override Group Setting	Enable	<input type="checkbox"/> Override Group Setting Enable
CE Adaptive	<input type="checkbox"/> Override Group Setting	Disable	
DTIM Period	<input type="checkbox"/> Override Group Setting	1 (1-255)	<input type="checkbox"/> Override Group Setting 1 (1-255)
RTS Threshold	<input type="checkbox"/> Override Group Setting	2347 (1-2347)	<input type="checkbox"/> Override Group Setting 2347 (1-2347)
Fragment Threshold	<input type="checkbox"/> Override Group Setting	2346 (256-2346)	<input type="checkbox"/> Override Group Setting 2346 (256-2346)
Multicast Rate	<input type="checkbox"/> Override Group Setting	Auto	<input type="checkbox"/> Override Group Setting Auto
Tx Power	<input type="checkbox"/> Override Group Setting	100%	<input type="checkbox"/> Override Group Setting 100%
Beacon Interval	<input type="checkbox"/> Override Group Setting	100 (40-1000 ms)	<input type="checkbox"/> Override Group Setting 100 (40-1000 ms)
Station idle timeout	<input type="checkbox"/> Override Group Setting	60 (30-65535 seconds)	<input type="checkbox"/> Override Group Setting 60 (30-65535 seconds)
⊖ WDS Settings			
		Radio B/G/N (2.4 GHz)	Radio A/N (5.0 GHz)
WDS Functionality		None	None
WDS #1	AP Device Name	User-Defined	MAC Address
WDS #2	AP Device Name	User-Defined	MAC Address
WDS #3	AP Device Name	User-Defined	MAC Address
WDS #4	AP Device Name	User-Defined	MAC Address
WDS VLAN Mode		Untagged Port <small>(Enter at least one MAC address.)</small>	Untagged Port <small>(Enter at least one MAC address.)</small>
WDS VLAN ID		1	1
WDS Encryption		None <small>(Enter at least one MAC address.)</small>	None <small>(Enter at least one MAC address.)</small>

Radio Settings

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

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

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



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

Advanced Settings	
Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM (see 錯誤! 找不到參照來源。 錯誤! 找不到參照來源。).
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is “Short Preamble”.
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.

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

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

VIII-4-1-1-5 Edit WMM-EDCA Settings

WMM-EDCA Settings

Override Group Setting

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

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

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

Override Group Setting

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

VIII-4-1-1-6 Edit BandSteering Settings

BandSteering Settings

Bandsteering Override Group Setting Off 5G First Balanced User Define

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

Override Group Setting

VIII-4-1-1-7 Edit Profile Settings

Profile Settings		
	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
WLAN Group	<input type="checkbox"/> Override Group Setting Wizard WLAN 2.4G Group 1 ▼	<input type="checkbox"/> Override Group Setting Wizard WLAN 5G Group 2 ▼
Guest Network Group	<input type="checkbox"/> Override Group Setting Disable ▼	<input type="checkbox"/> Override Group Setting Disable ▼
RADIUS Group	<input type="checkbox"/> Override Group Setting Disable ▼	
MAC Access Control Group	<input type="checkbox"/> Override Group Setting Disable ▼	

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

Override Group Setting

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

VIII-4-1-1-8 Events

Press “Refresh” to refresh the event log

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

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

VIII-4-1-2 Add/Edit Access Point Group

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

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

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

**VIII-4-1-2-1 Edit Basic Group Settings**

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

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

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

VIII-4-1-2-2 Edit Web Account Group Settings

Web Account Group Settings		
Administrator Name	<input type="text" value="admin"/>	
Administrator Password	<input type="text" value="1234"/>	(6-32Characters)

VIII-4-1-2-3 Edit VLAN Group Settings

VLAN Group Settings		
Wired LAN Port	VLAN Mode	VLAN ID
Wired Port(#1)	Untagged Port ▾	<input type="text" value="1"/>
Wired Port(#2)	Untagged Port ▾	<input type="text" value="1"/>
Management VLAN ID	<input type="text" value="1"/>	

VIII-4-1-2-4 Edit Radio Group Settings

Radio Group Settings			
	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)
Wireless	Enable ▾		Enable ▾
Band	11b/g/n ▾		11a/n/ac ▾
Auto Pilot	Disable ▾		Disable ▾
Auto Pilot Sensitivity	Low ▾		Low ▾
Auto Pilot Range	Ch 1 - 11 ▾		Band 1 ▾
Auto Pilot Interval	Half day ▾		Half day ▾
	<input type="checkbox"/> Change channel even if clients are connected		<input type="checkbox"/> 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	<input type="text" value="1"/> (1-255)		<input type="text" value="1"/> (1-255)
RTS Threshold	<input type="text" value="2347"/> (1-2347)		<input type="text" value="2347"/> (1-2347)
Fragment Threshold	<input type="text" value="2346"/> (256-2346)		<input type="text" value="2346"/> (256-2346)
Multicast Rate	Auto ▾		Auto ▾
Tx Power	100% ▾		100% ▾
Beacon Interval	<input type="text" value="100"/> (40-1000 ms)		<input type="text" value="100"/> (40-1000 ms)
Station idle timeout	<input type="text" value="60"/> (30-65535 seconds)		<input type="text" value="60"/> (30-65535 seconds)

Radio Group Settings	
Wireless	Enable or disable the access point group's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the access point group. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Pilot	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point group's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
Auto Pilot Sensitivity	Select sensitivity of Auto Pilot.
Auto Pilot Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Pilot Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel	When Auto Pilot is disabled, select a channel (1-11) manually.
Channel Bandwidth	Set the channel bandwidth or use Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

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



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

Advanced Settings	
Contention Slot	Select "Short" or "Long" – this value is used for contention windows in WMM (see 錯誤! 找不到參照來源。 錯誤! 找不到參照來源。).

Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is "Short Preamble".
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
CE Adaptive	The measurement procedure follows clause 5.3.11.2.2 of the ETSI EN 300 328 V1.8.1
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the "Auto" setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the access point to a wireless client to verify if the station is still alive/active.

VIII-4-1-2-5 Edit WMM-EDCA Settings

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

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

VIII-4-1-2-6 Edit BandSteering Settings

BandSteering Group Settings	
Bandsteering	<input checked="" type="radio"/> Off <input type="radio"/> 5G First <input type="radio"/> Balanced <input type="radio"/> User Define

VIII-4-1-2-7 Edit Profile Settings

Profile Group Settings			
	Radio B/G/N (2.4 GHz)		Radio A/N/AC (5.0 GHz)
WLAN Group	Disable ▼		Disable ▼
Guest Network Group	Disable ▼		Disable ▼
RADIUS Group	Disable ▼		
MAC Access Control Group	Disable ▼		

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

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

VIII-4-1-2-8 Edit Group Settings

Group Settings

Search

Group Name : Wizard AP Group 2

<input type="checkbox"/>	MAC Address ▲	Device Name ▼
<input type="checkbox"/>	74-DA-38-1D-26-4E	AP74DA381D264E

Members

<<

>>

Search

Group Name : System Default

<input type="checkbox"/>	MAC Address ▲	Device Name ▼ ▲
<input type="checkbox"/>	74-DA-38-1D-26-5A	AP74DA381D265A

VIII-4-2 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**.

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
<input type="checkbox"/>	wap1750	1	WPA2PSK	AES	No additional authentication

Add Edit Clone Delete Selected Delete All

WLAN Groups

Search Match whole words

	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
<input type="checkbox"/>	Wizard WLAN 2.4G Group 1	1	wap1750	AP74DA381D264E	Wizard AP Group 2
<input type="checkbox"/>	Wizard WLAN 5G Group 2	1	wap1750	AP74DA381D264E	Wizard AP Group 2

Add Edit Clone Delete Selected Delete All

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



VIII-4-2-1 Add/Edit WLAN

WLAN Settings	
Name/ESSID	<input type="text"/>
Description	<input type="text"/>
VLAN ID	<input type="text" value="1"/>
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
802.11k	Disable ▾
Load Balancing	<input type="text" value="50"/> /100
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

WLAN Access Policy	
Traffic Shaping Settings	
Traffic Shaping	Disable ▾
Downlink	<input type="text" value="50"/> Mbps
Uplink	<input type="text" value="50"/> Mbps

WLAN Advanced Settings	
Smart Handover Settings	
Smart Handover	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RSSI Threshold	<input type="text" value="-80"/> dB
Active WLAN Schedule Settings <i>*Please enable (NMS Settings->Advanced->Date and Time->NTP Time Server) to make this function work.</i>	
Schedule Group	Disable ▾

Save Cancel Save & Apply

WLAN Settings	
Name/ESSID	Edit the WLAN name (SSID).
Description	Enter a description of the SSID 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 Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
802.11k	Enable / Disable to define and expose radio and network information (helps facilitate the management and maintenance of a mobile wireless LAN).
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu.
WPA Type	It can select WPA only or WPA2 only or WPA/WPA2 Mixed Mode-PSK
Encryption Type	Select TKIP/AES Mixed Mode or AES
Key Renewal Interval	Set the renewal interval time
Pre-Shared Key Type	Set Passphrase or Hex (64 characters)
Pre-Shared Key	Set a pre-shared key of 8-64 characters
Additional Authentication	Select an additional authentication method from the drop down menu.

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



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



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

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

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

VIII-4-2-2 Add/Edit WLAN Group

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

WLAN Group Settings			
Name	Wizard WLAN 2.4G Group 1		
Description	Created by Wizard		
Members	Search	<input type="text"/>	<input type="checkbox"/> Match whole words
	<input type="checkbox"/>	Name/ESSID	VLAN ID
	<input checked="" type="checkbox"/>	wap1750 <input type="checkbox"/> Override	1 <input type="checkbox"/> Override <input type="text" value="Disable"/>
*Schedule Group function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.			
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Save & Apply"/>			

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.

VIII-4-3 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**.

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

<input type="checkbox"/>	Name	RADIUS Server	Authentication Port	Session Timeout (sec)	Accounting
Please add External RADIUS Server setting					

Internal RADIUS Server

Search Match whole words

<input type="checkbox"/>	Name	EAP Authentication	Session Timeout (sec)	Termination-Action
Please add Internal RADIUS Server setting				

RADIUS Accounts (Max: 256 users)

Search Match whole words

<input type="checkbox"/>	Name	Password	Description
Please add User Account			

RADIUS Group

Search Match whole words

<input type="checkbox"/>	Name	2.4GHz	5GHz	RADIUS Accounts	Used AP	Used AP Group
Please add RADIUS group setting						

VIII-4-3-1 Add/Edit External RADIUS Server

External RADIUS Server	
Name	<input type="text"/>
Description	<input type="text"/>
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> Seconds
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Save & Apply"/>	

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 “MAC-RADIUS” password.
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.

VIII-4-3-2 Add/Edit Internal RADIUS Server

Upload EAP Certificate File	
EAP Certificate File Format	PKCS#12(*.pfx/*.p12)
Upload EAP Certificate File	Choose File No file chosen
Password of EAP Certificate File	<input type="text"/>
<input type="button" value="Upload"/>	
Internal RADIUS Server	
Name	<input type="text"/>
Description	<input type="text"/>
EAP Internal Authentication	PEAP(MS-PEAP) ▾
Shared Secret	<input type="text"/>
Session-Timeout	3600 Seconds
Termination-Action	<input checked="" type="radio"/> Reauthentication (RADIUS-Request) <input type="radio"/> Not-Reauthentication (Default) <input type="radio"/> Not-Send
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Save & Apply"/>	

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

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

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

VIII-4-3-3 Add/Edit/Import/Export RADIUS Accounts

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

RADIUS Accounts

User Name

Example: USER1, USER2, USER3

User Registration List

User Name	Password	Description	Action
Please add Account(s)			

Add

RADIUS Accounts

User Name
Example: USER1, USER2, USER3

EdimaxNew

Add
Reset

User Registration List

User Name	Password	Description	Action
EdimaxNew		Delete
Edimax1	Configured	Edimax1	

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

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

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

Edit

User Registration List		
User Name	Password	Description
Edimax1	Edimax1

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

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

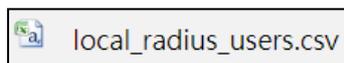
Import

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

upload RADIUS Accounts file	Choose File	No file chosen
<input type="button" value="Upload"/>	<input type="button" value="Cancel"/>	

Export

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



VIII-4-3-4 Add/Edit RADIUS Group

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

RADIUS Group Settings										
Group Name	<input type="text"/>									
Description	<input type="text"/>									
2.4GHz RADIUS	Primary : <input type="button" value="Disabled"/> Secondary : <input type="button" value="Disabled"/>									
5GHz RADIUS	Primary : <input type="button" value="Disabled"/> Secondary : <input type="button" value="Disabled"/>									
Members	Search <input type="text"/> <input type="checkbox"/> Match whole words <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Username</th> <th>Password</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Edimax1</td> <td>Configured</td> </tr> <tr> <td><input type="button" value="Add"/></td> <td><input type="text"/></td> <td><input type="text" value="....."/></td> </tr> </tbody> </table>	<input type="checkbox"/>	Username	Password	<input type="checkbox"/>	Edimax1	Configured	<input type="button" value="Add"/>	<input type="text"/>	<input type="text" value="....."/>
<input type="checkbox"/>	Username	Password								
<input type="checkbox"/>	Edimax1	Configured								
<input type="button" value="Add"/>	<input type="text"/>	<input type="text" value="....."/>								
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Save & Apply"/>										

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.

