

# EW-7428HCn

## User Manual

08-2012 / v1.0



## 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. For more information about this product, please refer to the user manual on the CD-ROM. The software and specifications are subject to change without notice. Please visit our website [www.edimax.com](http://www.edimax.com) for updates. All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

### **Edimax Technology Co., Ltd.**

Add: No. 3, Wu-Chuan 3rd Rd., Wu-Ku Industrial Park, New Taipei City, Taiwan

Tel: +886-2-77396888

Email: [sales@edimax.com.tw](mailto:sales@edimax.com.tw)

### **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.

# CONTENTS

<b>I. PRODUCT INFORMATION.....</b>	<b>5</b>
I-1. Package Contents .....	5
I-2. Physical Description.....	5
I-3. Front Panel .....	5
I-4. Back Panel .....	6
I-5. Safety Information.....	7
I-6. System Requirements.....	8
I-7. Hardware Installation .....	8
I-7-1. Connecting the Access Point to a Router or PoE Switch.....	8
I-7-2. Fixing the Access Point to a Ceiling.....	10
<b>II. GETTING STARTED .....</b>	<b>11</b>
II-1. Access Point Mode.....	14
II-2. Universal Wi-Fi Extender Mode.....	16
II-3. Wireless Client Mode .....	19
<b>III. BROWSER BASED CONFIGURATION INTERFACE.....</b>	<b>21</b>
III-1. Home .....	23
III-2. iQ Setup .....	25
III-3. Basic Setting.....	26
III-3-1. AP Mode.....	28
III-3-2. Station-Infrastructure Mode.....	33
III-3-3. AP Bridge-Point to Point Mode.....	35
III-3-4. AP Bridge-Point to Multi-Point Mode .....	36
III-3-5. AP Bridge-WDS.....	38
III-3-6. Universal Repeater Mode .....	43
III-4. WPS Setting.....	48
III-5. Wireless Advanced.....	51
III-5-1. Security .....	53
III-5-2. MAC Filtering .....	58
III-6. System Utility .....	60
III-6-1. Administrator .....	61
III-6-2. Time Setting .....	65
III-6-3. Power Saving.....	66
III-6-4. Scheduling setting .....	67
III-7. Configuration Tool.....	70
III-7-1. Diagnosis .....	72
III-7-2. Firmware Upgrade.....	73
III-7-3. Reboot.....	74
<b>IV. APPENDIX.....</b>	<b>76</b>
IV-1. Configuring your IP address.....	76
IV-1-1. Windows XP .....	76
IV-1-2. Windows Vista .....	77
IV-1-3. Windows 7 .....	79

IV-1-4. Mac OS.....	82
IV-2. Troubleshooting.....	86
IV-3. Glossary.....	88

# I. PRODUCT INFORMATION

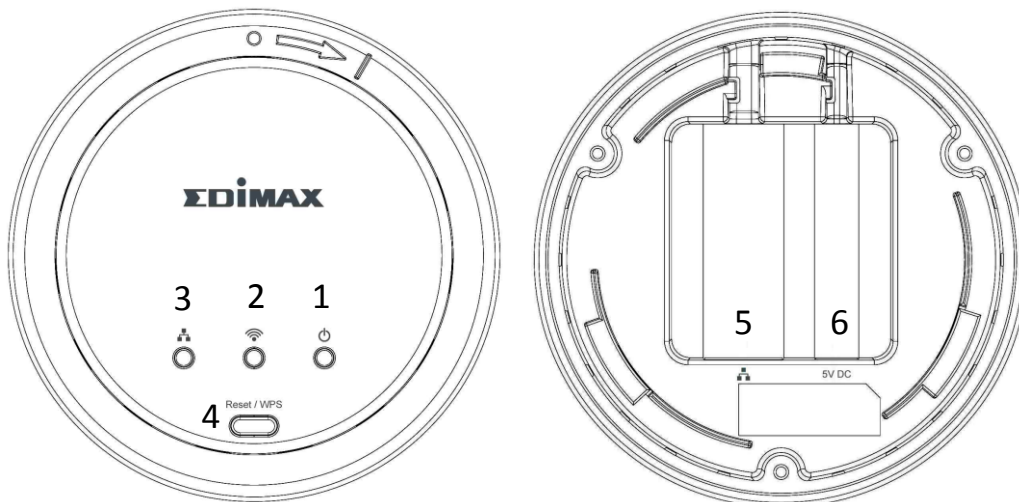
Thank you for purchasing the Edimax EW-7428HCn N300 High Power Ceiling Mount Wireless PoE Range Extender/Access Point! This device is an ideal choice for users looking to expand their home or office networking environment. Its easy installation procedure also allows any computer user to set up a network environment in a matter of minutes.

## I-1. Package Contents


Before you start using this device, please check if there is anything missing in the package, and contact your dealer to claim the missing item(s):



- Ceiling mount range extender/access point (1 pcs)
- Quick installation guide (1 pcs)
- CD with multi-language QIG and user manual (1 pcs)
- Power adapter (1 pcs)
- Ethernet cable (1 pcs)
- Mounting kit (1 pcs)
- Access key card (1 pcs)

## I-2. Physical Description



## I-3. Front Panel

LED	Light Status	Description
 (1)Power	On	Device correctly powered and initialized.
	Off	Device not powered or not correctly powered, or device not yet initialized.


	Flashing	Device is resetting to factory default settings.
 (2)Wi-Fi	On	WPS is activated and the device is waiting for a WPS signal from another device.
	Flashing	Wi-Fi activity (transferring data).
 (3)LAN	On	Connected to a local area network.
	Off	Not connected to a local area network.
	Flashing	LAN activity (transferring data).

Item	Function	Description
(4)Reset/ WPS	WPS	Press and hold this button for 2 seconds to activate WPS mode, during which this device will attempt to automatically connect to a WPS-enabled client device.
	Reset	To reset the device to factory default settings, press and hold the button for 10 seconds, until the Power LED starts flashing. Release the button to initiate reset procedures.



**Note:** Please note that the hardware WPS button only works when connecting to wireless clients. It will have no effect when the device itself is in Wireless Client Mode.

#### I-4. Back Panel

Item Name	Description
 (5) LAN Port	Connects to an Ethernet cable. This device is capable of Power over Ethernet (PoE), so if the cable is connected to a PoE switch, then this device will be powered by the Ethernet cable alone.
(6) 5V DC	Connects to the power adapter.



**Note:** Please do not connect the power adapter if the device is already connected to a PoE switch via the LAN port.

## **I-5. 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. Ensure that the access point is firmly secured to a wall or ceiling. In the event of damage due to the access point falling from its location, the warranty of the access point is void.
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 will become hot during use.
7. There are no user-serviceable parts inside the access point. If you experience problems with the access point, please contact your dealer of purchase and ask for help.
8. The access point is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.
9. If you smell burning or see smoke coming from access point or A/C power adapter, then disconnect the access point and A/C power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

## I-6. System Requirements

- Computer or network device with wired or wireless network interface card.
- Web browser (Microsoft Internet Explorer 7.0 or above, Opera web browser, or Safari web browser).
- Available AC power socket (100 – 240 V, 50/60Hz) or 802.3af Power Over Ethernet (PoE) Switch.

## I-7. Hardware Installation

The access point can be attached to a ceiling, or connected to a router or PoE switch.

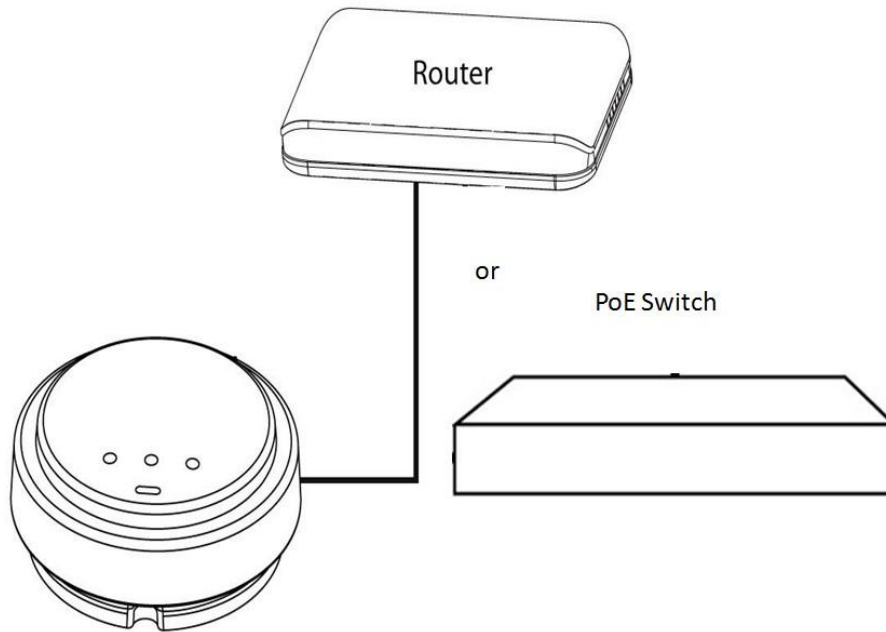


**Note:** You **must** first configure your access point using iQ Setup before proceeding with hardware installation. The following is for reference **after** you have chosen which mode to operate your access point. Please refer to **II. Getting Started** and follow the instructions to configure your access point.

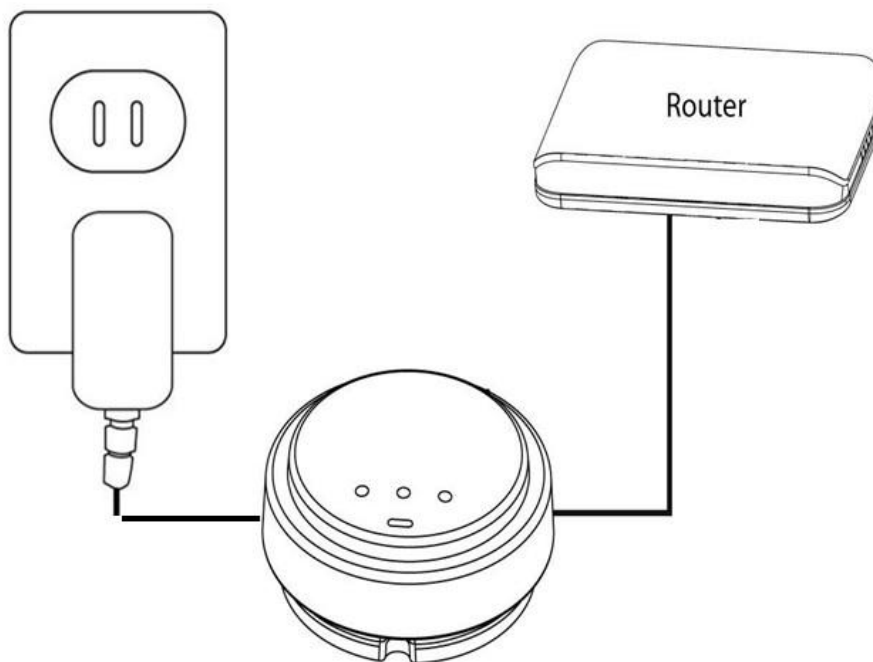
### I-7-I. Connecting the Access Point to a Router or PoE Switch

1. To connect the access point to a router or Power over Ethernet (PoE) switch, first carefully remove the back panel cover by twisting it counter-clockwise. This enables easier access to the LAN port and the power adapter.
2. Plug one end of an Ethernet cable into the Ethernet port on the access point. Plug the other end of the cable into a LAN port on a router or PoE switch, as shown in the following diagram:





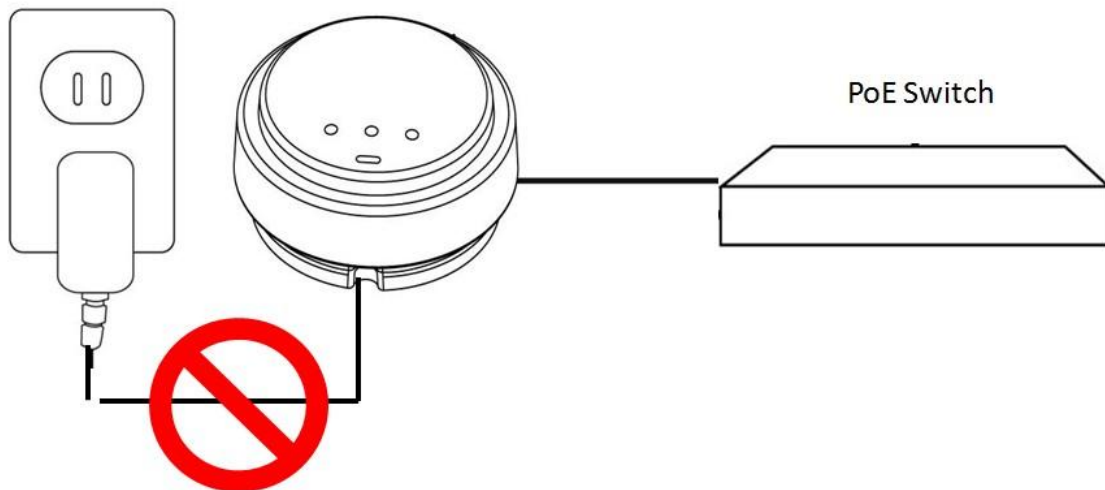
3. If you are using a **router** then plug the power adapter into a wall socket, and connect it to the 5V DC power port on the access point. Reattach the back panel cover, twisting it clockwise to secure it into place.



4. If you are using a **PoE switch** then it is not necessary to connect the access point to a power source via the 5V DC power adapter. The device will be powered by the PoE switch. Reattach the back panel cover, twisting it clockwise to secure it into place.

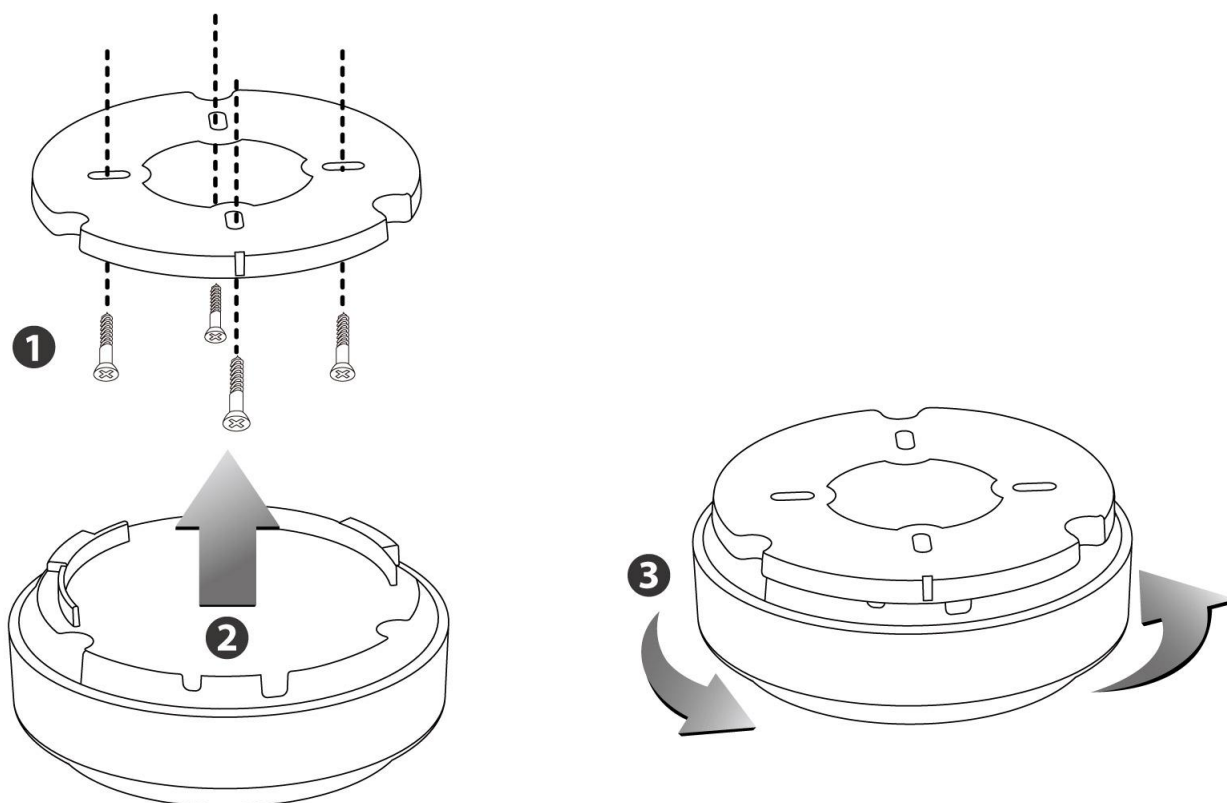


**Note:** If you are using a Power over Ethernet (PoE) switch, do not use the power adapter included in the package contents.



