

IAP1200

User Manual

11-2016 / v1.0

Edimax Technology Co., Ltd.

No.3, Wu-Chuan 3rd Road, Wu-Gu, New Taipei City 24891, Taiwan

Email: support@edimax.com.tw

Edimax Technology Europe B.V.

Fijenhof 2, 5652 AE Eindhoven, The Netherlands

Email: support@edimax.nl

Edimax Computer Company

3350 Scott Blvd., Bldg.15 Santa Clara, CA 95054, USA

Live Tech Support: 1(800) 652-6776

Email: support@edimax.com

CONTENTS

I. Product Information.....	2
I-1. Package Contents	2
I-2. System Requirements.....	3
I-3. Hardware Overview.....	3
I-4. LED Status	4
I-5. Reset	5
I-6. Safety Information.....	6
II. Quick Setup.....	6
II-1. Initial Setup	7
II-2. Managed AP Mode: Edimax Pro NMS	12
III. Wall Installation	16
IV. Browser Based Configuration Interface.....	19
IV-1. Information	21
IV-1-1. System Information	21
IV-1-2. Wireless Clients	25
IV-1-3. Wireless Monitor	27
IV-1-4. DHCP Client Table	29
IV-1-4. DHCP Client Table	29
IV-1-5. Log	30
IV-2. Network Settings	32
IV-2-1. LAN-Side IP Address.....	32
IV-2-2. LAN Port	34
IV-2-3. IGMP Snooping.....	35
IV-2-4. VLAN	36
IV-3. Wireless Settings	37
IV-3-1. 2.4GHz 11bgn	37
IV-3-1-1. Basic	37
IV-3-1-2. Advanced.....	41
IV-3-1-3. Security.....	43
IV-3-1-3-1. No Authentication.....	45
IV-3-1-3-2. WEP	45
IV-3-1-3-3. IEEE802.1x/EAP.....	45
IV-3-1-3-4. WPA-PSK.....	45
IV-3-1-3-5. WPA-EAP	46
IV-3-1-3-6. Additional Authentication	46

IV-3-1-4.	WDS.....	48
IV-3-1-5.	Guest Network.....	50
IV-3-2.	5GHz 11ac 11an.....	52
IV-3-2-1.	Basic	52
IV-3-2-2.	Advanced.....	54
IV-3-2-3.	Security.....	56
IV-3-2-4.	WDS.....	58
IV-3-2-5.	Guest Network.....	60
IV-3-3.	WPS.....	62
IV-3-4.	RADIUS.....	64
IV-3-4-1.	RADIUS Settings.....	65
IV-3-4-2.	Internal Server	67
IV-3-4-3.	RADIUS Accounts	69
IV-3-5.	MAC Filter	71
IV-3-6.	WMM.....	73
IV-3-7.	Schedule.....	75
IV-3-8.	Traffic Shaping.....	77
IV-4.	Management.....	78
IV-4-1.	Admin.....	78
IV-4-2.	Date and Time	80
IV-4-3.	Syslog Server	82
IV-4-4.	Ping Test.....	83
IV-5.	Advanced.....	84
IV-5-1.	LED Settings.....	84
IV-5-2.	Update Firmware.....	85
IV-5-3.	Save/Restore Settings.....	86
IV-5-4.	Factory Default	88
IV-5-5.	Reboot.....	89
IV-6.	Operation Mode	90

V. Appendix91

V-1.	Configuring your IP address	91
V-1-1.	Windows XP	92
V-1-2.	Windows Vista.....	94
V-1-3.	Windows 7	96
V-1-4.	Windows 8	100
V-1-5.	Mac	104

Federal Communication Commission Interference Statement107

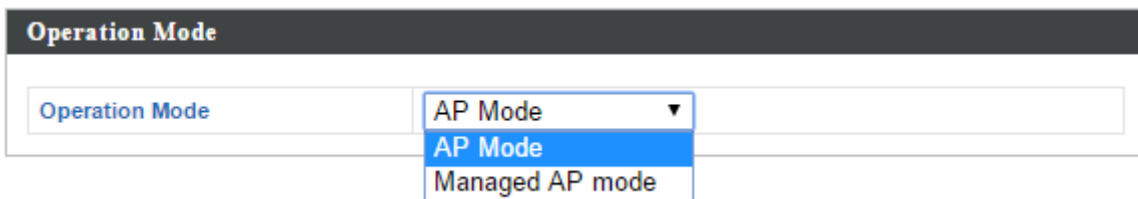
OVERVIEW

Your access point can function in two different modes.

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

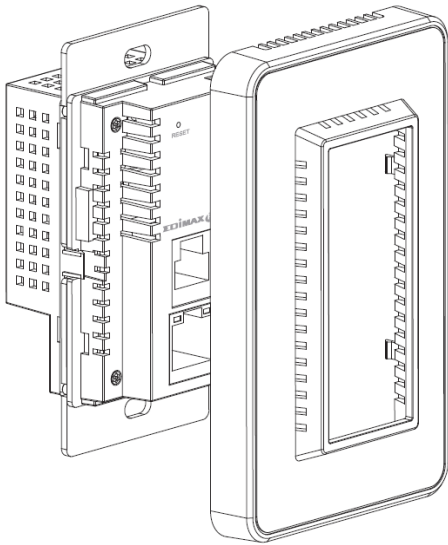
AP mode is a regular access point for use in your wireless network.

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



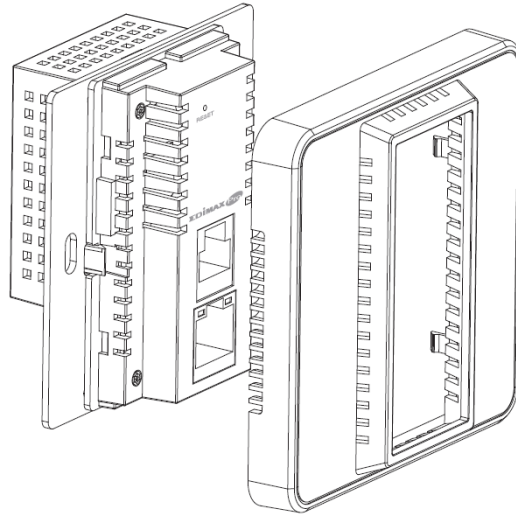
I. Product Information

I-1. Package Contents



IAP1200 (US)

or



IAP1200 (EU)



Quick Installation Guide

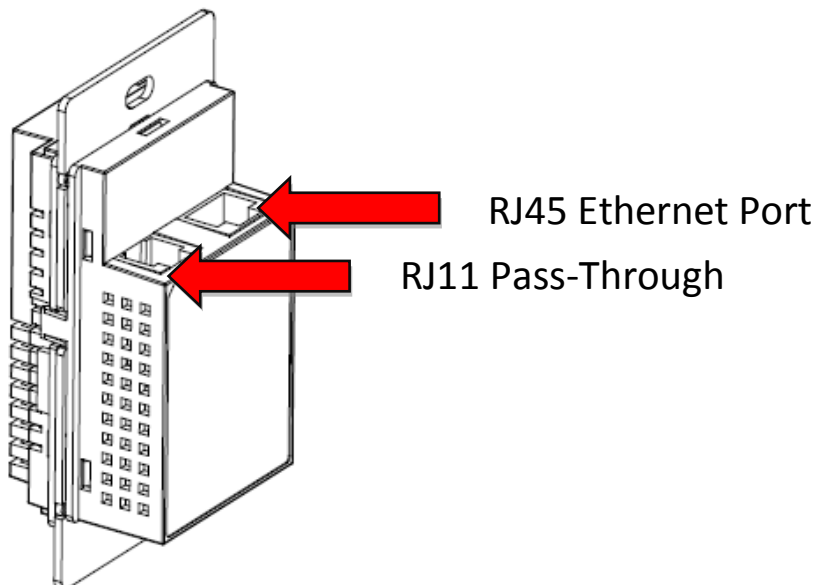
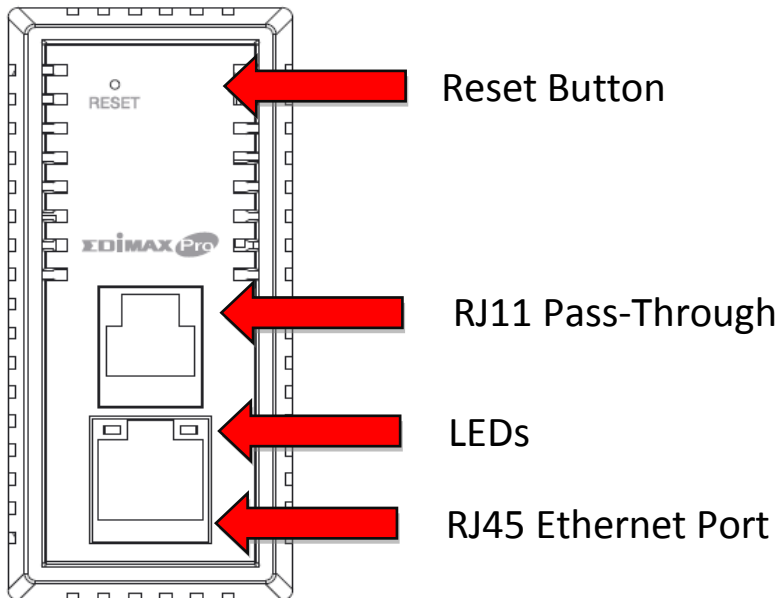


Screws x 2

I-2. System Requirements

- Ethernet cable
- PoE Switch
- Computer with web browser for access point configuration

I-3. Hardware Overview



I-4. LED Status

LED	LED Color	Status	Description
Power (Right)	Green	On	The access point is on.
		Flashing	The access point is starting up.
LAN (Left)	Green	On	LAN port is connected.
	Green	Flashing	LAN activity
	Orange	Flashing	Locating access point.
	Green & Orange	Flashing/ Alternating	Upgrading firmware. Do not switch off.

I-5. Reset

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

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



You may need to use a pencil 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 **green** power LED is **on**.

I-6. Safety Information

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

1. The access point is designed for indoor use only; do not place the access point outdoors.
 2. Do not place the access point in or near hot/humid places, such as a kitchen or bathroom.
 3. Do not pull any connected cable with force; carefully disconnect it from the access point.
 4. Handle the access point with care. Accidental damage will void the warranty of the access point.
 5. The device contains small parts which are a danger to small children under 3 years old. Please keep the access point out of reach of children.
 6. Do not place the access point on paper, cloth, or other flammable materials. The access point may become hot during use.
 7. There are no user-serviceable parts inside the access point. If you experience problems with the access point, please contact your dealer of purchase and ask for help.
 8. The access point is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.
1. If you smell burning or see smoke coming from the access point or power adapter, then disconnect the access point and power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

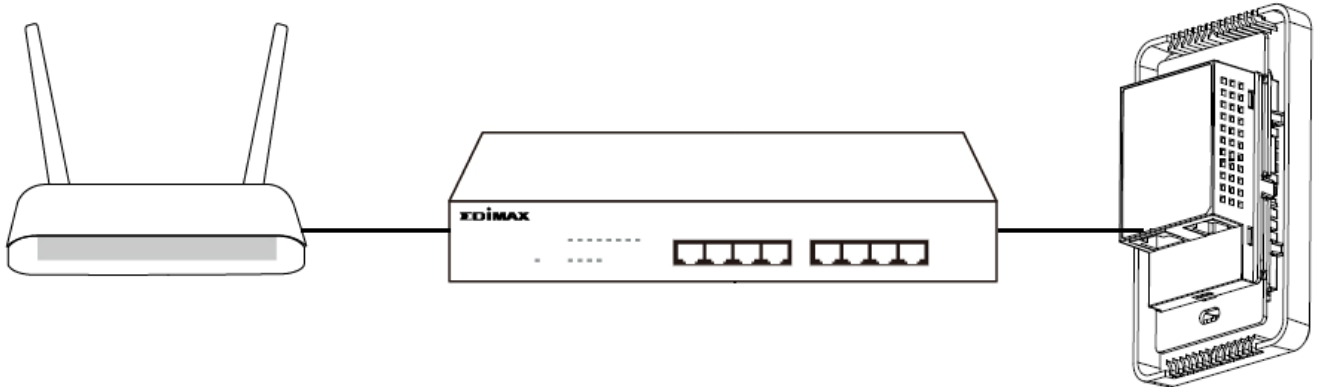
II. Quick Setup

Your access point can be up and running in just a few minutes. It can function as a standalone access point (AP mode) or as part of an AP array (Managed AP mode).

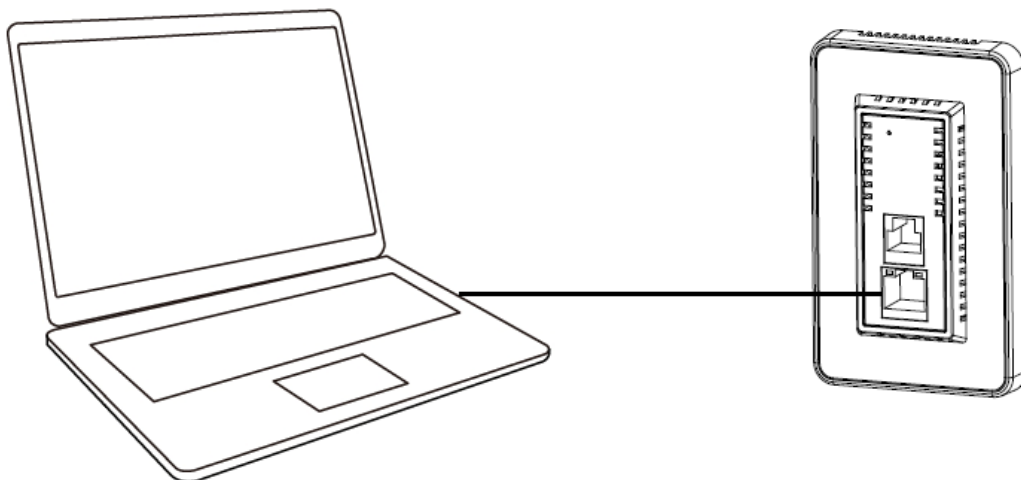
For use a Managed AP in an AP array, the access point will automatically switch mode when an AP Controller is configured as described in **Edimax Pro NMS**.