VIII-4-4 Access Control

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

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

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

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:

A search input field with the placeholder text "Search" and a cursor. To its right is a checkbox labeled "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:



The screenshot shows two configuration panels. The top panel is titled "MAC Access Control (Max: 256 items)". It contains a search box, a "Match whole words" checkbox, and a table with columns "MAC Address" and "Description". The table is currently empty with the text "Please add MAC Access Control setting". Below the table are buttons for "Add", "Delete Selected", and "Delete All".

The bottom panel is titled "MAC Access Control Group". It also contains a search box and a "Match whole words" checkbox. The table below has columns "Group Name", "Policy", "Members", "Used AP", and "Used AP Group". The table is empty with the text "No MAC Access Control Group". Below the table are buttons for "Add", "Edit", "Clone", "Delete Selected", and "Delete All".

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

VIII-4-4-1 Add/Edit MAC Access Control

Click “Add” to enter the page shown below:

MAC Access Control

Add MAC Address

Example: MAC1, MAC2, MAC3

Remain entries(256)

MAC Access Control List

MAC Address	Description	Delete
Please add MAC Addresses.		

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

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

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

VIII-4-4-2 Add/Edit/Clone MAC Access Control Group

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

Click “Add” to enter the page shown below:

The screenshot shows the 'MAC Filter Group Settings' interface. It has a dark header with the title. Below the header are four main sections: 'Group Name' with a text input field containing 'Please enter a new group name'; 'Description' with a text input field containing 'Please enter a new group description'; 'Action' with a dropdown menu set to 'Blacklist' and a search input field; and 'Members' which is a table with three columns: 'Members', 'MAC Address', and 'Description'. The 'Members' column has two rows, each with a checkbox. The 'MAC Address' column has one row with the value 'AA:BB:CC:DD:EE:FF'. The 'Description' column is empty. At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Save & Apply'.

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

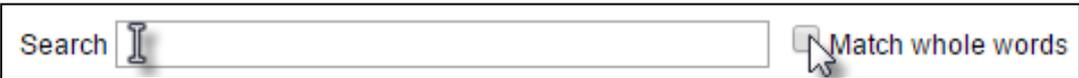
Press “Save” to save the above actions, “Cancel” to forfeit the changes, or “Save & Apply” to save and apply the above actions.

VIII-4-5 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**.

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

<input type="checkbox"/>	Name/ESSID	VLAN ID	Authentication	Encryption	Additional Authentication
Please add Guest Network setting					

Add Edit Clone Delete Selected Delete All

Guest Network Group

Search Match whole words

<input type="checkbox"/>	Group Name	Guest Network members	Guest Network member list	Used AP	Used AP Group
Please add Guest Network Group setting					

Add Edit Clone Delete Selected Delete All

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

VIII-4-5-1 Add/Edit Guest Network

Click “Add” to enter the page shown below:

Guest Network Settings

Name/ESSID	<input type="text"/>
Description	<input type="text"/>
VLAN ID	<input type="text" value="1"/>
Broadcast SSID	Enable ▾
Wireless Client Isolation	STA Separator ▾
802.11k	Disable ▾
Load Balancing	<input type="text" value="50"/> /100

Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

Guest Access Policy

Guest Portal Settings

Guest Portal	Disable ▾
--------------	-----------

Traffic Shaping Settings

Traffic Shaping	Disable ▾
Downlink	<input type="text" value="50"/> Mbps
Uplink	<input type="text" value="50"/> Mbps

Layer 3-Filtering Settings

Rules	Disable ▾																														
Exceptions	<table border="1"><thead><tr><th>Type</th><th>IP Address</th><th>Subnet Mask</th></tr></thead><tbody><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr><tr><td>Disable ▾</td><td>0.0.0.0</td><td>0.0.0.0</td></tr></tbody></table>	Type	IP Address	Subnet Mask	Disable ▾	0.0.0.0	0.0.0.0																								
	Type	IP Address	Subnet Mask																												
	Disable ▾	0.0.0.0	0.0.0.0																												
	Disable ▾	0.0.0.0	0.0.0.0																												
	Disable ▾	0.0.0.0	0.0.0.0																												
	Disable ▾	0.0.0.0	0.0.0.0																												
	Disable ▾	0.0.0.0	0.0.0.0																												
	Disable ▾	0.0.0.0	0.0.0.0																												
	Disable ▾	0.0.0.0	0.0.0.0																												
	Disable ▾	0.0.0.0	0.0.0.0																												
Disable ▾	0.0.0.0	0.0.0.0																													

Guest Network Advanced Settings

Schedule Group Settings

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

Schedule Group	Disable ▾
----------------	-----------

Save Cancel Save & Apply

Guest Network Settings	
Name/ESSID	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 Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
802.11k	Enable / Disable to define and expose radio and network information (helps facilitate the management and maintenance of a mobile wireless LAN).
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 100).
Authentication Method	Select an authentication method from the drop down menu.
Additional Authentication	Select an additional authentication method from the drop down menu.

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



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



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

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

Guest Network Advanced Settings	
Schedule Group	Select a schedule group.

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

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

VIII-4-5-2 Add/Edit Guest Network Group

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

Guest Group Settings

Name	<input type="text"/>								
Description	<input type="text"/>								
Members	Search <input type="text"/> <input type="checkbox"/> Match whole words								
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;"></th> <th style="width: 35%;">Name/ESSID</th> <th style="width: 15%;">VLAN ID</th> <th style="width: 45%;">Schedule Group</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>EdimaxGuest</td> <td><input type="checkbox"/> Override <input type="text" value="1"/></td> <td><input type="checkbox"/> Override <input type="text" value="Disable"/></td> </tr> </tbody> </table>		Name/ESSID	VLAN ID	Schedule Group	<input type="checkbox"/>	EdimaxGuest	<input type="checkbox"/> Override <input type="text" value="1"/>	<input type="checkbox"/> Override <input type="text" value="Disable"/>
		Name/ESSID	VLAN ID	Schedule Group					
<input type="checkbox"/>	EdimaxGuest	<input type="checkbox"/> Override <input type="text" value="1"/>	<input type="checkbox"/> Override <input type="text" value="Disable"/>						
*Schedule Group function will not work until (NMS Settings->Advanced->Date and Time->NTP Time Server) are enabled.									

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

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

VIII-4-6 Users

Users (Max: 128 users)

Search Match whole words

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

User Group

Search Match whole words

<input type="checkbox"/>	Group Name	User members	User member list	Description	Role Type
<input type="checkbox"/>	Default	0			Default
<input type="checkbox"/>	test	1	aaa		Front Desk manager
<input type="checkbox"/>	111	1	test1		Guest Portal user
<input type="checkbox"/>	w1	1	t2	w1	Guest Portal user

User Panel

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

User Settings

Name	<input type="text"/>
Description	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>
User Group	Default ▼

Usage Traffic Management

Maximum Usage Traffic	<input type="checkbox"/> Enable	<input type="text" value="100"/>	<input type="text" value="MB"/>	(Max: 1 TB)
------------------------------	---------------------------------	----------------------------------	---------------------------------	-------------

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

Press “Delete All Expired Users” to delete the expired users.

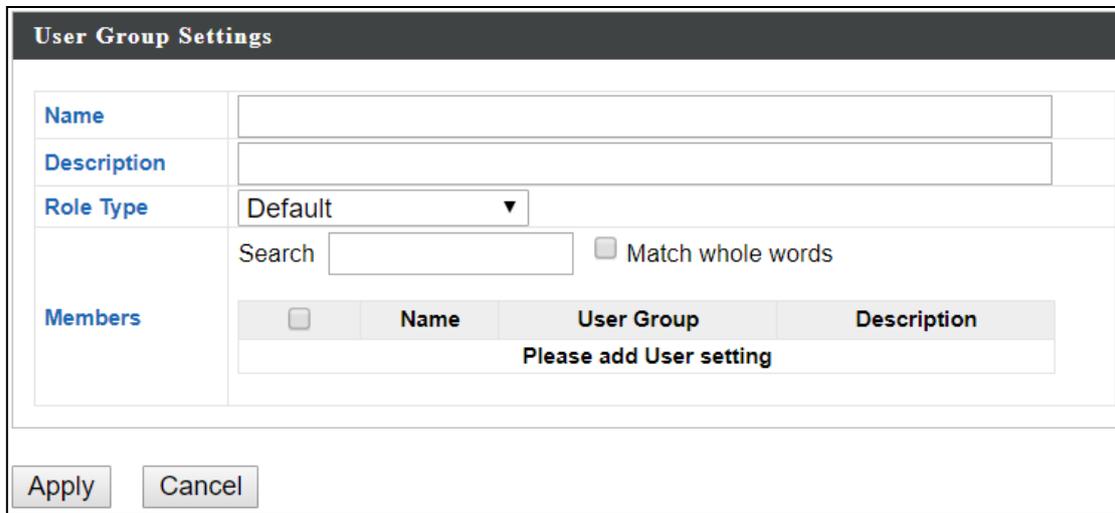
Press “Delete All” to delete all users.

Use “Upload List” to upload a user list.

Use “Download List” to download existing list for possible future reference.

User Group Panel

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



The screenshot shows a dialog box titled "User Group Settings". It contains several input fields and a table. The fields are: "Name" (text input), "Description" (text input), "Role Type" (dropdown menu with "Default" selected), and "Search" (text input) with a "Match whole words" checkbox. Below the search field is a table with columns "Name", "User Group", and "Description". The table is currently empty and contains the text "Please add User setting". At the bottom of the dialog are "Apply" and "Cancel" buttons.

Name	User Group	Description
Please add User setting		

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

VIII-4-7 Guest Portal

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

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

Press “Delete All” to delete all portals.

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

Add / Edit

Enter the fields according to the selected “Guest Portal Type” below:

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

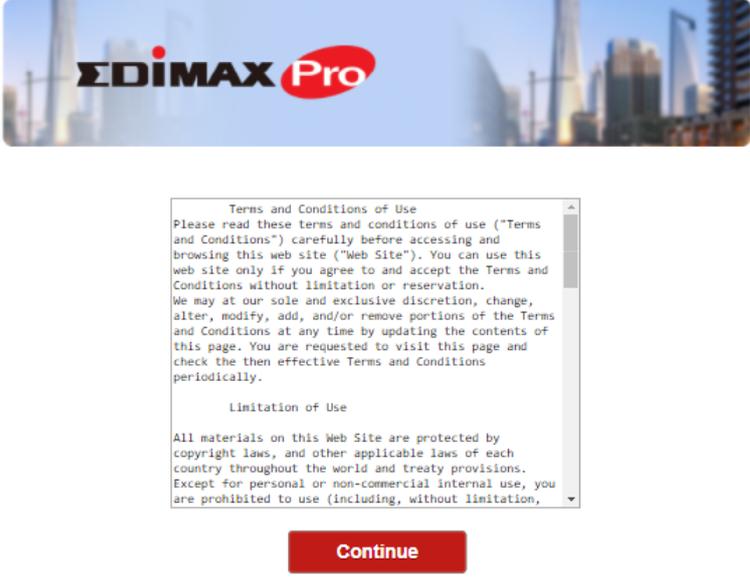
VIII-4-7-1 Free Guest Portal Type

Guest Portal Settings	
Name	portal1
Description	portl1
Guest Portal Type	Free ▼
Landing Page	<input checked="" type="radio"/> Promotion URL <input type="text" value="http://"/> ▼ <input type="text"/>
<input type="button" value="Save & Apply"/> <input type="button" value="Cancel"/>	

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

VIII-4-7-2 User Level Agreement Guest Portal Type

Guest Portal Settings	
Name	portal1
Description	portl1
Guest Portal Type	Service Level Agreement ▼
Landing Page	<input checked="" type="radio"/> Redirect to the original URL <input type="radio"/> Promotion URL <input type="text" value="http://"/>
Default Language	Global (English) ▼

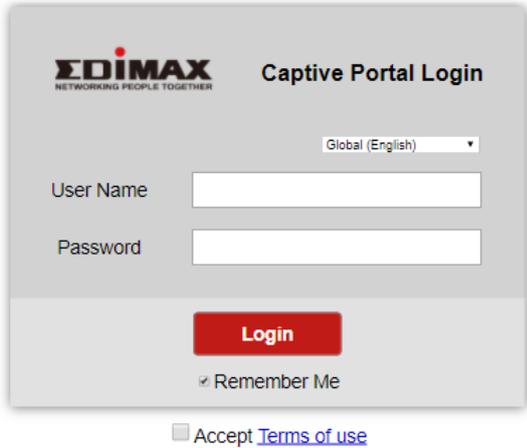
Guest Portal Customization	
Login Portal	Edit
<p>Login page preview</p> 	

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

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

VIII-4-7-3 Static Users Guest Portal Type

Guest Portal Settings	
Name	portal1
Description	portl1
Guest Portal Type	Static Users ▼
Authentication Server	Local Database ▼
Authentication User Group	111 ▼
Landing Page	<input checked="" type="radio"/> Redirect to the original URL <input type="radio"/> Promotion URL <input type="text" value="http://"/>
Default Language	Global (English) ▼

Guest Portal Customization	
Login Portal	<input type="button" value="Edit"/>
Login page preview	 

Guest Portal Settings	
Name	Enter / edit portal name.
Description	Enter / edit description of the portal for reference.
Authentication Server	Select an authentication server.
Authentication User Group	Select an authentication user group.
Landing Page	Select between “Redirect to the original URL” or “Promotion

	URL” (enter the promotion URL).
Default Language	Choose a default language.