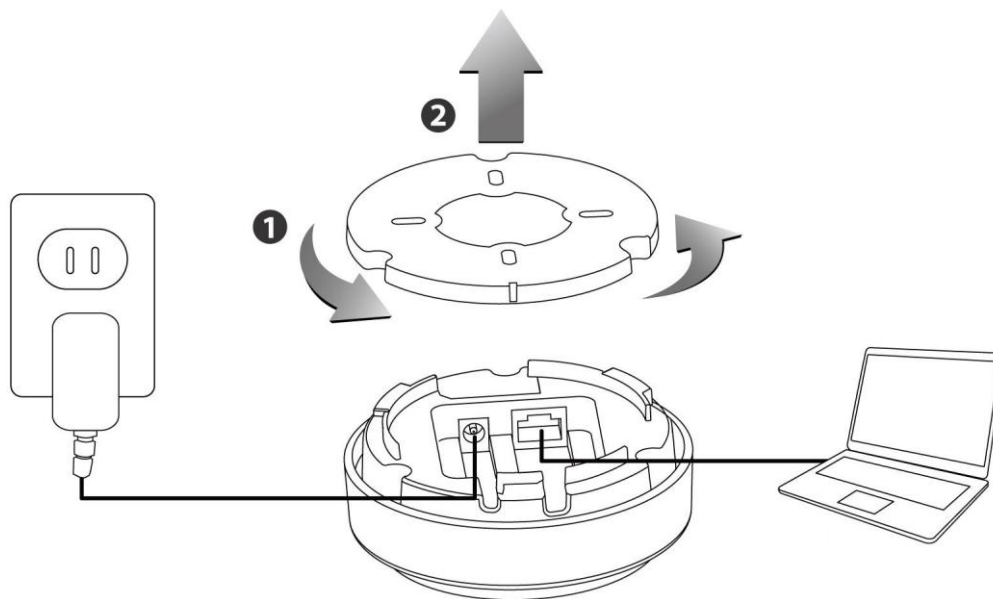
### I-7-2. Fixing the Access Point to a Ceiling

1. To attach the device to the ceiling in its final location, attach the device's back panel to the ceiling with the included screws (mounting kit). Then, attach the rest of the device to the back panel, twisting it clockwise to lock it into place.



## II. GETTING STARTED

1. Carefully remove the back panel cover by twisting it counter-clockwise. This enables easier access to the LAN port and the power adapter.
2. Plug one end of an Ethernet cable into the device's Ethernet port, plug the other end into your computer's Ethernet port.
3. Plug the power adapter into a wall socket, then connect it to the 5V DC power port. Reattach the back panel cover, twisting it clockwise to secure it into place.

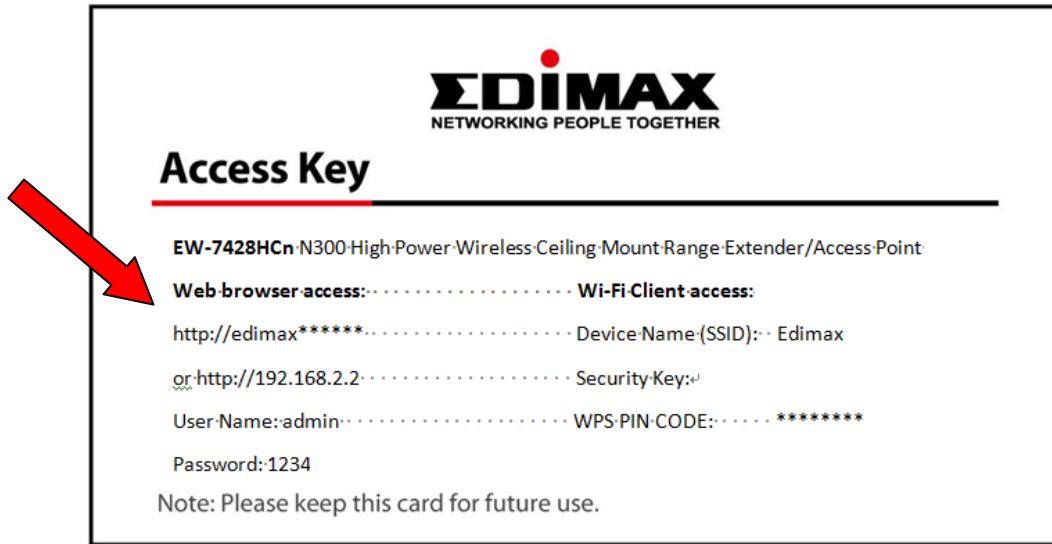


4. The device will begin to initialize. After 30 seconds, the power LED will turn on, which indicates the device has completed its initialization.



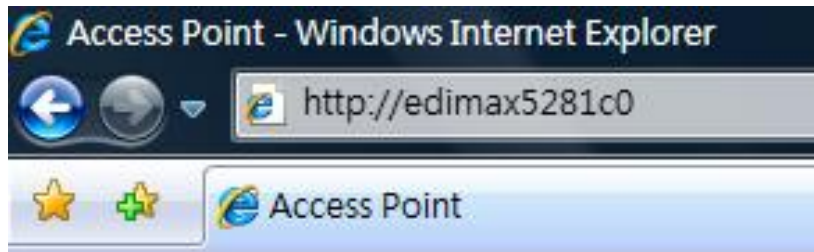
**Note:** Make sure that your computer is set as a DHCP client. If you are unsure, please see **APPENDIX IV-1. Configuring your IP address** to set your PC IP to “Obtain an IP address automatically”.

5. Enclosed in the product box is an Access Key card to indicate device factory default information, containing a URL to access the device's browser-based configuration interface, similar to the example below.  
“Web browser access” is necessary information for you to login web-based firmware.  
“Wi-Fi Client access” is necessary information for your wireless client device (for example your computer, tablet, smart phone) to connect to this device.



**Note:** The URL on your card will likely differ from the example shown in this guide. Please enter the URL you see on your card, and not the URL used in the examples here.

6. Open a web browser, such as Internet Explorer. Enter the access key into the browser URL bar. **(Windows PCs only)**

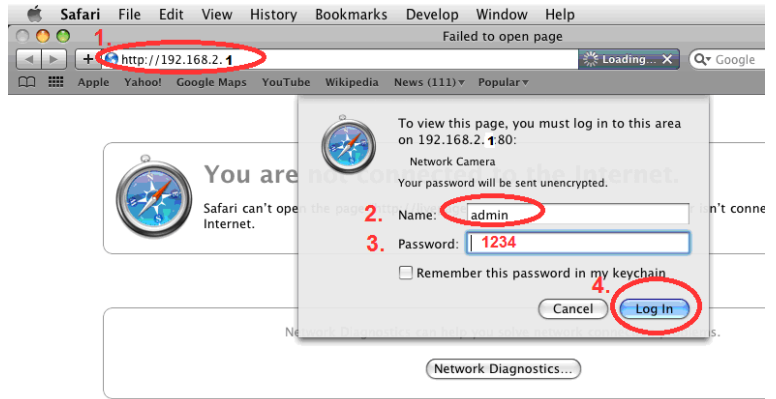


Or enter the default IP address (<http://192.168.2.2>) into your browser's address bar. **(MacOS and Linux)**

7. You will be prompted to enter a username and password. The default username is **admin**, and the default password is **1234**.



<Windows PC>



<Mac PC>

8. You will then enter the iQ Setup screen, where you can choose which mode to activate.

**iQ Setup**

Please select the operation mode of your device. If you would like to set other operation modes, please select "Setup Manually".

	<p><b>Access Point Mode:</b> Allows wireless clients to connect to access point and exchange data with the devices which are connected to the wired network.</p>
	<p><b>Universal Wi-Fi Extender Mode:</b> Connect to a Root AP and service all wireless clients within its coverage.</p>
	<p><b>Wireless Client Mode:</b> Enable the Ethernet device such as TV and Game player connected to the access point to a wireless client.</p>

[Setup Manually](#)

The default mode for the device is Access Point Mode.

1. **For Access Point Mode, please see section II-1. Access Point Mode**
2. **For Universal Wi-Fi Extender Mode, please see section II-2. Universal Wi-Fi Extender Mode**
3. **For Wireless Client Mode, please see section II-3. Wireless Client Mode**

## II-1. Access Point Mode

Access Point Mode allows the device to broadcast a wireless Internet signal, which your wireless devices – such as a notebook computer, a smartphone, or a tablet computer – can connect to.

1. Select Access Point Mode from the iQ Setup list.
2. You will be asked if you want to change the login information for this device. For now, simply click 'NEXT' without changing anything. You will later have an opportunity to change this in the browser-based setup, should you wish.

**Access Point Mode Settings**

If you wish to customize the login information for your Access Point, please enter the new user name and password in the following columns.

Username	<input type="text" value="admin"/>
New Password	<input type="password"/>
Re-Enter Password	<input type="password"/>



**Note:** If you changed the username and password in this step, you will be prompted to relogin. Enter the new information into the login prompt.

3. You will be prompted to set the device's access point settings. If you want to, you can give the device an ID in the 'Device Name' field, and if you want to set a Wi-Fi password, select 'Enabled' from the drop-down menu and enter your desired password in the 'Wi-Fi Network Password field'. Otherwise, if you keep the default settings, the device's wireless network will have the default ID of **Edimax** and will use no password.

**Access Point Mode Settings**

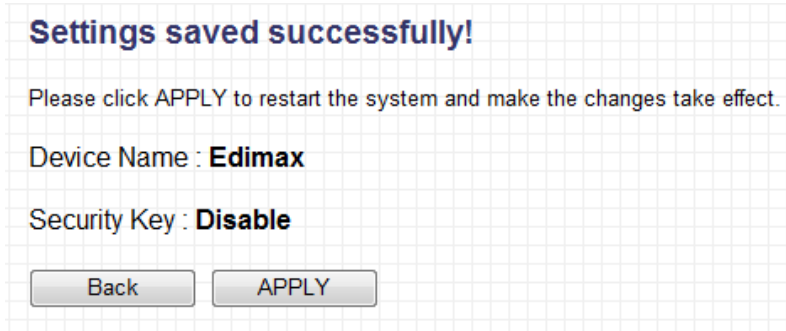
Band	2.4 GHz (B+G+N) ▾
Device Name	<input type="text" value="Edimax"/>
Channel Number	11 ▾
Wi-Fi Network Password	Disabled ▾ <input type="password"/>

Obtain an IP address automatically  
 Use the following IP address

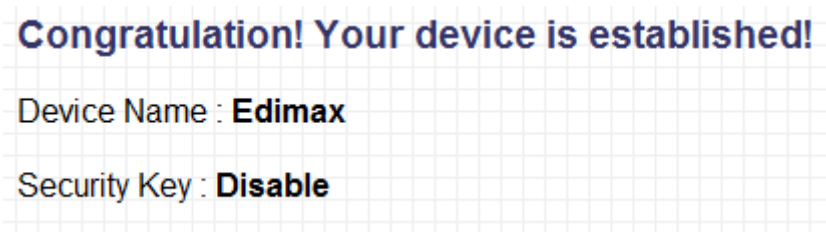


**Note:** If the device is not set to “Obtain an IP address automatically”, then please select that option by clicking on the radio button circled in the above image.

- Click ‘APPLY’ when you are done. You will see a confirmation screen, with your Wi-Fi settings.

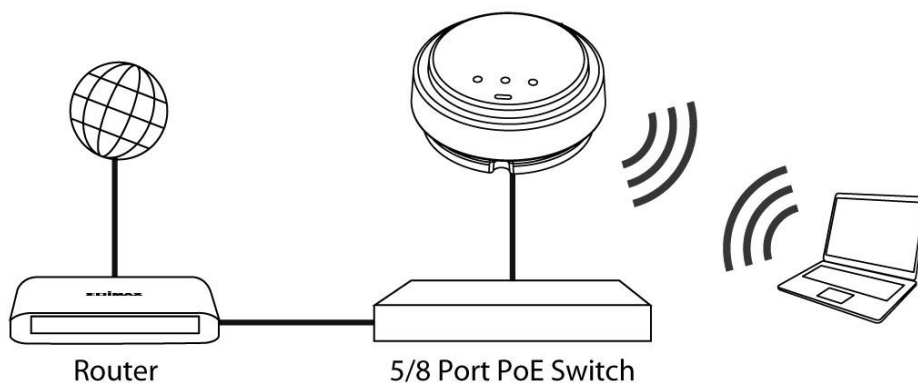


- Click ‘APPLY’ and the device will save settings and restart. When it has finished, you will see a final congratulations screen.



- Disconnect the access point from your computer via Ethernet cable and connect the access point to a router or PoE switch. See **I-7-I. Connecting the Access Point to a Router or Power over Ethernet (PoE) Switch.**

In the diagram below, the access point is connected to a PoE switch:





7. You may now connect to the device wirelessly by selecting its ID from your list of Wi-Fi networks, and entering the password you set (if you set one).

## II-2. Universal Wi-Fi Extender Mode

Universal Wi-Fi Extender Mode allows you to extend the range of an existing Wi-Fi network; expanding wireless coverage and eliminating dead spots.

1. Select Universal Wi-Fi Extender Mode from the list. iQ Setup will start detecting available Wi-Fi networks automatically. All detected Wi-Fi networks will be displayed in the list. Select the one you wish to connect to.

iQ Setup				
Please connect this device to one of the following Wi-Fi networks.				
Select	SSID	Channel	Encryption	Signal
<input type="radio"/>	Edimax	11	WPA2-PSK	80



**Note:** If the Wi-Fi network you wish to connect to does not appear, click “Refresh” to detect again or try to move the device closer to the root wireless access point.

2. Input the password of the existing Wi-Fi network in the “Key” field and click “Next” to continue. The device must have the same Wi-Fi password as the root wireless access point.

iQ Setup				
Please connect this device to one of the following Wi-Fi networks.				
Select	SSID	Channel	Encryption	Signal
<input checked="" type="radio"/>	Edimax	11	WPA2-PSK	80
Device SSID:		Edimax3A7E46		
Key:		12345678		

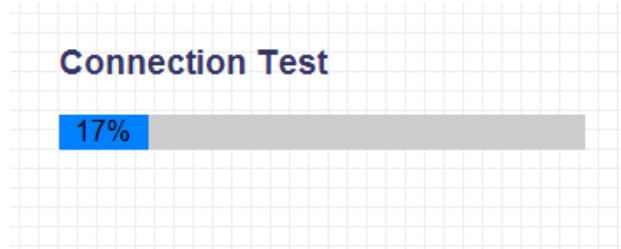


**Note:** The device will be unable to connect to the Wi-Fi network if you enter the wrong password. If you do not know your Wi-Fi password, you may find it via your Wi-Fi router’s configuration, or consult the network administrator who set up the Wi-Fi



network.

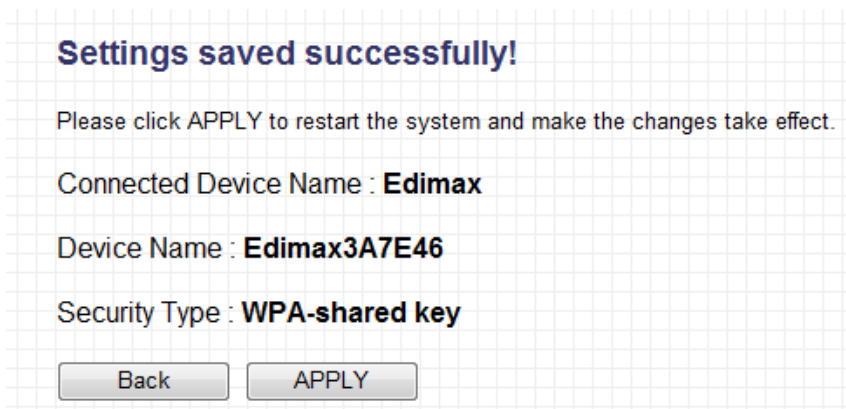
3. By default, the device's SSID is the root access point's SSID plus the last six characters of the device's access key. You can change the device's SSID if you want. Click "Next" to complete the setup.
4. The device will test the connection between itself and the root wireless access point.



If the connection is successful, the message "Connection Test Successfully" will appear on-screen. Click "Next" to save settings.

If the connection failed, the message "Connection Test Failed" will appear on-screen. Click "Back" to restart the setup process.

5. The device will show a brief summary of the name of the root wireless access point, the name of the device, and the security type used. Click "APPLY" to continue, or click "Back" to restart the setup process.



6. After you click "APPLY" the device will restart and save its settings. You will see a final congratulations page. Your computer will be disconnected from the extender at this time. To reconnect to the extender, select its SSID from your list of Wi-Fi networks.

## Congratulation! Your device is connected.

Device Name : **Edimax3A7E46**

Security Key : **1234567890**

7. You may test the connectivity of the device by disconnecting the Ethernet cable from your computer's Ethernet port, and then attempting to connect to the device wirelessly (select its SSID from your list of wireless networks, **not** the SSID of your root Wi-Fi access point). Then, attempt to open a web page with your web browser.
8. After you have connected the device to the existing Wi-Fi network and confirmed it works, you can move this device to another location for optimal Wi-Fi extension. To move the device, turn it off and unplug it from its socket. The device will remember the Wi-Fi network it is assigned to. Move the device to its new location and plug it in, then turn the device on again. It will go through its initialization process after being turned on. You will be unable to connect to the device while it is initializing.