II-1. Initial Setup

1. Connect the IAP1200's **rear** Ethernet port to a PoE switch (LAN port) using an Ethernet cable.



2. Use a computer that's connected to the LAN or connect to the IAP1200's **front** Ethernet port using an Ethernet cable.



3. Open a web browser and enter the access point's IP address in the address field. The default IP address is **192.168.2.2**



Your computer's IP address must be in the same subnet as the AP access point.



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

4. Login with the default username & password: **admin** & **1234**

Connect to 192.168.2.2

The server 192.168.2.2 at localhost requires a username and password.

User name: admin

Password: ••••••

Remember my password

OK Cancel

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

EDIMAX Pro Home | Logout | Global (English)

IAP1200 Information Network Settings Wireless Settings Management Advanced Operation Mode

System Information

System	
Model	IAP1200
Product Name	AP801F02000004
Uptime	0 day 02:13:46
System Time	2012/01/01 02:13:33
Boot from	Internal memory
Firmware Version	1.6.0
MAC Address	80:1F:02:00:00:04
Management VLAN ID	1
IP Address	192.168.2.106 Refresh
Default Gateway	192.168.2.1
DNS	185.37.37.37 185.37.39.39
DHCP Server	192.168.2.1

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

The next steps will help you to configure the following basic settings of the access point:

- **LAN IP Address**
- **2.4GHz & 5GHz SSID & Security**
- **Administrator Name & Password**
- **Time & Date**



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

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

LAN-side IP Address	
IP Address Assignment	DHCP Client ▼
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	From DHCP ▼
Primary DNS Address	From DHCP ▼ 0.0.0.0
Secondary DNS Address	From DHCP ▼ 0.0.0.0

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



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

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



To utilize multiple 2.4GHz SSIDs, open the drop down menu labelled "Enable SSID number" and select how many SSIDs you

require. Then enter a new SSID in the corresponding numbered fields below, before clicking “Apply”.

2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n ▼
Enable SSID number	1 ▼
SSID1	IAP1200-000004_G VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11 ▼
Auto Channel Interval	One day ▼ <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	40 MHz ▼
BSS BasicRateSet	1,2,5,5,11 Mbps ▼

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



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

2.4GHz Wireless Security Settings	
SSID	IAP1200-000004_G ▼
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
Load Balancing	50 /50
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

5. Go to **“Wireless Settings” > “5GHz 11ac 11an”** and repeat steps 3 & 4 for the access point’s 5GHz wireless network.
6. To change the administrator name and password for the browser based configuration interface, go to **“Management” > “Admin”**.

Account to Manage This Device	
Administrator Name	<input type="text" value="admin"/>
Administrator Password	<input type="password" value="•••••"/> (4-32 Characters)
	<input type="password" value="•••••"/> (Confirm)
<input type="button" value="Apply"/>	

- Complete the “Administrator Name” and “Administrator Password” fields and click “Apply”.
- To set the correct time for your access point, go to “Management” > “Date and Time Settings”.

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
Server Name	<input type="text"/>
Update Interval	24 hours
Time Zone	
Time Zone	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

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



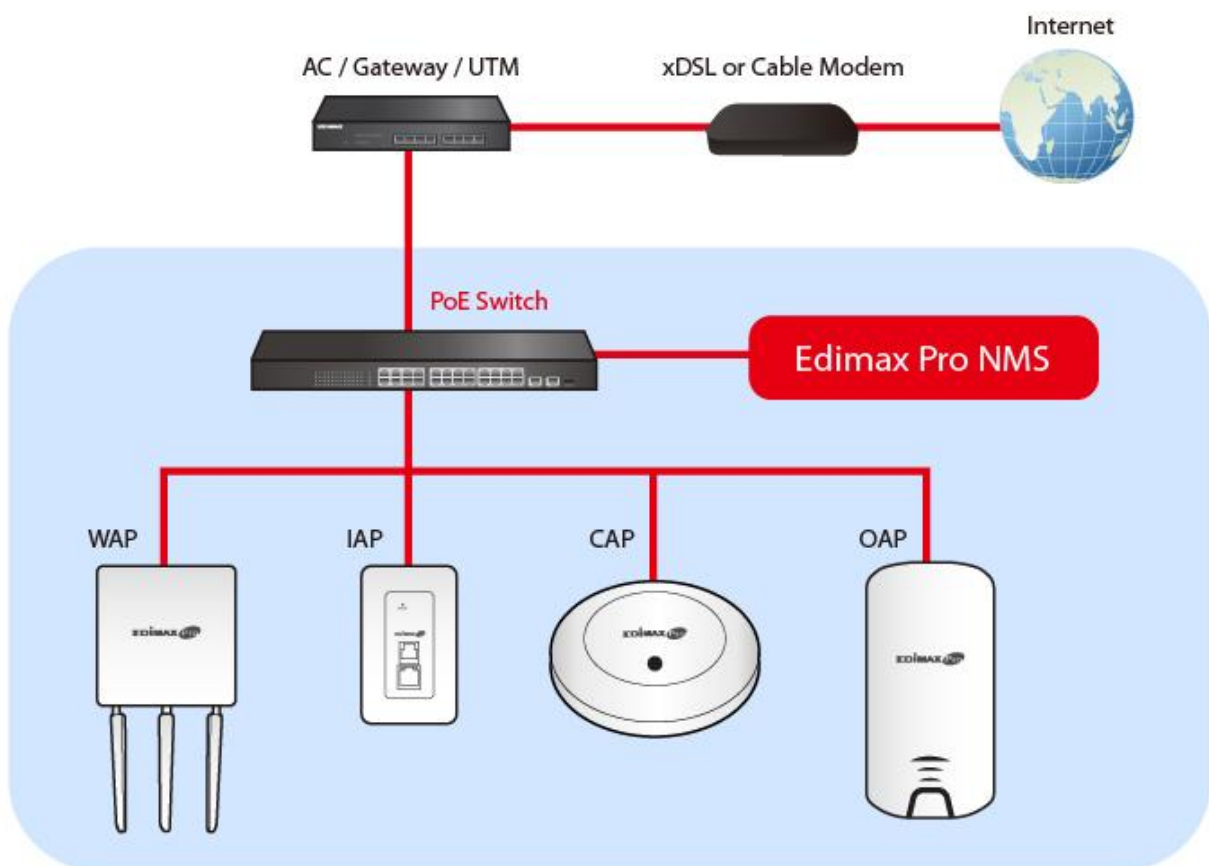
You can use the “Acquire Current Time from your PC” button if you wish to set the access point to the same time as your PC.

- The basic settings of your access point are now configured.

II-2. Managed AP Mode: Edimax Pro NMS

Edimax Pro Network Management Suite (NMS) supports the central management of a group of access points, otherwise known as an AP Array. NMS supports up to 16 Edimax Pro access points with no additional wireless controller required or 128 access points with the APC 500 AP controller - reducing costs and facilitating efficient remote AP management.

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




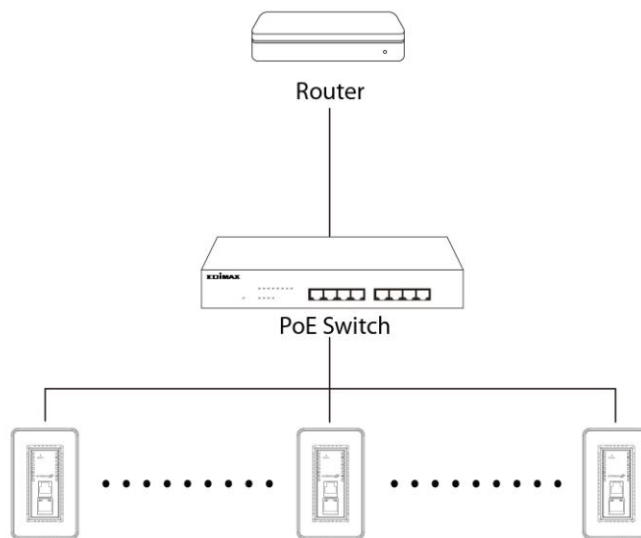
One AP (access point) is designated as the AP Controller (master) and other connected Edimax Pro APs are automatically designated as Managed APs (slaves). Using Edimax Pro NMS you can monitor, configure and manage all Managed APs (up to 128) from the single AP Controller.

The IAP1200 functions as a Managed AP and cannot act as an AP Controller.

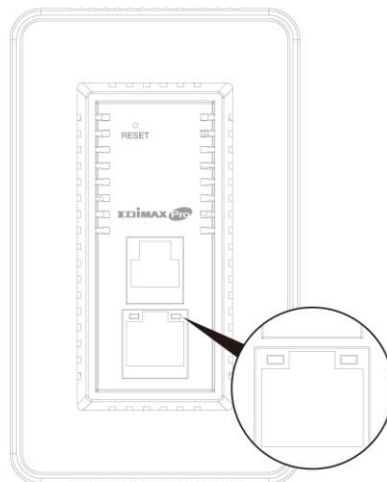
When using an Edimax NMS AP controller, other connected APs are automatically set to Managed APs. In the case that the AP Controller cannot find your IAP1200 as a Managed AP, you can configure the setting manually as below:

1. Ensure all APs including your IAP1200 are connected to an Ethernet or PoE switch which is connected to a gateway/router.

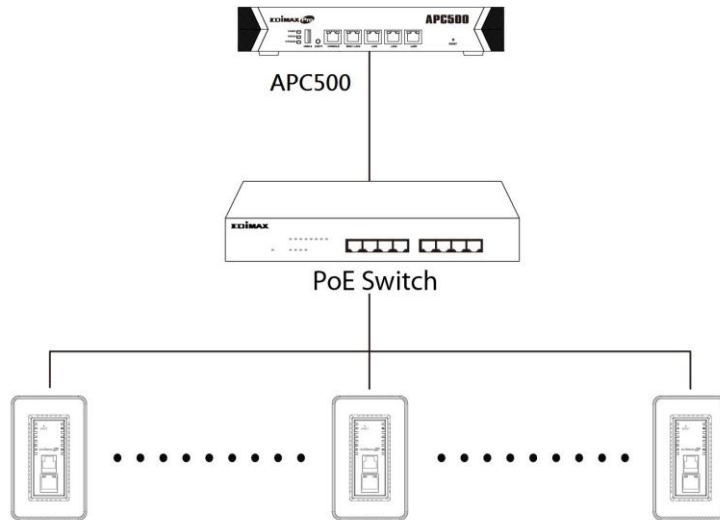
 **You can use your router as a DHCP server or you can later configure your AP Controller as a DHCP server.**



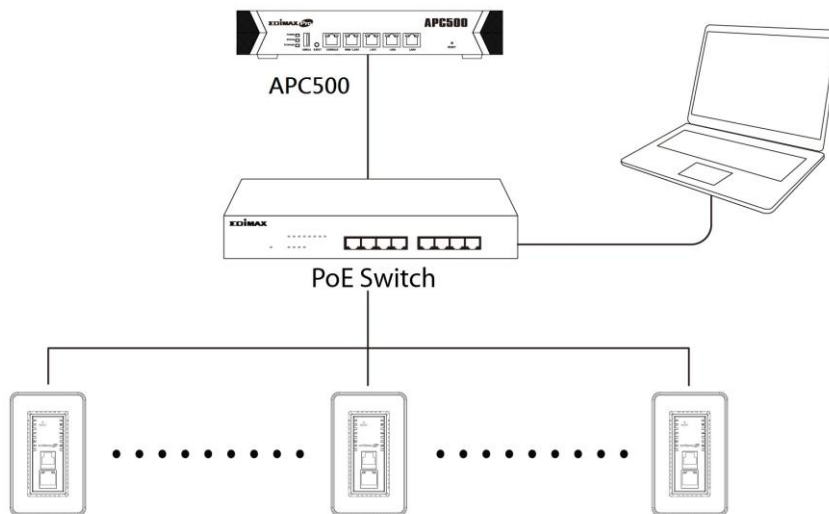
2. Ensure all APs are powered on and check LEDs.



3. Connect the APC500 as the AP Controller which will manage all other connected APs (up to 128 depending on model).



4. Connect a computer to the IAP1200 via PoE switch using an Ethernet cable.



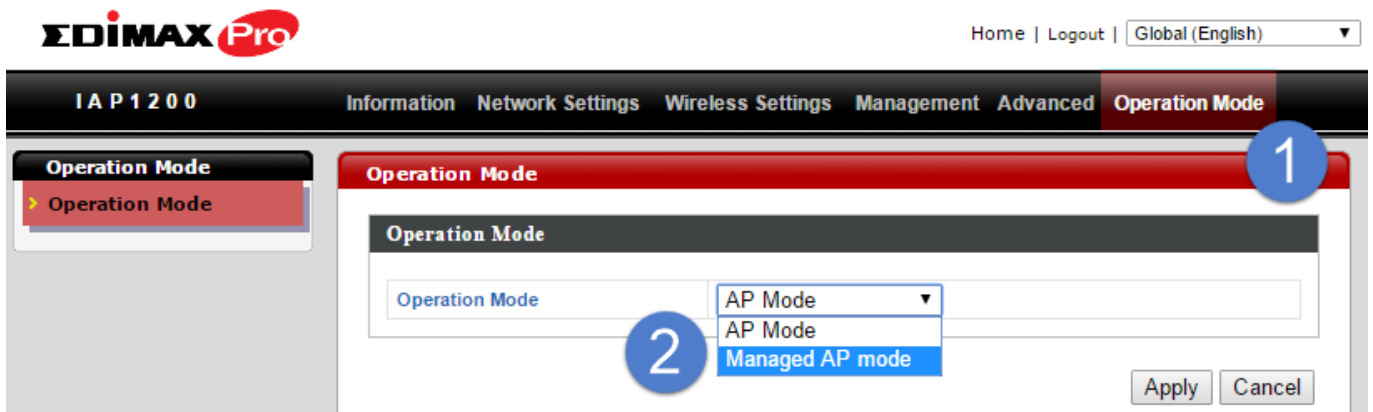
5. Open a web browser and enter the IAP1200's IP address in the address field. The default IP address is **192.168.2.2**



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

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

7. You will arrive at the Edimax Pro NMS Dashboard. Go to “**Operation Mode**” and select “**Managed AP Mode**” from the drop down menu.