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

VIII-4-7-4 Dynamic Users Guest Portal Type

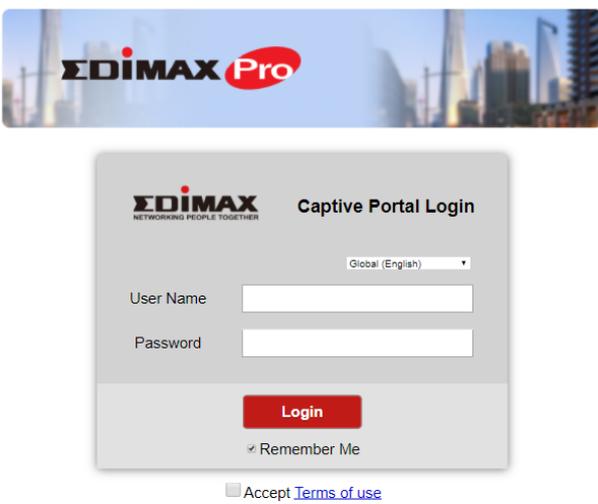
Guest Portal Settings

Name	portal1
Description	port1
Guest Portal Type	Dynamic Users ▼
Authentication Server	Local Database ▼
Authentication User Group	111 ▼
Landing Page	<input checked="" type="radio"/> Redirect to the original URL <input type="radio"/> Promotion URL <input type="text" value="http://"/> ▼
Default Language	Global (English) ▼

Front Desk Settings

User Group	test ▼
Generation URL	http://192.168.2.3/frontdesk.html
Guest Account Creation	<input checked="" type="checkbox"/> Replace expired user, when user table is full
Printout Message	<input type="button" value="Edit"/>
Notification Method	<input checked="" type="checkbox"/> Printout

Guest Portal Customization

Login Portal	<input type="button" value="Edit"/>
Login page preview	 <p>The preview shows a login page with the EDIMAX Pro logo at the top. Below the logo is a login form with fields for User Name and Password, a red Login button, a checked Remember Me checkbox, and an unchecked checkbox for Accept Terms of use.</p>

Guest Portal Settings	
Name	Enter / edit portal name.

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

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

Definition Table	
Symbol	Description
{SSID}	The SSID for Guest Portal user
{USERNAME}	The Name of Guest Portal user
{PASSWORD}	The Password of Guest Portal user
{EXPIRETIME}	The expire time of user account
{CREATETIME}	The create time of user account
{SN}	The Serial number of user account
* While printing the user data in Front Desk page, the "Symbol" will be replaced by the value in Users database.	

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

Preview Confirm Cancel

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

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

VIII-4-7-5 External Captive Portal Guest Portal Type

Guest Portal Settings	
Name	<input type="text"/>
Description	<input type="text"/>
Guest Portal Type	External Captive Portal ▾
Landing Page	<input checked="" type="radio"/> Use external redirect URL <input type="radio"/> Promotion URL <input type="text" value="http://"/> ▾ <input type="text"/>

External Settings	
External Type	Authentication Text ▾
Login URL	http:// <input type="text" value="172.217.27.132"/> <input type="button" value="Resolve"/>
Authentication Text	<input type="text"/> (16-32Characters) <small>To know how to use Authentication Text. Please, Click me.</small>

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

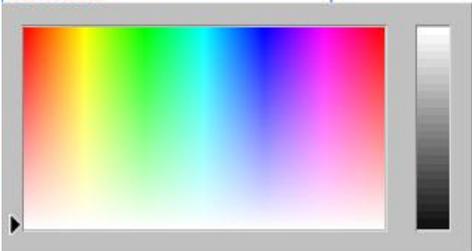
External Settings	
Login URL	Enter / edit a login URL.
Authentication Text	Enter an authentication text. Click “Click me” for help.

VIII-4-7-6 Editing “Login Portal”

Login Portal Customization

Header Image	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <input type="button" value="Choose File"/> No file chosen </div>  <p style="font-size: small; color: red;">Size: 800x200 pixels</p>
Logo Image	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <input type="button" value="Choose File"/> No file chosen </div>  <p style="font-size: small; color: red;">Size: 200x50 pixels</p>
Title Message	<input type="text" value="Captive Portal Login"/>
Background Color	<input type="text" value="FFFFFF"/>
Terms of use	<input type="checkbox"/> Accept by Default <div style="border: 1px solid #ccc; padding: 5px; font-size: small;"> <p style="text-align: center; margin: 0;">Terms and Conditions of Use</p> <p>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.</p> </div>

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



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

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

VIII-4-8 Zone Edit

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

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



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



Zone Edit

Search Match whole words

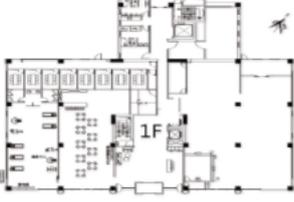
655360 bytes Available (655360 bytes Total)

<input type="checkbox"/>	Name/Location	Map	Map Size	Number of APs
Please add Zone Edit setting				

Add/Edit Zone

Upload Zone Image

Map Image File



Member(s) Settings

Name/Location

Description

Search

 Match whole words

	MAC Address	Device Name	Model	Status
<input type="checkbox"/>	System Default			
<input type="checkbox"/>	74:DA:38:1D:26:5A	AP74DA381D265A	WAP1200	●
Wizard AP Group 2				
<input type="checkbox"/>	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	●

Upload Zone Image

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

Member(s) Setting

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

VIII-4-9 Schedule

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

The screenshot shows two sections: "Schedule" and "Schedule Groups".

Schedule Section:

- Search: Match whole words
- Table with columns: Name, Description, Day of week, Time
- Placeholder: Please add Schedule setting
- Buttons: Add, Edit, Delete Selected, Delete All

Schedule Groups Section:

- Search: Match whole words
- Table with columns: Group Name, Schedule members, Schedule member list
- Placeholder: Please add Schedule group setting
- Buttons: Add, Edit, Delete Selected, Delete All

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

Add / Edit

The screenshot shows the "Schedule Settings" form with the following fields:

- Name:
- Description:
- Day of week selection table:

Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
<input type="checkbox"/>						
- Start Time: : :
- End Time: : :
- Buttons: Save, Cancel, Save & Apply

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

VIII-4-10 Smart Roaming

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

Roaming Groups				
<input type="checkbox"/>	Group Name	Used WLAN/GUEST SSID	Used WLAN/GUEST Group	Used AP Number
Please add Roaming Group setting				
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/>				

Add / Edit

Roaming Group Settings	
Name	<input type="text"/>
Description	<input type="text"/>
Mobility Domain	<input type="text"/>
Encryption Key	<input type="text"/>
Over the DS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SSID Type	<input checked="" type="radio"/> WLAN <input type="radio"/> GUEST
GUEST SSID	GUEST Group: <input type="text" value="1234"/> GUEST: <input type="text" value="None"/>
WLAN SSID	WLAN Group: <input type="text" value="group1"/> WLAN: <input type="text" value="None"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Save & Apply"/>	

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

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

VIII-4-11 Device Monitoring

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

Device Monitoring

Search Match whole words

<input type="checkbox"/>	Device IP	Description	Status
Please add devices			

Add / Edit

Device Monitoring

Add IP Address

Devices List

Device IP	Description	Delete
192.168.2.100	cap300	

Enter an IP Address(es) and click “Add” to add the device(s). Click “Reset” to clear the field.

Press “Apply” to apply the above action or “Cancel” to forfeit the addition.

VIII-4-12 Firmware Upgrade

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

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

Firmware Upgrade

Update firmware from	<input checked="" type="radio"/> Local <input type="radio"/> External FTP Server	
Firmware File	<input type="button" value="Choose File"/>	No file chosen
Timeout	<input type="text" value="150"/>	Seconds

Firmware Name	Firmware Version	NMS Version	Model	Size (bytes)

Access Point Group

	Group Name	Index	MAC Address	Device Name	Model	IP Address	Status	Firmware Version	NMS Version	Progress
<input type="checkbox"/>	System Default (1)									
<input type="checkbox"/>		1	74:DA:38:1D:26:5A	AP74DA381D265A	WAP1200	192.168.2.102	●	1.8.1	1.3.2.0	<input type="text" value="0%"/>
<input type="checkbox"/>	Wizard AP Group 2 (1)									
<input type="checkbox"/>		1	74:DA:38:1D:26:4E	AP74DA381D264E	WAP1200	192.168.2.101	●	1.8.1	1.3.2.0	<input type="text" value="0%"/>

VIII-4-13 Advanced

VIII-4-13-1 System Security

Configure the NMS system login name and password.

System Security	
NMS Security Name	administrator
NMS Security Key	1234567890123456 (8~16 Characters)
Sync NMS Security with Active Managed APs	<input type="checkbox"/> Enable <i>*Before changing NMS Security Name and Key, please make sure all Managed APs are connected; all other configuration update is complete, and status color is green.</i>
<input type="button" value="Apply"/>	

Press “Apply” to apply the settings.

VIII-4-13-2 Date & Time

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

Date and Time Settings	
Local Time	2012 ▼ Year Jan ▼ Month 1 ▼ Day 0 ▼ Hours 00 ▼ Minutes 00 ▼ Seconds
<input type="button" value="Acquire Current Time from Your PC"/>	
NTP Time Server	
Use NTP	<input type="checkbox"/> Enable
Auto Daylight Saving	<input checked="" type="checkbox"/> Enable
Server Name	User-Defined ▼ <input type="text"/>
Update Interval	24 (Hours)
Time Zone	
Time Zone	(GMT+08:00) Taipei, Taiwan ▼
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Save & Apply"/>	

Date and Time Settings

Local Time	Set the access point’s date and time manually using the drop
-------------------	--

	down menus.
Acquire Current Time from your PC	Click “Acquire Current Time from Your PC” to enter the required values automatically according to your computer’s current time and date.

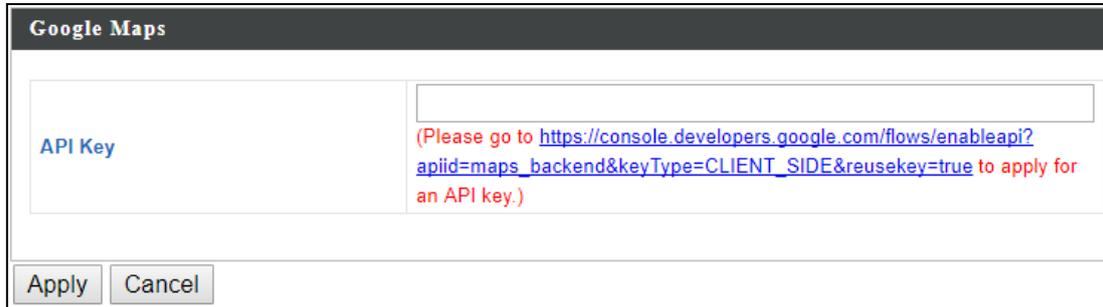
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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

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

VIII-4-13-3 Google Maps

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



The screenshot shows a dialog box titled "Google Maps". It contains a text input field for the API key. Below the input field, there is a red instruction: "(Please go to https://console.developers.google.com/flows/enableapi?apiid=maps_backend&keyType=CLIENT_SIDE&reusekey=true to apply for an API key.)". At the bottom of the dialog, there are two buttons: "Apply" and "Cancel".