### II-3. Wireless Client Mode

Wireless Client Mode allows Ethernet devices such as smart televisions and video game consoles to connect to a wireless access point.

1. Select Wireless Client Mode from the list. iQ Setup will start detecting available Wi-Fi networks automatically. All detected Wi-Fi networks will be displayed in the list. Select the one you wish to connect to.

iQ Setup				
Please connect this device to one of the following Wi-Fi networks.				
Select	SSID	Channel	Encryption	Signal
<input type="radio"/>	Edimax	11	WPA2-PSK	80



**Note:** If the Wi-Fi network you wish to connect to does not appear, click “Refresh” to detect again or try to move the device closer to the root wireless access point.

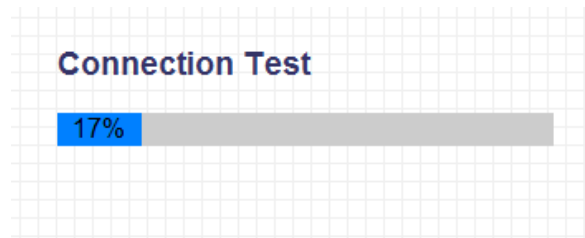
2. Input the password of the existing Wi-Fi network in the “Key” field and click “Next” to continue. The device must have the same Wi-Fi password as the root wireless access point.

iQ Setup				
Please connect this device to one of the following Wi-Fi networks.				
Select	SSID	Channel	Encryption	Signal
<input checked="" type="radio"/>	Edimax	11	WPA2-PSK	95
Password:		<input type="text" value="1234567890"/>		



**Note:** The device will be unable to connect to the Wi-Fi network if you enter the wrong password. If you do not know your Wi-Fi password, you may find it via your Wi-Fi router’s configuration, or consult the network administrator who set up the Wi-Fi network.

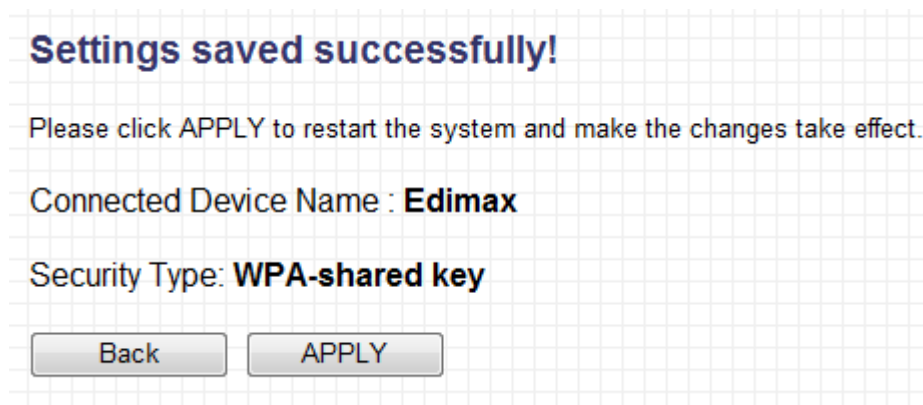
3. The device will test the connection between itself and the root wireless access point.



If the connection is successful, the message “Connection Successfully” will appear on-screen. Click “Next” to save settings.

If the connection failed, the message “Connection Test Failed” will appear on-screen. Click “Back” to restart the setup process.

- The device will show a brief summary of the name of the root wireless access point, the name of the device, and the security type used. Click “APPLY” to continue, or click “Back” to restart the setup process.



- After you click “APPLY” the device will restart and save its settings. You will see a final congratulations page.



- You may now transfer this device to another Ethernet appliance, such as a computer, a smart TV or a game console, by disconnecting the Ethernet cable from your computer’s Ethernet port, and then connecting it to the appliance’s Ethernet port. The device will remember the wireless network it is assigned to.

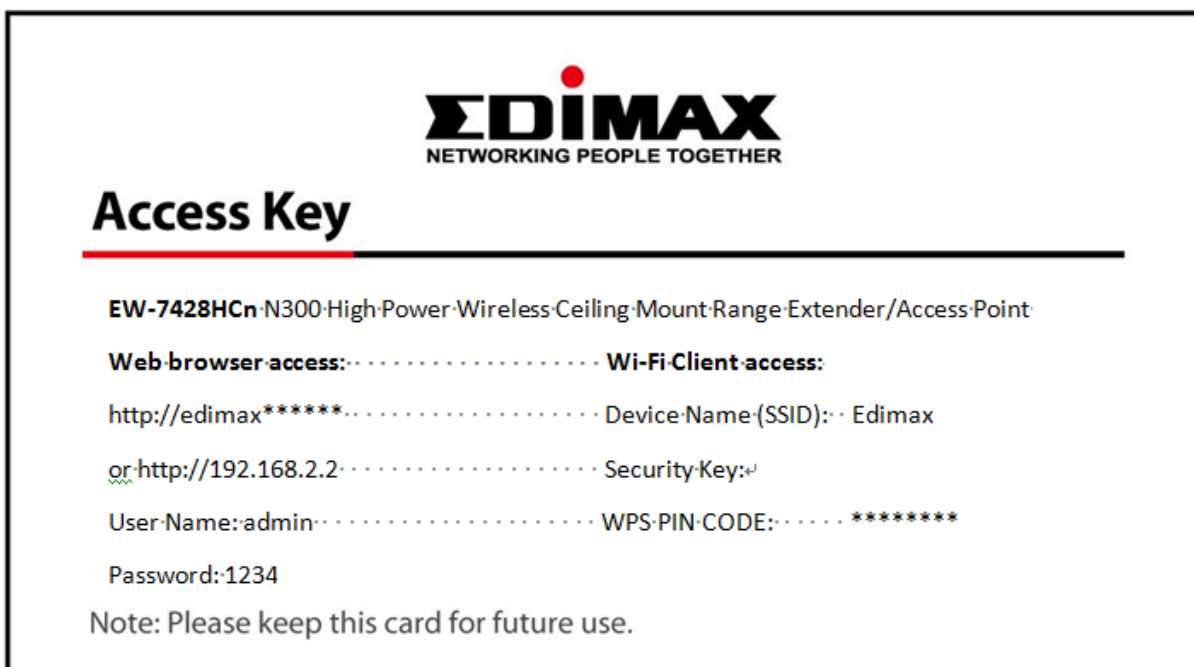


### III. BROWSER BASED CONFIGURATION INTERFACE

9. The configurations and settings of this device may be accessed through the browser-based configuration interface. Enclosed in the product box is an Access Key card to indicate device factory default information, containing a URL to access the device's browser-based configuration interface, similar to the example below.

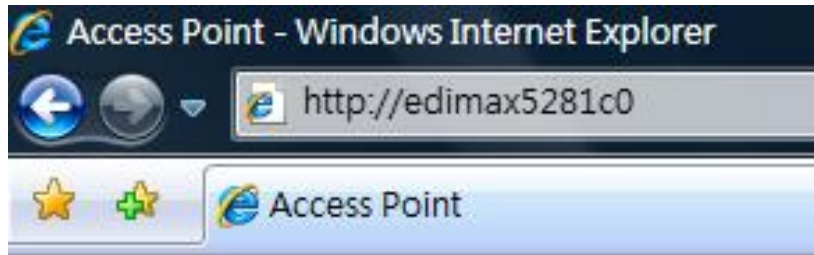
“Web browser access” is necessary information for you to login web-based firmware.

“Wi-Fi Client access” is necessary information for your wireless client device(for example your computer, tablet, smart phone) to connect to this device.



**Note:** The URL on your card will likely differ from the example shown in this guide. Please enter the URL you see on your card, and not the URL used in the examples here.

Open a web browser, such as Internet Explorer. Enter the access key (http://edimax\*\*\*\*\*) or default IP address into the browser URL bar.  
**(Windows PCs only)**



For Mac users, enter the default IP address (<http://192.168.2.2>) into your browser's address bar. **(MacOS and Linux)**



**Note:** The access point uses the default IP address 192.168.2.2, which may not be in the same IP address subnet of your network. Accordingly, you **may** need to modify the IP address of your PC or Macintosh to 192.168.2.10, before you can access the browser-based configuration interface.

In the event that you cannot access the browser-based configuration interface using either the access key or the default IP address, please refer to **IV-1. Configuring your IP Address** for guidance on how to modify your IP address.

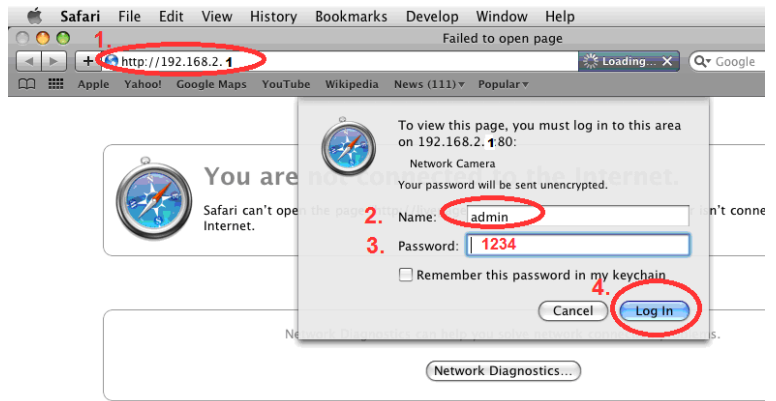


**Note:** For guidance on how to assign a new IP address to the **access point**, so that it is within the same IP address subnet of your network, please refer to **III-6-1. Administrator**. If the default IP of the access point remains unchanged, you may need to repeat this process and modify the IP of your PC or Macintosh every time you wish to configure the access point.

You will be prompted to enter the device's username and password. The default username is **admin** and the default password is **1234**.

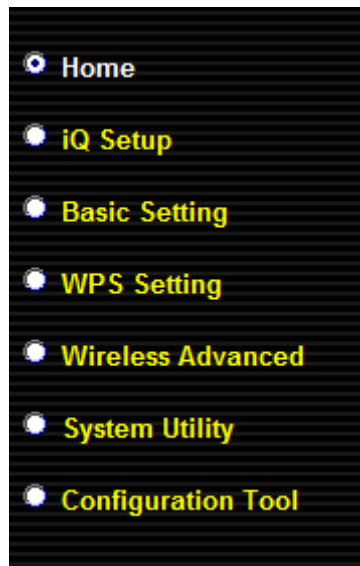


<Windows PC>



<Mac PC>

Options are listed in the sidebar on the left side of the interface.



### III-1. Home

The Home page shows the basic status and information of the device.

## Status and Information

You can check the device's MAC address, runtime code, hardware version, and network status below.

System	
Uptime	0day:0h:3m:21s
Hardware Version	Rev. A
Runtime Code Version	NFR
Wireless Settings	
Mode	AP
ESSID	Edimax
Channel Number	11
Security	Disabled
BSSID (MAC)	80:1F:02:52:81:C0
Associated Clients	0 <input type="button" value="Show Active Clients"/>
LAN Settings	
IP Address	192.168.2.2
Subnet Mask	255.255.255.0
Default Gateway	
MAC Address	80:1F:02:52:81:C0



**Note:** This screenshot is an example. The information you see on your screen will likely differ from this screenshot.

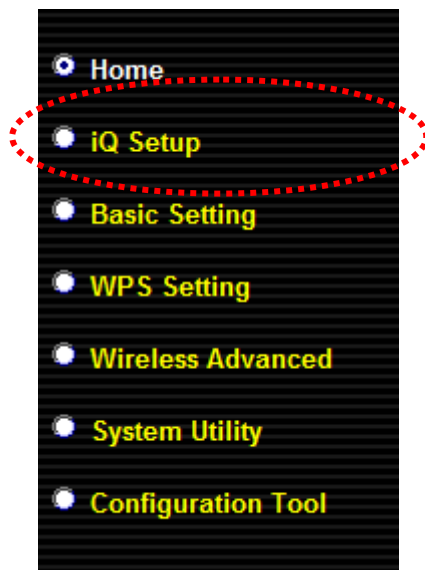
Uptime	Displays the total passed time since the device was turned on
Hardware Version	Displays the hardware version. This information is helpful when you need online help from the dealer of purchase.
Runtime Code Version	Displays the current firmware version. If you want to perform a firmware upgrade, this number will help you to determine if you have the latest version of the firmware.
Mode	Displays the current wireless operating mode (see next section)
ESSID	Displays the current ESSID (the name used to identify this wireless access point)
Channel	Displays the current wireless channel



Number	number
Security	Displays the current wireless security setting
BSSID (MAC)	Displays the device's MAC address. A MAC address is a unique identifier for this device, it cannot be modified by users)
Associated Clients	Displays the number of connected wireless client
Show Active Clients	Displays a list of connected devices, along with relevant information on each one
IP Address	Displays the IP address of this device
Subnet Mask	Displays the subnet mask of the IP address
Default Gateway	Displays the IP address of the default gateway
MAC address	Displays the MAC address of the LAN interface

### III-2. iQ Setup

If you wish to perform the initial setup process again, for example to change the operation mode of the device, select iQ Setup to restart the setup process.



This will bring you back to the initial setup screen.

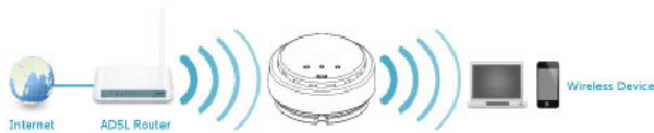
## iQ Setup

Please select the operation mode of your device. If you would like to set other operation modes, please select "Setup Manually".



### Access Point Mode:

Allows wireless clients to connect to access point and exchange data with the devices which are connected to the wired network.



### Universal Wi-Fi Extender Mode:

Connect to a Root AP and service all wireless clients within its coverage.



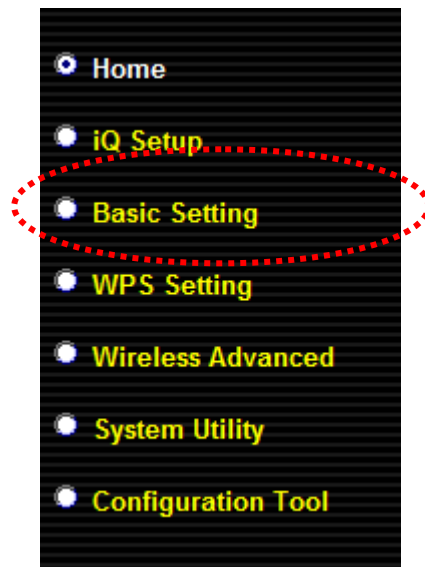
### Wireless Client Mode:

Enable the Ethernet device such as TV and Game player connected to the access point to a wireless client.

Setup Manually

### III-3. Basic Setting

This device can be set to operate in different modes. You can select the mode you want by selecting Basic Setting from the sidebar.



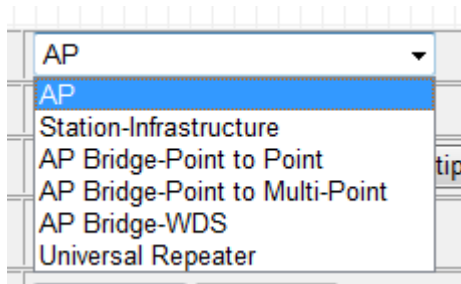
You can select a mode of operation from the drop-down menu.

### Basic Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode	AP ▼	
Band	2.4 GHz (B+G+N) ▼	
MAIN ESSID	Edimax	<input type="button" value="Multiple ESSID"/>
AP Isolation (Client user isolation)	Disabled ▼	
SSID isolation (VLAN ID)	Disabled ▼	<input type="text" value="0"/>
Channel Number	11 ▼	
Associated Clients	<input type="button" value="Show Active Clients"/>	

There are six modes available:



AP	Access point mode, allows wireless clients to connect to this device and exchange data with the devices connected to the wired network.
Station-Infrastructure	Also known as wireless client mode. Enables Ethernet-only devices such as smart TVs and game consoles to connect to a wireless network
AP Bridge-Point to Point	Establishes a wireless connection with another wireless access point using the

	same mode, and links any wired networks connected to these two wireless access points together. Only one access point can be connected in this mode.
AP Bridge-Point to Multi-Point	Establishes a wireless connection with other wireless access points using the same mode, and links any wired networks connected to these wireless access points together. Up to 4 access points can be connected in this mode.
AP Bridge-WDS	This mode is similar to “AP Bridge to Multi-Point”, but the device is not in bridge-dedicated mode, and will be able to accept wireless clients while the device is working as a wireless bridge.
Universal Repeater	The device will act as a wireless range extender that will help you to extend your Wi-Fi network. The device acts as a client and AP at the same time. In its client function to connect to a root AP, and uses its AP function to service wireless clients within its coverage.

### III-3-1. AP Mode

When in AP mode, this device acts as a bridge between IEEE 802.11b/g/n wireless devices and a wired Ethernet network, and exchanges data between them.