8. Click “Apply” to save the settings and your AP Controller & Managed APs should be fully functional. Use Edimax NMS on your AP controller to manage & monitor your Managed APs.

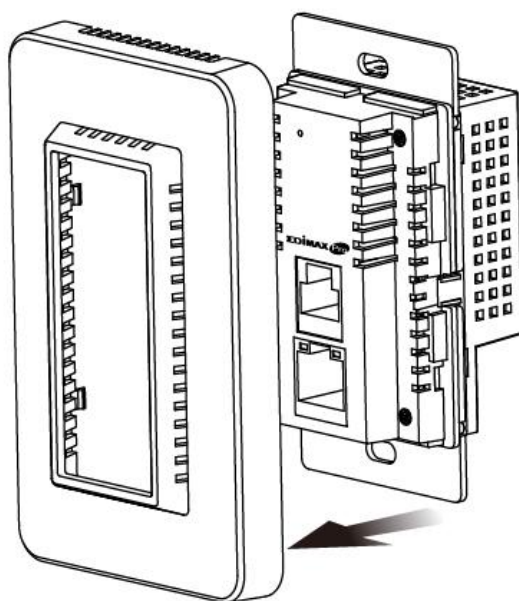


Refer to your AP controller's user manual for help with Edimax NMS.

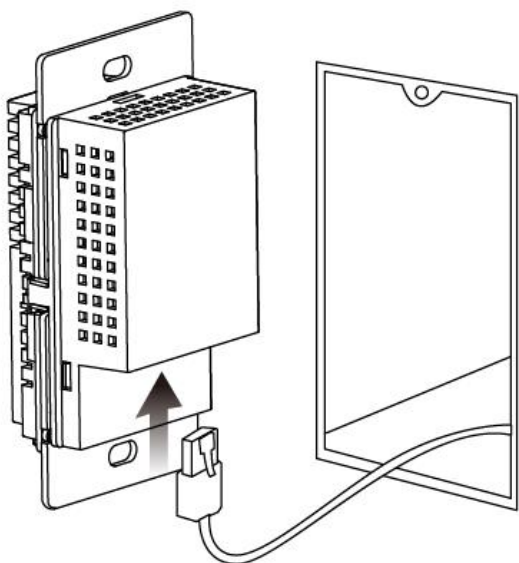
III. Wall Installation

The IAP1200 In-Wall access point comes with EU or US wall plates per your region and fits standard sized wall boxes. The Ethernet cable in your wall box must be connected to a PoE switch.

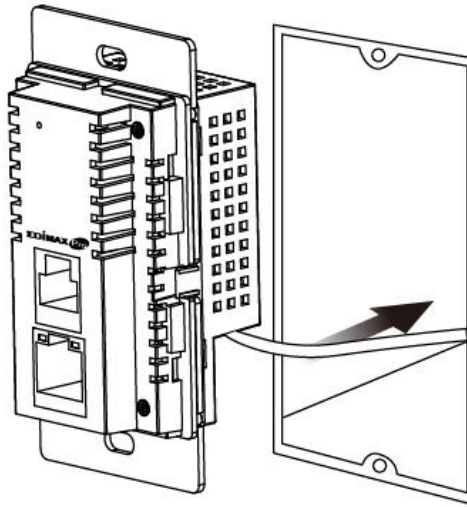
- 1.** Carefully remove the wall plate from the IAP1200 by pulling the plate with a light force to unclip it.



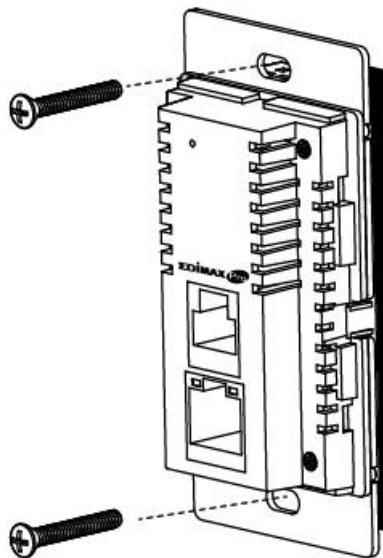
- 2.** Connect the PoE cable from your wall box the rear of the IAP1200.



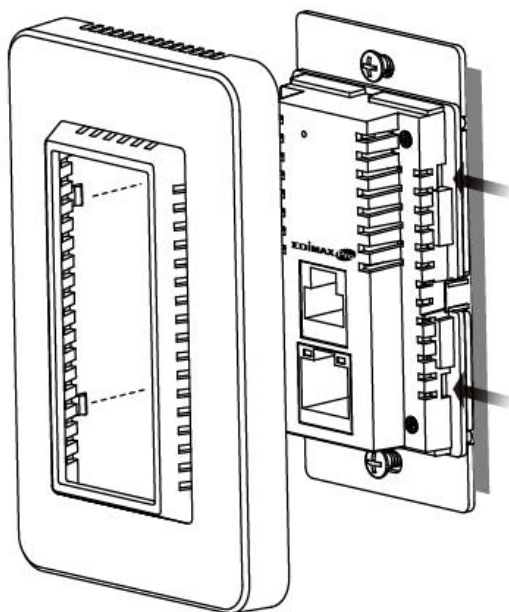
- 3.** Insert the IAP1200 into the wall box, taking care to position the cable properly so it's not strained.




- 4.** Use the included screws to screw the IAP1200 securely into place and ensure a flush fit with the wall.



5. Re-attach the wall plate to the IAP1200 by snapping it back into place.



IV. Browser Based Configuration Interface

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

The multi-language browser-based configuration interface enables you to configure the access point's advanced features. The IAP1200 features a range of advanced functions such as MAC filtering, MAC RADIUS authentication, VLAN configurations, 802.11ac Wi-Fi, up to 32 SSIDs and many more. To access the browser based configuration interface:

- 1.** Connect a computer to your access point using an Ethernet cable.
- 2.** Enter the access point's IP address into the URL bar of a web browser. The default IP is **192.168.2.2**. If the AP is connected to a DHCP server, ensure you use the correct address.



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

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

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

I A P 1 2 0 0

Information Network Settings Wireless Settings Management Advanced Operation Mode

Information

- > System Information
- > Wireless Clients
- > Wireless Monitor
- > DHCP Clients
- > Log

System Information

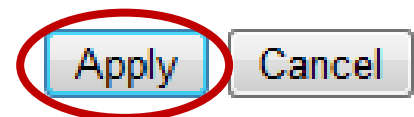
System


Model	IAP1200
Product Name	AP801F02000004
Uptime	0 day 02:13:46
System Time	2012/01/01 02:13:33
Boot from	Internal memory
Firmware Version	1.6.0
MAC Address	80:1F:02:00:00:04
Management VLAN ID	1
IP Address	192.168.2.106 <input type="button" value="Refresh"/>
Default Gateway	192.168.2.1
DNS	185.37.37.37 185.37.39.39
DHCP Server	192.168.2.1

Wired LAN Port Settings

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

4. Use the menu across the top and down the left side to navigate, and select language with the drop-down menu in the top right corner. Click “Apply” to save changes and reload the access point, or “Cancel” to cancel changes.



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

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

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

IV-1. Information

Information Network Settings Wireless Settings Management Advanced Operation Mode



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

IV-1-1. System Information

> System Information

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

System	
Model	
Product Name	AP801F0275EFA8
Uptime	0 day 00:38:18
System Time	2012/01/01 00:55:18
Boot from	Internal memory
Firmware Version	1.3.0
MAC Address	80:1F:02:75:EF:A8
Management VLAN ID	1
IP Address	192.168.0.107 <input type="button" value="Refresh"/>
Default Gateway	192.168.0.1
DNS	192.168.0.1
DHCP Server	192.168.0.1

Wired LAN Port Settings

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

Wireless 2.4GHz

Status	Enabled
MAC Address	80:1F:02:00:00:04
Channel	Ch 3 + 7 (Auto)
Transmit Power	100%
RSSI	-60/-66

Wireless 2.4GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
IAP1200-000004_G	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 2.4GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
80:1F:02:00:00:00	AES	Untagged Port / 1

Wireless 5GHz

Status	Enabled
MAC Address	80:1F:02:75:EF:A9
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Transmit Power	100%
RSSI	0/0

Wireless 5GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
EDIMAX-75EFA8_A	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.
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.
Status	Displays the status of the specified LAN port (connected or disconnected).
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port. See IV-2-3. VLAN

Wireless 2.4GHz (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	Displays Received Signal Strength Indicator.

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

Wireless 2.4GHZ (5GHz) / WDS Status	
MAC Address	Displays the peer access point's MAC address.
Encryption Type	Displays the encryption type for the specified WDS. See IV-3-1-4. WDS
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See IV-3-1-4. WDS

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

IV-1-2. Wireless Clients

> Wireless Clients

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

Refresh Time	
Auto Refresh Time	<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	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time	Vendor
1	EDIMAX-75EFA 8_G	A4:77:33:1E:0C:47	1.5 MBytes	123.7 KBytes	100	6 min 5 secs	0	Google
2	EDIMAX-75EFA 8_G	F8:A9:D0:0B:7D:A8	31.8 KBytes	39.2 KBytes	100	1 min 54 secs	0	LG Electronics

5GHz WLAN Client Table								
#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time	Vendor
1	EDIMAX-75EFA 8_A	BC:EE:7B:4B:FA:3A	24.8 KBytes	164.7 KBytes	100	1 min 46 secs	0	ASUSTek COMPUTER INC.

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

2.4GHz (5GHz) WLAN Client Table	
SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.

Signal (%)	Displays the wireless signal strength for the specified client.
Connected Time	Displays the total time the wireless client has been connected to the access point.
Idle Time	Client idle time is the time for which the client has not transmitted any data packets i.e. is idle.
Vendor	The vendor of the client's wireless adapter is displayed here.

IV-1-3. Wireless Monitor

➤ 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 2.4GHz						
Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
1	Matt	00:E0:4C:81:96:C1	WPA2PSK/AES	100	11b/g/n	REALTEK SEMICONDUCTOR CORP.

Wireless 5GHz						
Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

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

Site Survey Results	
Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/access point for the specified SSID.
Security	Displays the authentication/encryption type of the specified SSID.

Signal (%)	Displays the current signal strength of the SSID.
Type	Displays the 802.11 wireless networking standard(s) of the specified SSID.
Vendor	Displays the vendor of the wireless router/access point for the specified SSID.

IV-1-4. DHCP Client Table

> DHCP Clients

The DHCP client table displays information about DHCP clients when DHCP server is enabled.

DHCP Client Table		
IP Address	MAC Address	Expiration Time
192.168.2.120	A4:77:33:1E:0C:47	Expired

DHCP Client Table	
IP Address	Displays the IP address of listed DHCP client.
MAC Address	Displays the MAC address of listed DHCP client.
Expiration Time	Displays the expiration time for listed DHCP client.

IV-1-5. Log

> Log

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



When the log is full, old entries are overwritten. Use the Search function to quickly locate log entries.

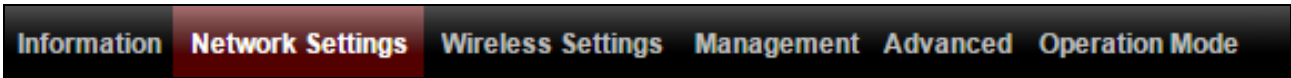
All Events/Activities					
Search	<input type="text"/>	<input type="checkbox"/> Match whole words			
ID ▼	Date and Time	Category ▲	Severity ▲	Users ▲	Events/Activities
72	2012/01/01 00:04:45	SYSTEM	Low	admin	WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
71	2012/01/01 00:04:41	SYSTEM	Low	admin	WLAN[2.4G], Best channel selection start, switch to channel 2


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:

- ◆ **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

IV-2. Network Settings



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

IV-2-1. LAN-Side IP Address

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

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

LAN-side IP Address	
IP Address Assignment	DHCP Client ▼
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	From DHCP ▼
Primary DNS Address	From DHCP ▼ 0.0.0.0
Secondary DNS Address	From DHCP ▼ 0.0.0.0

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

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

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

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

IV-2-2. LAN Port

> LAN Port

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

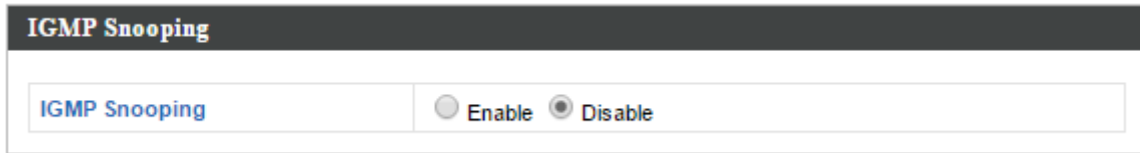
Wired LAN Port Settings			
Wired LAN Port	Speed & Duplex	Flow Control	802.3az
LAN1	Auto ▼	Enabled ▼	Enabled ▼
USB net	Auto ▼	Enabled ▼	Enabled ▼

Wired LAN Port	Identifies LAN port.
Enable	Enable/disable specified LAN port.
Speed & Duplex	Select a speed & duplex type for specified LAN port, or use the “Auto” value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packets transfer/receive.
Flow Control	Enable/disable flow control. Flow control can pause new session request until current data processing is complete, in order to avoid device overloads under heavy traffic.
802.3az	Enable/disable 802.3az. 802.3az is an Energy Efficient Ethernet feature which disables unused interfaces to reduce power usage.