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

VIII-4-13-4 SMS

SMS	
Provider	Please Select ▾
Username	<input type="text"/>
Password	<input type="password"/>
SMS Quota Limit	<input type="text" value="0"/>
Number of SMS Sent	<input type="text" value="0"/> <input type="button" value="Reset"/>
<input type="button" value="Test Account"/>	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Provider	Select a service provider from the drop down menu. Plivo and Stream Telecom are the available options.
-----------------	--

Pilivo:

Provider	Plivo ▾ https://www.plivo.com
Username	<input type="text"/>
Password	<input type="password"/>
Phone Number	<input type="text"/>
SMS Quota Limit	<input type="text" value="0"/>
Number of SMS Sent	<input type="text" value="0"/> <input type="button" value="Reset"/>
<input type="button" value="Test Account"/>	

Username	Enter the username for the service provider.
Password	Enter the password for the service provider.
Phone Number	Enter the phone number.
SMS Quota Limit	Enter a number for SMS quota limit.
Number of SMS Sent	This keeps track of the number of sent SMS. Click "Reset" to restart the sent SMS count.

Click "Test Account" to test the validity of the above-entered fields.

Stream Telecom:

Provider	Stream Telecom ▾ https://web.szk-info.ru
Username	<input type="text"/>
Password	<input type="password"/>
Sender Name	<input type="text"/>
SMS Quota Limit	<input type="text" value="0"/>
Number of SMS Sent	<input type="text" value="0"/> <input type="button" value="Reset"/>
<input type="button" value="Test Account"/>	

Username	Enter the username for the service provider.
Password	Enter the password for the service provider.
Sender Name	Enter the sender's name.
SMS Quota Limit	Enter a number for SMS quota limit.
Number of SMS Sent	This keeps track of the number of sent SMS. Click "Reset" to restart the sent SMS count.

Click "Test Account" to test the validity of the above-entered fields.

Click "Apply" to apply the settings, or "Cancel" to forfeit the changes.

VIII-5 Local Network

To see information of current local network settings such as IP address, DHCP server, 2.4GHz & 5Ghz Wi-Fi and security, WPS, RADIUS server, MAC filtering and WMM settings, go through this section.

VIII-6 Local Settings

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

The screenshot shows the 'Local Settings' web interface. On the left is a navigation menu with categories: System Settings (System Information, Wireless Clients, Wireless Monitor, Log), Management (Admin, Date and Time, Syslog Server Settings, Syslog E-mail Settings, I'm Here), and Advanced (LED Settings, Update Firmware, Save/Restore Settings, Factory Default, Reboot). The main content area is titled 'Operation Mode' and contains three sections:

- Operation Mode:** A dropdown menu currently set to 'AP Controller Mode'.
- Wireless Mode:** Two dropdown menus, both set to 'Access Point'.
- Management:** A dropdown menu currently set to 'Disable'.

'Apply' and 'Cancel' buttons are located at the bottom right of the main content area.

VIII-6-1 Operation Mode

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

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

Operation Mode	
Operation Mode	AP Controller Mode ▼

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

Management	
Self AP Management Mode	Disable ▼

- AP Mode ▼
- AP Mode**
- Repeater Mode
- AP Controller Mode
- Managed AP mode
- Client Bridge Mode



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



In AP Controller Mode the access point will switch to Office 1-2-3 user interface.

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

VIII-6-2 Network Settings

VIII-6-2-1 System Information

“System Information” page displays basic system information.

System						
Model						
Product Name	AP801F02F1968A					
Uptime	1 day 23:51:09					
System Time	 /01/02 23:53:07					
Boot from	Internal memory					
Firmware Version	1.8.1					
MAC Address	80:1F:02:F1:96:8A					
Management VLAN ID	1					
IP Address	192.168.2.103					<input type="button" value="Refresh"/>
Default Gateway	192.168.2.70					
DNS	192.168.2.70					
DHCP Server	192.168.2.70					

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

Wireless 2.4GHz	
Status	Enabled
MAC Address	80:1F:02:F1:96:8A
Channel	Ch 7 (Auto)
Transmit Power	100% 28dbm
RSSI	-63/-79/-80

Wireless 2.4GHz /SSID						
SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation	
	No Authentication	No Encryption	1	No additional authentication	Disabled	
	No Authentication	No Encryption	1	No additional authentication	Disabled	

Wireless 2.4GHz /WDS Disabled		
MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

Wireless 5GHz	
Status	Enabled
MAC Address	80:1F:02:F1:96:8B
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Transmit Power	100% 24dbm
RSSI	0/0

Wireless 5GHz /SSID						
SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation	
	No Authentication	No Encryption	1	No additional authentication	Disabled	

Wireless 5GHz /WDS Disabled		
MAC Address	Encryption Type	VLAN Mode/ID
No WDS entries.		

System	
Model	Displays the model number of the access point.
Product Name	Displays the product name for reference, which consists of “AP” plus the MAC address.
Uptime	Displays the total time since the device was turned on.
System Time	Displays the system time.
Boot From	Displays information for the booted hardware, booted from internal memory.
Firmware Version	Displays the firmware version.
MAC Address	Displays the access point’s MAC address.
Management VLAN ID	Displays the management VLAN ID.
IP Address	Displays the IP address of this device. Click “Refresh” to update this value.
Default Gateway	Displays the IP address of the default gateway.
DNS	IP address of DNS (Domain Name Server)
DHCP Server	IP address of DHCP Server.

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

Wireless 2.4GHz (5GHz)	
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or disabled).
MAC Address	Displays the access point’s MAC address.
Channel	Displays the channel number the specified wireless frequency is using for broadcast.
Transmit Power	Displays the wireless radio transmit power level as a percentage.
RSSI	Received signal strength indicator (RSSI) is a measurement of

	the power present in a received radio signal.
--	---

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

Wireless 2.4GHZ (5GHz) / WDS Status	
MAC Address	Displays the peer access point's MAC address.
Encryption Type	Displays the encryption type for the specified WDS.
VLAN Mode/ID	Displays the VLAN ID for the specified WDS.

Select "Refresh" to refresh all information.

VIII-6-2-2 Wireless Clients

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

Refresh Time	
Auto Refresh Time	<input checked="" type="radio"/> 5 seconds <input type="radio"/> 1 second <input type="radio"/> Disable
Manual Refresh	<input type="button" value="Refresh"/>

2.4GHz WLAN Client Table											
#	SSID	IP Address	MAC Address	Tx	Rx	Signal (%)	RSSI (dbm)	Connected Time	Idle Time	Vendor	Kick
No wireless client											

5GHz WLAN Client Table											
#	SSID	IP Address	MAC Address	Tx	Rx	Signal (%)	RSSI (dbm)	Connected Time	Idle Time	Vendor	Kick
No wireless client											

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

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

VIII-6-2-3 Wireless Monitor

“Wireless Monitor” is a tool built into the access point to scan and monitor the surrounding wireless environment. Select a frequency and click “Scan” to display a list of all SSIDs within range along with relevant details for each SSID.

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

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

VIII-6-2-4 Log

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



Older entries will be overwritten when the log is full

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

Search Match whole words

Save Clear Refresh

186-167

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

The following information/events are recorded by the log:

- ◆ **USB**
Mount & unmount
- ◆ **Wireless Client**
Connected & disconnected
Key exchange success & fail
- ◆ **Authentication**
Authentication fail or successful.
- ◆ **Association**
Success or fail
- ◆ **WPS**
M1 - M8 messages

WPS success

◆ **Change Settings**

◆ **System Boot**

Displays current model name

◆ **NTP Client**

◆ **Wired Link**

LAN Port link status and speed status

◆ **Proxy ARP**

Proxy ARP module start & stop

◆ **Bridge**

Bridge start & stop.

◆ **SNMP**

SNMP server start & stop.

◆ **HTTP**

HTTP start & stop.

◆ **HTTPS**

HTTPS start & stop.

◆ **SSH**

SSH-client server start & stop.

◆ **Telnet**

Telnet-client server start or stop.

◆ **WLAN (2.4G)**

WLAN (2.4G) channel status and country/region status

◆ **WLAN (5G)**

WLAN (5G) channel status and country/region status

VIII-6-3 Management

VIII-6-3-1 Admin

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

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

Account to Manage This Device	
Administrator Name	<input type="text" value="admin"/>
Administrator Password	<input type="password" value="....."/> (4-32Characters)
	<input type="password" value="....."/> (Confirm)
Username	<input type="text" value="frontdesk"/>
Password	<input type="password" value="....."/>
	<input type="password" value="....."/> (Confirm)
<input type="button" value="Apply"/>	
Advanced Settings	
Product Name	<input type="text" value="AP74DA38D36B60"/>
HTTP Port	<input type="text" value="80"/> (80, 1024-65535)
HTTPS Port	<input type="text" value="443"/> (443, 1024-65535)
Management Protocol	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> TELNET <input type="checkbox"/> SSH
Login Timeout	<input type="text" value="5"/> (mins)
<input type="button" value="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).

Front Desktop Account	
Name	Set the system's front desktop account name.
Password	Set the system's front desktop account password.

The Front Desktop account is for creating guest accounts and ticket printing only.

Press "Apply" to apply the configuration.

Advanced Settings	
Product Name	Edit the product name according to your preference consisting of 1-32 alphanumeric characters. This name is used for reference purposes.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below).
Login Timeout	Specify the idle time (in minutes) before being kicked from the server.

HTTP

Internet browser HTTP protocol management interface

TELNET

Client terminal with telnet protocol management interface

Press "Apply" to apply the configuration.

VIII-6-3-2 Date and Time

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

Date and Time Settings	
Local Time	2012 ▼ Year Jan ▼ Month 1 ▼ Day 0 ▼ Hours 00 ▼ Minutes 00 ▼ Seconds
<input type="button" value="Acquire Current Time from Your PC"/>	
NTP Time Server	
Use NTP	<input type="checkbox"/> Enable
Auto Daylight Saving	<input checked="" type="checkbox"/> Enable
Server Name	User-Defined ▼ <input type="text"/>
Update Interval	24 <input type="text"/> (Hours)
Time Zone	
Time Zone	(GMT+08:00) Taipei, Taiwan ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

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

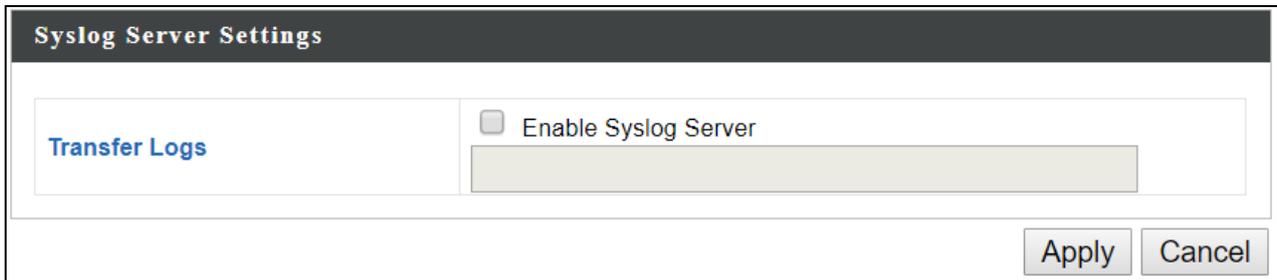
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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

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

VIII-6-3-3 Syslog Server Settings

The system log can be sent to a server.



The screenshot shows a dialog box titled "Syslog Server Settings". On the left, there is a section labeled "Transfer Logs". To the right of this section is a checkbox labeled "Enable Syslog Server", which is currently unchecked. Below the checkbox is a text input field. At the bottom right of the dialog box are two buttons: "Apply" and "Cancel".

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

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

VIII-6-3-4 Syslog E-mail Settings

Syslog E-mail Settings	
E-mail Logs	<input type="checkbox"/>
E-mail Subject	<input type="text"/>
SMTP Server Address	<input type="text"/>
SMTP Server Port	<input type="text"/>
Sender E-mail	<input type="text"/>
Receiver E-mail	<input type="text"/>
Authentication	Disable ▾

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

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

VIII-6-3-5 I'm Here

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

Duration of Sound

Duration of Sound
 (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.

VIII-6-4 Advanced

VIII-6-4-1 LED Settings

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

LED Settings	
Power LED	<input checked="" type="radio"/> On <input type="radio"/> Off
Diag LED	<input checked="" type="radio"/> On <input type="radio"/> Off

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

VIII-6-4-2 Update Firmware

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

Firmware Location

Update firmware from
 a file on your PC

Update Firmware from PC

Firmware Update File
 No file chosen



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

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

VIII-6-4-3 Save/Restore Settings

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

Save Settings to PC**Save Settings**

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

Restore Settings from PC**Restore Settings**

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

VIII-6-4-4 Factory Default

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

This will restore all settings to factory defaults.

Factory Default

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.