When you select AP Mode, the following appears:

Mode	AP ▼
Band	2.4 GHz (B+G+N) ▼
MAIN ESSID	Edimax <input type="button" value="Multiple ESSID"/>
AP Isolation (Client user isolation)	Disabled ▼
SSID isolation (VLAN ID)	Disabled ▼ <input type="text" value="0"/>
Channel Number	11 ▼
Associated Clients	<input type="button" value="Show Active Clients"/>

Band	<p>Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny wireless clients using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this access point.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g bands will be able to connect to this access point.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 2.4GHz (B+G+N).</p>
MAIN ESSID	<p>Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. <b>Please note that the ESSID is case sensitive.</b></p>
Multiple ESSID	<p>When you press this button, a new window will appear, allowing you to assign up to four ESSIDs to this access point. Please see the following page for more details.</p>
AP Isolation	<p>When this is set to "Enabled", wireless clients connected to this device will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.</p>
SSID Isolation	<p>When the access point uses multiple SSIDs and this is set to "Enabled", then wireless clients connected to the same SSID will be able to communicate with each other, but will not be able to communicate with other wireless clients connected to another of this</p>

	access point's SSIDs. You can input a numeric VLAD ID value between 1 – 4094 for the MAIN ESSID.
Channel Number	Please select a channel number you wish to use. If you know a certain channel number is being used by other wireless access points nearby, please refrain from using the same channel number
Associated Clients	Click the "Show Active Clients" button and a new window will appear, which contains information about all wireless clients connected to this access point. You can click the "Refresh" button in the popup window to keep the information up-to-date.

Click "APPLY" to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE

APPLY

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click "APPLY" to restart the device and implement any changes. The device will restart itself.

## Multiple ESSID

When you click the "Multiple ESSID" button, a new window will open, as shown below. This page allows you to configure the wireless settings for multiple ESSID's.



**Note:** The security settings for multiple ESSID's can be configured from the Security screen. Please see **III-5-1. Security** for more information.

## Multiple ESSID

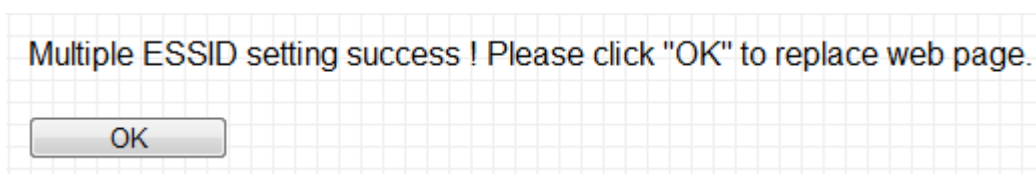
This page allows you to configure the wireless settings for Multiple ESSIDs. The wireless security settings for these ESSIDs can be configured in Security page.

No.	Enable	Basic Setting		Advanced Setting				
		SSID	Broadcast SSID	WMM	Band	AP Isolation (Client user isolation)	SSID isolation (VLAN ID)	
ESSID1	<input checked="" type="checkbox"/>	2	Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID2	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID3	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID4	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0

No.	Displayed here is the number of each additional ESSID.
Enable	Check the box to enable or disable a specific ESSID accordingly.
SSID	Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. <b>Please note that the ESSID is case sensitive.</b>
Broadcast SSID	Decide if the device will broadcast its own ESSID. You can hide the ESSID of your wireless access point (set the option to "Disable"), so only people who know the ESSID of your wireless access point can connect to it.
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable WMM, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responses. This improves the performance of such network applications.
Band	Please select the wireless band you wish to use. By selecting different band settings,

	<p>you'll be able to allow or deny wireless clients using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this access point.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g bands will be able to connect to this access point.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 2.4GHz (B+G+N).</p>
AP Isolation	<p>When this is set to "Enabled", wireless clients connected to this device will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the specified ESSID only.</p>
SSID Isolation	<p>When the access point uses multiple SSIDs and this is set to "Enabled", then wireless clients connected to the same SSID will be able to communicate with each other, but will not be able to communicate with other wireless clients connected to another of this access point's SSIDs. You can input a numeric VLAD ID value between 1 – 4094 for each specific ESSID.</p>

Click "APPLY" to make changes take effect. The following message will appear:



Click "OK" to return to the "Basic Setting" screen.



### III-3-2. Station-Infrastructure Mode

When in Station-Infrastructure mode, the device acts as a wireless client, and can be connected to Ethernet-only Internet devices, such as smart televisions or video game consoles. This gives these devices the capability to connect to the Internet wirelessly.

**Basic Setting**

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode	Station-Infrastructure ▼
Band	2.4 GHz (B+G+N) ▼
MAIN ESSID	Edimax
Site Survey	Select Site Survey

Band	<p>Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny access points using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only access points using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this device.</p> <p>If you select 2.4GHz (B+G), then only access points using the 802.11b and 802.11g bands will be able to connect to this device.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n access points to connect to this device, select 2.4GHz (B+G+N).</p>
MAIN ESSID	<p>Please input the ESSID (the name used to identify the wireless device) of the access point you want to connect to here. You can input up to 32 alphanumerical characters. <b>Please note that the ESSID is case sensitive.</b></p>

Site Survey	When you use this device to give an Ethernet network device wireless capability, you have to associate it with a working access point. Click the “Select Site Survey” button, and a “Wireless Site Survey Table” will pop up. It will list all available access points nearby. Select one access point in the table for this device to connect to. (Please see below)
-------------	---

Click “APPLY” to make changes take effect. The following message will appear:

**Settings saved successfully!**

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.



Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

**Wireless Site Survey**

When you click the “Select Site Survey” button, a “Wireless Site Survey Table” will pop up. It will list all available access points nearby.

**Wireless Site Survey**

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Select	SSID	BSSID	Band	Channel	Type	Encryption	Signal
<input type="radio"/>	Ken1	00:1d:73:22:42:9a	(B+G+N)	2	AP	WPA-PSK/WPA2-PSK	44
<input type="radio"/>	6478	00:1f:1f:c3:f8:58	(B+G+N)	11	AP	WPA2-PSK	44
<input type="radio"/>	6F-6400N	00:1f:1f:3a:36:34	(B+G+N)	6	AP	WPA2-PSK	36
<input type="radio"/>	Edimax	00:1f:1f:59:00:11	(B+G+N)	6	AP	no	36
<input type="radio"/>	INNOBAND4000R1	00:64:78:01:01:10	(B+G+N)	1	AP	WPA-PSK/WPA2-PSK	32

If you don’t see the SSID of the access point you wish to connect to, you may try clicking the “Refresh” button. It is also possible the access point has hidden

its SSID, in which case you will need to manually enter the SSID in the “MAIN SSID” field on the previous page.

### III-3-3. AP Bridge-Point to Point Mode

In this mode, the access point connects to another wireless access point in the same mode, and all connected Ethernet clients of both devices will be connected together. This allows two physically isolated networks to communicate with each other.



**Note:** When you set the device to this mode, it will not accept regular wireless clients any more.

**Basic Setting**

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode	AP Bridge-Point to Point ▾
Band	2.4 GHz (B+G+N) ▾
Channel Number	11 ▾
MAC Address 1	000000000000
Set Security	<input type="button" value="Set Security"/>

Band	<p>Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny access points using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only access points using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this device.</p> <p>If you select 2.4GHz (B+G), then only access points using the 802.11b and 802.11g bands will be able to connect to this device.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n access points to connect to this device, select 2.4GHz (B+G+N).</p>
Channel	Please select the channel number you wish

Number	to use. The channel number must be same as the other wireless access point you wish to connect to.
MAC address 1	Please input the MAC address of the wireless access point you wish to connect to.
Set Security	Click this button to select an encryption mode for this wireless link. A popup window with security options will appear.

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE

APPLY

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

### III-3-4. AP Bridge-Point to Multi-Point Mode

In this mode, this access point will connect to up to four other wireless access points also using the same mode, and all connected Ethernet clients of all access points will be connected together. This allows several physically isolated networks to communicate with each other.



**Note:** When you set the device to this mode, it will not accept regular wireless clients any more.

## Basic Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode	AP Bridge-Point to Multi-Point ▾
Band	2.4 GHz (B+G+N) ▾
Channel Number	11 ▾
MAC Address 1	000000000000
MAC Address 2	000000000000
MAC Address 3	000000000000
MAC Address 4	000000000000
Set Security	<input type="button" value="Set Security"/>



Band	<p>Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny access points using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only access points using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this device.</p> <p>If you select 2.4GHz (B+G), then only access points using the 802.11b and 802.11g bands will be able to connect to this device.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n access points to connect to this device, select 2.4GHz (B+G+N).</p>
Channel Number	<p>Please select a channel number you wish to use. The channel number must be same as the other wireless access points you wish to connect to.</p>
MAC address 1-4	<p>Please input the MAC addresses of the wireless access points you wish to connect to.</p>
Set Security	<p>Click this button to select an encryption mode for this wireless link. A popup window</p>

with security options will appear.

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

### III-3-5. AP Bridge-WDS

In this mode, this access point will connect to up to four other wireless access points also using the same mode, and all connected Ethernet clients of all access points will be connected together. This allows several physically isolated networks to communicate with each other.



**Note:** When you set the device to this mode, it will still be able to accept regular wireless clients.

**Basic Setting**

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode	AP Bridge-WDS
Band	2.4 GHz (B+G+N)
MAIN ESSID	Edimax <input type="button" value="Multiple ESSID"/>
AP Isolation (Client user isolation)	Disabled
SSID isolation (VLAN ID)	Disabled 0
Channel Number	11
Associated Clients	<input type="button" value="Show Active Clients"/>
MAC Address 1	000000000000
MAC Address 2	000000000000
MAC Address 3	000000000000
MAC Address 4	000000000000
Set Security	<input type="button" value="Set Security"/>

Band	<p>Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny devices using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only devices using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this device.</p> <p>If you select 2.4GHz (B+G), then only devices using the 802.11b and 802.11g bands will be able to connect to this device.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n devices to connect to this device, select 2.4GHz (B+G+N).</p>
MAIN ESSID	<p>Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumeric characters. <b>Please note that the ESSID is case sensitive.</b></p>
Multiple ESSID	<p>When you press this button, a new window will appear, allowing you to assign up to four ESSIDs to this access point. Please see the following page for more details.</p>
AP Isolation	<p>When this is set to "Enabled", wireless clients connected to this device will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.</p>
SSID Isolation	<p>When the access point uses multiple SSIDs and this is set to "Enabled", then wireless clients connected to the same SSID will be able to communicate with each other, but will not be able to communicate with other wireless clients connected to another of this</p>

	access point's SSIDs. You can input a numeric VLAD ID value between 1 – 4094 for the MAIN ESSID.
Channel Number	Please select a channel number you wish to use. The channel number must be same as the other wireless access points you wish to connect to.
Associated Clients	Click the "Show Active Clients" button and a new window will appear, which contains information about all wireless clients connected to this access point. You can click the "Refresh" button in the popup window to keep the information up-to-date.
MAC address 1-4	Please input the MAC addresses of the wireless access point you wish to connect to.
Set Security	Click this button to select an encryption mode for this wireless link. A popup window with security options will appear.

Click "APPLY" to make changes take effect. The following message will appear:

**Settings saved successfully!**

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE

APPLY

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click "APPLY" to restart the device and implement any changes. The device will restart itself.

## Multiple ESSID

When you click the "Multiple ESSID" button, a new window will open, as shown below. This page allows you to configure the wireless settings for



multiple ESSID's.



**Note:** The security settings for multiple ESSID's can be configured from the Security screen. Please see **III-5-1. Security** for more information.

### Multiple ESSID

This page allows you to configure the wireless settings for Multiple ESSIDs. The wireless security settings for these ESSIDs can be configured in Security page.

No.	Enable	Basic Setting		Advanced Setting				
		SSID	Broadcast SSID	WMM	Band	AP Isolation (Client user isolation)	SSID isolation (VLAN ID)	
ESSID1	<input checked="" type="checkbox"/>	2	Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID2	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID3	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID4	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0

No.	Displayed here is the number of each additional ESSID.
Enable	Check the box to enable or disable a specific ESSID accordingly.
SSID	Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. <b>Please note that the ESSID is case sensitive.</b>
Broadcast SSID	Decide if the device will broadcast its own ESSID. You can hide the ESSID of your wireless access point (set the option to "Disable"), so only people who know the ESSID of your wireless access point can connect to it.
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable WMM, the access point will define the priority of different

	<p>kinds of data, to give higher priority to applications which require instant responses. This improves the performance of such network applications.</p>
Band	<p>Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny wireless clients using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this access point.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g bands will be able to connect to this access point.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 2.4GHz (B+G+N).</p>
AP Isolation	<p>When this is set to "Enabled", wireless clients connected to this device will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the specified ESSID only.</p>
SSID Isolation	<p>When the access point uses multiple SSIDs and this is set to "Enabled", then wireless clients connected to the same SSID will be able to communicate with each other, but will not be able to communicate with other wireless clients connected to another of this access point's SSIDs. You can input a numeric VLAD ID value between 1 – 4094 for each specific ESSID.</p>

Click "APPLY" to make changes take effect. The following message will appear:

Multiple ESSID setting success ! Please click "OK" to replace web page.

OK

Click "OK" to return to the "Basic Setting" screen.

### III-3-6. Universal Repeater Mode

In this mode, this device acts as a wireless extender, simultaneously performing the functions of a client and an access point. It can extend the wireless signal of an access point, thus expanding Wi-Fi coverage and eliminating dead spots.



**Note:** In repeater mode, this device will demodulate the received signal, check the noise level, then modulate and amplify the signal again. The output power of this mode is the same as that of WDS and normal AP mode.

#### Basic Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode	Universal Repeater
Band	2.4 GHz (B+G+N)
MAIN ESSID	Edimax <input type="button" value="Multiple ESSID"/>
AP Isolation (Client user isolation)	Disabled
SSID isolation (VLAN ID)	Disabled <input type="text" value="0"/>
Channel Number	11
Associated Clients	<input type="button" value="Show Active Clients"/>
Root AP SSID	<input type="text"/>
Select Site Survey	<input type="button" value="Select Site Survey"/>

#### Band

Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny devices using certain bands.

If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only devices using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this device.

	<p>If you select 2.4GHz (B+G), then only devices using the 802.11b and 802.11g bands will be able to connect to this device.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n devices to connect to this device, select 2.4GHz (B+G+N).</p>
MAIN SSID	<p>Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. <b>Please note that the ESSID is case sensitive.</b></p>
Multiple ESSID	<p>When you press this button, a new window will appear, allowing you to assign up to four ESSIDs to this access point. Please see the following page for more details.</p>
AP Isolation	<p>When this is set to “Enabled”, wireless clients connected to this device will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the MAIN ESSID only.</p>
SSID Isolation	<p>When the access point uses multiple SSIDs and this is set to “Enabled”, then wireless clients connected to the same SSID will be able to communicate with each other, but will not be able to communicate with other wireless clients connected to another of this access point’s SSIDs. You can input a numeric VLAN ID value between 1 – 4094 for the MAIN ESSID.</p>
Channel Number	<p>Please select a channel number you wish to use. The channel number must be same as the other wireless access points you wish to connect to.</p>
Associated Clients	<p>Click the “Show Active Clients” button and a new window will appear, which contains information about all wireless clients connected to this access point. You can click the “Refresh” button in the popup window to keep the information up-to-date.</p>
Root AP SSID	<p>In Universal Repeater mode, this device will</p>

	act as a station and connect to a root AP. Enter the SSID of the root AP here, or click the “Select Site Survey” button to choose a root AP.
Select Site Survey	Click the “Select Site Survey” button, and a “Wireless Site Survey Table” will pop up. It will list all available access points nearby. Select one access point in the table for this device to connect to. (Please see below)

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.



Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

## Wireless Site Survey

When you click the “Select Site Survey” button, a “Wireless Site Survey Table” will pop up. It will list all available access points nearby.

**Wireless Site Survey**

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

Select	SSID	BSSID	Band	Channel	Type	Encryption	Signal
<input type="radio"/>	Ken1	00:1d:73:22:42:9a	(B+G+N)	2	AP	WPA-PSK/WPA2-PSK	44
<input type="radio"/>	6478	00:1f:1f:c3:f8:58	(B+G+N)	11	AP	WPA2-PSK	44
<input type="radio"/>	6F-6400N	00:1f:1f:3a:36:34	(B+G+N)	6	AP	WPA2-PSK	36
<input type="radio"/>	Edimax	00:1f:1f:59:00:11	(B+G+N)	6	AP	no	36
<input type="radio"/>	INNOBAND4000R1	00:64:78:01:01:10	(B+G+N)	1	AP	WPA-PSK/WPA2-PSK	32

If you don’t see the SSID of the access point you wish to connect to, you may try clicking the “Refresh” button. It is also possible the access point has hidden its SSID, in which case you will need to manually enter the SSID in the “MAIN

SSID” field on the previous page.

## Multiple ESSID

When you click the “Multiple ESSID” button, a new window will open, as shown below. This page allows you to configure the wireless settings for multiple ESSID’s.



**Note:** The security settings for multiple ESSID’s can be configured from the Security screen. Please see **III-5-1. Security** for more information.