IV-2-3. IGMP Snooping

> IGMP Snooping

IGMP snooping monitors Internet Group Management Protocol (IGMP) network traffic in order to optimize wireless multicast traffic performance.



IGMP Snooping	
IGMP Snooping	Enable or disable IGMP snooping.

IV-2-4. VLAN

> VLAN

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



VLAN IDs in the range 1 – 4095 are supported.

VLAN Interface		
Wired LAN Port	VLAN Mode	VLAN ID
LAN1	Untagged Port ▾	1
USB net	Untagged Port ▾	1

Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [EDIMAX-75EFA8_G]	Untagged Port	1

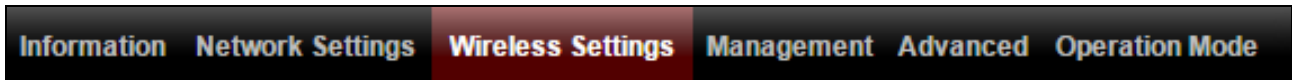
Wireless 5GHz	VLAN Mode	VLAN ID
SSID [EDIMAX-75EFA8_A]	Untagged Port	1


Management VLAN	
VLAN ID	1

VLAN Interface	
Wired LAN Port/Wireless	Identifies LAN port number and wireless SSIDs.
VLAN Mode	Select “Tagged Port” or “Untagged Port” for specified LAN interface.
VLAN ID	Set a VLAN ID for specified interface, if “Untagged Port” is selected.

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

IV-3. Wireless Settings



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

IV-3-1. 2.4GHz 11bgn

 **2.4GHz 11bgn**

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

IV-3-1-1. Basic

 **Basic**

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

2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n ▼
Enable SSID number	1 ▼
SSID1	EDIMAX-75EFA8_G VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11 ▼
Auto Channel Interval	One day ▼ <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto ▼
BSS BasicRateSet	1,2,5.5,11 Mbps ▼



Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Ch 11, 2462MHz ▼
Channel Bandwidth	Auto, +Ch 7 ▼
BSS BasicRate Set	1,2,5,5,11 Mbps ▼

Wireless	Enable or disable the access point's 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g & 802.11n can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of 16 can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (higher performance but potentially higher interference) or Auto (automatically select based on interference level).
BSS BasicRateSet	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

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

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

IV-3-1-2. Advanced

> Advanced

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



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

2.4GHz Advanced Settings	
Contention Slot	Short ▼
Preamble Type	Short ▼
Guard Interval	Short GI ▼
802.11g Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
802.11n Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256-2346)
Multicast Rate	Auto ▼
Tx Power	100% ▼
Beacon Interval	100 (40-1000 ms)
Station idle timeout	60 (30-65535 seconds)

Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM (see IV-3-6. WMM).
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is “Short Preamble”.
Guard Interval	Set the guard interval. A shorter interval can improve performance.

802.11g Protection	Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the "Auto" setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keepalive messages from the access point to a wireless client to verify if the station is still alive/active.

IV-3-1-3. Security

> Security

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



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



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

2.4GHz Wireless Security Settings	
SSID	EDIMAX-75EFA8_G ▼
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
Load Balancing	50 /50
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

2.4GHz Wireless Advanced Settings	
Smart Handover Settings	
Smart Handover	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
RSSI Threshold	-80 ▼ dB

2.4GHz Wireless Security Settings	
SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu and refer to the information below (IV-3-1-3-6.) appropriate for your method.

2.4GHz Wireless Advanced Settings	
Smart Handover	Enable or disable smart handover.
RSSI Threshold	Set the Received Signal Strength Indicator (RSSI) threshold to maintain quality connection speeds (minimum receiver sensitivity required for a connection).

IV-3-1-3-1. No Authentication

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



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

IV-3-1-3-2. WEP

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

Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.
Key Type	Choose from "ASCII" (any alphanumerical character 0-9, a-z and A-Z) or "Hex" (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key (1 – 4 below) is the default key. For security purposes, you can set up to four keys (below) and change which is the default key.
Encryption Key 1 – 4	Enter your encryption key/password according to the format you selected above.

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

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

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

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

WPA Type	Select from WPA/WPA2 Mixed Mode-PSK, WPA2 or WPA only. WPA2 is safer than WPA only, but not supported by all wireless clients. Please make sure your wireless client supports
-----------------	---

	your selection.
Encryption	Select “TKIP/AES Mixed Mode” or “AES” encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.
Pre-Shared Key Type	Choose from “Passphrase” (8 – 63 alphanumeric characters) or “Hex” (up to 64 characters from 0-9, a-f and A-F).
Pre-Shared Key	Please enter a security key/password according to the format you selected above.

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

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



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

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

Additional wireless authentication methods can also be used:



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

MAC Address Filter

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



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

MAC Filter & MAC-RADIUS Authentication

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

MAC-RADIUS Authentication

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



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



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

MAC RADIUS Password

Use MAC address

Use the following password

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

IV-3-1-4. WDS

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



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

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

2.4GHz	
WDS Functionality	Disabled
Local MAC Address	Disabled
	WDS with AP
	Dedicated WDS

WDS Peer Settings	
WDS #1	MAC Address <input type="text"/>
WDS #2	MAC Address <input type="text"/>
WDS #3	MAC Address <input type="text"/>
WDS #4	MAC Address <input type="text"/>

WDS VLAN	
VLAN Mode	Untagged Port <input type="text"/> (Enter at least one MAC address.)
VLAN ID	1 <input type="text"/>

WDS Encryption method	
Encryption	None <input type="text"/> (Enter at least one MAC address.)

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

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

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

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

IV-3-1-5. Guest Network

> Guest Network

You can setup an additional “Guest” Wi-Fi network so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. Enable a guest network and then configure the settings.

Guest Network	
2.4GHz SSID	-06E190_G ▼
Guest Network	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Guest Access Policy			
Traffic Shaping Settings			
Traffic Shaping	Enable ▼		
Downlink	40 Mbps		
Uplink	20 Mbps		
Filtering Settings			
IP Filtering	Disable ▼		
Rules	<input type="checkbox"/>	IP/Subnet Mask	
	<input type="checkbox"/>	0.0.0.0	/0.0.0.0
	<input type="checkbox"/>	0.0.0.0	/0.0.0.0
	<input type="checkbox"/>	0.0.0.0	/0.0.0.0

Guest Network	
2.4GHz SSID	Displays the guest network name (SSID).
Guest Network	Enable or disable the guest network.

Guest Access Policy	
Traffic Shaping	Enable or disable traffic shaping for the guest network.
Downlink	Enter a downlink limit in MB.
Uplink	Enter an uplink limit in MB.
IP Filtering	Select “Deny” or “Allow” to deny or allow specified IP addresses to access the guest network. Select “Disable” to disable IP filtering.
Rules	Enter IP addresses to be filtered according to

	the Deny or Allow rule specified above and check the box for each IP address to be filtered.
--	--

IV-3-2. 5GHz 11ac 11an

> 5GHz 11ac 11an

The “5GHz 11ac 11an” menu allows you to view and configure information for your access point’s 5GHz wireless network across five categories: Basic, Advanced, Security, WDS & Schedule.

IV-3-2-1. Basic

> Basic

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

5GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11a/n/ac ▼
Enable SSID number	1 ▼
SSID1	EDIMAX-75EFA8_A VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Band 1 ▼
Auto Channel Interval	One day ▼ <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz ▼
BSS BasicRateSet	6,12,24 Mbps ▼



Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Ch 36, 5.18GHz ▼
Channel Bandwidth	Auto 80/40/20 MHz ▼
BSS BasicRateSet	6,12,24 Mbps ▼

Wireless	Enable or disable the access point’s 5GHz wireless radio. When disabled, no 5GHz SSIDs will be active.
Band	Select the wireless standard used for the

	access point. Combinations of 802.11a, 802.11n & 802.11ac can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 5GHz frequency from the drop down menu. A maximum of 16 can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 5GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

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

Channel	Select a wireless channel.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is a

	series of rates to control communication frames for wireless clients.
--	---

IV-3-2-2. Advanced

> **Advanced**

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



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

5GHz Advanced Settings	
Guard Interval	Short GI ▾
802.11n Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256-2346)
Multicast Rate	Auto ▾
Tx Power	100% ▾
Beacon Interval	100 (40-1000 ms)
Station idle timeout	60 (30-65535 seconds)

Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.


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

IV-3-2-3. Security

Security

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

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

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

5GHz Wireless Security Settings	
SSID	EDIMAX-75EFA8_A ▼
Broadcast SSID	Enable ▼
Wireless Client Isolation	Disable ▼
Load Balancing	50 /50
Authentication Method	No Authentication ▼
Additional Authentication	No additional authentication ▼

SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.

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

Please refer back to **IV-3-1-3. Security** for more information on authentication and additional authentication types.

IV-3-2-4. WDS

➤ WDS

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



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

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

5GHz WDS Mode	
WDS Functionality	Disabled
Local MAC Address	Disabled WDS with AP Dedicated WDS

WDS Peer Settings	
WDS #1	MAC Address <input type="text"/>
WDS #2	MAC Address <input type="text"/>
WDS #3	MAC Address <input type="text"/>
WDS #4	MAC Address <input type="text"/>

WDS VLAN	
VLAN Mode	Untagged Port <input type="text"/> (Enter at least one MAC address.)
VLAN ID	1

Encryption method	
Encryption	None <input type="text"/> (Enter at least one MAC address.)

5GHz WDS Mode	
WDS Functionality	Select “WDS with AP” to use WDS with access point or “WDS Dedicated Mode” to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your access point.

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

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

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

IV-3-2-5. Guest Network

> Guest Network

You can setup an additional “Guest” Wi-Fi network so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. Enable a guest network and then configure the settings.

Guest Network	
5GHz SSID	-06E190_A ▼
Guest Network	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Guest Access Policy			
Traffic Shaping Settings			
Traffic Shaping	Disable ▼		
Downlink	20 Mbps		
Uplink	40 Mbps		
Filtering Settings			
IP Filtering	Disable ▼		
Rules	<input type="checkbox"/>	IP/Subnet Mask	
	<input type="checkbox"/>	0.0.0.0	/0.0.0.0
	<input type="checkbox"/>	0.0.0.0	/0.0.0.0
	<input type="checkbox"/>	0.0.0.0	/0.0.0.0

Guest Network	
5GHz SSID	Displays the guest network name (SSID).
Guest Network	Enable or disable the guest network.

Guest Access Policy	
Traffic Shaping	Enable or disable traffic shaping for the guest network.
Downlink	Enter a downlink limit in MB.
Uplink	Enter an uplink limit in MB.
IP Filtering	Select “Deny” or “Allow” to deny or allow specified IP addresses to access the guest network. Select “Disable” to disable IP filtering.
Rules	Enter IP addresses to be filtered according to

	the Deny or Allow rule specified above and check the box for each IP address to be filtered.
--	--

IV-3-3. WPS

> WPS

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



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

WPS	
2.4GHz WPS	<input checked="" type="checkbox"/> Enable
5GHz WPS	<input checked="" type="checkbox"/> Enable
<input type="button" value="Apply"/>	

2.4GHz WPS	
Product PIN	01977608 <input type="button" value="Generate PIN"/>
Push-button WPS	<input type="button" value="Start"/>
WPS by PIN	<input type="text"/> <input type="button" value="Start"/>

5GHz WPS	
Product PIN	01977608 <input type="button" value="Generate PIN"/>
Push-button WPS	<input type="button" value="Start"/>
WPS by PIN	<input type="text"/> <input type="button" value="Start"/>

WPS Security	
2.4G WPS Status	Not Configured
5G WPS Status	Not Configured

Wireless 2.4GHz	
SSID	EDIMAX-75EFA8_G
Security	WPA/WPA2-PSK TKIP/AES Mixed Mode
Encryption	

Wireless 5GHz	
SSID	EDIMAX-75EFA8_A
Security	WPA/WPA2-PSK TKIP/AES Mixed Mode
Encryption	

WPS	Check/uncheck this box to enable/disable WPS functionality. WPS must be disabled when using MAC-RADIUS authentication (see IV-3-1-3-6 & IV-3-4).
------------	--

WPS	
Product PIN	Displays the WPS PIN code of the device, used for PIN code WPS. You will be required to enter this PIN code into another WPS device for PIN code WPS. Click "Generate PIN" to generate a new WPS PIN code.
Push-Button WPS	Click "Start" to activate WPS on the access point for approximately 2 minutes. This has the same effect as physically pushing the access point's WPS button.
WPS by PIN	Enter the PIN code of another WPS device and click "Start" to attempt to establish a WPS connection for approximately 2 minutes.

WPS Security	
WPS Status	WPS security status is displayed here. Click "Release" to clear the existing status.

Wireless 2.4GHz/5GHz	
SSID	Displays the SSID name(s) for the specified frequency.
Security	Displays the security for the specified SSID.
Encryption	Displays the encryption type for the specified SSID. See IV-3. Wireless Settings

IV-3-4. RADIUS

RADIUS

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

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

The access point can utilize both a primary and secondary (backup) external RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz)..



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

IV-3-4-1. RADIUS Settings

➤ Radius Settings

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

RADIUS Server (2.4GHz)	
Primary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>
Secondary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

RADIUS Server (5GHz)	
Primary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>
Secondary RADIUS Server	
RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input type="text"/>
Authentication Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Session Timeout	<input type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input type="text" value="1813"/>

RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535.
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in IV-3-1-3-6 or IV-3-2-3 .
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Accounting	Enable or disable RADIUS accounting.
Accounting Port	When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between 1 – 65535.