VIII-6-4-5 Reboot

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

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

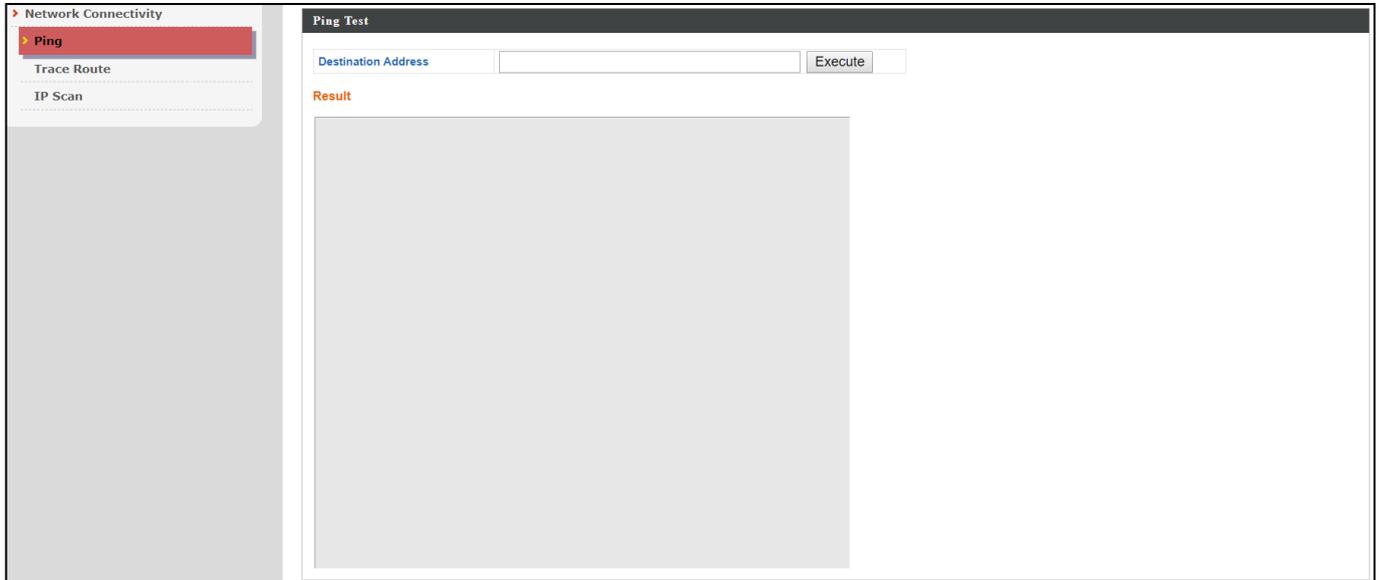
Reboot

Reboot

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

VIII-7 Toolbox

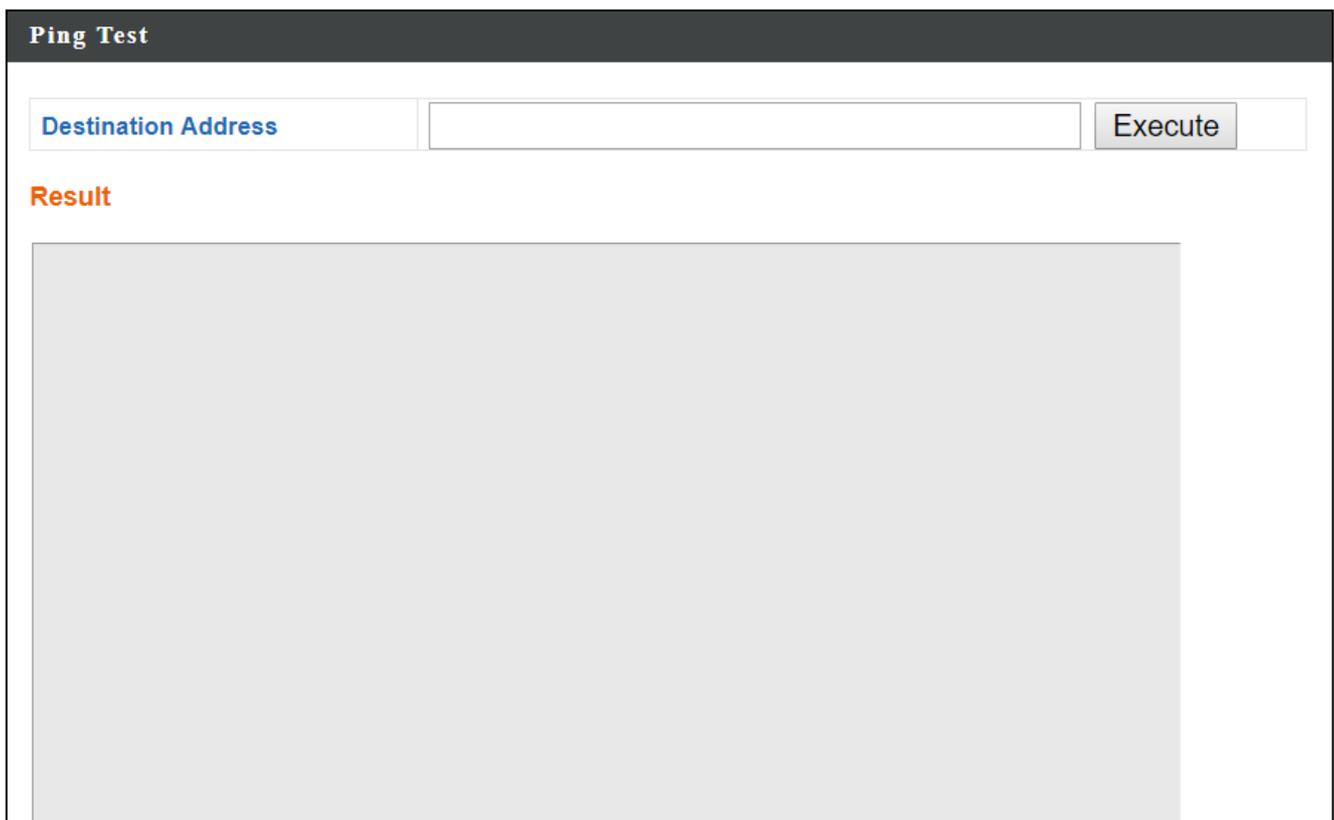
The Toolbox panel provides network diagnostic tools: *Ping*, *Traceroute*, and *IP Scan*.



VIII-7-1 Network Connectivity

VIII-7-1-1 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.

VIII-7-1-2 Trace Route

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

Traceroute Test

Destination Address

Result

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

VIII-7-1-3 IP Scan

IP Scan

IP domain: . . . *

Result

Graphic Illustration: un-used distributed non-distributable scanning

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

IX Appendix

IX-1 Configuring your IP address

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

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

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



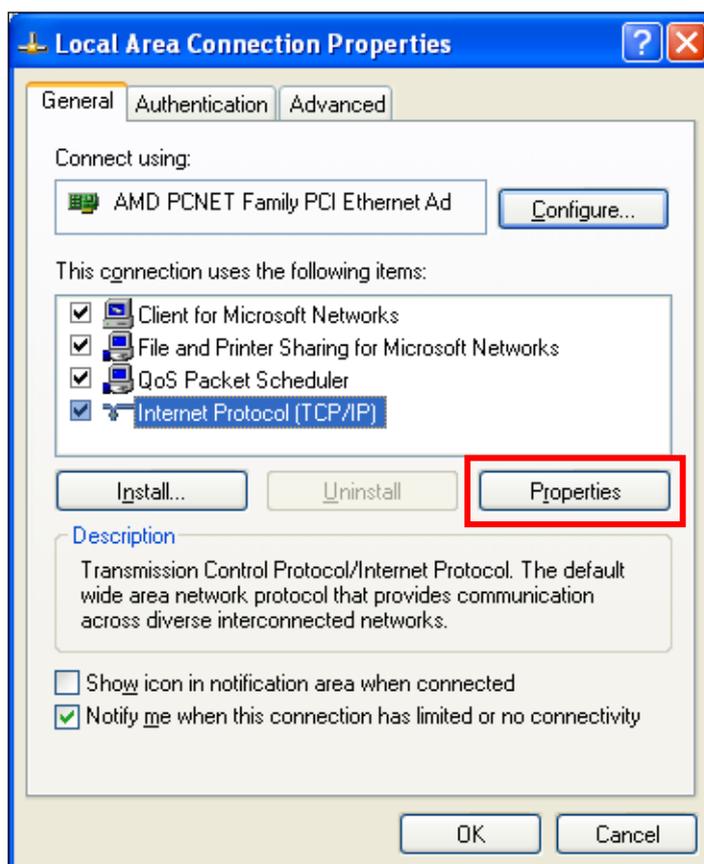
If you've changed the Master ap's IP address, or if your gateway/router uses a DHCP server, make sure you enter the correct IP address. Refer to your gateway/router's settings. Your computer's IP address must be in the same subnet as the Master ap.



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

IX-1-1 Windows XP

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

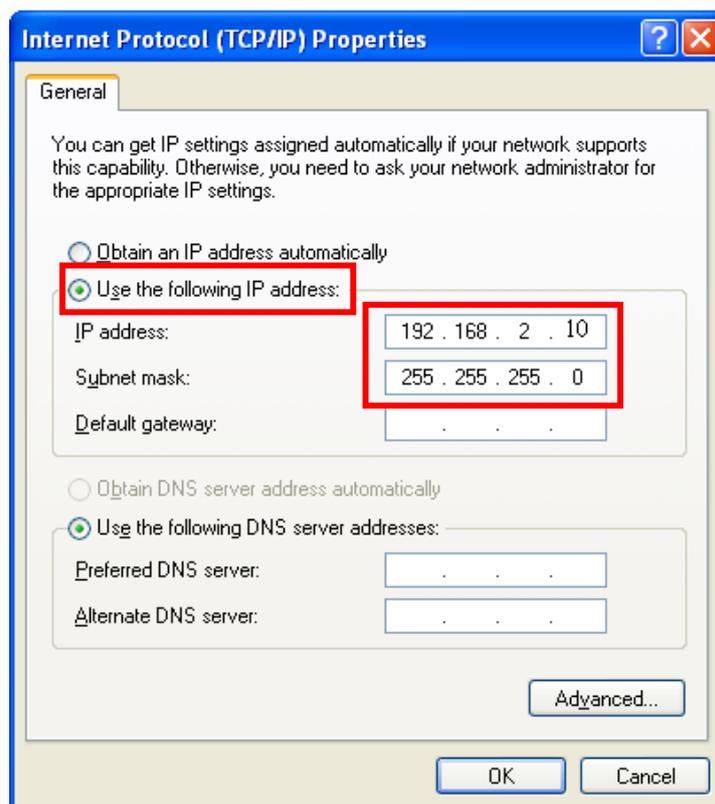


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

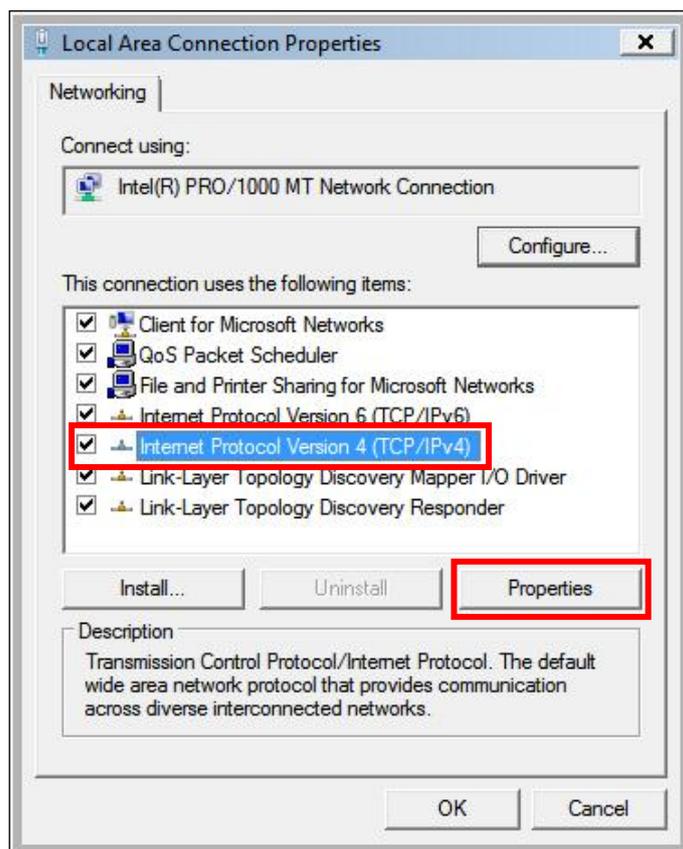
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