### Multiple ESSID

This page allows you to configure the wireless settings for Multiple ESSIDs. The wireless security settings for these ESSIDs can be configured in Security page.

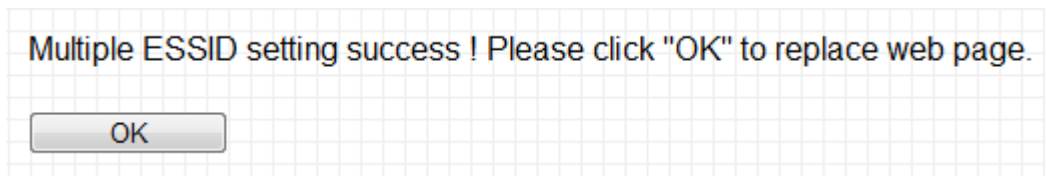
No.	Enable	Basic Setting		Advanced Setting				
		SSID	Broadcast SSID	WMM	Band	AP Isolation (Client user isolation)	SSID isolation (VLAN ID)	
ESSID1	<input checked="" type="checkbox"/>	2	Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID2	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID3	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0
ESSID4	<input type="checkbox"/>		Enable ▾	Disable ▾	2.4 GHz (B+G+N) ▾	Disable ▾	Disable ▾	0

No.	Displayed here is the number of each additional ESSID.
Enable	Check the box to enable or disable a specific ESSID accordingly.
SSID	Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. <b>Please note that the ESSID is case sensitive.</b>
Broadcast SSID	Decide if the device will broadcast its own ESSID. You can hide the ESSID of your wireless access point (set the option to “Disable”), so only people who know the ESSID of your wireless access point can connect to it.

WMM	<p>WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable WMM, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responses. This improves the performance of such network applications.</p>
Band	<p>Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny wireless clients using certain bands.</p> <p>If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this access point.</p> <p>If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g bands will be able to connect to this access point.</p> <p>If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 2.4GHz (B+G+N).</p>
AP Isolation	<p>When this is set to "Enabled", wireless clients connected to this device will be able to access the Internet, but will not be able to communicate with each other. This applies to clients connected to the specified ESSID only.</p>
SSID Isolation	<p>When the access point uses multiple SSIDs and this is set to "Enabled", then wireless clients connected to the same SSID will be able to communicate with each other, but will not be able to communicate with other wireless clients connected to another of this</p>

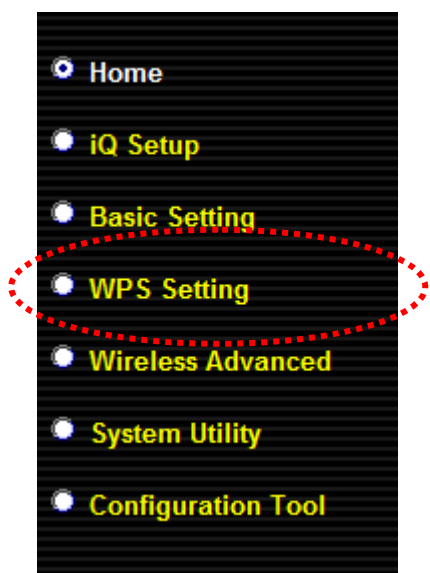
	access point's SSIDs. You can input a numeric VLAD ID value between 1 – 4094 for each specific ESSID.
--	---

Click “APPLY” to make changes take effect. The following message will appear:



Click “OK” to return to the “Basic Setting” screen.

### III-4. WPS Setting



Wi-Fi Protected Setup (WPS) is the simplest way to build a connection between wireless network clients and this access point. You don't have to select an encryption mode and enter a long encryption passphrase every time you want to set up a wireless client, you only have to press a button on the wireless client and this access point, and WPS will do the rest for you.

This access point supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you will need to switch this access point to WPS mode and push a specific button on the wireless client. You can push the Reset/WPS button on this access point, or click the “Start PBC” button in the web configuration interface to do this; if you want to use PIN code, you will need to enter the PIN code of the wireless client you wish to connect to, and then activate WPS mode in the wireless client.



## WPS (Wi-Fi Protected Setup) Settings

This page allows you to configure WPS (Wi-Fi Protected Setup) settings. WPS allows wireless clients to connect to this device automatically.

**Enable WPS**

• **Wi-Fi Protected Setup Information**

WPS Status:	unConfigured
Device PIN Code:	89616000
SSID:	Edimax
Authentication Mode:	Disabled
Passphrase Key:	

• **Device Configuration**

Config Mode:	Registrar ▼
Configure via Push Button:	<input type="button" value="Start PBC"/>
Input Client PIN Code :	<input type="text"/> <input type="button" value="Send PIN"/>

Enable WPS	Check this box to enable or disable WPS
Wi-Fi Protected Setup Information	All information related to WPS will be displayed here.
WPS Status	Displays WPS status. If data encryption settings for this access point have never been set, “unConfigured” will be shown here. If data encryption settings have been set, “Configured” will be shown here.
Device PIN Code	This is the WPS PIN code of this access point. This code is used when you need to build a wireless connection by WPS with other WPS-enabled wireless devices.
SSID	Displays the SSID (ESSID) of this access point.
Authentication Mode	The wireless security authentication mode of this access point will be shown here. If you don’t enable the security functions of the access point before WPS is activated, the access point will automatically set the security to WPA (AES) and generate a passphrase key for WPS connection.

Passphrase Key	Shows the WPA passphrase here, though all characters will be replaced by asterisks for security reasons. If encryption is not set on this access point, this field will be blank.
Device Configuration	Configuration options for the device's WPS settings can be found here.
Config Mode	There are "Registrar" and "Enrollee" modes for the WPS connection. When "Registrar" is enabled, the wireless clients will follow the access point's wireless settings for WPS connections. When "Enrollee" mode is enabled, the access point will follow the wireless settings of wireless client for WPS connections.
Configure via Push Button	Click "Start PBC" to start Push-Button style WPS setup. This access point will wait for WPS requests from wireless clients for 2 minutes. The "WLAN" LED on the access point will stay on for 2 minutes while this access point waits for incoming WPS requests.
Input Client PIN Code	Please input the PIN code of the wireless client you wish to connect, and click the "Start PIN" button. The "WLAN" LED on the access point will stay on while this access point waits for incoming WPS requests.



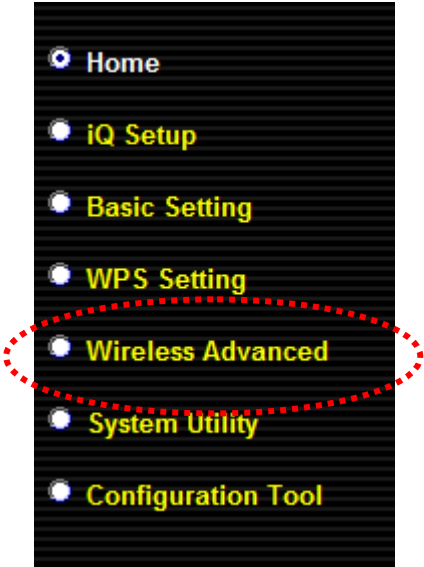
**Note:** When using PBC-type WPS setup, you must press the hardware or software WPS button on the wireless client within 120 seconds. If you do not do so in time, you will need to activate WPS on this access point again.

### III-5. Wireless Advanced

This device has many advanced wireless features, which can be found in the Wireless Advanced menu.



**Note:** The settings in the Wireless Advanced menu are for experienced users only. Please do not change the settings in this menu unless you are sure what they do.



Wireless Advanced	
These settings are only for more technical advanced users who have sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effects the changes will have.	
Fragment Threshold:	2346 (256-2346)
RTS Threshold:	2347 (0-2347)
Beacon Interval:	100 (20-1000 ms)
DTIM Period:	3 (1-10)
Data Rate:	Auto
N Data Rate:	Auto
Channel Width:	<input checked="" type="radio"/> Auto 20/40MHz <input type="radio"/> 20MHz
Preamble Type:	<input checked="" type="radio"/> Short Preamble <input type="radio"/> Long Preamble
Broadcast ESSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
WMM:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
CTS Protect:	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> None
Tx Power:	100 %

Fragment Threshold	Set the Fragment threshold of the wireless radio. <b>Please do not modify the default value if you don't know what this does, the default value is 2346</b>
RTS Threshold	Set the RTS threshold of the wireless radio. <b>Please do not modify the default value if you don't know what this does, the default value is 2347</b>
Beacon Interval	Set the beacon interval of the wireless radio. <b>Please do not modify the default value if you don't know what this does, the default value is 100</b>
DTIM Period	Set the DTIM period of wireless radio. <b>Please do not modify default value if you don't know what it is, the default value is 3</b>
Data Rate	Set the wireless data transfer rate. Since most wireless devices will negotiate with each other and pick a proper data transfer rate automatically, <b>it's not necessary to change this value unless you know what will happen after modification.</b>
N Data Rate	Set the data rate of 802.11n clients, available options are MCS 0 to MCS 15. It's safe to set this option to "Auto" and <b>it's not necessary to change this value unless you know what will happen after modification.</b>
Channel Width	Select wireless channel width (bandwidth used by wireless signals from this access point). It's suggested you select "Auto 20/40MHz". Do not change to "20 MHz" unless you know what that does.
Preamble Type	Set the wireless radio preamble type. <b>Please do not modify the default value if you don't know what this does, the default value is "Short Preamble".</b>
Broadcast ESSID	Decide if the device will broadcast its own ESSID. You can hide the ESSID of your wireless access point (set the option to "Disable"), so only people who know the ESSID of your wireless access point can

	connect to it.
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable WMM, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responses. This improves the performance of such network applications.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It's recommended to set this option to "Auto".
TX Power	You can set the output power of the wireless radio. Unless you're using this wireless access point in a very large space, you may not require 100% output power. <b>This will enhance security (malicious/unknown users in distant areas will not be able to reach your wireless access point).</b>

Click "APPLY" to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE

APPLY

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click "APPLY" to restart the device and implement any changes. The device will restart itself.

### III-5-1. Security

This device provides a variety of wireless security options (wireless data

encryption). When the data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.



**Note:** It is very important to set up wireless security. Without security enabled, hackers or intruders may gain access to your local network and cause damage to your computers and servers.



**Tips:** There are several things you can do to improve your wireless security.

1. Use complicated, hard-to-guess phrases as your security password. Use a random combination of letters, numbers and symbols.
2. Use WPA whenever possible. It's more secure than WEP.
3. Change your security password regularly.

**Security**

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

- **Select SSID**  
SSID choice: Edimax
- **Security Settings**  
Encryption: Disable

Enable 802.1x Authentication

APPLY Cancel

Select SSID	If the device uses multiple SSIDs, you can select the SSID you wish to configure security settings for.
-------------	---

Security Settings	Here you choose the type of encryption you wish to use with this SSID.
-------------------	--

## Disable

When you select “Disable”, wireless encryption for the network is disabled. This means anyone who knows the device’s SSID can connect to it.

## WEP

WEP (Wired Equivalent Privacy) is a common encryption mode, it's generally safe enough for home and personal use. But if you need a higher level of security, please consider using WPA encryption (see next section).

However, some wireless clients don't support WPA, but only support WEP, so WEP is still a good choice if you have such a client in your network environment.

• Security Settings

Encryption	WEP
Key Length	64-bit
Key Format	HEX (10 Characters)
Default Key	Key 1
Key	*****

Enable 802.1x Authentication

Key Length	There are two types of WEP key length: 64-bit and 128-bit. Using “128-bit” is safer than “64-bit”, but will reduce some data transfer performance.
Key Format	There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of the key will be displayed. For example, if you select a “64-bit” key length, and “Hex” as the key format, you’ll see the message “Hex (10 characters)” to the right, which means the length of the WEP key is 10 characters.
Default Key	You can set up to four sets of WEP keys, and you can decide which key is used the default. <b>If you don’t know which one you should use, select “Key 1”.</b>
Key	Input WEP key characters here, the number of characters must be the same as the number displayed in the “Key Format” field. If you select the “ASCII” key format, you can use any alphanumerical characters (0-9, a-z, and A-Z). If you select “Hex” as the key

	format, you can use the characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be same as each other.
Enable 802.1x Authentication	Check this box to enable 802.1x user authentication. Please refer to Section 2-7-5 for detailed instructions.

## WPA pre-shared key

WPA pre-shared key is the safest encryption method, and it's recommended to use this encryption type to safeguard the integrity of your data.

WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. AES is safer than TKIP, but not every wireless client supports it. Please make sure your wireless client supports the cipher you selected.
Pre-shared Key Format	Please select the format of the pre-shared key here, available options are “Passphrase” (8 to 63 alphanumerical characters) and “Hex (64 characters)” – 0 to 9 and a to f.
Key	Please enter the key according to the key format you selected above. For security reasons, it's best to use a complex, hard-to-guess key.

## WPA RADIUS



WPA RADIUS is a combination of WPA encryption and RADIUS user authentication. If you have a RADIUS authentication server, you can check the identity of every wireless client by using a user database.

**Security**

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

- **Select SSID**

SSID choice	Edimax ▾
-------------	----------

- **Security Settings**

Encryption	WPA RADIUS ▾
WPA Unicast Cipher Suite	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
RADIUS Server IP Address :	<input type="text"/>
RADIUS Server Port :	1812
RADIUS Server Password :	<input type="text"/>

WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. AES is safer than TKIP, but not every wireless client supports it. Please make sure your wireless client supports the cipher you selected.
RADIUS Server IP address	Enter the IP address of the RADIUS authentication server here.
RADIUS Server Port	Enter the port number of the RADIUS authentication server here. Default value is 1812.
RADIUS Server Password	Enter the password of the RADIUS authentication server here.

## Enable 802.1x Authentication

When you select “Disable” or “WEP” as your encryption type, you will have the option of enabling 802.1x authentication based on a RADIUS user authentication server. Check the “Enable 802.1x Authentication” box to activate it.

**Enable 802.1x Authentication**

RADIUS Server IP Address :	<input type="text"/>
RADIUS Server Port :	1812
RADIUS Server Password :	<input type="text"/>

Enable 802.1x Authentication	Enable or disable the use of 802.1x user authentication.
RADIUS Server IP Address	Enter the IP address of the RADIUS authentication server here.
RADIUS Server Port	Enter the port number of the RADIUS authentication server here. Default value is 1812.
RADIUS Server Password	Enter the password of the RADIUS authentication server here.

After you've set your security options, click "APPLY" to make changes take effect. The following message will appear:

**Settings saved successfully!**

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE

APPLY

Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click "APPLY" to restart the device and implement any changes. The device will restart itself.

### III-5-2. MAC Filtering

The MAC filtering feature allows you to define a "white list" of wireless devices permitted to connect to this access point. Devices are identified by their unique MAC address. When devices not on the white list of MAC addresses attempt to connect to this access point, they will be denied.

### MAC Address Filtering

For security reason, the Access Point features MAC Address Filtering that only allows authorized MAC Addresses associating to the Access Point.

Select SSID: Edimax

**• MAC Address Filtering Table**  
It allows to entry 64 sets address only.

NO.	MAC Address	Comment	Select
1	11:11:11:11:11:11		<input type="checkbox"/>
2	11:11:11:22:22:22		<input type="checkbox"/>

Enable Wireless Access Control

MAC Address: 
 Comment:

Select SSID (1)

Address filtering table (2)

Add new entries here (3)

(1) Select SSID: Here you select the SSID you wish to configure.

(2) MAC Address Filtering Table: This table lists the MAC addresses you have currently added to the white list.

(3) Here you enter the information for new MAC addresses to add to the white list.

Select	Check this box to select one or more MAC address(es) for deletion.
Delete Selected	Click this button to delete all selected MAC address(es).
Delete All	Delete all MAC addresses in the table.
Reset	Uncheck all selected MAC address entries.
Enable Wireless Access Control	Check this box to enable MAC address filtering. If unchecked, no MAC restrictions will be enforced, and any wireless client with proper encryption settings will be able to connect to this wireless access point.
MAC address	Input a MAC address allowed using this wireless access point here. Do not add any colons (:) or hyphens (-) only enter 0 to 9 and a to f here, such as "112233445566" or "aabbccddeeff".

Comment	You can input any text here as the comment of this MAC address, such as “ROOM 2A Computer” or something else to identify the MAC address. You can enter up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it’s recommended to use this field to write a comment for every MAC addresses as a memory aid.
Add	When you finish entering the MAC address and (optional) comment, click this button to add the MAC address entry to the list.
Clear	Remove all characters in the “MAC address” and “Comments” fields.