IV-3-4-2. Internal Server

> Internal Server

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



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

Internal Server	
Internal Server	<input type="checkbox"/> Enable
EAP Internal Authentication	PEAP(MS-PEAP) ▼
EAP Certificate File Format	PKCS#12(*.pfx/*.p12)
EAP Certificate File	<input type="button" value="Upload"/>
Shared Secret	<input type="text"/>
Session-Timeout	3600 second(s)
Termination-Action	<input checked="" type="radio"/> Reauthentication (RADIUS-Request) <input type="radio"/> Not-Reauthentication (Default) <input type="radio"/> Not-Send

Internal Server	Check/uncheck to enable/disable the access point’s internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click “Upload” to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.
Shared Secret	Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 –

	99 characters in length. This should match the "MAC-RADIUS" password used in IV-3-1-3-6 or IV-3-2-3 .
Session Timeout	Set a duration of session timeout in seconds between 0 – 86400.
Termination Action	Select a termination-action attribute: "Reauthentication" sends a RADIUS request to the access point, "Not-Reauthentication" sends a default termination-action attribute to the access point, "Not-Send" no termination-action attribute is sent to the access point.

IV-3-4-3. RADIUS Accounts

> 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: EDIMAX-USER1, EDIMAX-USER2, EDIMAX-USER3, EDIMAX-USER4


Enter user name here

User Registration List

Select	User Name	Password	Customize
<input type="checkbox"/>	EDIMAX	Not Configured	<input type="button" value="Edit"/>

Edit User Registration List

User Name	<input type="text" value="EDIMAX"/> (4-16characters)
Password	<input type="text"/> (6-32characters)



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

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

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

Edit User Registration List


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

IV-3-5. MAC Filter

> MAC Filter

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

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

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

The MAC address filtering table is displayed below:

Add MAC Addresses

MAC Address Filtering Table

Select	MAC Address
<input type="checkbox"/>	FC:F8:AE:43:43:7E

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

	commas, e.g. 'aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg'
Add	Click "Add" to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

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

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

IV-3-6. WMM

> WMM

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides

Quality of Service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four categories: background, best effort, video and voice.

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

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

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

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

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

CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value reaches the number defined by CWMax (below). The CWMin value must be lower than the CWMax value. The contention window scheme helps to avoid frame collisions and determine priority of frame transmission. A shorter window has a higher probability (priority) of transmission.
CWMax	Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above).
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
TxOP	Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized. A value of 0 means only one frame per transmission. A greater value effects higher priority.

IV-3-7. Schedule

> Schedule

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

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



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

Schedule	<input checked="" type="checkbox"/> Enable
----------	--

Apply

Schedule List				
#	SSID	Day of Week	Time	Select
1	EDIMAX-75EFA8_G	Mon. Tue. Wed. Thu. Fri.	07:00-20:30	<input type="checkbox"/>

Add Edit Delete Selected Delete All



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

- 1.** Check **Enable** and use the **Select**, **Add**, **Edit** or **Delete** checkboxes to select and modify schedule(s).
- 2.** When you click **Add**, specify day(s), start time and end time for the schedule using the drop-down menus and click **Apply**.

Settings

2.4GHz SSID		5GHz SSID	
<input checked="" type="checkbox"/>	EDIMAX-75EFA8_G	<input type="checkbox"/>	EDIMAX-75EFA8_A

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

Start Time 07 : 00 End Time 20 : 30

Apply Cancel

3. Remember to **Apply** your changes and make sure **Enable** is checked.

Schedule Enable



IV-3-8. Traffic Shaping

> Traffic Shaping

The traffic shaping function allows you to regulate network data transfer to ensure or prioritize performance by limiting uplink and downlink speeds according to SSID.

Traffic Shaping for ssid(2.4GHz)

Enable

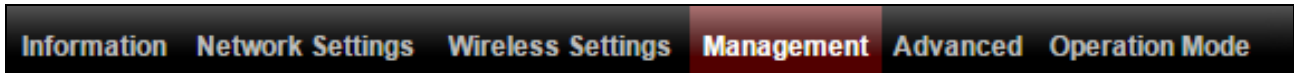
Unlimited : 0 Mbps


Down Link/Up Link Maximum : 1024 Mbps

SSID	Down Link		Up Link	
-06E190_G	0	Mbps	0	Mbps
-06E190_G_2	0	Mbps	0	Mbps
-06E190_G_3	0	Mbps	0	Mbps
-06E190_G_4	0	Mbps	0	Mbps
-06E190_G_5	0	Mbps	0	Mbps
-06E190_G_6	0	Mbps	0	Mbps
-06E190_G_7	0	Mbps	0	Mbps
-06E190_G_8	0	Mbps	0	Mbps
-06E190_G_9	0	Mbps	0	Mbps
-06E190_G_10	0	Mbps	0	Mbps
-06E190_G_11	0	Mbps	0	Mbps
-06E190_G_12	0	Mbps	0	Mbps
-06E190_G_13	0	Mbps	0	Mbps
-06E190_G_14	0	Mbps	0	Mbps
-06E190_G_15	0	Mbps	0	Mbps
-06E190_G_16	0	Mbps	0	Mbps


Enable Unlimited: 0 Mbps	Check/uncheck to enable or disable unlimited transfer speed.
Downlink/Uplink Maximum	The maximum down/uplink capacity in Mbps.
Downlink	Enter a downlink limit in MB for the listed SSID.
Uplink	Enter an uplink limit in MB for the listed SSID.


IV-4. Management



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

IV-4-1. Admin

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

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

Account to Manage This Device	
Administrator Name	<input type="text" value="admin"/>
Administrator Password	<input type="password" value="....."/> (4-32Characters)
	<input type="password" value="....."/> (Confirm)
<input type="button" value="Apply"/>	

Advanced Settings	
Product Name	<input type="text" value="AP801F02000004"/>
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
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).

Advanced Settings	
Product Name	Edit the product name according to your preference consisting of 1-32 alphanumeric characters. This name is used for reference purposes.
HTTP Port	Specify HTTP port number.
HTTPS Port	Specify HTTPS port number.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below). When SNMP is enabled, complete the SNMP fields below.
Login Timeout	Set the login timeout in minutes for the management protocol.

HTTP

Internet browser HTTP protocol management interface

IV-4-2. Date and Time

> Date and Time

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

Date and Time Settings

Local Time	<div style="display: flex; justify-content: space-between;"> 2012 ▼ Year Jan ▼ Month 1 ▼ Day </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> 0 ▼ Hours 00 ▼ Minutes 00 ▼ Seconds </div>
<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	<div style="border: 1px solid #ccc; padding: 2px;">User-Defined ▼</div> <div style="border: 1px solid #ccc; height: 20px; width: 100%; margin-top: 2px;"></div>
Update Interval	<div style="border: 1px solid #ccc; padding: 2px;">24</div> (Hours)

Time Zone

Time Zone	<div style="border: 1px solid #ccc; padding: 2px;">(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna ▼</div>
-----------	---

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.
Auto Daylight	Automatically adjust time for daylight saving or

Saving	not.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.

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

IV-4-3. Syslog Server

> Syslog Server

The system log can be sent to a server.

The image shows two configuration panels. The top panel, titled 'Syslog Server Settings', contains a 'Transfer Logs' section with an unchecked checkbox labeled 'Enable Syslog Server' and a text input field. The bottom panel, titled 'Syslog E-mail Settings', contains an 'E-mail Logs' section with an unchecked checkbox, and several text input fields for 'E-mail Subject', 'SMTP Server Address', 'SMTP Server Port', 'Sender E-mail', and 'Receiver E-mail'. At the bottom of this panel is a dropdown menu for 'Authentication' currently set to 'Disable'.

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

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

IV-4-4. Ping Test

> Ping Test

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



The screenshot shows a web interface for a ping test. At the top is a dark grey header with the text "Ping Test". Below the header, there is a form with a label "Destination Address" in blue text, followed by a white input field and a grey "Execute" button. Underneath the input field, the word "Result" is written in red text, followed by a large, empty grey rectangular box for displaying the test results.

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

IV-5. Advanced

Information Network Settings Wireless Settings Management **Advanced** Operation Mode



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

IV-5-1. LED Settings

> 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
2.4GHz LED	<input checked="" type="radio"/> On <input type="radio"/> Off
5GHz LED	<input checked="" type="radio"/> On <input type="radio"/> Off
Diag LED	<input checked="" type="radio"/> On <input type="radio"/> Off

Power/2.4GHz/5GHz/ Diag LED	Select on or off.
--	-------------------

IV-5-2. Update Firmware

> Update Firmware

The “Firmware” page allows you to update the system firmware to a more recent version. Updated firmware versions often offer increased performance and security, as well as bug fixes. You can download the latest firmware from the Edimax website.

The screenshot shows two parts of a web interface. The top part, titled "Firmware Location", has a dropdown menu set to "Update firmware from" and a radio button selected for "a file on your PC". The bottom part, titled "Update Firmware from PC", features a "Firmware Update File" field with a "Choose File" button and the text "No file chosen". Below this is an "Update" button.



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

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

IV-5-3. Save/Restore Settings

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

Save / Restore Settings	
Using Device	Select “Using your PC” to save the access point’s settings to your local computer.

Save Settings to PC	
Save Settings	Click “Save” to save settings and a new window will open to specify a location to save the settings file. You can also check the “Encrypt the configuration file with a password” box and enter a password to protect the file in the field underneath, if you wish.

Restore Settings from PC

Restore Settings

Click the browse button to find a previously saved settings file on your computer, then click “Restore” to replace your current settings. If your settings file is encrypted with a password, check the “Open file with password” box and enter the password in the field underneath.

IV-5-4. Factory Default

> Factory Default

If the access point malfunctions or is not responding, then it is recommended that you reboot the device (see **IV-5.5**) or reset the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the location of the access point is not convenient to access the reset button.

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.

IV-5-5. Reboot

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

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.
---------------	--

IV-6. Operation Mode



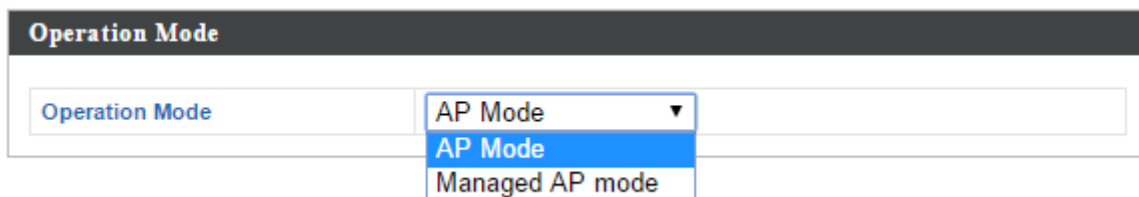
 ***Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.***

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

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

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

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



V. Appendix

V-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)**.



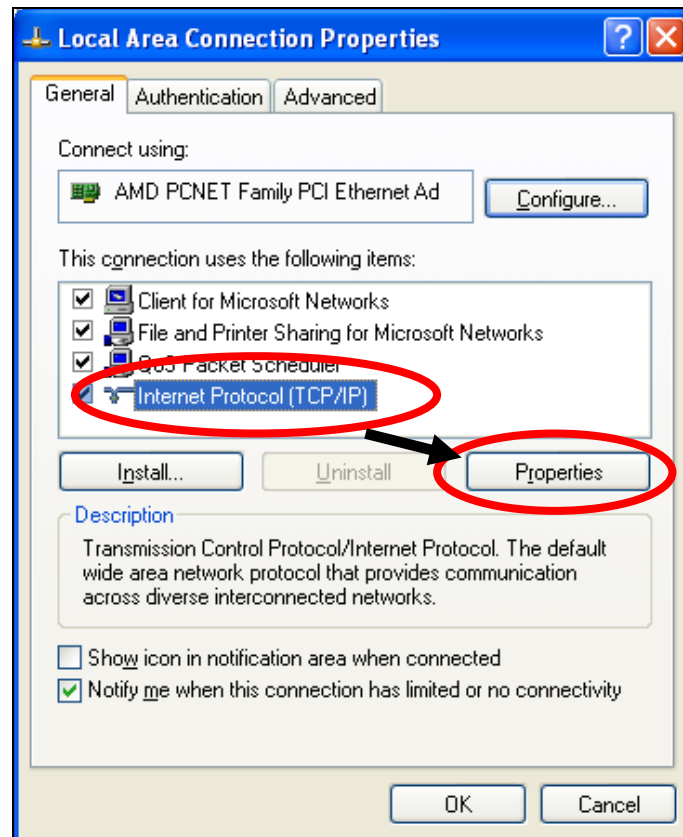
If you changed the AP's IP address, or if your gateway/router uses a DHCP server, ensure you enter the correct IP address. Refer to your gateway/router's settings. Your computer's IP address must be in the same subnet as the AP Controller.



