

EW-7416APn v2 & EW-7415PDn

User Manual

12-2012 / v1.1



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 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

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

I. Product Information	5
I-1. Package Contents	5
I-2. Description	5
I-3. Safety Information	8
I-4. System Requirements	8
II. Quick Installation	9
II-1. Mac	9
II-2. Windows	13
II-2-1. Access Point Mode	15
II-2-2. AP Client Mode	17
II-2-3. Repeater Mode (Wi-Fi Extender)	19
II-6. Hardware Installation	21
III. Browser Based Configuration Interface	22
III-1. Home	25
III-2. Basic Settings	27
III-2-1. AP Mode	28
III-2-2. Station Infrastructure Mode	29
III-2-3. AP Bridge-Point to Point Mode	31
III-2-4. AP Bridge-Point to Multi-Point Mode	32
III-2-5. AP Bridge-WDS	33
III-2-6. Universal Repeater Mode	34
III-3. WPS Setting	36
III-4. Advanced Settings	38
III-5. Security	41
III-5-1. Disable	42
III-5-2. Enable 802.1x Authentication	42
III-5-3. WEP	43
III-5-4. WPA Pre-Shared Key	44
III-5-5. WPA Radius	45
III-6. Radius Server	47
III-7. MAC Filtering	49
III-8. System Utility	51
III-8-1. Password Settings	51
III-8-2. Management IP	52
III-8-3. DHCP Server	53
III-9. Configuration Tool	55
III-10. Upgrade	56
III-11. Reset	57
IV. APPENDIX	60
IV-1. Configuring your IP address	60
IV-1-1. Windows XP	60
IV-1-2. Windows Vista	62

IV-1-3. Windows 7	63
IV-1-4. Windows 8	67
IV-1-5. Mac OS	71
IV-2. How to Find your Network Security Key	74
IV-2-1. Windows 7 & Windows Vista	74
IV-2-2. Windows 8	76
IV-2-3. Mac	78
IV-3. Troubleshooting	81
IV-4. Glossary	82
IV-5. Technical Support	85

I. Product Information

Thank you for purchasing an Edimax EW-7416APn V2/EW-7415PDn wireless access point. This product provides wireless access to an existing wired Ethernet network, at speeds of up to 300Mbps for 802.11n compatible wireless devices.

I-1. Package Contents

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

- Wireless access point x 1
- CD (EZmax Setup Wizard, Multi-language Quick Installation Guide and User Manual) x 1
- Power adapter x 1
- 3dBi antenna x 2
- Accessory kit x 1
- Quick installation guide x 1

I-2. Description

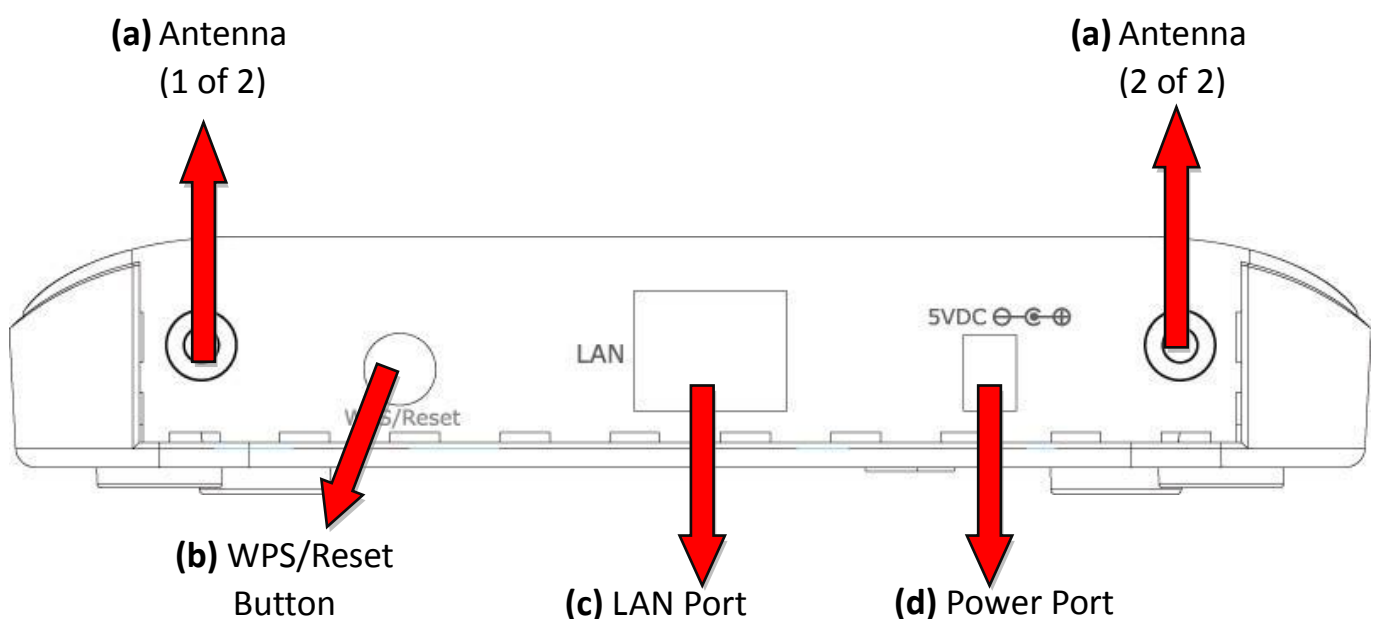
Front panel



Item	Color	Status	Description
PWR (Power)	Green	On	Device is powered.
		Flashing	Device is booting up/resetting.
		Off	Device is not powered.
WLAN	Orange	On	WPS mode is enabled.

(Wireless LAN)		Flashing	Data is being transmitted wirelessly.
		Off	Data is not being transmitted wirelessly.
LAN	Green	On	Ethernet port is connected to a valid device.
		Flashing	Data is being transmitted through the Ethernet cable.
		Off	No valid connection.

Back panel



a. Antenna Connector

This is where you connect the antennas. It is a round connector (standard reverse SMA).

b. WPS/Reset Button

Press this button for less than 5 seconds to activate the WPS function. Press and hold this button for 10 seconds, until the PWR LED starts flashing, to reset the access point to factory default settings.

c. LAN Port

Connects this access point to other Ethernet devices (switches, routers or other wired network devices) – for the EW-7415PDn this is where you connect the access point to a PoE switch.

d. 5V DC

This is where you connect the power adapter.