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE

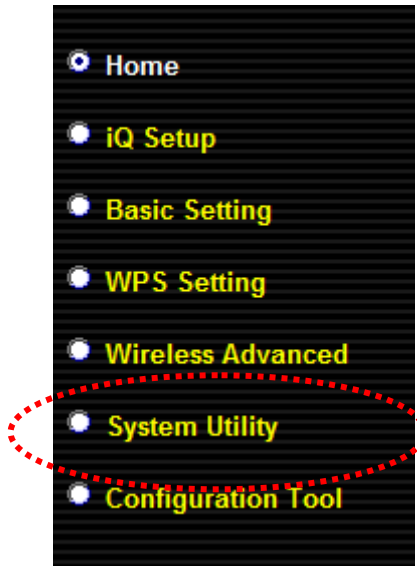
APPLY

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

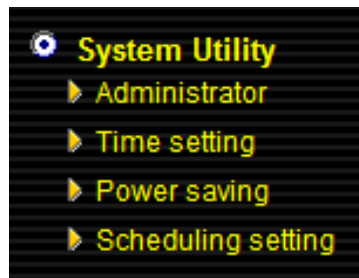
Click “APPLY” to restart the device and implement any changes. The device will restart itself.

## III-6. System Utility

You can configure basic system and administrative parameters by selecting “System Utility” from the sidebar.



“System Utility” consists of four main functions.



The default screen you will see upon selecting “System Utility” is the “Administrator” screen.

### III-6-1. Administrator

#### Password Settings

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

• Password Settings

Current Password :	<input type="text"/>
New Password :	<input type="text"/>
Re-Enter Password :	<input type="text"/>

Current Password	Enter your current password. The default password is <b>1234</b> .
------------------	--

New Password	Enter your desired new password here. You can use any combination of letters, numbers and symbols up to 20 characters.
Re-Enter Password	Confirm your new password.

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.



Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

## Management IP

You can modify the IP address of the access point, enabling it to become a part of your local area network. To do so, select “Use the following IP address” and input the information manually.

Or you can select “Obtain an IP address automatically” which will assign an automatic IP address to the access point. **(Windows PCs only)**



**Note:** If you choose “Obtain an IP address automatically” then you will need to use the access key ([http://edimax\\*\\*\\*\\*\\*](http://edimax*****)) to access the browser-based configuration device. This is because the access point will act as a DHCP client and receive a dynamic IP from the DHCP server, i.e. your broadband router.



**Note:** Mac users, please do not select “Obtain an IP address automatically”.

• Management IP

<input type="radio"/> Obtain an IP address automatically	
<input checked="" type="radio"/> Use the following IP address	
IP Address :	192.168.2.2
Subnet Mask :	255.255.255.0
Gateway Address :	

IP Address	Specify an IP address here. This IP address will be assigned to your access point, and will replace the default IP address 192.168.2.2.
Subnet Mask	Input the subnet mask of the new IP address.
Gateway Address	Input the network's gateway IP address.

Typically, your ISP will provide you with such information as IP address, subnet mask and gateway address.



**Note:** Please write down and remember the new IP address you assigned to the access point. If you forget this IP address you will not be able to connect to the browser-based configuration interface in the future.



**Note:** To reset the IP address back to its default value of 192.168.2.2, press and hold the **WPS** button on the access point for 10 seconds. Be aware that doing so restores **all** settings and passwords back to factory defaults.

Click "APPLY" to make changes take effect. The following message will appear:

**Settings saved successfully!**

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

## DHCP Server

The access point can be configured to act as a DHCP server for your network. By default DHCP is disabled.

• DHCP Server

DHCP Server :	Enabled ▾
Default Gateway :	192.168.2.2
Domain Name Server IP :	0.0.0.0
Start IP :	192.168.2.100
End IP :	192.168.2.200
Domain Name :	
Lease Time :	Forever ▾

DHCP Server	Select “Enabled” to enable DHCP server functionality. Select “Disabled” to disable it, in which case subsequent fields will be grayed out.
Default Gateway	Input the IP address of the default gateway of your network here.
Domain Name Server IP	Input the IP address of the domain name server (DNS).
Start IP	Input the start address of the IP range.
End IP	Input the end address of the IP range.
Domain Name	Input the domain name for your network (optional).
Lease Time	Specify a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by the access point.



Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.



Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

### III-6-2. Time Setting

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.

#### Time setting

Set the time zone of device system by synchronizing with time server, this information is used for scheduling configuration.

Time Zone	(GMT-12:00)Eniwetok, Kwajalein
Time Server Address	<input type="radio"/> asia.pool.ntp.org-Asia <input checked="" type="radio"/> 0.0.0.0 (Manual IP Setting)
Daylight Savings	<input type="checkbox"/> Enable Function January 1 To January 1

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.
Time Server Address	This access point supports NTP (Network Time Protocol) for automatic time and date setup. Choose a time server from the drop down menu, or input the host name or IP address of the IP server manually.
Daylight Savings	If your country/region uses daylight saving time, please check the “Enable Function” box and select the start and end date.

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

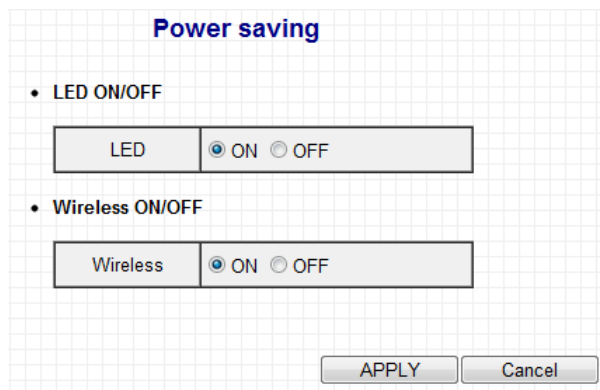


Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

### III-6-3. Power Saving

You can configure the operation of the LEDs and wireless capability of the access point in order the conserve power.



LED ON/OFF	Select “ON” or “OFF” to switch the LEDs on or off accordingly.
Wireless ON/OFF	Select “ON” or “OFF” to switch the wireless capability of the access point on or off accordingly.

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.



Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

### III-6-4. Scheduling setting

The access point includes a scheduling function, where power saving functions and an automatic reboot can be automated for specific times. By default, scheduling setting is disabled. Please select “Enable” if you wish to continue.



**Note:** Ensure you have configured the time settings of your access point before you enable scheduling.

**Scheduling setting**

Schedule Table (Up to 10 sets) :  Enable  Disable

NO.	Service	Schedule description	Schedule	Select
<input type="button" value="Add"/>				
<input type="button" value="APPLY"/> <input type="button" value="Cancel"/>				

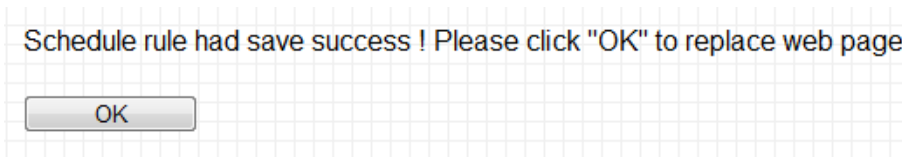
Click “Add” to open a new screen and create a scheduled event.

Service : Wireless off ▼      Schedule description :

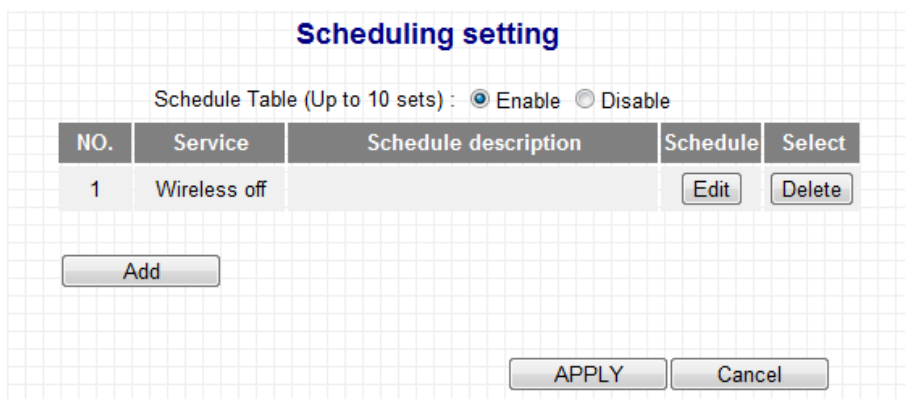
	Start Time (hh.mm)	End Time (hh.mm)	Select
Sunday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>
Monday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>
Tuesday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>
Wednesday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>
Thursday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>
Friday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>
Saturday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>
Everday	0 ▼ : 0 ▼	0 ▼ : 0 ▼	<input type="checkbox"/>

Service	Select the event to be scheduled from the drop down menu. "Wireless off" will disable the wireless capability of the access point, "Led off" will switch off the LEDs and "Auto reboot" will restart the device.
Schedule Description	Assign the event a name or description for reference (optional).
Start Time	Specify a start time (hh.mm) for the event, for a specific day or to recur every day.
End Time	Specify an end time (hh.mm) for the event, for a specific day or to recur every day.
Select	Check the box to select and confirm your event.

Click "Save" to save your scheduled event. The following message will appear:



Click "OK" to return to the "Scheduling setting" screen. You should now see your scheduled event listed.



Up to 10 events can be scheduled, and you can edit or delete each event.

Edit	Click "Edit" to change the type, description, start time or end time of the scheduled event.
------	--

Delete	Click “Delete” to delete the event permanently.
--------	---

Click “APPLY” to make changes take effect. The following message will appear:

### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

CONTINUE

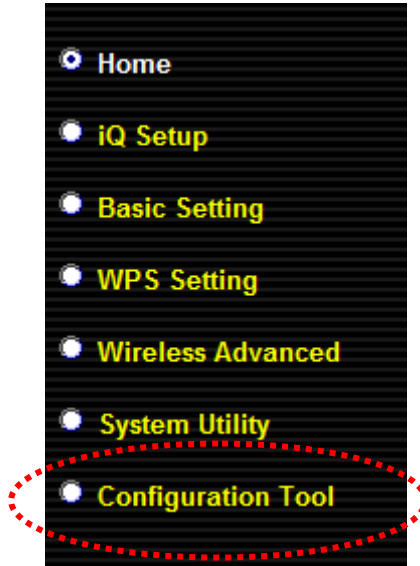
APPLY

Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

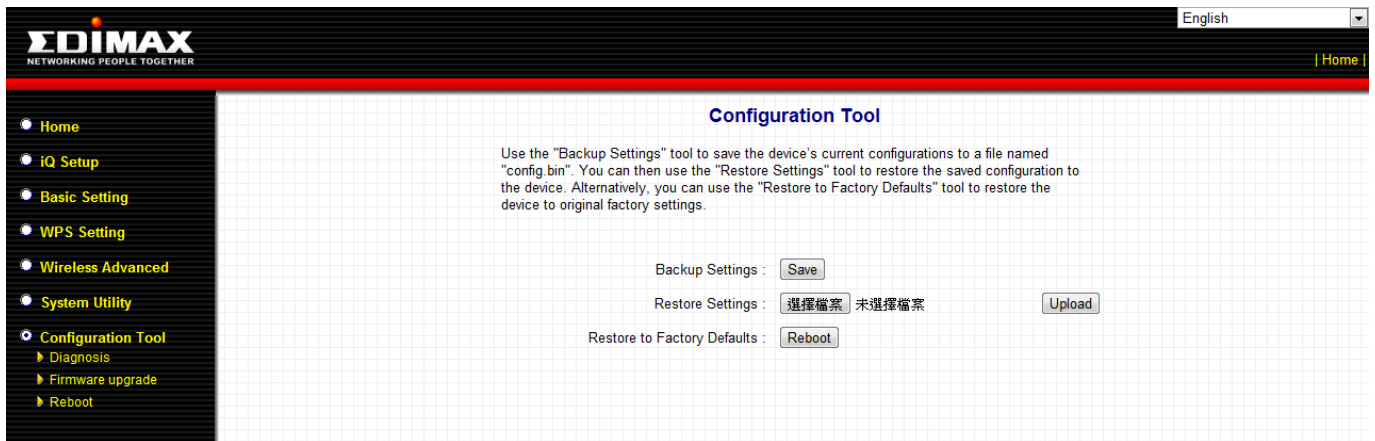
Click “APPLY” to restart the device and implement any changes. The device will restart itself.

### III-7. Configuration Tool

The access point’s configuration tool enables you to back up the settings, upgrade the firmware and reset the device. Select “Configuration tool” from the sidebar.



You will see the following screen:




Backup Settings	Click “Save” to save the current settings on your computer as config.bin file.
Restore Settings	Click the browse button to find a previously saved config.bin file and then click “Upload” to replace your current settings.
Restore to Factory Defaults	Click “Reset” to restore settings to the factory default. A pop-up window will appear and ask you to confirm and enter your log in details. Enter your username and

password and click “Ok”. See below for more information.







**Note:** Restoring settings to the factory default will restore **all** settings, configurations and passwords back to the factory default.



**Note:** You can also reset the device to the factory default by pressing and holding the **Reset/WPS** button for 10 seconds, until the Power LED (  ) goes out. The **Reset/WPS** button is located on the front panel of the device.

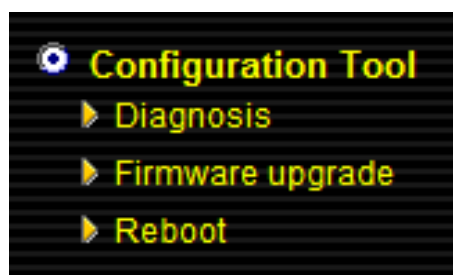
## Restore to factory defaults

When you restore to factory defaults, the Power LED (  ) on the device will go out. The access point will then begin its initialization process. The Wi-Fi LED (  ) will flash rapidly, until the Power LED (  ) lights back up. When the Power LED (  ) lights up and stays on steadily, the device has successfully reinitialized and is ready for further configuration.



**Note:** Take care to hold down the **Reset/WPS** button for at least 10 seconds. Releasing the button too early will cause the device to enter WPS connection mode.

In the sidebar, there are 3 further tools within the “Configuration Tools” menu.



### III-7-1. Diagnosis

Using the diagnosis tool, you can ping a specific IP address and automatically reboot the device if there is no response.

**Diagnosis**

This device can ping a specific IP address, if can't get response from ping, device will be rebooted automatically.

Watchdog and reboot device :  Enable  Disable

Ping address	<input type="text" value="0.0.0.1"/>
Time interval	<input type="text" value="1"/> (1~60 minutes, default:1)

Watchdog and reboot device	Select “Enable” or “Disable” for the automatic reboot function.
Ping Address	Specify the IP address to ping.
Time interval	Specify the frequency of the ping as a time interval, in minutes. Enter a value from 1-60.

Click “APPLY” to make changes take effect. The following message will appear:

**Settings saved successfully!**

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.

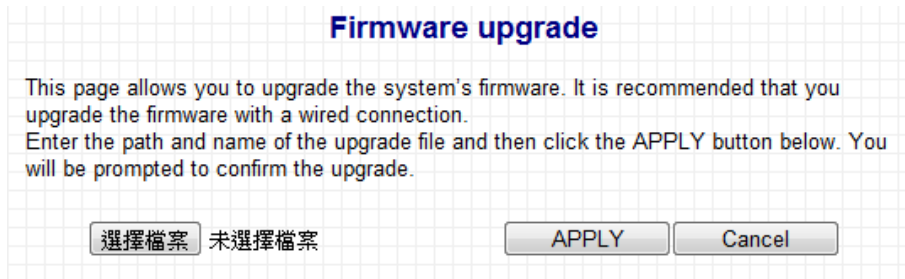
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.



### III-7-2. Firmware Upgrade

Selecting “Firmware upgrade” from the “Configuration Tool” menu allows you to update the system firmware to a more recent version. You can download the latest firmware from the Edimax website.



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



**Note:** It is recommended that you use a wired Ethernet connection to upload the firmware file.

Click on the browse button to open a window and locate the downloaded firmware file in your computer. Confirm your selection and click “APPLY” to make changes take effect. The following message will appear:

#### Settings saved successfully!

Click CONTINUE to continue other configuring settings, or click APPLY to restart the system and make the changes take effect.



Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

Click “APPLY” to restart the device and implement any changes. The device will restart itself.

### III-7-3. Reboot

If the access point malfunctions or is not responding, then it is recommended that you reboot the device. This is useful if the location of the access point is not convenient.

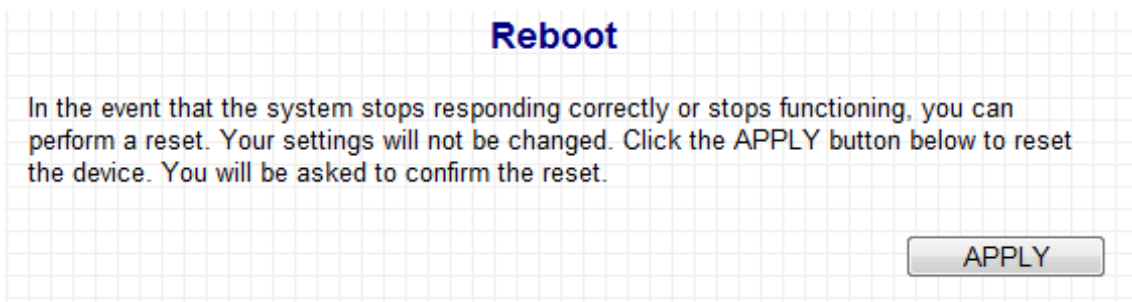


**Note:** If the access point is still not responding after a system reboot, switch off the device by unplugging the power supply. Plug it back in after 10 seconds.