IX-1-2 Windows Vista

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

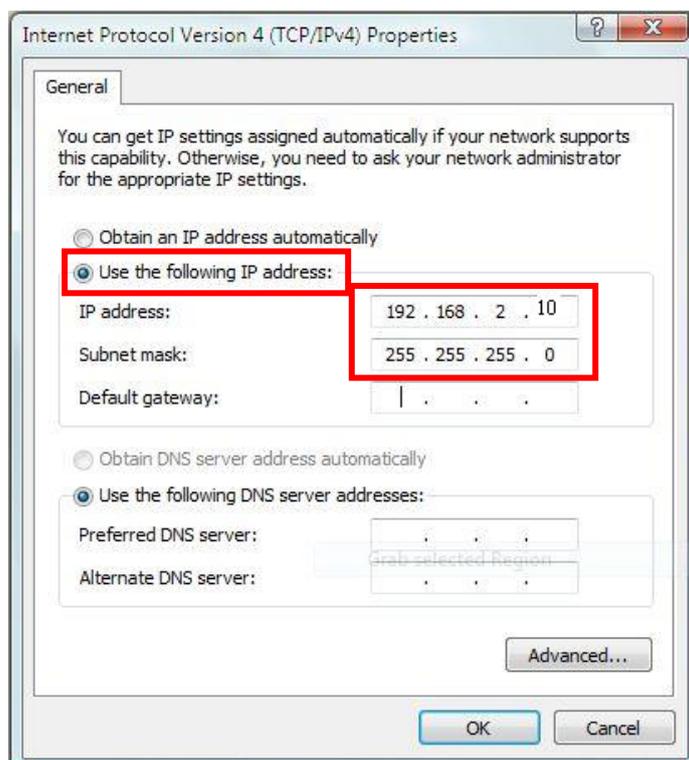


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

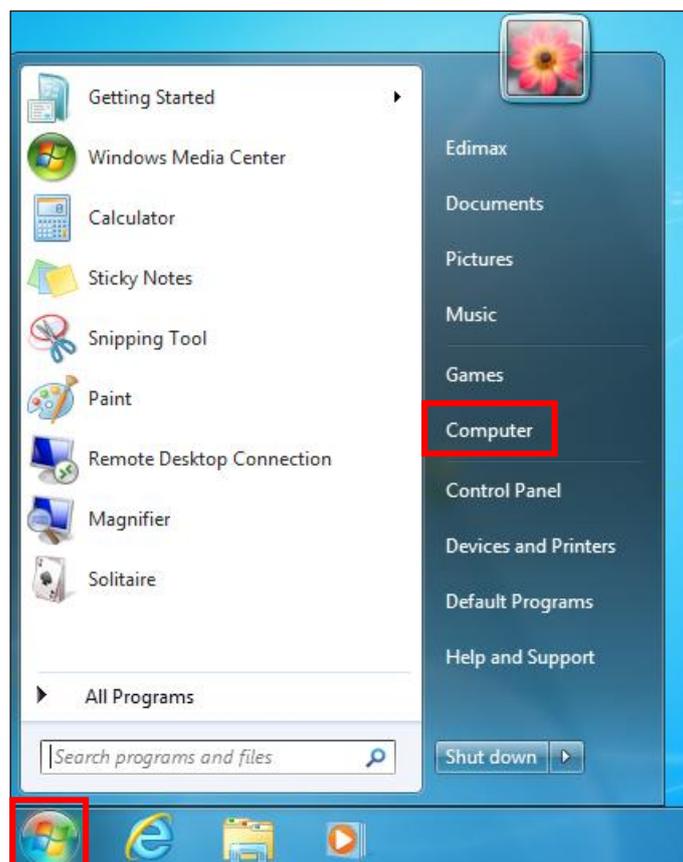
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

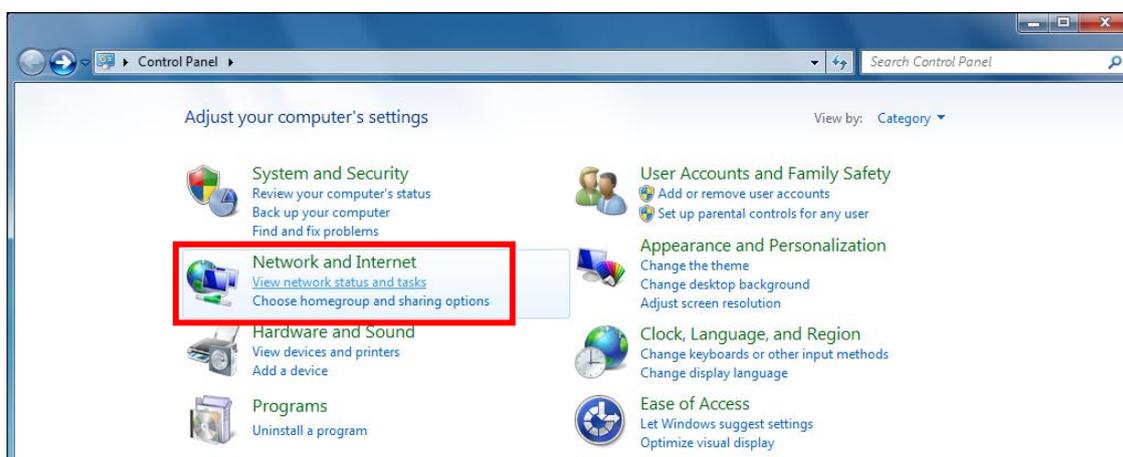


IX-1-3 Windows 7

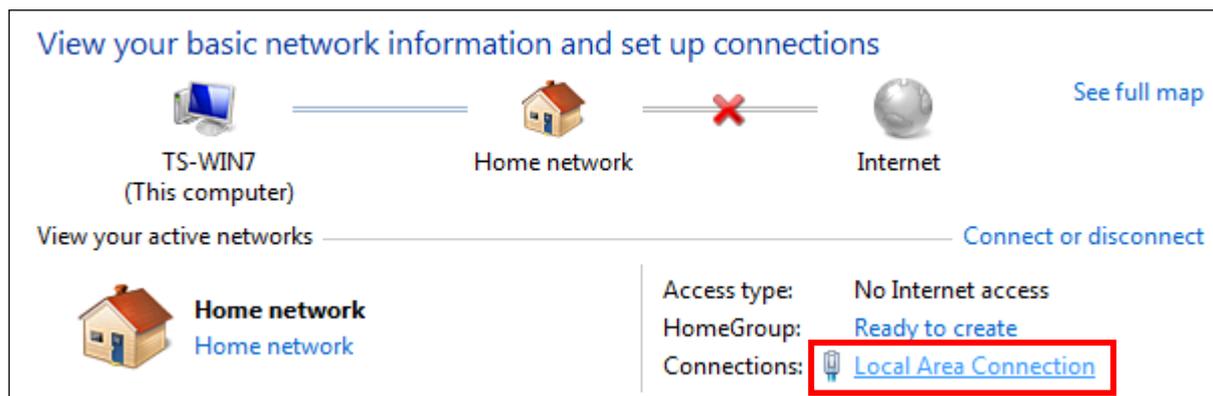
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



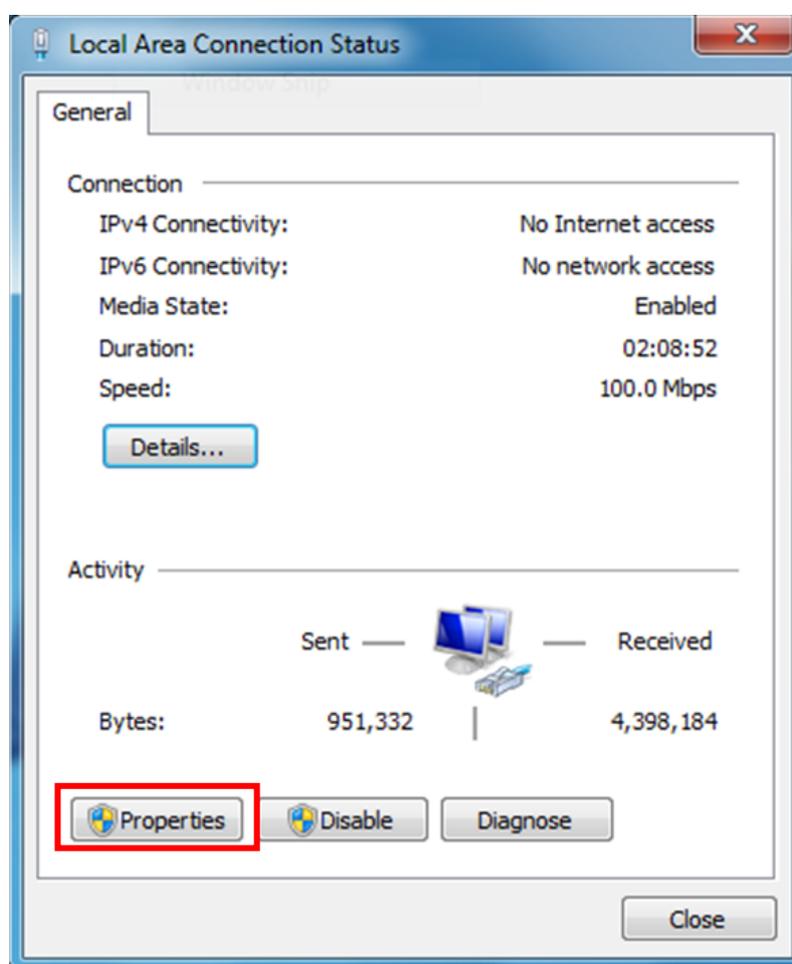
2. Under “Network and Internet” click “View network status and tasks”.



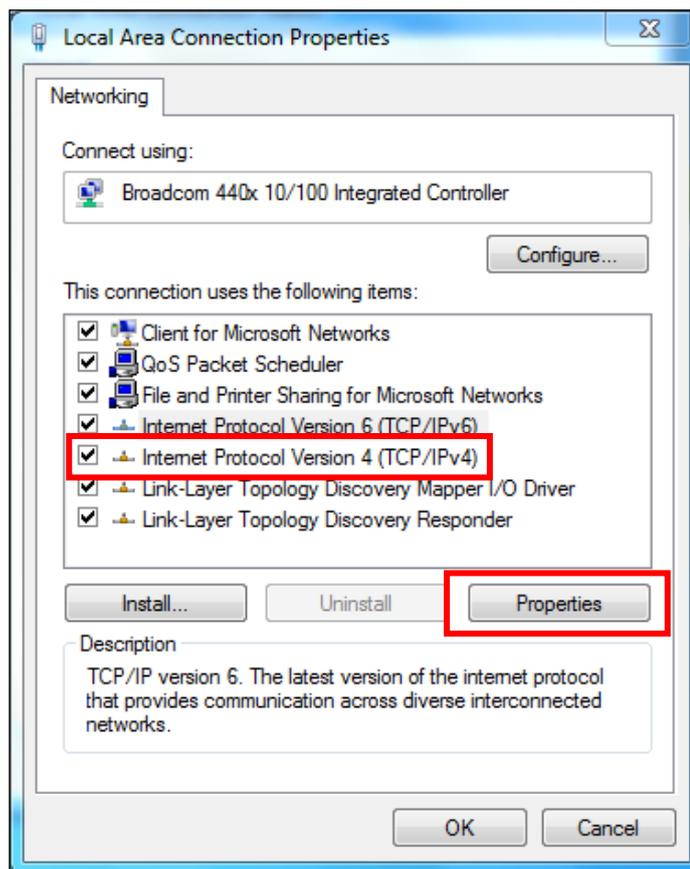
3. Click “Local Area Connection”.