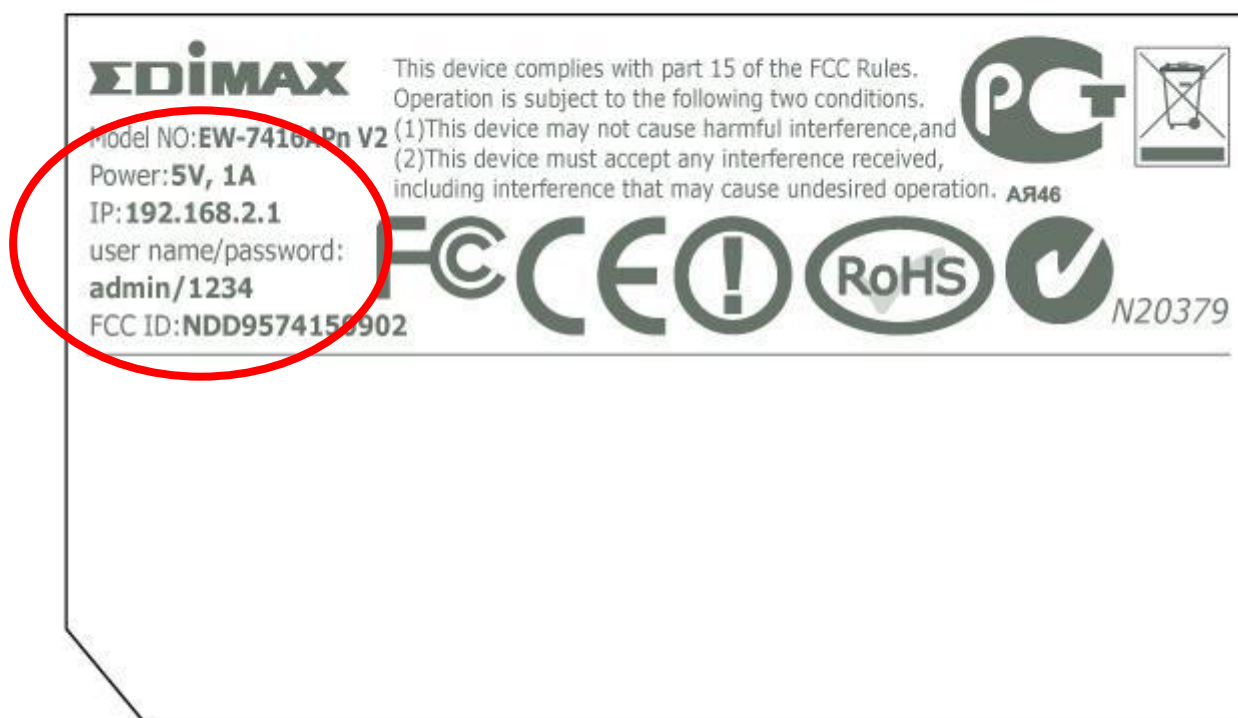


Note: If you are using the EW-7415PDn with a PoE switch, you **do not** need to connect the power adapter.

Product Label

The product label on the underside of the device displays the default IP address, username and password of the access point.

50x30mm



I-3. Safety Information

In order to ensure the safe operation of the access point 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. Take care when moving and handling the access point; accidental damage is not covered by the access point's warranty.
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 the access point, then disconnect the access point immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

I-4. System Requirements

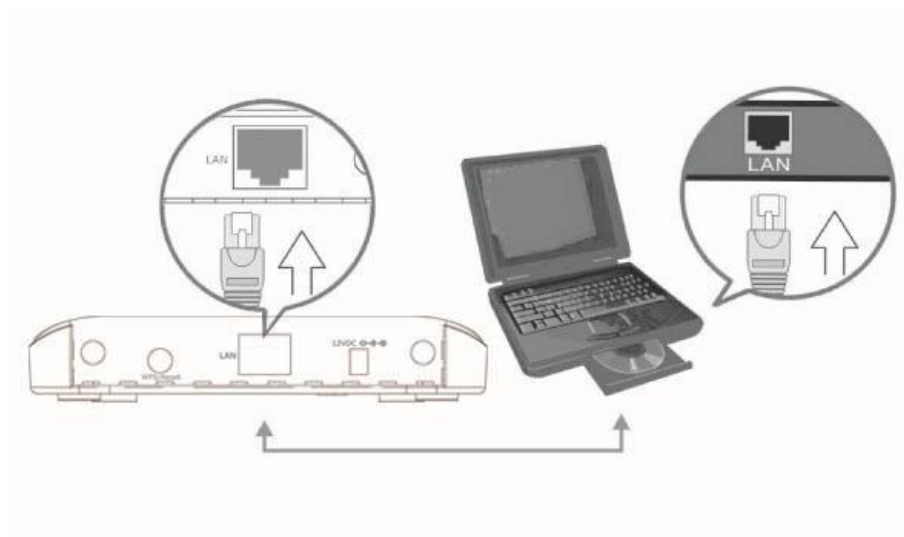
- Computer (with Fast Ethernet adapter or wireless adapter) running Windows XP/Vista/7, Mac OS.
- Web Browser for software configuration (Internet Explorer 7 or above, Google Chrome, Firefox, Safari)

II. Quick Installation

Your wireless access point can be up and running in a matter of minutes.

If you need to make more detailed configurations after setup, you can refer to [III. Browser Based Configuration Interface.](#)

1. 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.



2. Plug the power adapter into the device's 5V power port, and plug the adapter into a wall socket. The PWR LED should light up.

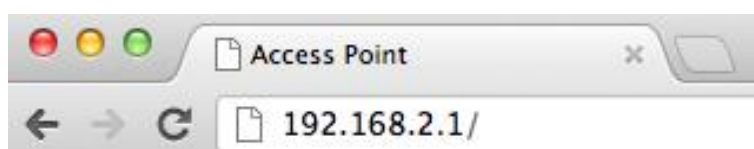
Refer to the following instructions appropriate for your operating system.

II-1. Mac

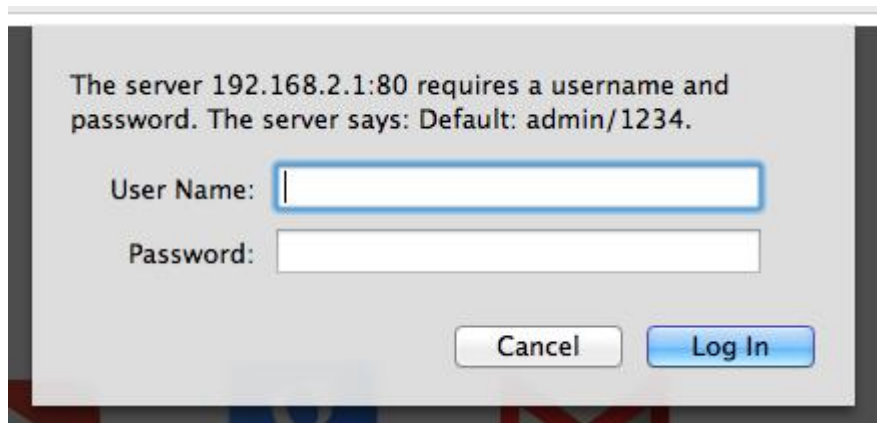


Note: You need to modify the IP address of your computer before you can setup the access point. For guidance on how to do this, please see [Appendix IV-1. Configuring your IP Address.](#)

For Mac users it is necessary to configure the access point manually, using the browser based configuration interface. Please open a web browser and enter the access point's default IP address "**http://192.168.2.1**" into the URL bar.