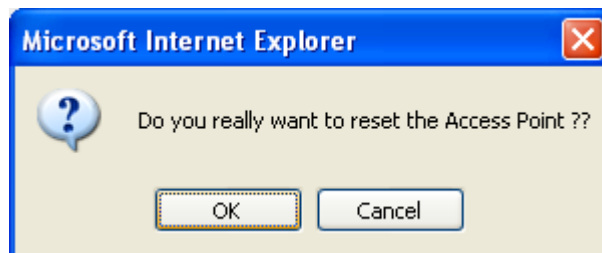


**Note:** Rebooting the access point will not affect the current configuration of the device.

To reboot the device, please click “Reboot” from the “Configuration Tool” menu in the sidebar. The following screen will be displayed:



Click “Apply” to reboot the device.



A pop up window will ask you to confirm, please click “Ok” to confirm or “Cancel” to abort. If you click “Ok” to continue, all connections between wireless client and access will be disconnected at this point.

You will see the following screen, and a timer will count down from 60 seconds. When the timer reaches zero, click “OK” to return to the browser-based configuration interface.

**System restarting. Please wait for a moment.**

OK(55)

## IV. APPENDIX

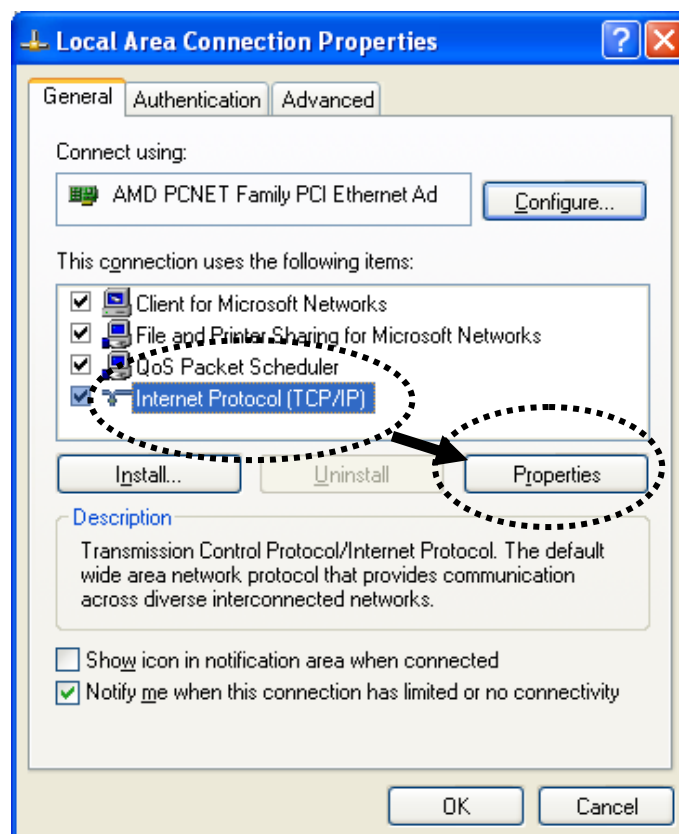
### IV-1. Configuring your IP address

The access point uses the default IP address 192.168.2.2, which may not be in the same IP address subnet of your network; meaning you are unable to access the browser based configuration interface. In this case, you need to modify the IP address of your PC or Macintosh to 192.168.2.10, in order to access the browser-based configuration interface.

The procedure for doing so varies across different operating systems; please follow the guide appropriate for your operating system.

#### IV-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”.

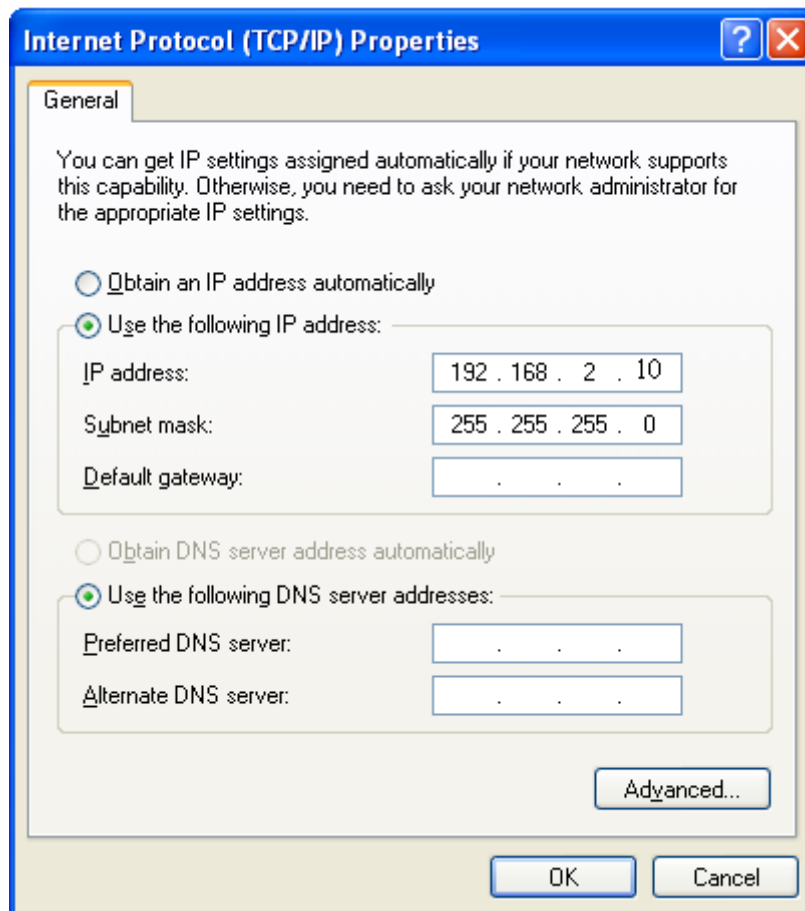


2. Select “Use the following IP address”, then input the following values:

**IP address:** 192.168.2.10

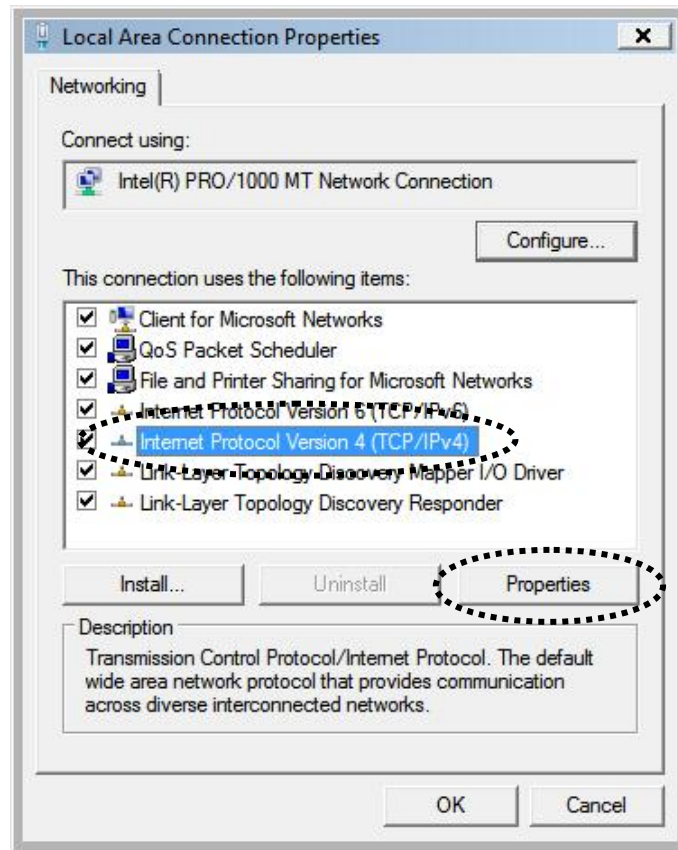
**Subnet Mask:** 255.255.255.0

Click ‘OK’ when finished.



## IV-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”.

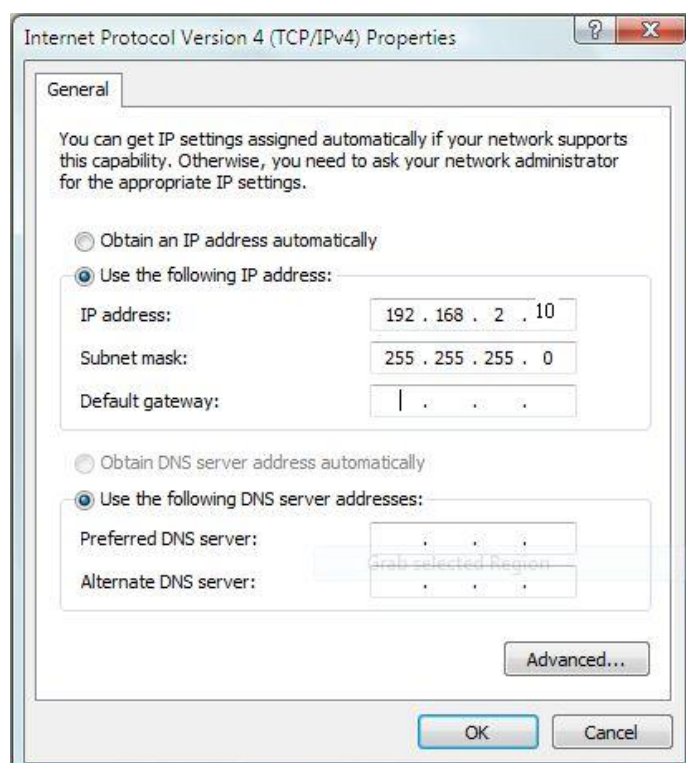


2. Select “Use the following IP address”, then input the following values:

**IP address:** 192.168.2.10

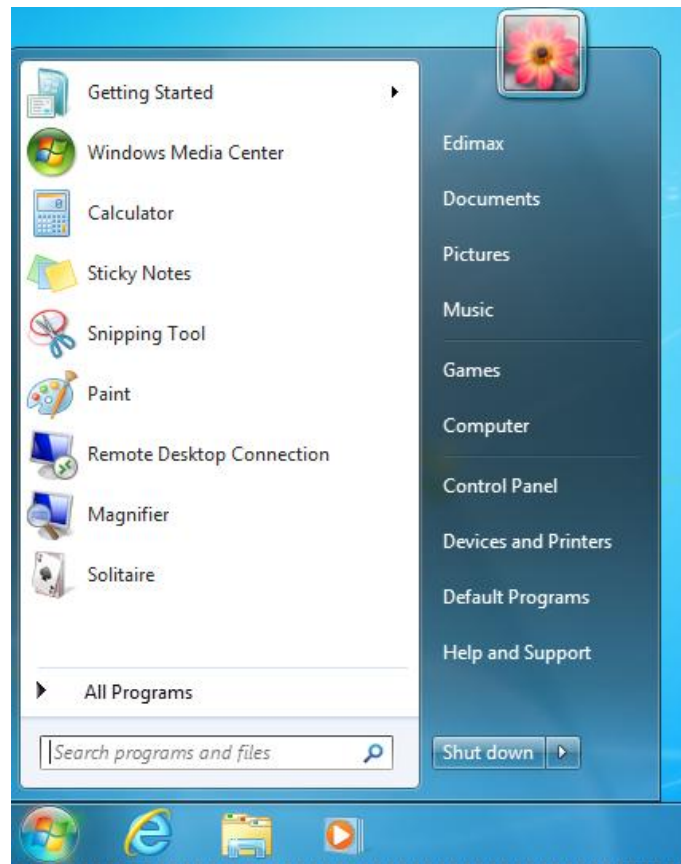
**Subnet Mask:** 255.255.255.0

Click ‘OK’ when finished.

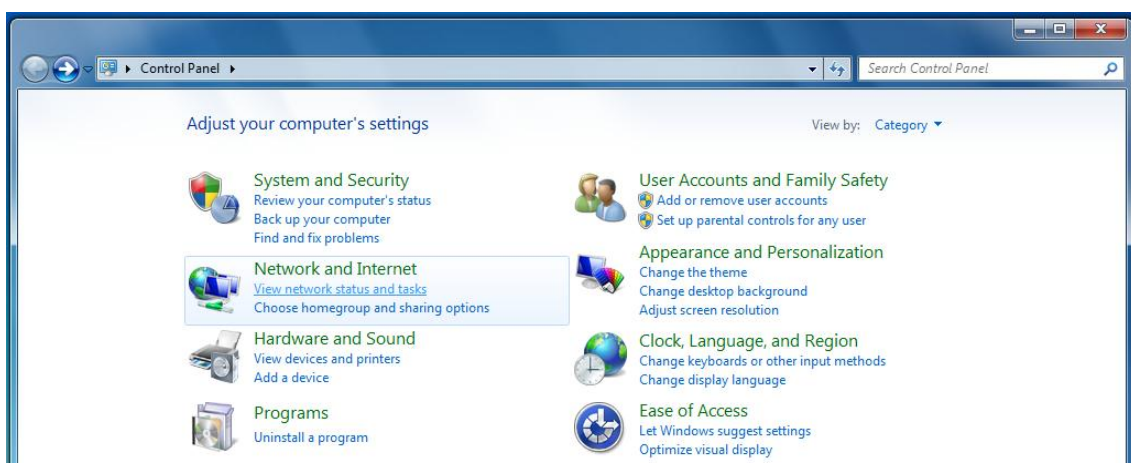


### IV-1-3. Windows 7

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




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





3. Click “Local Area Connection”.

## View your basic network information and set up connections

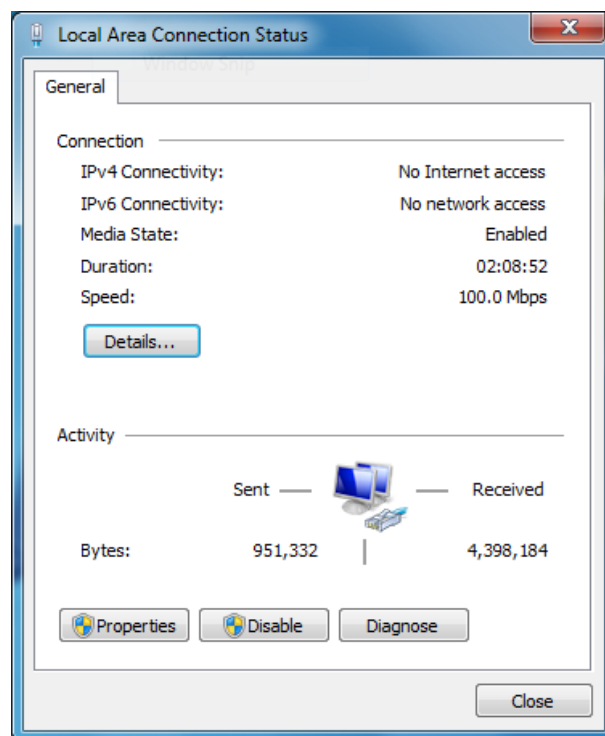
TS-WIN7 (This computer) — Home network —  — Internet [See full map](#)

View your active networks [Connect or disconnect](#)

 **Home network**  
Home network

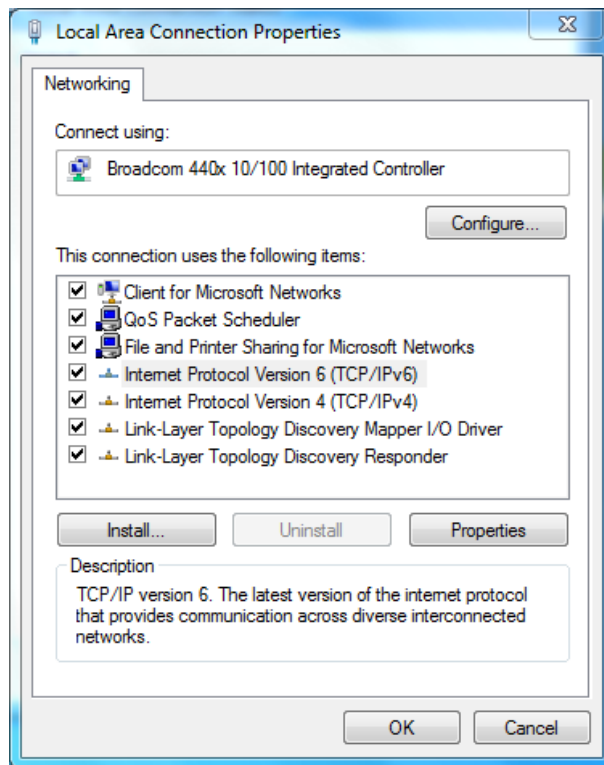
Access type: No Internet access  
HomeGroup: [Ready to create](#)  
Connections:  [Local Area Connection](#)

4. Click “Properties”.



5. Select “Internet Protocol Version 4 (TCP/IPv6) and then click “Properties”.



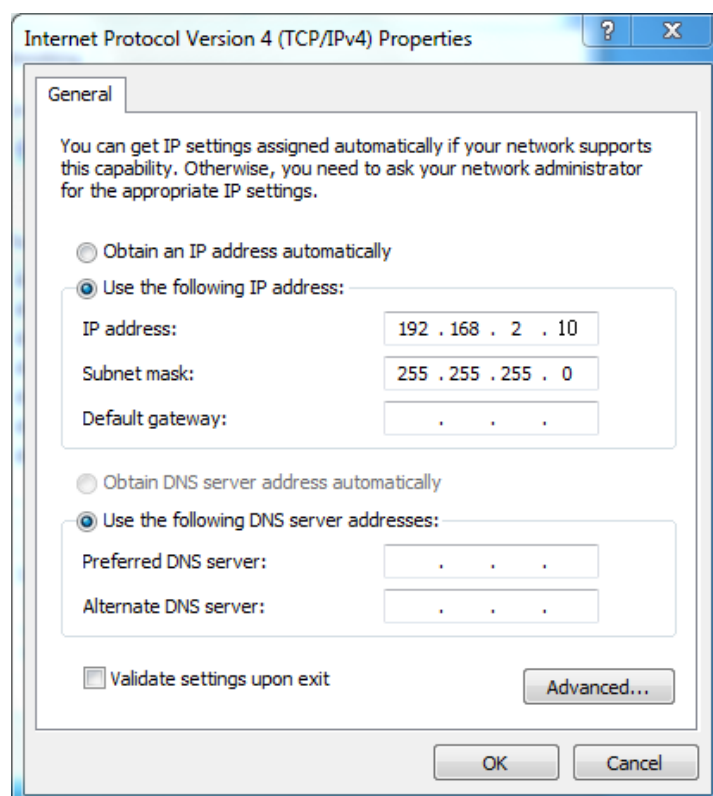


6. Select “Use the following IP address”, then input the following values:

**IP address:** 192.168.2.10

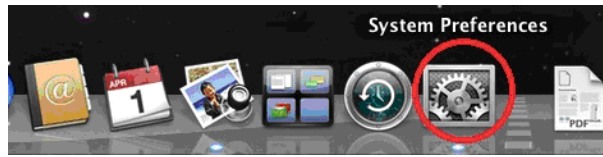
**Subnet Mask:** 255.255.255.0

Click ‘OK’ when finished.