4. Click “Properties”.



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

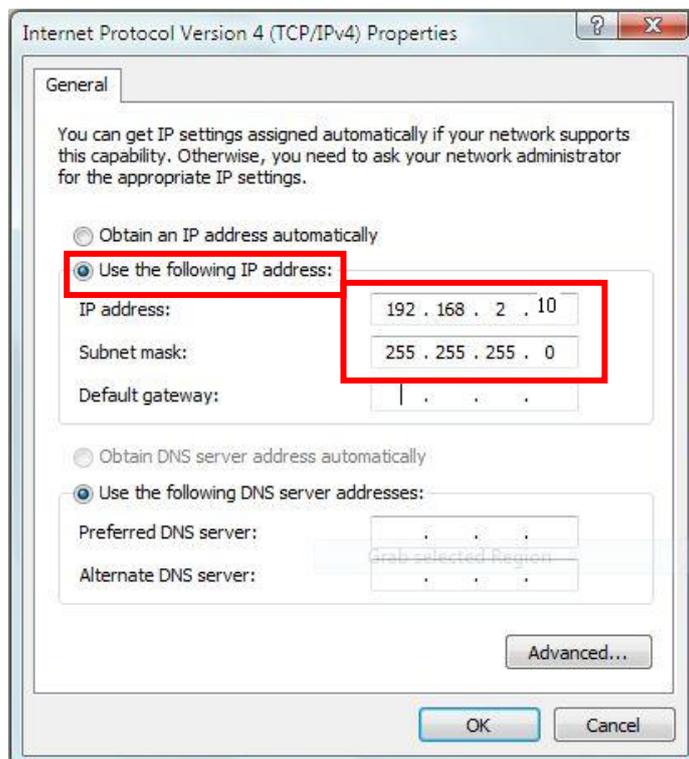


6. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

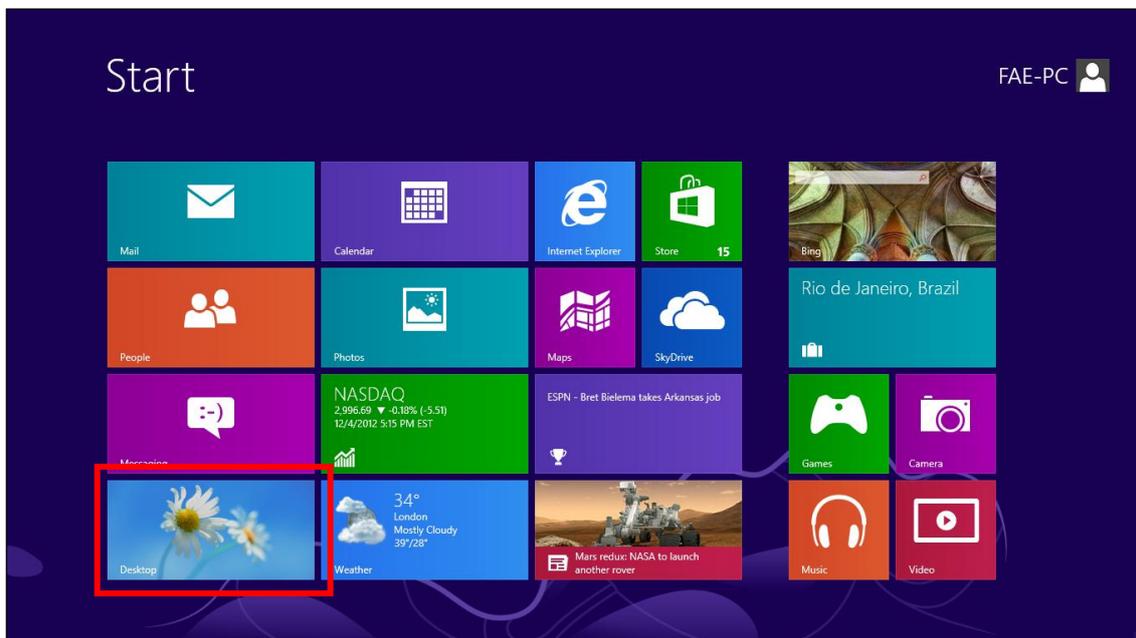
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

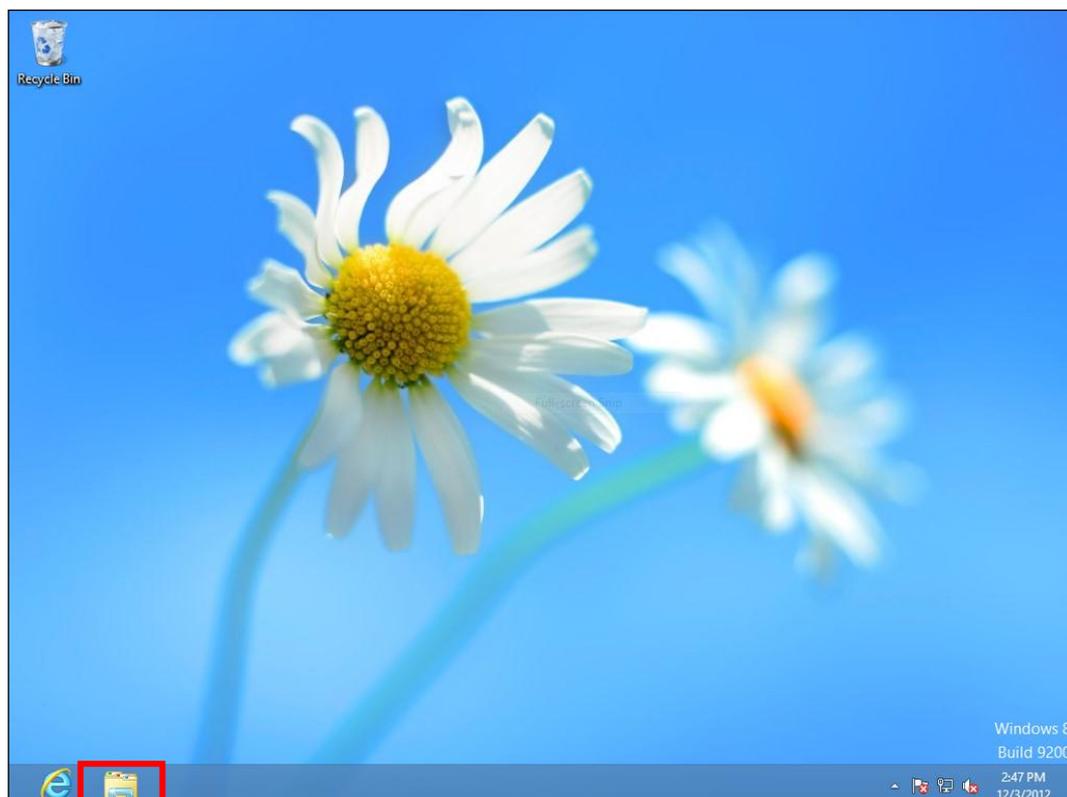


IX-1-4 Windows 8

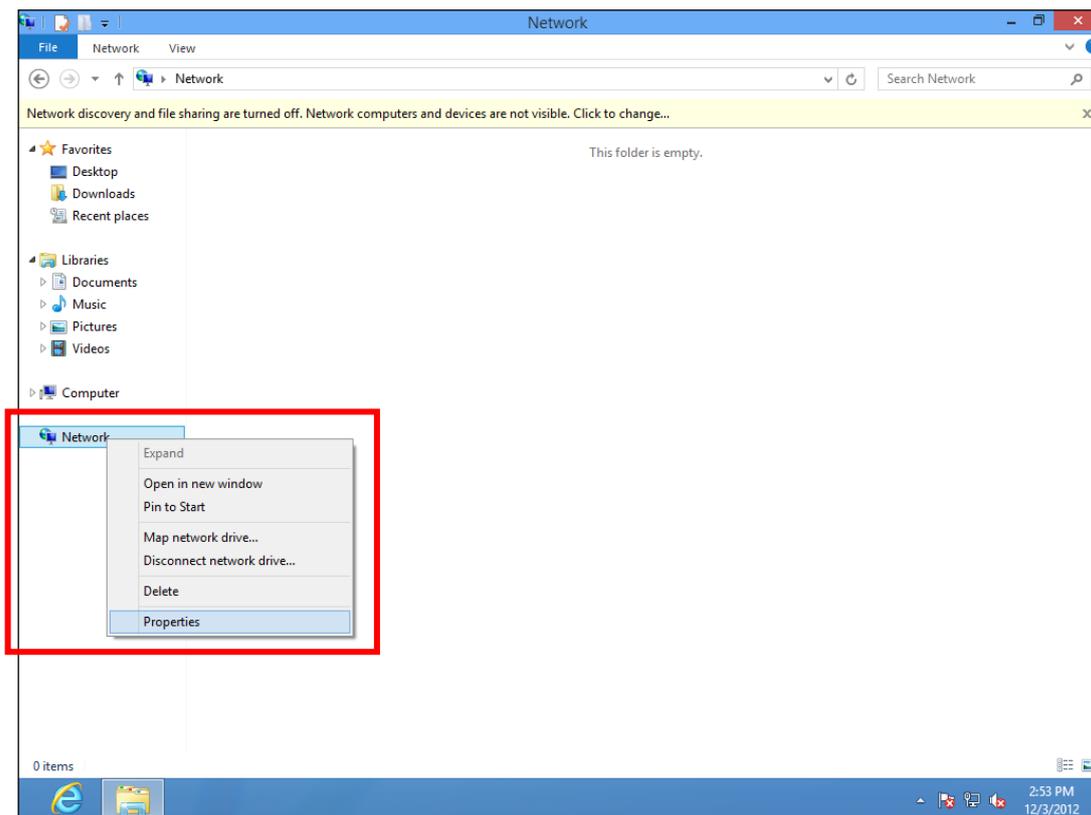
1. From the Windows 8 Start screen, switch to desktop mode by clicking the “Desktop” box.



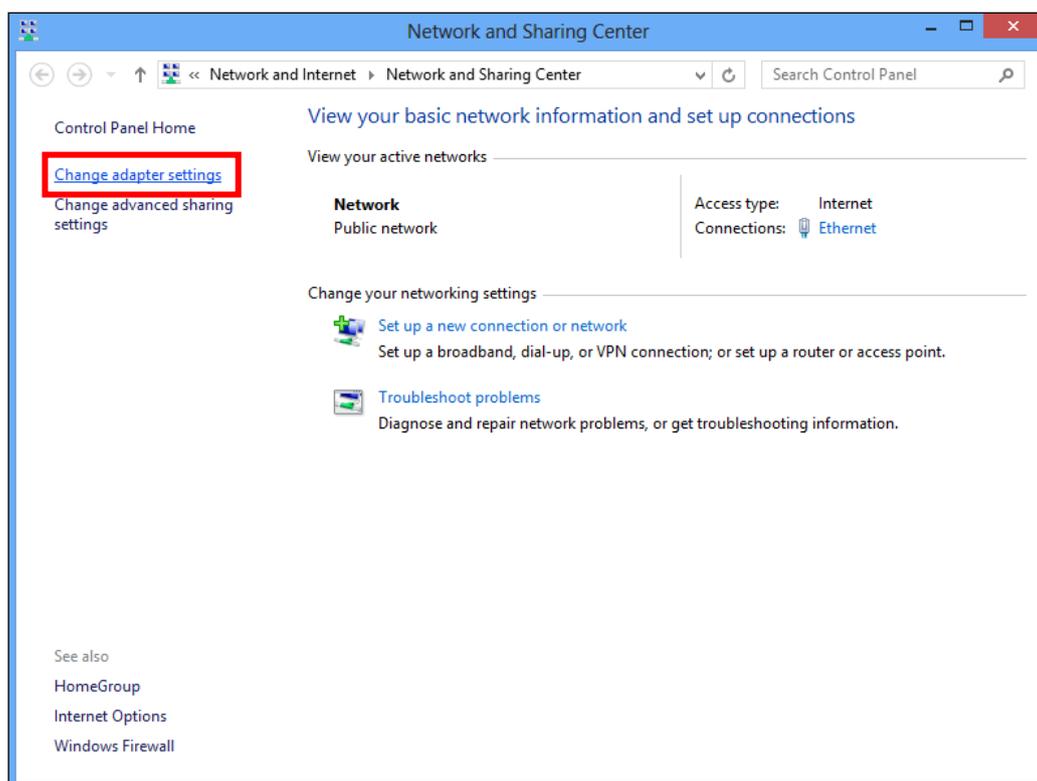
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



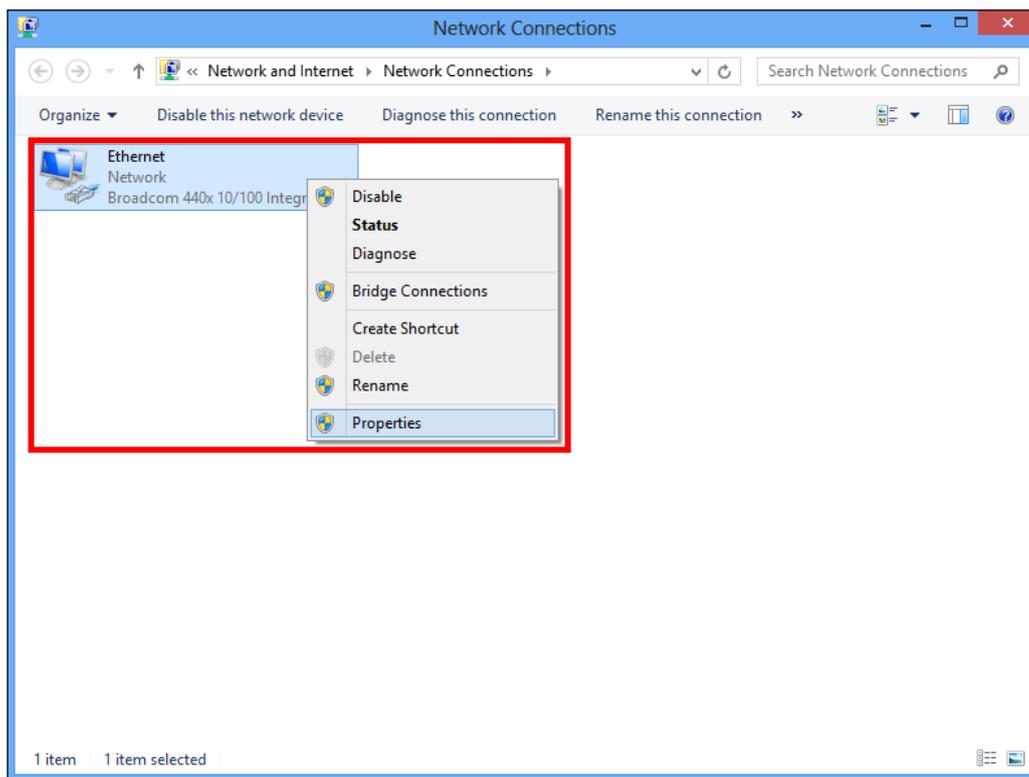
3. Right click “Network” and select “Properties”.