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

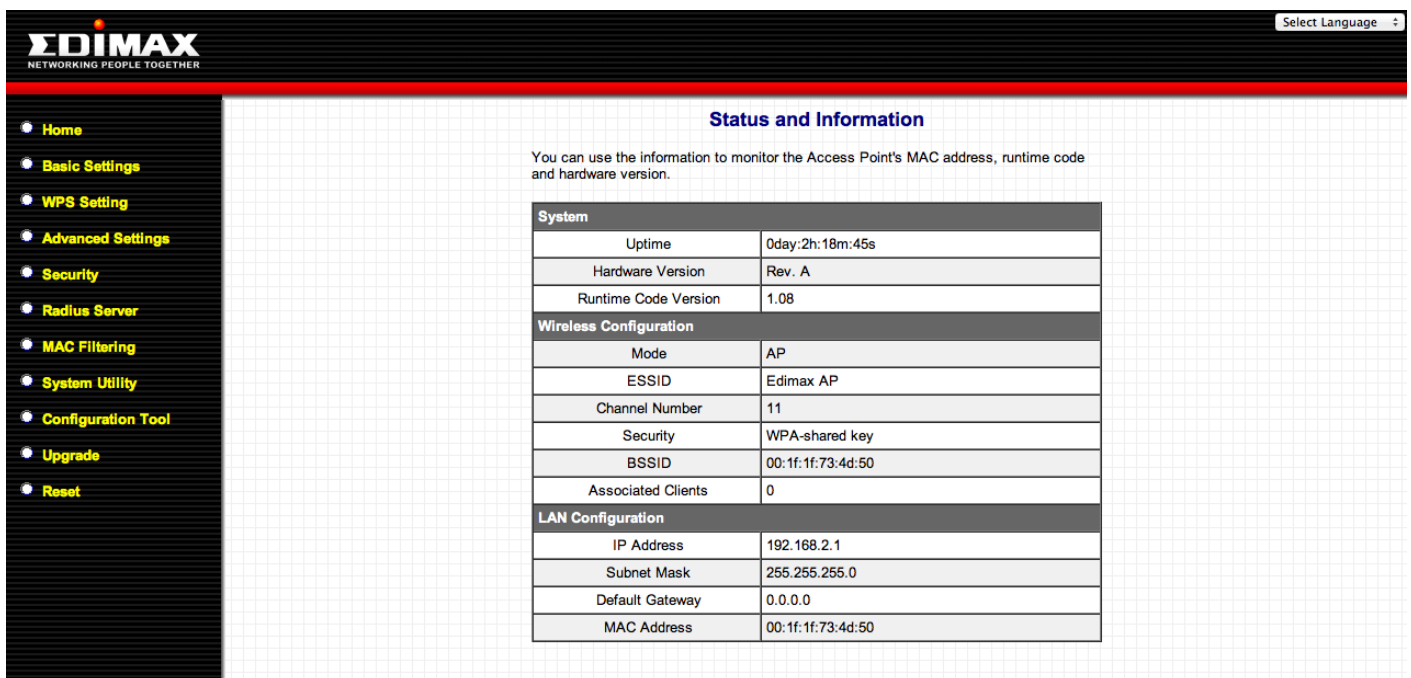


The server 192.168.2.1:80 requires a username and password. The server says: Default: admin/1234.

User Name:

Password:

From here, you will see the browser based configuration interface home screen.



EDIMAX
NETWORKING PEOPLE TOGETHER

Select Language

- Home
- Basic Settings
- WPS Setting
- Advanced Settings
- Security
- Radius Server
- MAC Filtering
- System Utility
- Configuration Tool
- Upgrade
- Reset

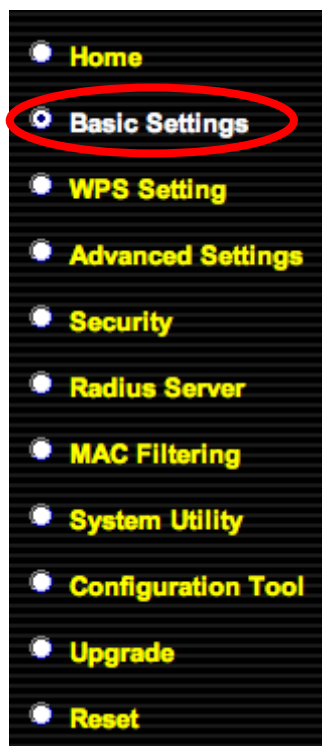
Status and Information

You can use the information to monitor the Access Point's MAC address, runtime code and hardware version.

System	
Uptime	0day:2h:18m:45s
Hardware Version	Rev. A
Runtime Code Version	1.08

Wireless Configuration	
Mode	AP
ESSID	Edimax AP
Channel Number	11
Security	WPA-shared key
BSSID	00:1f:1f:73:4d:50
Associated Clients	0

LAN Configuration	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:1f:1f:73:4d:50



Select “Basic Settings” from the menu on the left side of the screen. “Basic Settings” allows you to set the mode of the access point and configure the settings accordingly.

Open the drop down menu labeled “Mode” and select from the 6 available modes:

The available modes are:

AP	Access point mode allows wireless clients to connect to this device and exchange data with 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. It its client function to connect to a root AP, and uses its AP function to service wireless clients within its coverage.
--	---

Please refer to the appropriate chapter of the user manual for your desired operating mode:

- [III-2-1. AP Mode](#)
- [III-2-2. Station Infrastructure Mode](#)
- [III-2-3. AP Bridge-Point to Point Mode](#)
- [III-2-4. AP Bridge-Point to Multi-Point Mode](#)
- [III-2-5. AP Bridge-WDS](#)
- [III-2-6. Universal Repeater Mode](#)

II-2. Windows

1. Windows users can run the setup wizard on the included CD. Insert the Edimax CD into your computer's CD drive. When the AutoPlay screen appears, select "Run Autorun.exe."

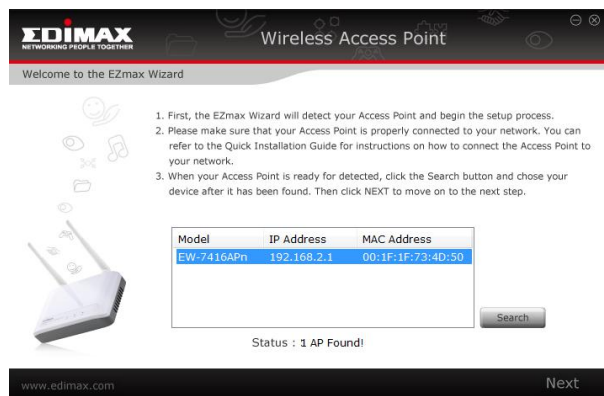


Note: *If a popup window appears asking "Do you want to allow the following program to make changes to this computer", please click "Yes" to continue.*

3. Click on "Setup Utility" in the main menu, then select "English" to continue.



4. The setup wizard will search for the access point. When it has successfully found the device, click "Next" to continue.