## IV-1-4. Mac OS

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



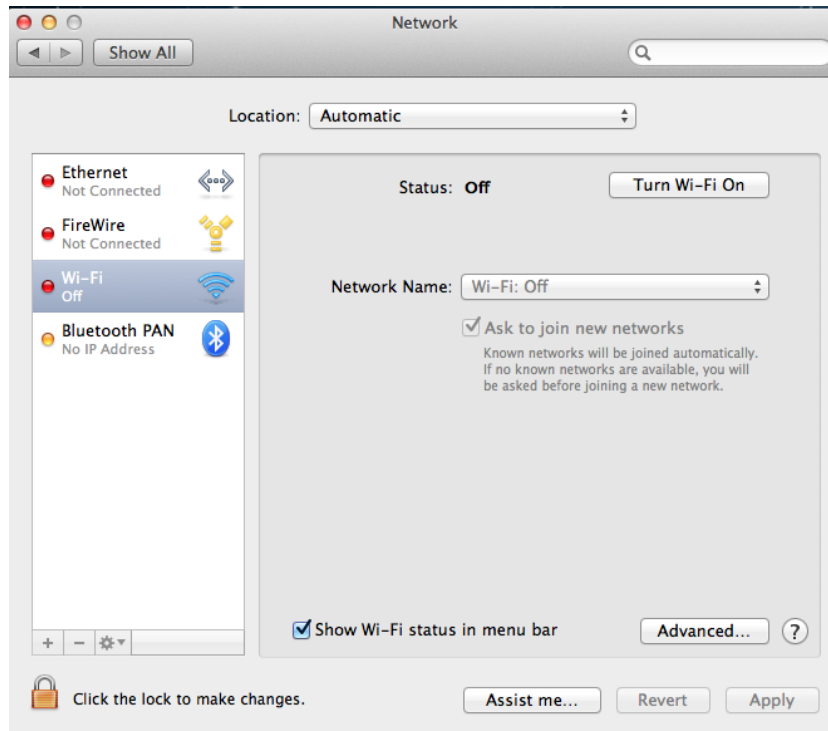
2. In System Preferences, click on “Network”.



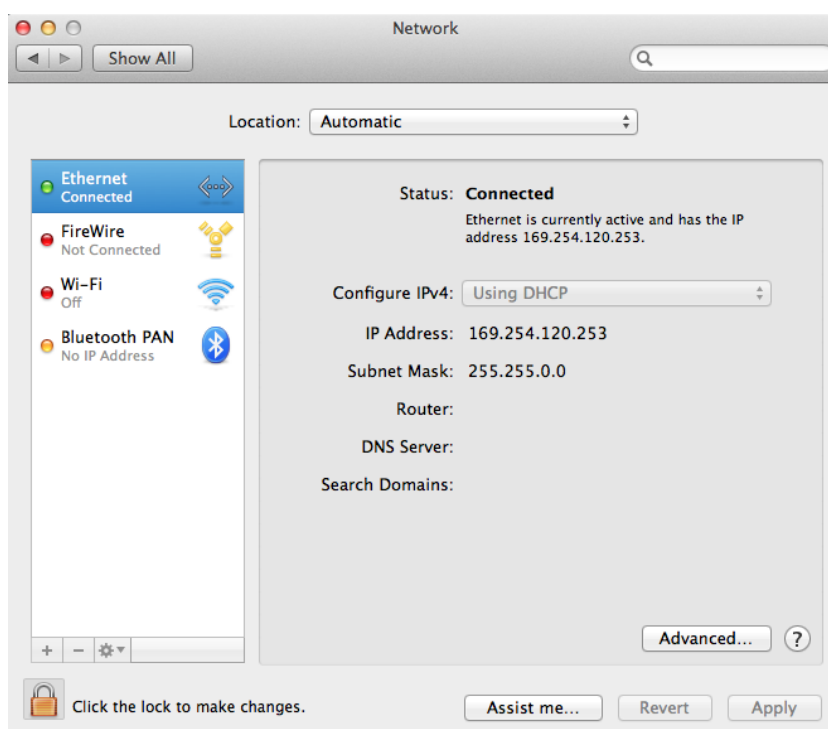
3. Here you will see all of your network connections. You need to remove any Ethernet cable that may be connected, so that the “Ethernet” status in the left sidebar displays “Not Connected”, as shown below. Then, you need to switch off your Macintosh’s Wi-Fi. Select “Wi-Fi” from the left sidebar.



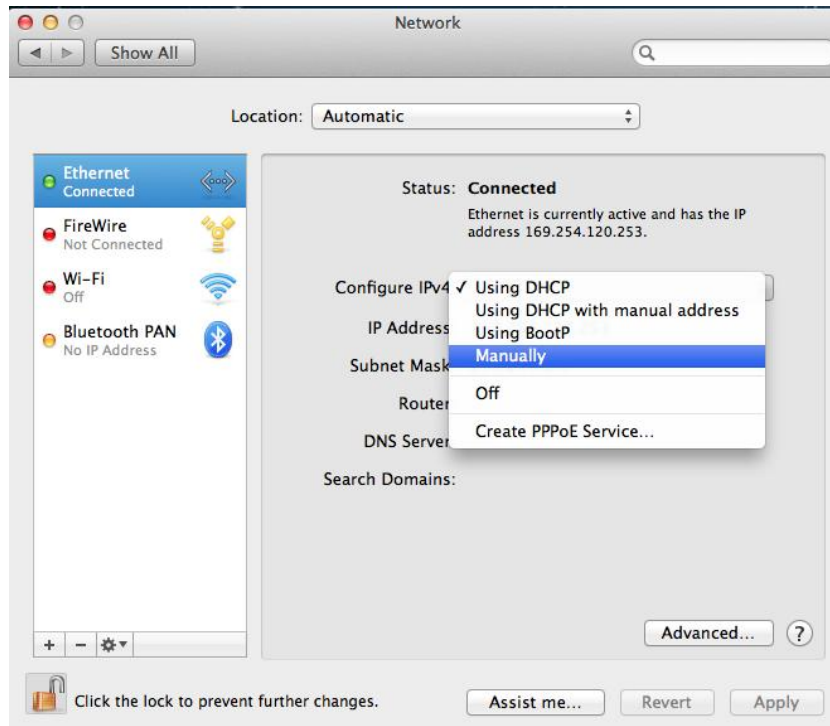
4. If your Wi-Fi is switched on, click on the button labeled “Turn Wi-Fi Off”. The “Network” screen should now look like the screen below, where under the heading “Wi-Fi” in the left sidebar, the status is shown as “Off”.



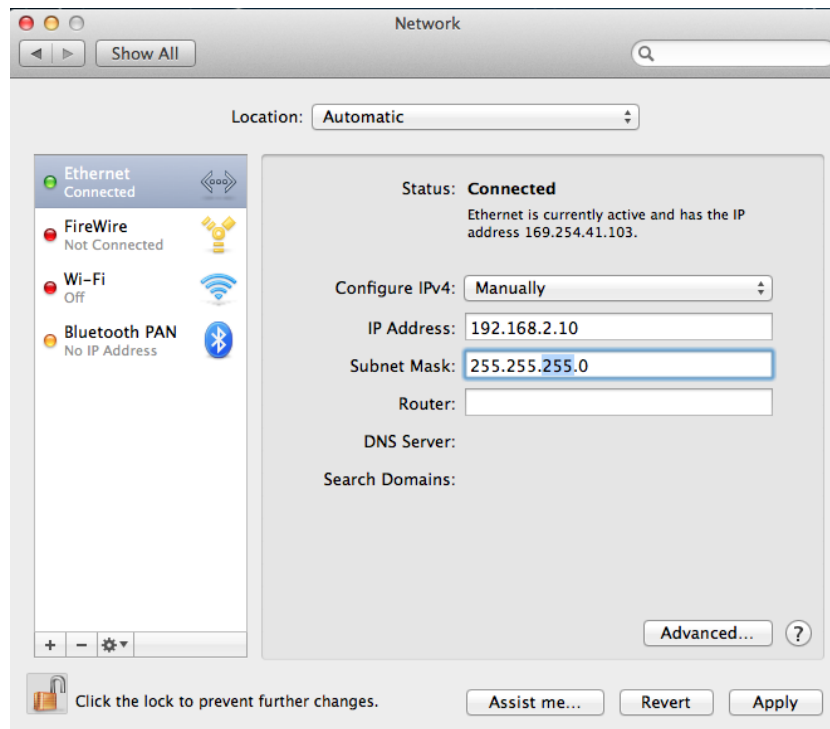
5. Connect one end of an Ethernet cable to the Ethernet port on your computer. Connect the other end to an Ethernet port on the access point.
6. Plug the power adapter into the device's 5V power port, and plug the adapter into a wall socket. The PWR LED and corresponding LAN LED should light up.
7. Network Preferences will now display an Ethernet adapter, as shown below. The status of "Ethernet" should be "Connected".



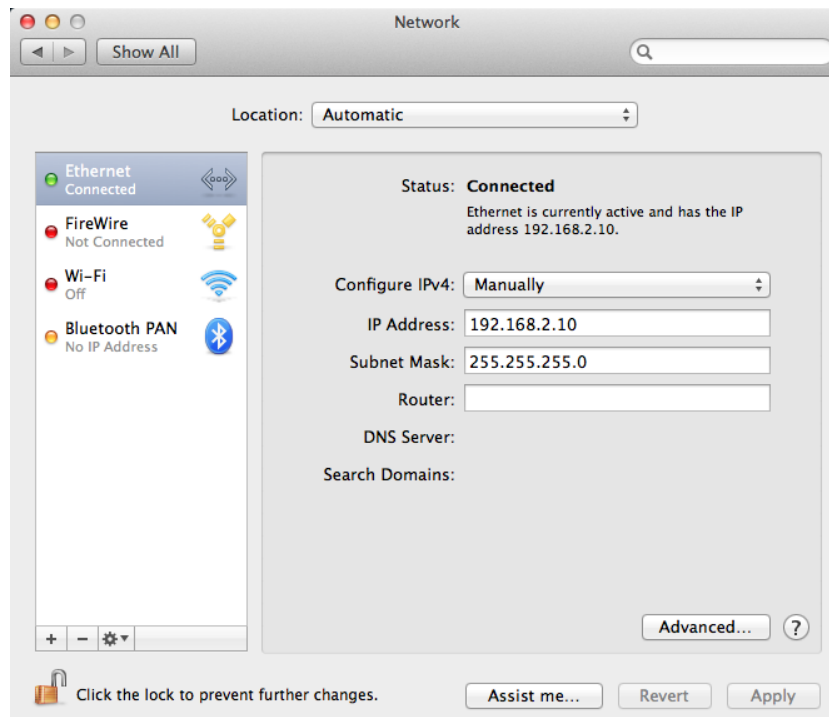
8. Click on “Ethernet” in the left panel and then click the drop down arrow for the menu labeled “Configure IPv4” in the right panel. From the drop down menu, select “Manually”.



9. In the panel on the right side, enter IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on “Apply”.



10. In the left sidebar, “Ethernet” should now display “Connected” as shown below. In the right panel, you should see the IP address 192.168.2.10 and subnet mask 255.255.255.0.



## IV-2. Troubleshooting

If you are experiencing problems with your access point, please refer to this troubleshooting guide before contacting your dealer of purchase for help.

Scenario	Solution
I can't log onto the browser-based configuration interface: the access point is not responding.	<ol style="list-style-type: none"><li>a. Please check the connection of the power cord and network cable. All cords and cables should be correctly and firmly inserted.</li><li>b. Check the LEDs on the front panel. If all the LEDs are out, then check the A/C power adapter.</li><li>c. Make sure you are using the correct IP address.</li><li>d. If you are using a MAC or IP address filter, try to connect the access point to another computer.</li><li>e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can obtain an IP address.</li><li>f. If you are experiencing problems after a firmware upgrade, please contact your dealer of purchase for help.</li><li>g. If all of the above solutions don't work, contact your dealer of purchase for help.</li></ol>
I can't establish a connection to my wireless access point.	<ol style="list-style-type: none"><li>a. If encryption is enabled, please re-check WEP or WPA passphrase settings on your wireless client.</li><li>b. Try moving closer to the wireless access point.</li><li>c. Unplug the A/C adapter of the access point, and plug it back again after 10 seconds.</li><li>d. Check the LEDs on the front panel. If all the LEDs are out, then check the A/C power adapter.</li></ol>
I can't locate the access point with	<ol style="list-style-type: none"><li>a. Check if "Broadcast ESSID" (in the "Wireless Advanced" section of the</li></ol>

my wireless client.	<p>browser-based configuration interface) is “Enabled” or “Disabled”. If “Disabled” you need to input the ESSID into your wireless client manually.</p> <p>b. Try moving closer to the wireless access point.</p>
File downloads are very slow or frequently interrupted.	<p>a. Reset the access point.</p> <p>b. Try again later. Your local network may be experiencing technical difficulties or very high usage.</p> <p>c. Change channel number.</p>
I can't log onto the browser-based configuration interface: incorrect password.	<p>a. Password is case-sensitive. Make sure the “Caps Lock” light is not illuminated.</p> <p>b. If you do not know your password, restore the device to factory settings.</p>
The access point is extremely hot.	<p>a. It is normal for the access point to heat up during frequent use. If you can safely place your hand on the access point, the temperature of the device is at a normal level.</p> <p>b. If you smell burning or see smoke coming from access point or A/C power adapter, then disconnect the access point and A/C power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.</p>

### IV-3. Glossary

**Default Gateway (Access point):** Every non-access point IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

**DHCP:** Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

**DNS Server IP Address:** DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as `www.Broadbandaccesspoint.com`) and one or more IP addresses (such as `192.34.45.8`). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "`Broadbandaccesspoint.com`" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

**DSL Modem:** DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

**Ethernet:** A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

**Idle Timeout:** Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

**IP Address and Network (Subnet) Mask:** IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: `192.168.2.1`. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": `aaa.aaa.aaa.aaa`, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers



separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's. When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000

It means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

**ISP Gateway Address:** (see ISP for definition). The ISP Gateway Address is an IP address for the Internet access point located at the ISP's office.

**ISP:** Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

**LAN:** Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

**MAC Address:** MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

**NAT:** Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband access point's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

**Port:** Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

**PPPoE:** Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers.

**Protocol:** A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

**Access point:** A access point is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

**Subnet Mask:** A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a

particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

**TCP/IP, UDP:** Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocols. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

**WAN:** Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

**Web-based management Graphical User Interface (GUI):** Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.



**Edimax Technology co., Ltd**  
6F., No.3, Wu-Chuan 3rd Road, Wu-Gu,  
New Taipei

**Edimax Technology Europe B.V.**  
Nijverheidsweg 25 5683 CJ Best  
The Netherlands

**Edimax Computer Company**  
3350 Scott Blvd., Bldg.15 Santa Clara,  
CA 95054, USA