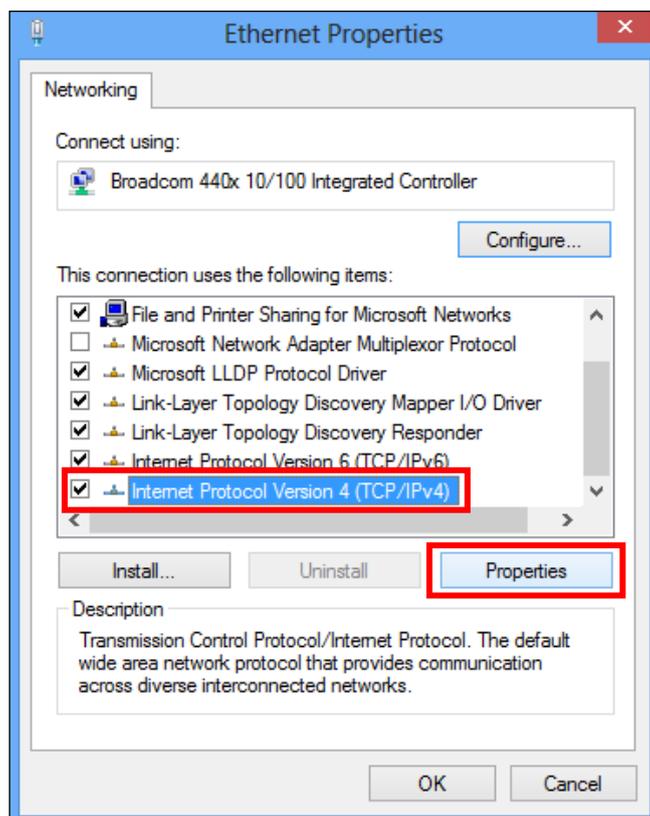
4. In the window that opens, select “Change adapter settings” from the left side.



5. Right click the connection and 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.

Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

Obtain an IP address automatically

Use the following IP address:

IP address: 192 . 168 . 128 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Validate settings upon exit

Advanced...

OK Cancel

IX-1-5 Mac

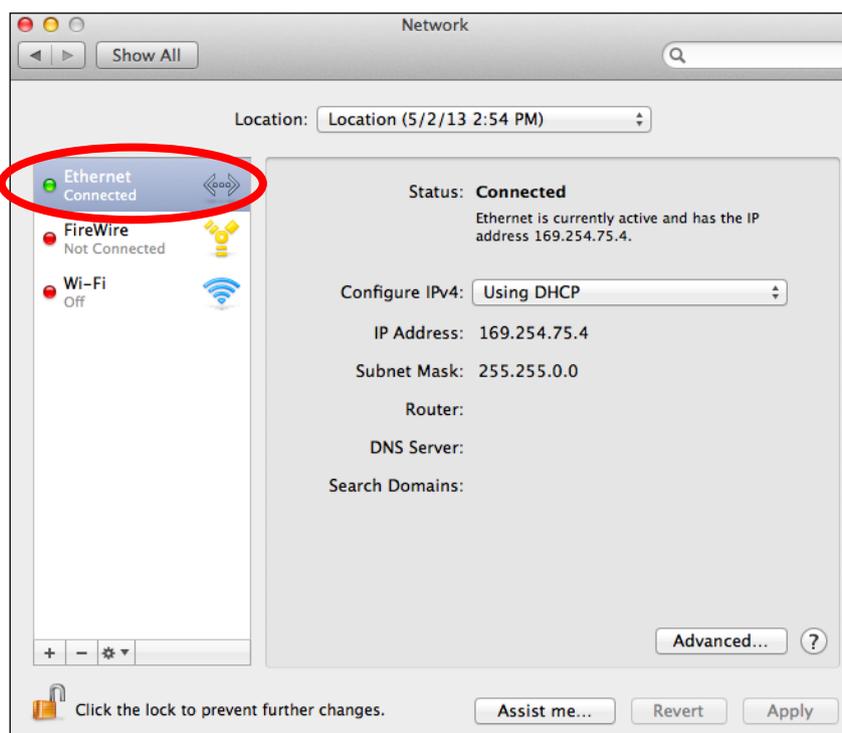
1. Have your Macintosh computer operate as usual, and click on “System Preferences”



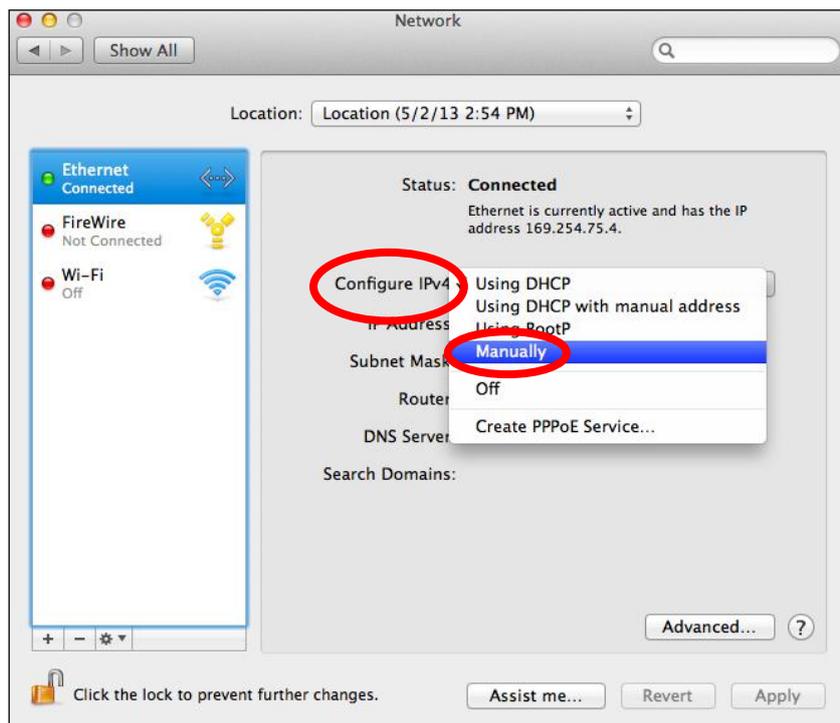
2. In System Preferences, click on “Network”.



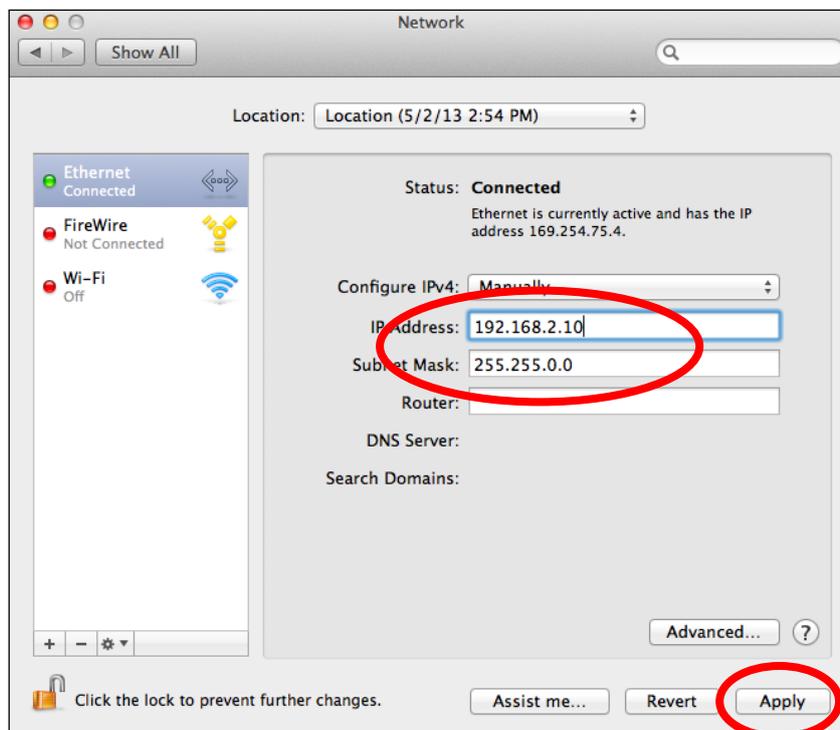
3. Click on “Ethernet” in the left panel.



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.



X FAQ

- 1.** What needs to be prepared to quickly setup the Office 1-2-3 Wi-Fi system?

A Device Network

We will be setting up MAC Address Control List for the device network. Please prepare the list.

Guest Network

We will be setting up captive portal for your guest network. Please prepare the associated guest user account list, captive portal header image (size: 800x200 pixels), logo image (size: 200x50 pixels), Title Message, background color, terms of use message and landing page.

- 2.** What format or formats are used for control / account lists?

A For all control / account lists, please follow the template of the system.

Easiest way to get the template of the system is to use the “Export” function. Go to the section where the control / account list is needed and click “Export” to download the template.

- 3.** The user interface is not very responsive after uploading a list, why?

A The operating system may be uploading the list into the Office 1-2-3 Wi-Fi system. Please wait a few seconds after using the “Upload” function before continuing with further setup.

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.

	AT	BE	BG	HR	CY	CZ	DK
	EE	FI	FR	DE	EL	HU	IE
	IT	LV	LT	LU	MT	NL	PL
	PT	RO	SK	SI	ES	SE	UK

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

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

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

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.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is restricted to indoor use.

Federal Radiation Exposure Statement

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body or nearby persons.

RED Compliance Statement

Compliance with 2014/53/EU Radio Equipment Directive (RED)

In accordance with Article 10.8(a) and 10.8(b) of the RED, the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

Frequency range (MHz)	Max. transmit power (dBm)
2400-2483.5	19.90 dBm
5150-5250	22.93 dBm
5250-5350	22.92 dBm
5470-5725	29.29 dBm

A simplified DoC shall be provided as follows: Article 10(9)

Hereby, Edimax Technology Co., Ltd. declares that the radio equipment type **AC1300 DBDC Ceiling-mount AP** is in compliance with Directive 2014/53/EU

The full text of the EU declaration of conformity is available at the following internet address: <http://www.edimax.com/edimax/global/>

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 2014/53/EU, 2014/35/EU.
- Français:** Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/53/EU, 2014/35/EU.
- Čeština:** Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/53/EU, 2014/35/EU.
- Polski:** Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/53/EU, 2014/35/EU.
- Română:** Acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 2014/53/UE, 2014/35/UE.
- Русский:** Это оборудование соответствует основным требованиям и положениям Директивы 2014/53/EU, 2014/35/EU.
- Magyar:** Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/53/EU, 2014/35/EU).
- Türkçe:** Bu cihaz 2014/53/EU, 2014/35/EU direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.
- Українська:** Обладнання відповідає вимогам і умовам директиви 2014/53/EU, 2014/35/EU.
- Slovenčina:** Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/53/EU, 2014/35/EU.
- Deutsch:** Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/53/EU, 2014/35/EU.
- Español:** El presente equipo cumple los requisitos esenciales de la Directiva 2014/53/EU, 2014/35/EU.
- Italiano:** Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/53/EU, 2014/35/UE.
- Nederlands:** Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/53/EU, 2014/35/EU.
- Português:** Este equipamento cumpre os requisitos essenciais da Directiva 2014/53/EU, 2014/35/EU.
- Norsk:** Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/53/EU, 2014/35/EU.
- Svenska:** Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/53/EU, 2014/35/EU.
- Dansk:** Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/53/EU, 2014/35/EU.
- suomen kieli:** Tämä laite täyttää direktiivien 2014/53/EU, 2014/35/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 Radio Equipment Directive.

Equipment: AC1300 DBDC Ceiling-mount AP
Model No.: Office 1-2-3

The following European standards for essential requirements have been followed:

Directives 2014/53/EU

Spectrum : EN 300 328 V2.1.1 (2016-11)
EN 301 893 V2.1.1 (2017-05)
EMC : Draft EN 301 489-1 V2.2.1 (2019-03)
Draft EN 301 489-17 V3.2.0 (2017-03)
EMF : EN 62311:2008
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', written over a horizontal line.

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