5. The setup wizard will prompt you for a password. Enter the default password "1234".



EDIMAX
NETWORKING PEOPLE TOGETHER

Wireless Access Point

Please enter the username and password

Username : admin

Password : 1234

www.edimax.com Back Next

6. The setup wizard will then show the access point's IP information. The default IP is 192.168.2.1. Click "Next" to continue.



Note: Please do not select "Automatically assign an IP address from your network" unless you are performing more advanced setup. For first-time installation, please use the default IP address.



EDIMAX
NETWORKING PEOPLE TOGETHER

Wireless Access Point

Set the Local IP Address for your AP/Bridge

This IP Address is used to access the advanced menu of your Access Point from a web browser.

☐ Automatically Assign an IP Address from your Network
☒ Manually Assign an Address

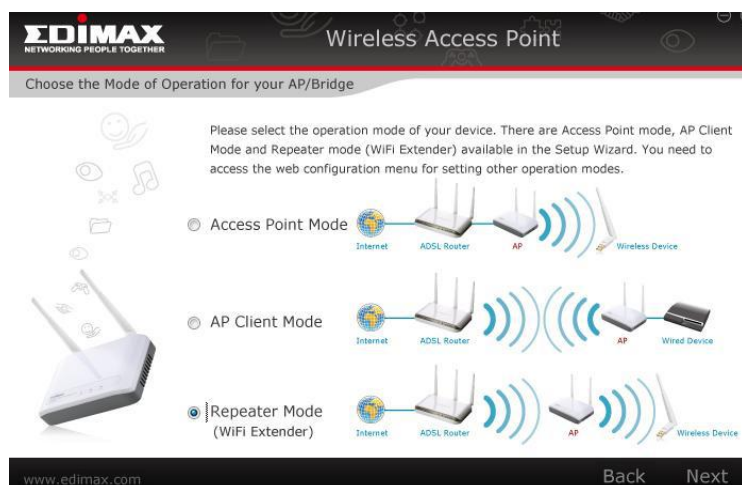
IP Address : 192 . 168 . 2 . 1

Subnet Mask : 255 . 255 . 255 . 0

Gateway : 0 . 0 . 0 . 0

www.edimax.com Back Next

7. You now have the option of selecting which mode you want to use.



EDIMAX
NETWORKING PEOPLE TOGETHER

Wireless Access Point

Choose the Mode of Operation for your AP/Bridge

Please select the operation mode of your device. There are Access Point mode, AP Client Mode and Repeater mode (WiFi Extender) available in the Setup Wizard. You need to access the web configuration menu for setting other operation modes.

☐ Access Point Mode
☐ AP Client Mode
☒ Repeater Mode (WiFi Extender)

www.edimax.com Back Next

II-2-1. Access Point Mode

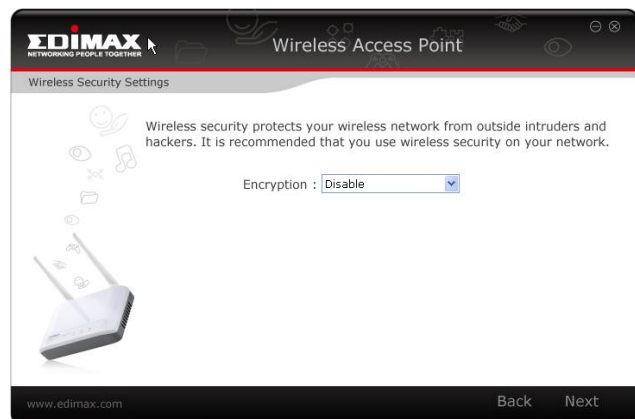
1. Select Access Point Mode and click “Next”.

2. You will be prompted to set the SSID of this access point. The SSID will be the name of the access point when you connect to it wirelessly. The default SSID is **Edimax AP**. This page also offers the option to change the password used to access the device’s configuration settings.

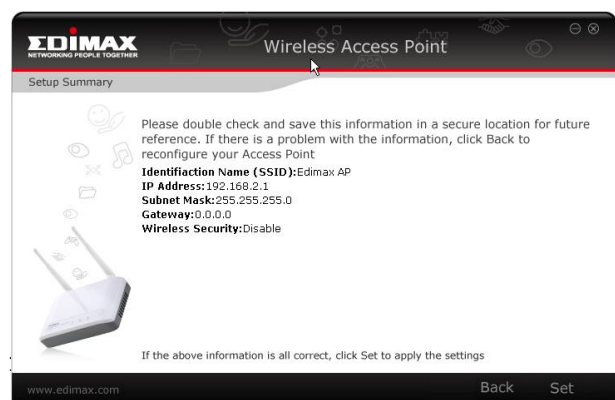


For first time setup, please simply click “Next” without changing anything.

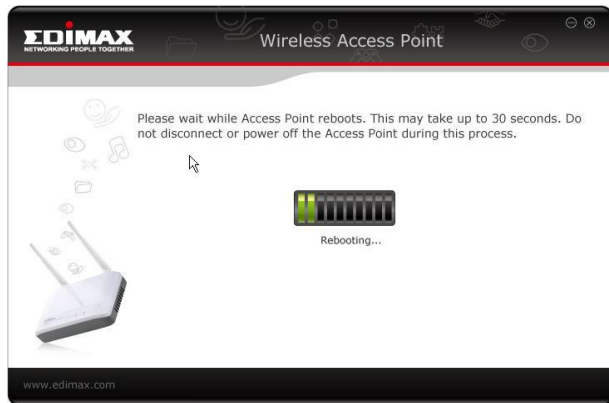
3. You will now be prompted to set up a wireless encryption password. You have the option of using no security encryption, or selecting the **WEP** or **WPA pre-shared key** encryption schemes. It is recommended that you set up an encryption method, though, for security reasons.



4. You will see a final confirmation screen, listing the settings you have selected. If everything is correct, click “Set” to continue.