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

V-1-1. Windows XP

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

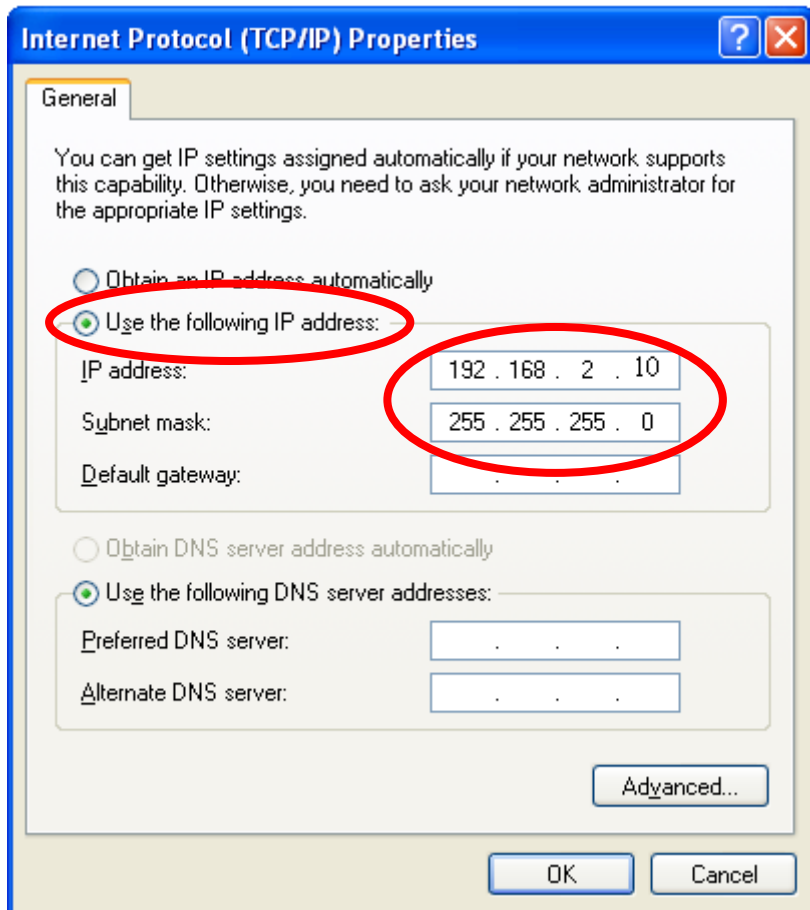


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

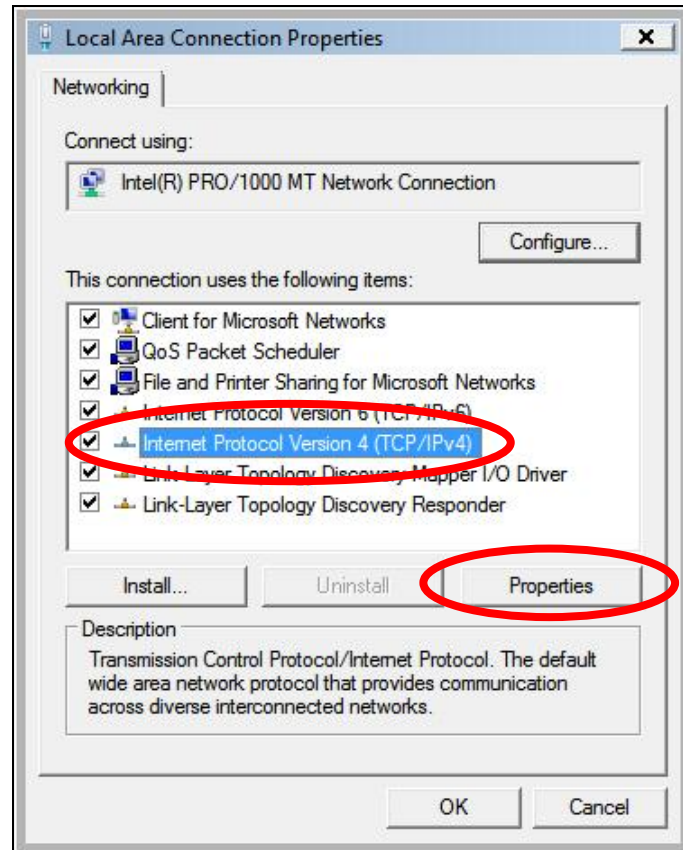
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



V-1-2. Windows Vista

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

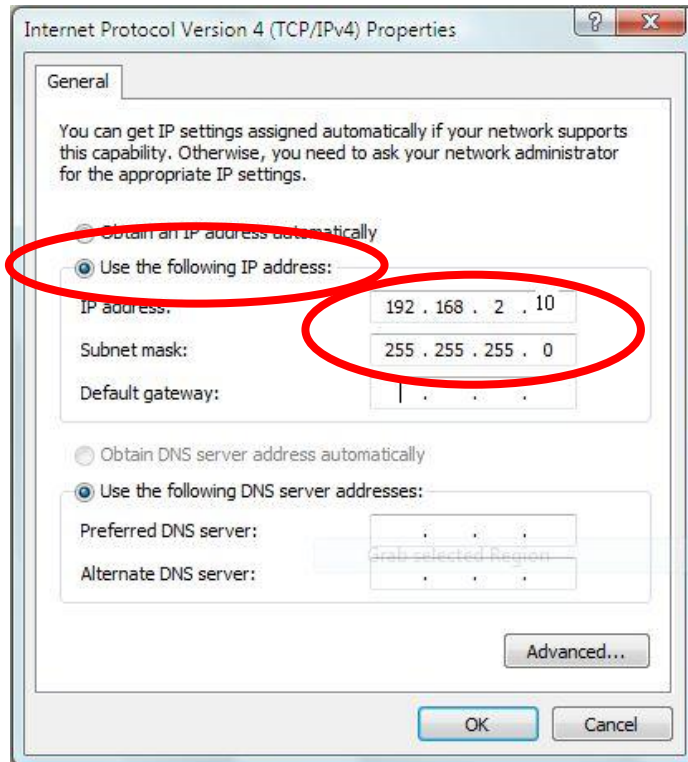


2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

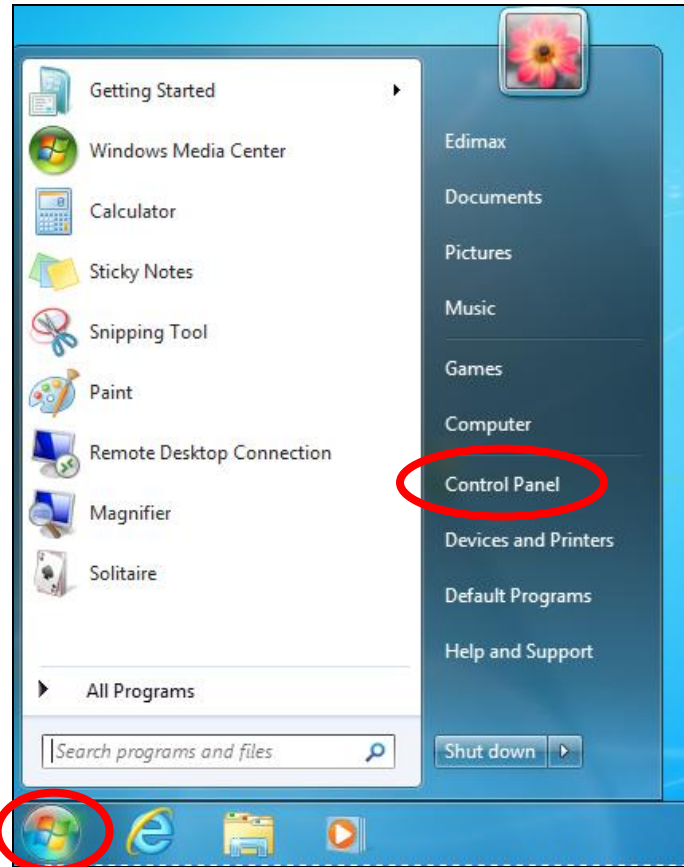
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

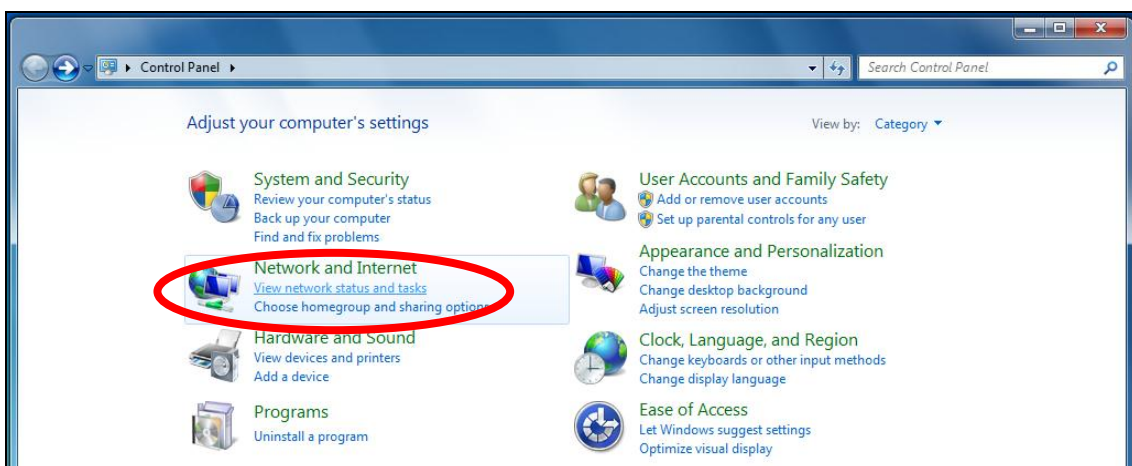


V-1-3. Windows 7

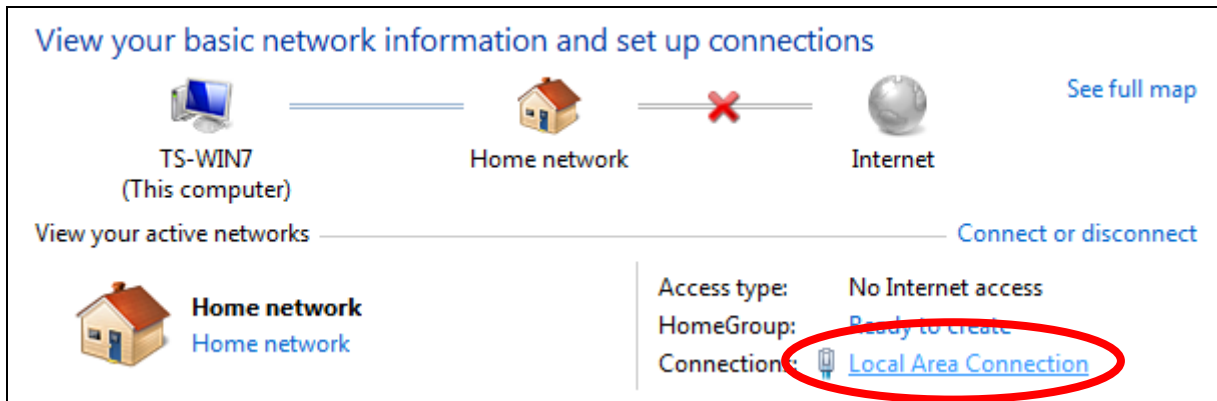
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



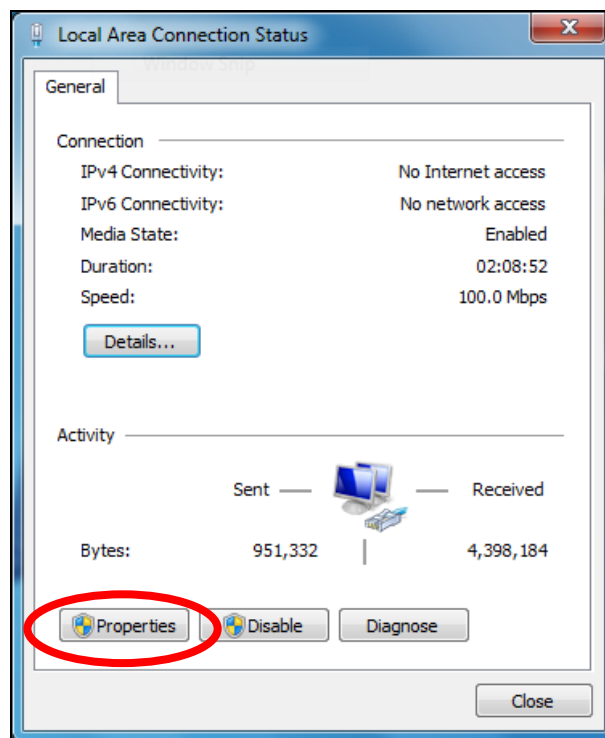
2. Under “Network and Internet” click “View network status and tasks”.



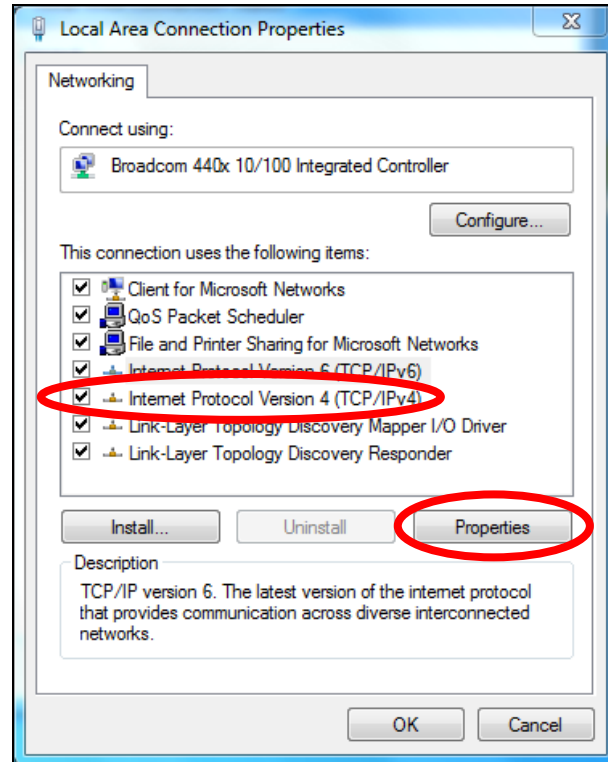
3. Click “Local Area Connection”.