5. The device will save your settings, then reboot. Please do not disconnect or turn off the device during this process.



6. After the device reboots, you will see a final congratulation screen. Click "Finish" to complete the setup.



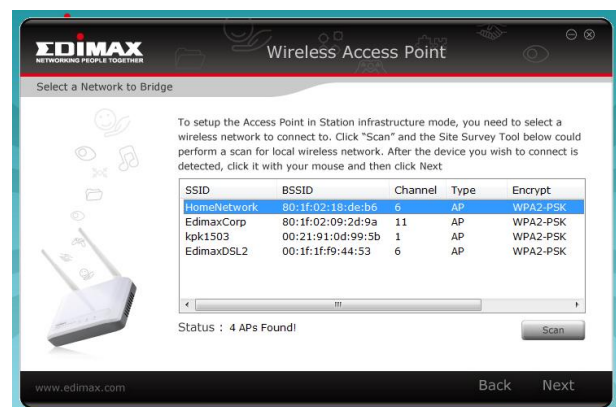
II-2-2. AP Client Mode

1. Select AP Client Mode and click “Next”.

2. You will have the option to change the password used to access the device’s configuration settings. For first time setup, please simply click “Next” without changing anything.



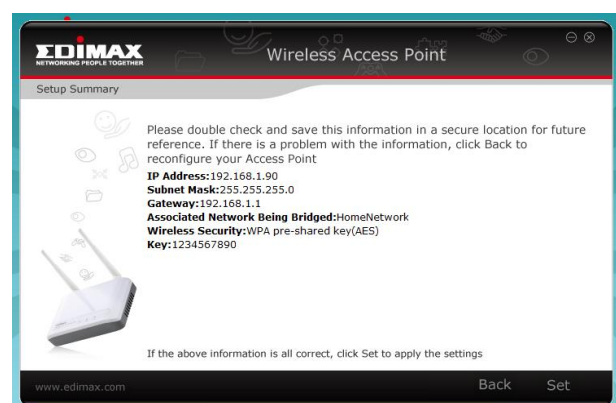
3. The device will search for nearby wireless networks to connect to. If you cannot find the access point you wish to connect to, click “Scan” to refresh the list of wireless networks. Select the wireless network you wish to connect to, and click “Next” to continue.



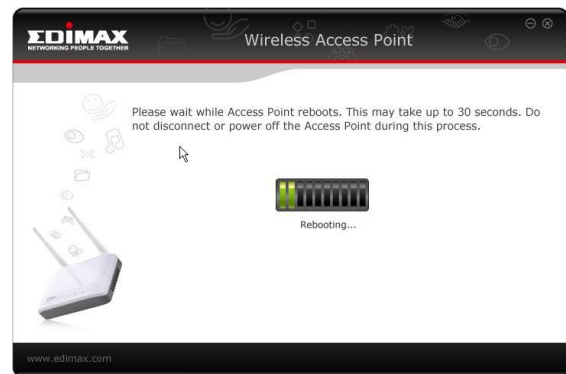
4. If the wireless network you selected requires a network security key, enter it here. If you do not know the network security key then please refer to Appendix “**How to Find Your Network Security Key**” for guidance. Click “Next” to continue when finished.



5. You will see a final confirmation screen, listing the settings you have selected. If everything is correct, click “Set” to continue.



6. The device will save your settings, then reboot. Please do not disconnect or turn off the device during this process.



7. After the device reboots, you will see a final congratulation screen. Click "Finish" to complete the setup.



II-2-3. Repeater Mode (Wi-Fi Extender)

1. Select Repeater Mode and click “Next”.

2. You will be prompted to set the SSID of this device. The SSID will be the name of the device when you connect to it wirelessly. The default SSID is **Edimax AP**, you are option to change it to the same SSID as your current wireless network. This page also offers the option to change the password used to access the device’s configuration settings.

The screenshot shows the 'Wireless Access Point' configuration page. It has a header with the Edimax logo and the title 'Wireless Access Point'. Below the header, it says 'Choose an Identification Name for your AP/Bridge'. There is a text input field for 'Identification Name (SSID)' with 'Edimax AP' entered. Below this, it says 'If you wish to customize the login information for your Access Point, please enter the new username and password in the following columns.' There is a checkbox labeled 'Set Password' which is checked. Below the checkbox, there are three text input fields: 'Username' with 'admin' entered, 'New Password', and 'Re-Enter Password'. At the bottom, there are 'Back' and 'Next' buttons. The Edimax logo and tagline 'NETWORKING PEOPLE TOGETHER' are in the top left corner.

3. The device will search for nearby wireless networks to connect to. If you cannot find the access point you wish to connect to, click “Scan” to refresh the list of wireless networks. Select the wireless network you wish to connect to, and click “Next” to continue.

The screenshot shows the 'Wireless Access Point' configuration page. It has a header with the Edimax logo and the title 'Wireless Access Point'. Below the header, it says 'Select a Network to Bridge'. There is a text input field for 'Identification Name (SSID)' with 'Edimax AP' entered. Below this, it says 'To setup the Access Point in Station infrastructure mode, you need to select a wireless network to connect to. Click “Scan” and the Site Survey Tool below could perform a scan for local wireless network. After the device you wish to connect is detected, click it with your mouse and then click Next'. There is a table with the following data:

SSID	BSSID	Channel	Type	Encry
EdimaxCorp	80:1f:02:09:2d:9a	11	AP	WPA2-P
HomeNetwork	80:1f:02:18:de:b6	11	AP	WPA2-P
Edimax	80:1f:02:19:01:2e	11	AP	no

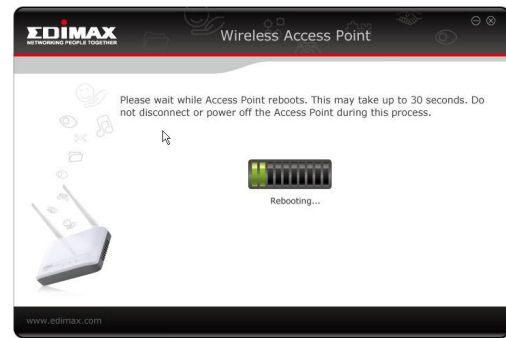
Below the table, there is a 'Status : 3 APs Found!' and a 'Scan' button. At the bottom, there are 'Back' and 'Next' buttons. The Edimax logo and tagline 'NETWORKING PEOPLE TOGETHER' are in the top left corner.

4. If the wireless network you selected requires a network security key, enter it here. If you do not know the network security key then please refer to Appendix “**How to Find Your Network Security Key**” for guidance. Click “Next” to continue when finished.

5. You will see a final confirmation screen, listing the settings you have selected. If everything is correct, click “Set” to continue.

The screenshot shows the 'Wireless Access Point' configuration page. It has a header with the Edimax logo and the title 'Wireless Access Point'. Below the header, it says 'Setup Summary'. There is a text input field for 'Identification Name (SSID)' with 'Edimax AP' entered. Below this, it says 'Please double check and save this information in a secure location for future reference. If there is a problem with the information, click Back to reconfigure your Access Point'. There is a list of settings: 'Identification Name (SSID):Edimax AP', 'IP Address:192.168.1.90', 'Subnet Mask:255.255.255.0', 'Gateway:192.168.1.1', 'Associated Network Being Bridged:HomeNetwork', 'Wireless Security:WPA pre-shared key(AES)', and 'Key:1234567890'. At the bottom, there is a 'Set' button circled in red. The Edimax logo and tagline 'NETWORKING PEOPLE TOGETHER' are in the top left corner.

6. The device will save your settings, then reboot. Please do not disconnect or turn off the device during this process.
7. After the device reboots, you will see a final congratulation screen. Click “Finish” to complete the setup.

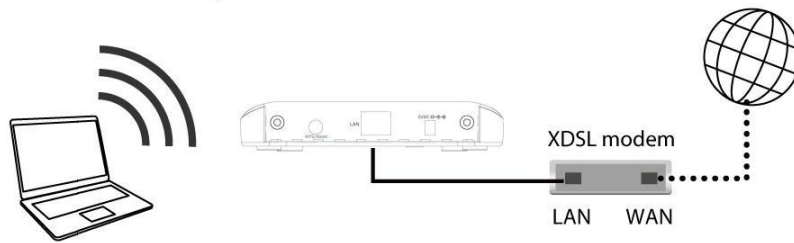


II-6. Hardware Installation

After configuring your device, you can install it in its final location.

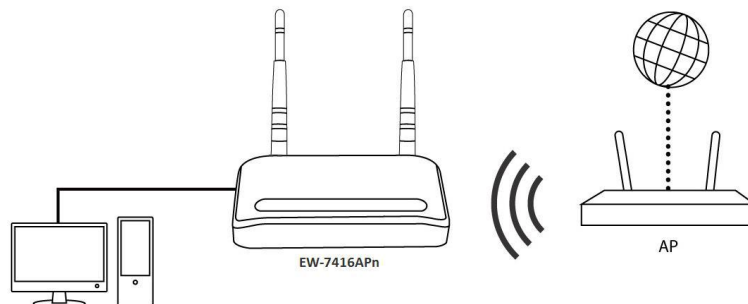
Access Point Mode

Connect one port of the device to your router or xDSL modem. You can now connect to the device through a wired connection by connecting your computer to it with an Ethernet cable, or connect to the device wirelessly by searching and connecting to the device name you set up.



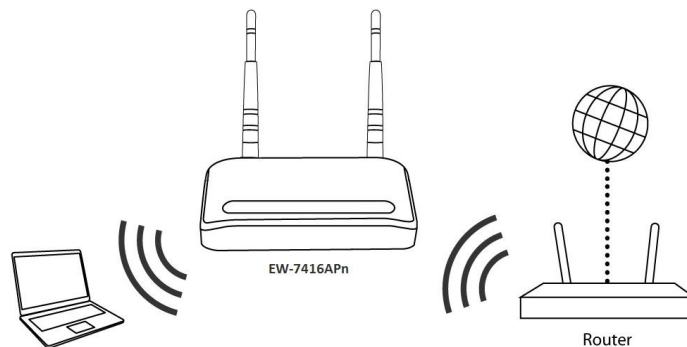
AP Client Mode

Connect one port of the device to the appliance you wish to connect to the Internet wirelessly, such as a computer, game console, or smart TV.



Repeater Mode

Position the device in a location for optimal wireless extension, such as the middle of your house. You can connect to the device wirelessly by searching and connecting to the device name you set up.



III. Browser Based Configuration Interface

Once you have setup the access point in its desired operating mode as detailed in [II. Quick Installation](#), you can further configure the settings of the access point anytime using the browser based configuration interface.



Note: You may need to modify the IP address of your PC or Macintosh before you can access the browser based configuration interface.

This is because the access point's default IP address 192.168.2.1 may not be in the same IP address subnet as your network. In this case, you need to modify the IP address of your PC or Macintosh to 192.168.2.10. For guidance on how to do this, please see [Appendix IV-1. Configuring your IP Address](#).

To access the browser based configuration interface, enter the access point's default IP address "**http://192.168.2.1**" into the URL bar of a web browser on a computer which is connected to the access point's Wi-Fi network, or via Ethernet cable as explained in [II. Quick Installation](#) steps 1 - 2.

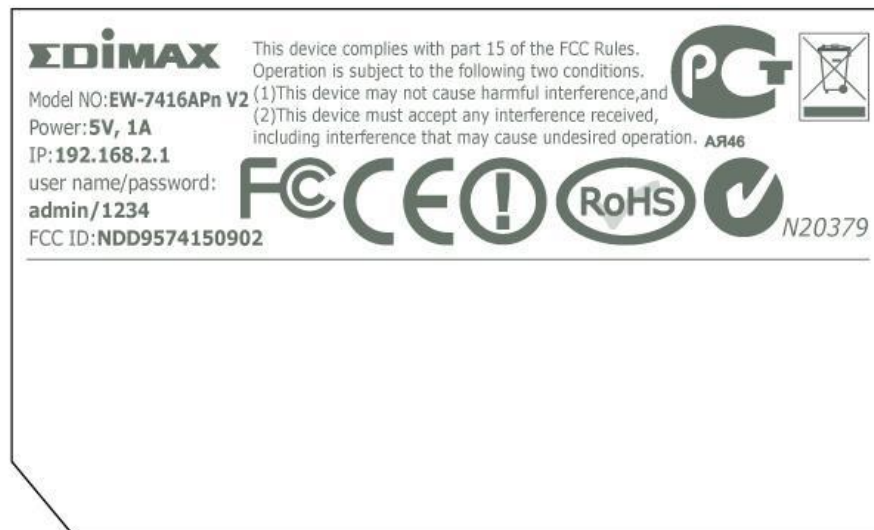


Note: If you modified the IP address of the access point during iQ Setup then enter this IP into the URL bar of a web browser instead of the default IP 192.168.2.1



Note: For your reference, the access point's default IP address, username and password are all displayed on the product label on the underneath of the device, as shown below.

50x30mm

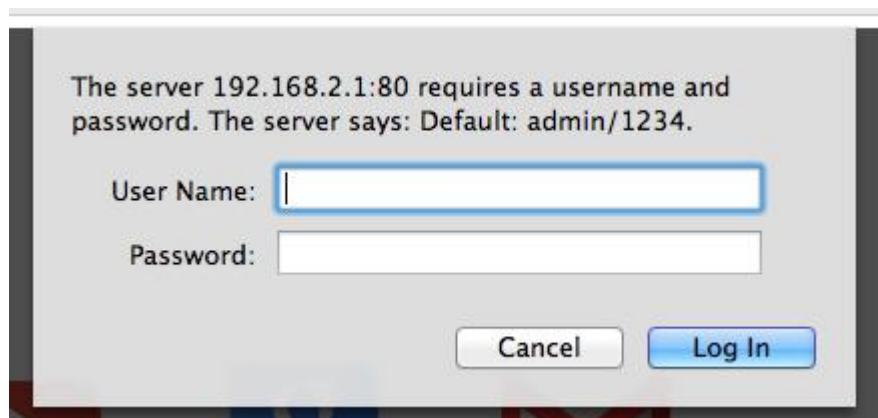


You will then be prompted to enter the device's username and password. The default username is **admin** and the default password is **1234**.