4. Click “Properties”.



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

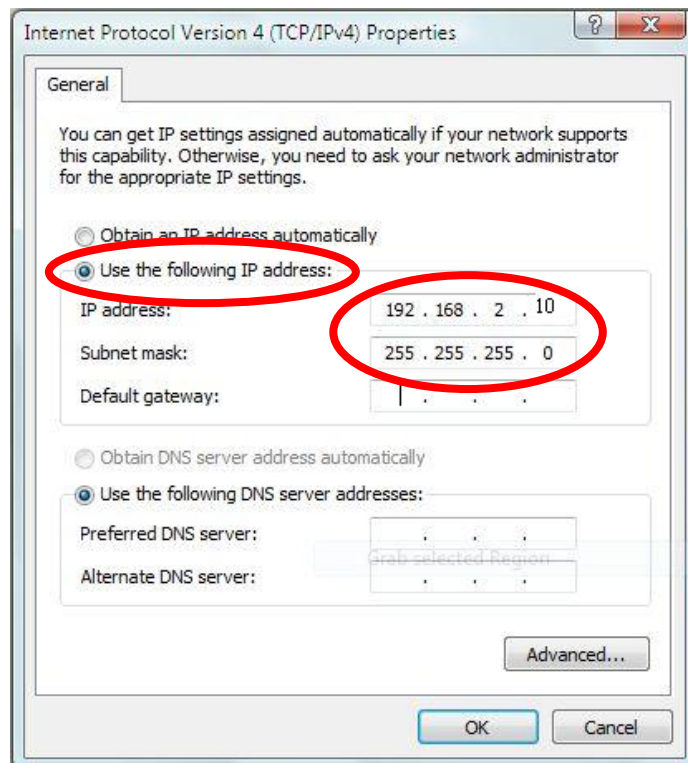


6. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10

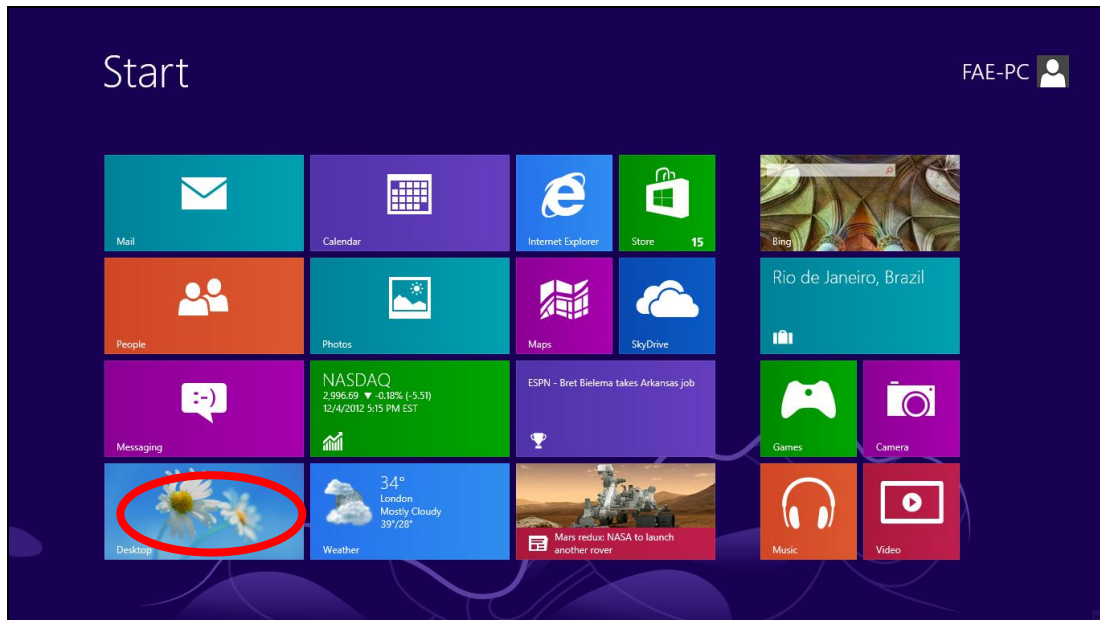
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

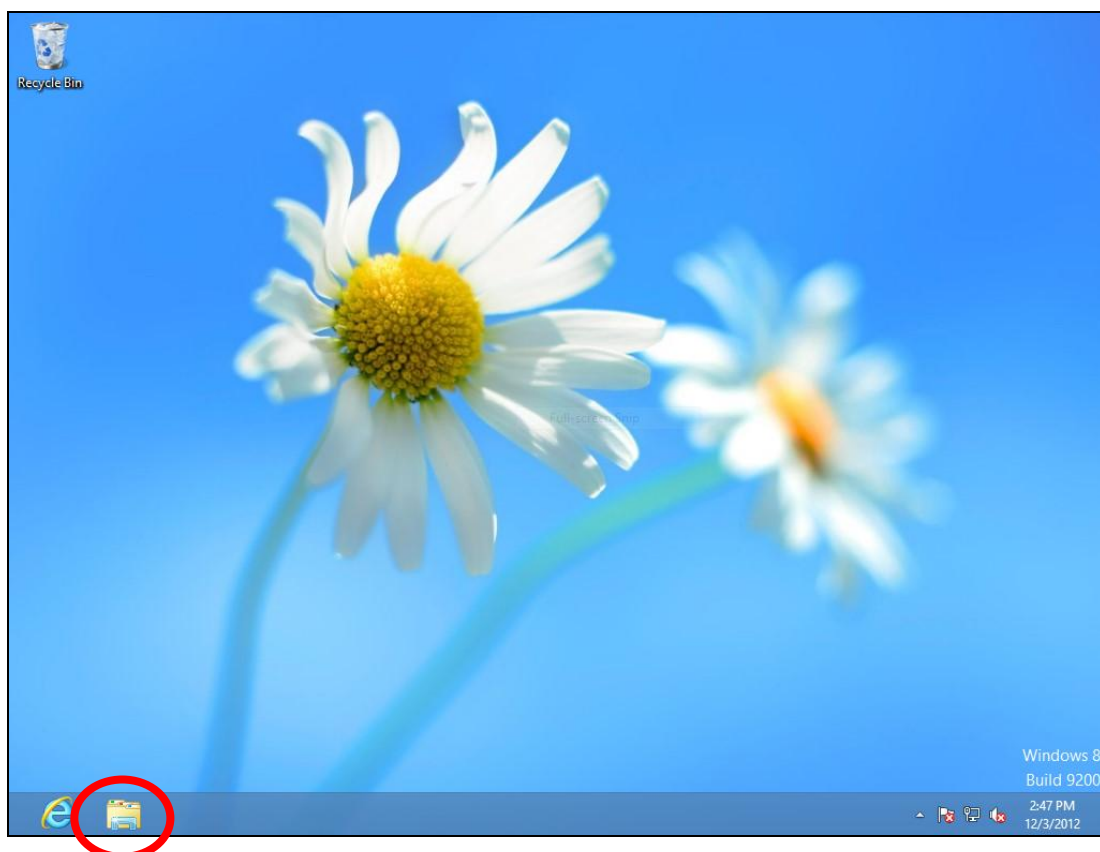


V-1-4. Windows 8

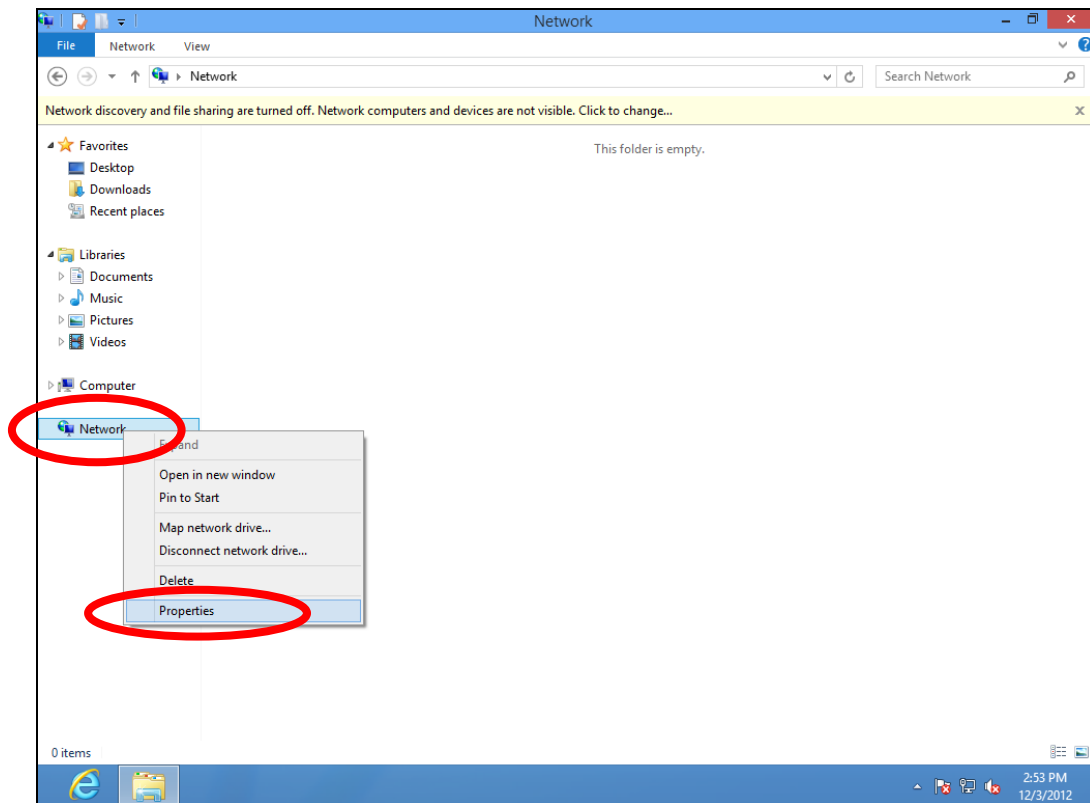
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your cursor to the bottom left of the screen and click.



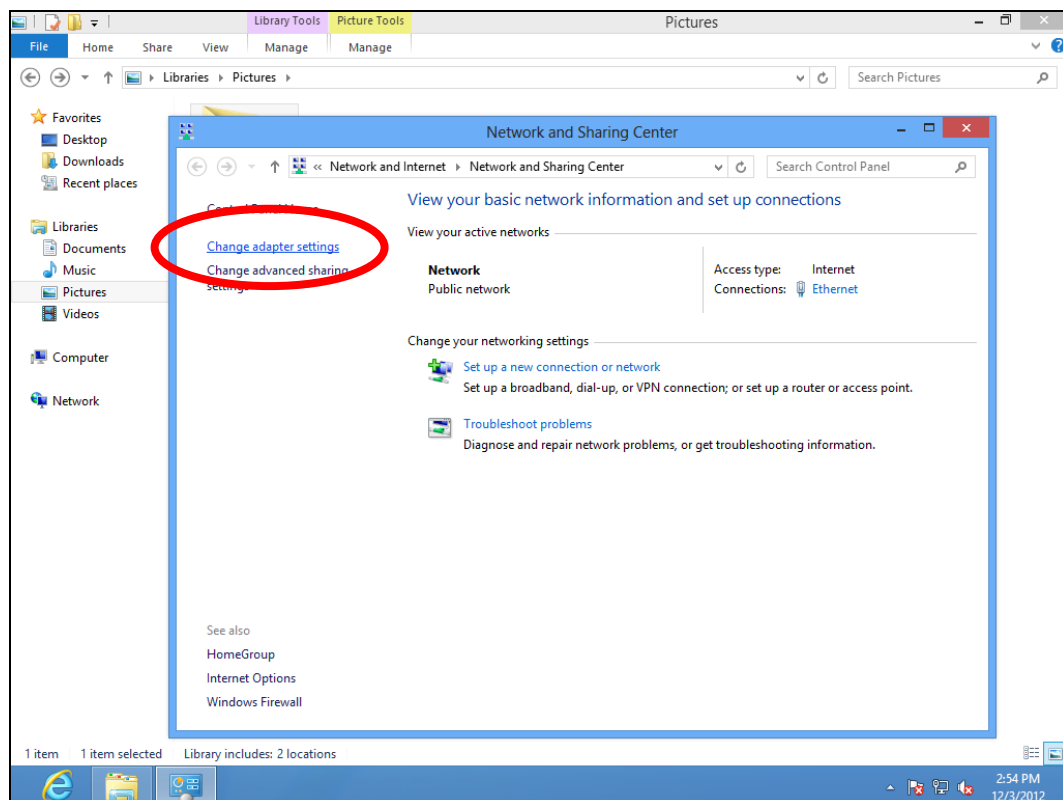
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



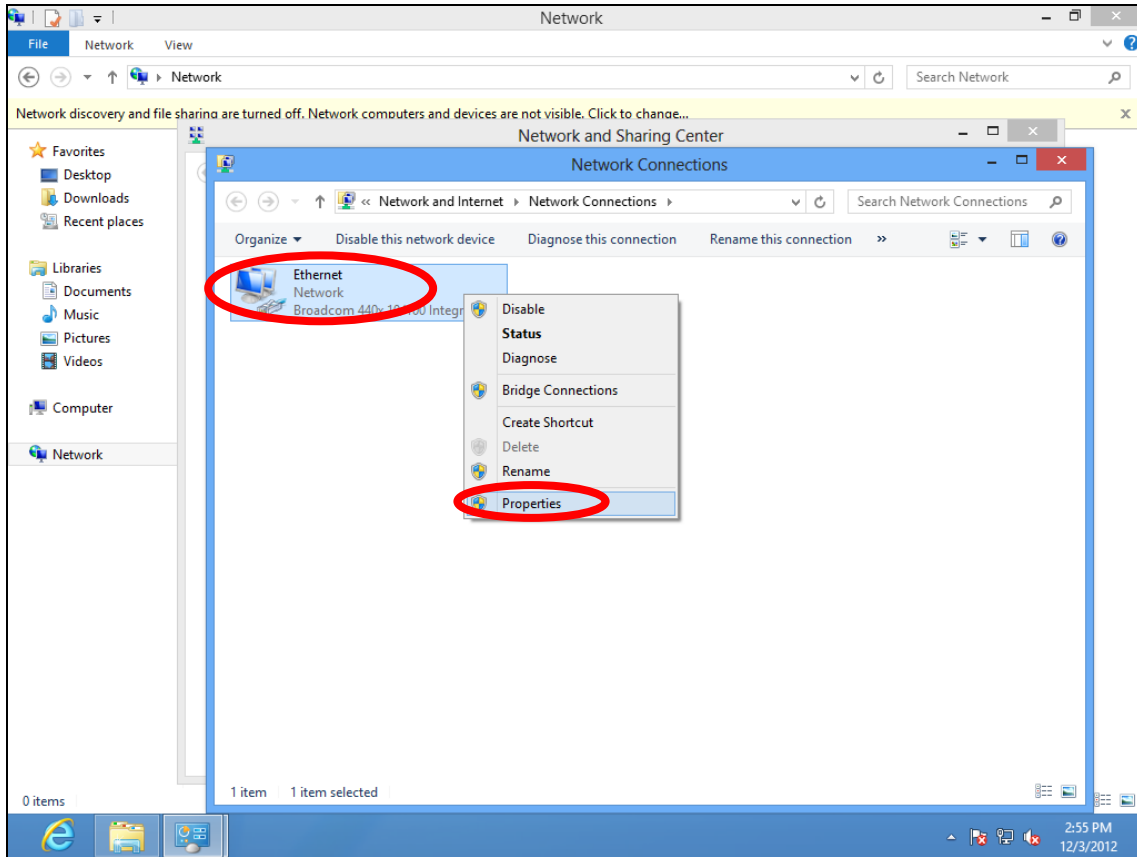
3. Right click “Network” and then select “Properties”.