Windows:



Mac:



From here, you will see the browser based configuration interface home screen.



Select Language

- Home
- Basic Settings
- WPS Setting
- Advanced Settings
- Security
- Radius Server
- MAC Filtering
- System Utility
- Configuration Tool
- Upgrade
- Reset

Status and Information

You can use the information to monitor the Access Point's MAC address, runtime code and hardware version.

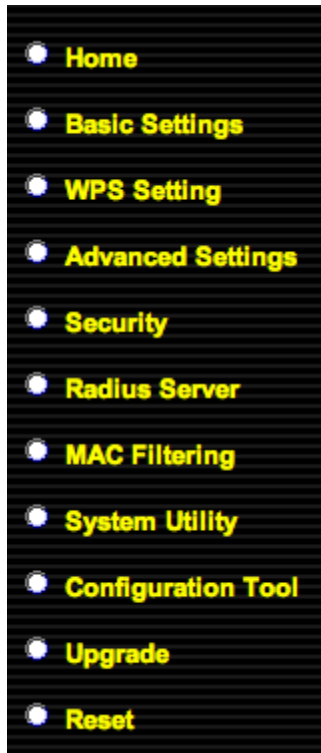
System	
Uptime	0day:2h:18m:45s
Hardware Version	Rev. A
Runtime Code Version	1.08

Wireless Configuration	
Mode	AP
ESSID	Edimax AP
Channel Number	11
Security	WPA-shared key
BSSID	00:1f:1f:73:4d:50
Associated Clients	0

LAN Configuration	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:1f:1f:73:4d:50

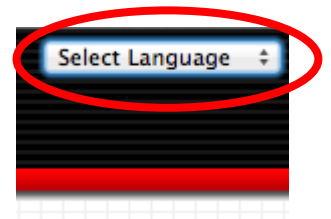
III-1. Home

The Home page displays 11 categories in the left panel which you can select:



- [III-1. Home](#)
- [III-2. Basic Settings](#)
- [III-3. WPS Setting](#)
- [III-4. Advanced Settings](#)
- [III-5. Security](#)
- [III-6. Radius Server](#)
- [III-7. MAC Filtering](#)
- [III-8. System Utility](#)
- [III-9. Configuration Tool](#)
- [III-10. Upgrade](#)
- [III-11. Reset](#)

At the top of the screen on the right side there is a drop down menu to change the language of the browser based configuration interface.



The “Status and Information” screen is displayed in the main window. This shows basic system information about the access point for reference, such as firmware version, wireless mode and SSID, and the access point’s IP and MAC address.

Status and Information

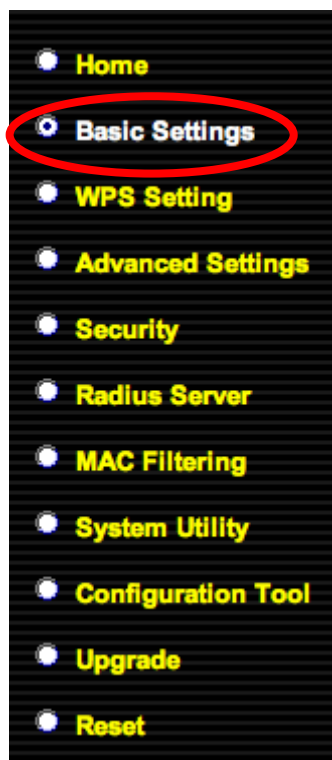
You can use the information to monitor the Access Point's MAC address, runtime code and hardware version.

System	
Uptime	0day:0h:13m:22s
Hardware Version	Rev. A
Runtime Code Version	1.09
Wireless Configuration	
Mode	AP
ESSID	Edimax AP
Channel Number	11
Security	Disable
BSSID	00:e0:4c:81:96:c1
Associated Clients	0
LAN Configuration	
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
MAC Address	00:e0:4c:81:96:c1

System	
Uptime	Displays the total time the access point has been operational since it was last switched on.
Hardware Version	Displays hardware version. This information is helpful if you experience problems with your access point and need technical support.
Runtime Code Version	Displays current firmware version. This information is useful when performing a firmware upgrade.
Wireless Configuration	
Mode	Displays the current operating mode of the access point.
ESSID	Displays current ESSID (the name used to identify the access point).
Channel Number	Displays current wireless channel number.
Security	Displays the current wireless security setting.
BSSID	Displays the current BSSID (a unique ID of the access point, which cannot be modified).
Associated Clients	Displays the number of connected wireless clients.

LAN Configuration	
IP Address	Displays the IP address of the access point.
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 Access Point.

III-2. Basic Settings



“Basic Settings” allows you to set the access point to any of several different modes and configure the settings accordingly.

Open the drop down menu labeled “Mode” and select from the 6 available modes:

The available modes are:

Basic Settings	
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	AP
MAIN ESSID	Station-Infrastructure
Channel Number	AP Bridge-Point to Point
	AP Bridge-Point to Multi-Point
	AP Bridge-WDS
	Universal Repeater
Associated Clients	Show Active Clients

AP	The device acts as a wireless “access point” to a wired Ethernet network. Wireless clients can connect to this device and exchange data with 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. Acting as both a client and access point at the same time, client function will connect to a root AP, while access point function will service wireless clients within range.

Please follow the appropriate chapter of the user manual for your desired operating mode:

- [III-2-1. AP Mode](#)
- [III-2-2. Station Infrastructure Mode](#)
- [III-2-3. AP Bridge-Point to Point Mode](#)
- [III-2-4. AP Bridge-Point to Multi-Point Mode](#)
- [III-2-5. AP Bridge-WDS](#)
- [III-2-6. Universal Repeater Mode](#)

III-2-1. AP Mode

In access point (AP) mode the device acts as a wireless access point to a wired Ethernet network for IEEE 802.11b/g/n wireless devices.

When you select AP Mode, the following appears:

Basic Settings

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 AP	Multiple ESSID
Channel Number	11	
Associated Clients	Show Active Clients	

Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected
------	--

	combinations of each. Only wireless clients of the same band or bands as you select will be able to connect.
MAIN ESSID	Specify an ESSID (the name used to identify the access point) of up to up to 32 alphanumerical characters. Please note that the ESSID is case sensitive.
Channel Number	Select a channel number for the access point. Where possible, select a channel number which is not already in use by another access point/router.
Associated Clients	Click the “Show Active Clients” button and a new window will appear which displays information about wireless clients connected to this access point. Click the “Refresh” button in the new window to refresh the list.