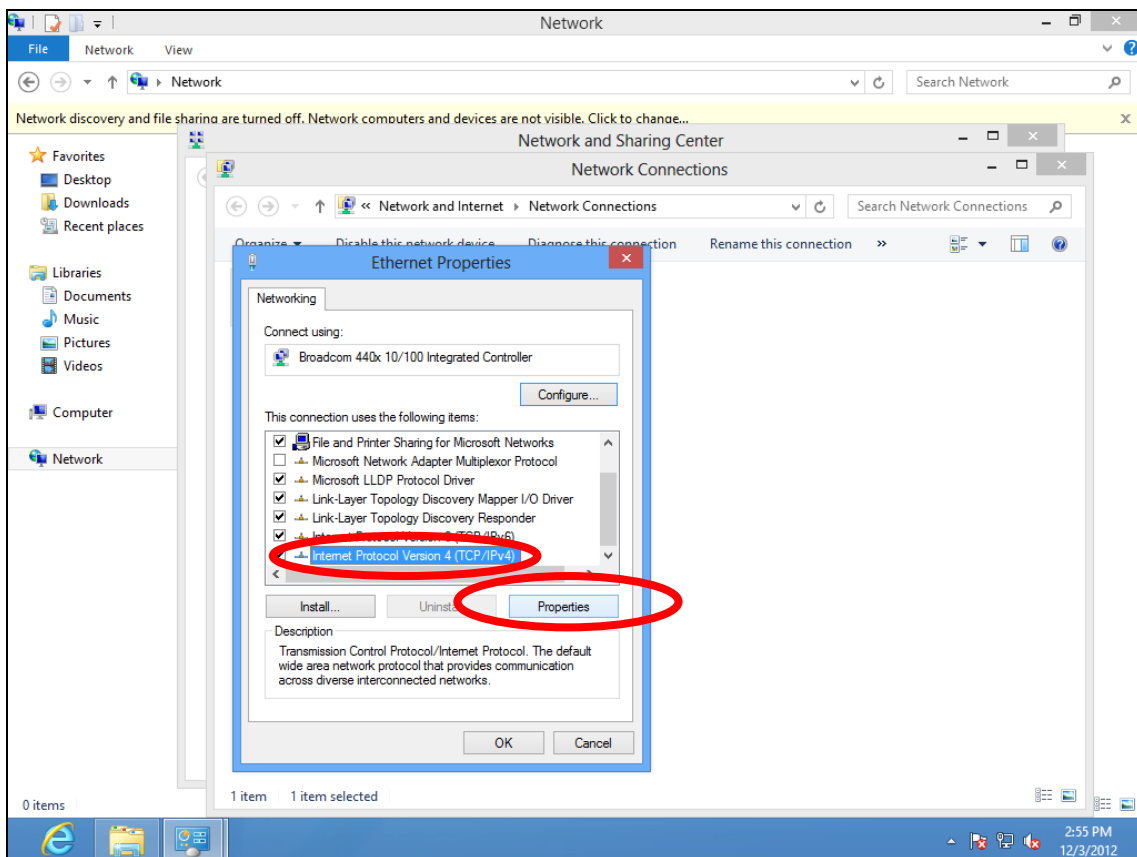
4. In the window that opens, select “Change adapter settings” from the left side.



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



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



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

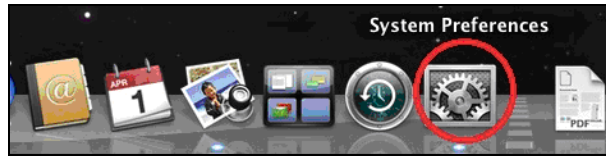
IP address: 192.168.2.10

Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

V-1-5. Mac

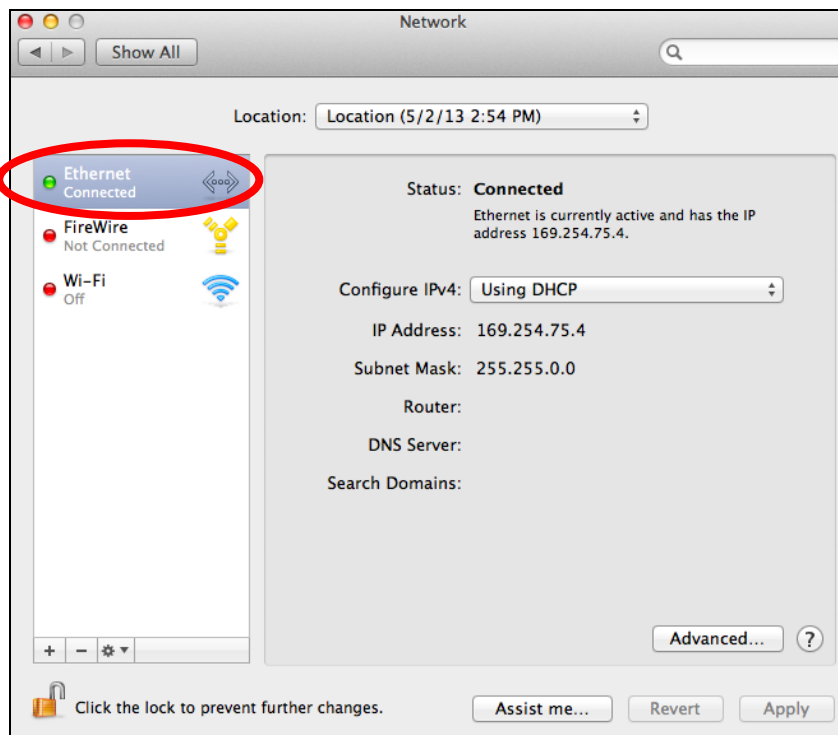
1. Have your Macintosh computer operate as usual, and click on “System Preferences”



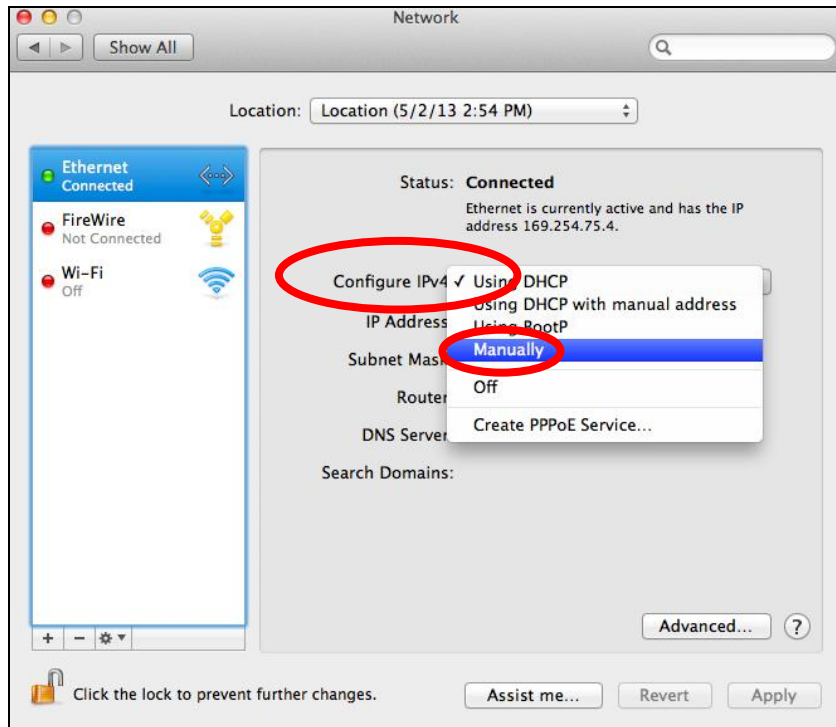
2. In System Preferences, click on “Network”.



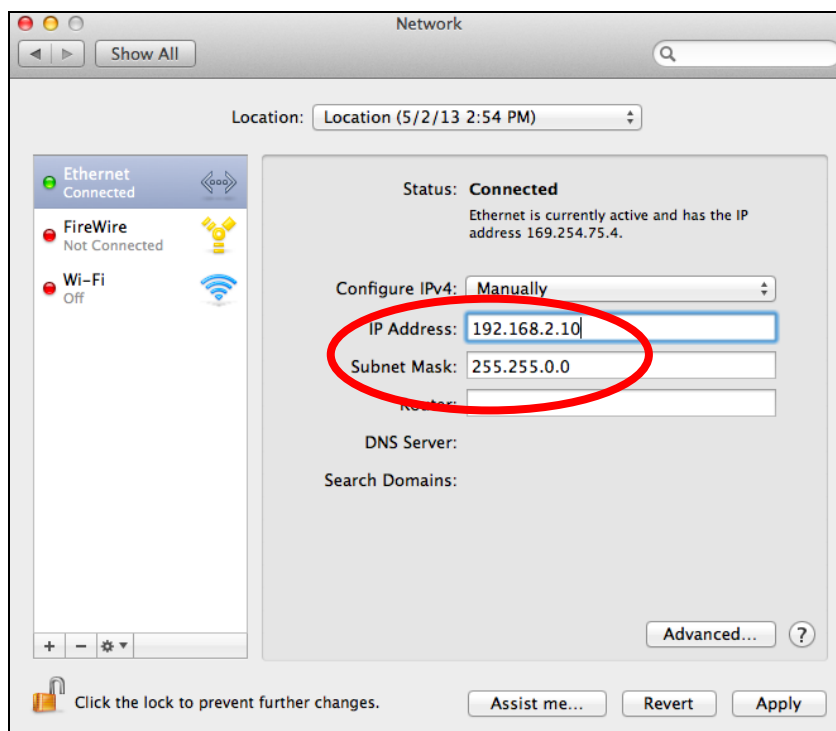
3. Click on “Ethernet” in the left panel.



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.



COPYRIGHT

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

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

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

Federal Communication Commission Interference Statement

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

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

FCC Caution

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

Federal Communications Commission (FCC) Radiation Exposure Statement

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

Federal Communications Commission (FCC) RF Exposure Requirements

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

R&TTE Compliance Statement

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

Safety

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

EU Countries Intended for Use


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

EU Countries Not Intended for Use

None

EU Declaration of Conformity

- English:** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- Français:** Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 1995/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.
- Čeština:** Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 1995/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.
- Polški:** Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..
- Română:** Acest echipament este în conformitate cu cerințele esențiale și alte prevederi relevante ale Directivei 1995/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.
- Русский:** Это оборудование соответствует основным требованиям и положениям Директивы 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- Magyar:** Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (1995/5/EK, 2009/125/EK, 2006/95/EK, 2011/65/EK).
- Türkçe:** Bu cihaz 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.
- Українська:** Обладнання відповідає вимогам і умовам директиви 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- Slovenčina:** Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 1995/5/ES, 2009/125/ES, 2006/95/ES, 2011/65/ES.
- Deutsch:** Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- Español:** El presente equipo cumple los requisitos esenciales de la Directiva 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- Italiano:** Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 1995/5/CE, 2009/125/CE, 2006/95/CE, 2011/65/CE.
- Nederlands:** Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC..
- Português:** Este equipamento cumpre os requisitos essenciais da Directiva 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- Norsk:** Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- Svenska:** Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 1995/5/EG, 2009/125/EG, 2006/95/EG, 2011/65/EG.
- Dansk:** Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 1995/5/EC, 2009/125/EC, 2006/95/EC, 2011/65/EC.
- suomen kieli:** Tämä laite täyttää direktiivien 1995/5/EY, 2009/125/EY, 2006/95/EY, 2011/65/EY oleelliset vaatimukset ja muut asiaankuuluvat määräykset.

FOR USE IN 



WEEE Directive & Product Disposal



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

Declaration of Conformity

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

Equipment: AC1200 In Wall Access Point
Model No.: IAP1200

The following European standards for essential requirements have been followed:

Directives 1999/5/EC

Spectrum : ETSI EN 300 328 V1.8.1 (2012-06);
EMC : EN 301 489-1 V1.9.2 (2011-09);
EN 301 489-17 V2.2.1 (2012-09);
Safety (LVD) : IEC 60950-1:2005 (2nd Edition);Am 1:2009+Am2:2013
EN 60950-1:2006+A11+A:2010+A12:20+A2:2013

Recommendation 1999/5/EC

EMF : EN 62311:2008

Directives 2006/95/EC; 2014/35/EU

Safety (LVD) : IEC 60950-1:2005 (2nd Edition);Am 1:2009+Am2:2013
EN 60950-1:2006+A11+A:2010+A12:20+A2:2013

Edimax Technology Co., Ltd.
No. 3, Wu Chuan 3rd Road,
Wu-Ku Industrial Park,
New Taipei City, Taiwan



Date of Signature: Dec, 2015

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.



EDIMAX
NETWORKING PEOPLE TOGETHER