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE APPLY

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

III-2-2. Station Infrastructure Mode

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.

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

Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only access points of the same band or bands as you select will be able to connect.
------	--

MAIN ESSID	Specify an ESSID (the name used to identify the access point) of up to up to 32 alphanumerical characters. Please note that the ESSID is case sensitive.
Site Survey	Click the “Select Site Survey” button to display the “Wireless Site Survey Table” which shows all available Wi-Fi networks. Select which network the access point will connect to (see below).

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

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

Wireless Site Survey

The “Wireless Site Survey Table” displays available Wi-Fi networks. Select one and click “Done”.

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	Channel	SSID	BSSID	Encryption	Type	Signal	Band
<input type="radio"/>	1	MEETING_ROOM_6F	00:1F:1F:1F:73:FC	NONE	OPEN	29	11b/g/n
<input type="radio"/>	1	AirPortExpress_Jimmy	28:37:37:46:D3:CA	AES	WPA2PSK	55	11b/g/n
<input type="radio"/>	2	PA-HamaRootAP	80:1F:02:0D:EF:DC	TKIPAES	WPA1PSKWPA2PSK	0	11b/g/n
<input type="radio"/>	2	PA-HamaRootAP	80:1F:02:4F:32:56	AES	WPA2PSK	0	11b/g/n
<input type="radio"/>	3	DemoRoom_Router1	00:1F:1F:61:C0:08	TKIPAES	WPA1PSKWPA2PSK	15	11b/g/n
<input type="radio"/>	5	XXXXXXXX	00:11:22:33:44:50	NONE	OPEN	20	11b/g/n
<input type="radio"/>	6	!_Ken_PassBook	00:17:31:D6:3B:B9	TKIPAES	WPA1PSKWPA2PSK	76	11b/g
<input type="radio"/>	7	6228NC	00:1F:1F:C0:24:31	AES	WPA2PSK	86	11b/g/n
<input type="radio"/>	9	EdimaxHQ	10:6F:3F:47:04:00	NONE	OPEN	100	11b/g/n
<input type="radio"/>	9	EdimaxHQ	10:6F:3F:47:03:D0	NONE	OPEN	65	11b/g/n
<input type="radio"/>	9	EdimaxHQ	10:6F:3F:47:07:30	NONE	OPEN	20	11b/g/n
<input type="radio"/>	9	EdimaxHQ	00:10:20:30:40:50	NONE	OPEN	24	11b/g/n
<input type="radio"/>	11	OBM-AirPort-2.4G	10:9A:DD:87:47:CF	TKIPAES	WPA1PSKWPA2PSK	55	11b/g/n
<input type="radio"/>	11	6258GN Test	80:1F:02:1A:D9:64	AES	WPA2PSK	34	11b/g/n
<input type="radio"/>	11	Edimax	00:E0:4C:81:96:C1	NONE	OPEN	86	11b/g/n
<input type="radio"/>	11	Belkin-Demo-2.4	80:1F:02:57:22:78	NONE	OPEN	29	11b/g/n



Note: If the SSID of the access point you wish to connect to is not listed, try clicking the “Refresh”

button.

III-2-3. AP Bridge-Point to Point Mode

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



Note: The access point will not accept regular wireless clients in this mode.

Mode	AP Bridge-Point to Point ▼
Band	2.4 GHz (B+G+N) ▼
Channel Number	9 ▼
MAC address 1	000000000000
Set Security	Set Security

Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only access points of the same band or bands as you select will be able to connect.
Channel Number	Select a channel number for the access point. The channel number must be the same as the other access point you wish to connect to.
MAC address 1	Enter MAC address of the wireless access point you wish to connect to.
Set Security	Click “Set Security” to select an encryption mode for this wireless link. A new window with security options will appear.

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

Click “CONTINUE” to save the changes and continue configuring other settings,

or click “APPLY” to restart the system and make the changes take effect.

III-2-4. AP Bridge-Point to Multi-Point Mode

In AP bridge-point to multi-point mode the access point can 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: The access point will not accept regular wireless clients in this mode.

Mode	AP Bridge-Point to Multi-Point ▼
Band	2.4 GHz (B+G+N) ▼
Channel Number	9 ▼
MAC address 1	000000000000
MAC address 2	000000000000
MAC address 3	000000000000
MAC address 4	000000000000
Set Security	Set Security

Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only access points of the same band or bands as you select will be able to connect.
Channel Number	Select a channel number for the access point. The channel number must be the same as the other access points you wish to connect to.
MAC address 1-4	Enter the MAC addresses of the wireless access points you wish to connect to.
Set Security	Click “Set Security” to select an encryption mode for this wireless link. A new window with security options will appear.

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-2-5. AP Bridge-WDS

In this mode, the access point can 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: The access point will still be able to accept regular wireless clients in this mode.

Mode	AP Bridge-WDS
Band	2.4 GHz (B+G+N)
MAIN ESSID	Edimax AP
Channel Number	9
Associated Clients	Show Active Clients
MAC address 1	000000000000
MAC address 2	000000000000
MAC address 3	000000000000
MAC address 4	000000000000
Set Security	Set Security

Band	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only wireless devices of the same band or bands as you select will be able to connect.
MAIN ESSID	Specify an ESSID (the name used to identify the access point) of up to up to 32 alphanumerical characters. Please note that the ESSID is case sensitive.
Channel Number	Select a channel number for the access point. The

	channel number must be the same as the other access points you wish to connect to.
Associated Clients	Click the “Show Active Clients” button and a new window will appear which displays information about wireless clients connected to this access point. Click the “Refresh” button in the new window to refresh the list.
MAC address 1-4	Enter the MAC addresses of the wireless access points you wish to connect to.
Set Security	Click “Set Security” to select an encryption mode for this wireless link. A new window with security options will appear.

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-2-6. Universal Repeater Mode

In universal repeater mode, the access point acts as a wireless extender, performing both the functions of a client and an access point. It can extend the Wi-Fi coverage of an access point and eliminate Wi-Fi dead zones.

Basic Settings

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 AP <input type="button" value="Multiple ESSID"/>
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	Select the wireless band you wish to use for the access point: 802.11b, 802.11g, 802.11n or selected combinations of each. Only wireless devices of the same band or bands as you select will be able to connect.
MAIN SSID	Specify an ESSID (the name used to identify the access point) of up to up to 32 alphanumeric characters. Please note that the ESSID is case sensitive.
Channel Number	Select a channel number for the access point. The channel number must be the same as the other access point you wish to connect to.
Associated Clients	Click the “Show Active Clients” button and a new window will appear which displays information about wireless clients connected to this access point. Click the “Refresh” button in the new window to refresh the list.
Root AP SSID	Enter the SSID of the root access point/router here or click the “Select Site Survey” button to select from a list of available SSIDs.
Select Site Survey	Click the “Select Site Survey” button to display the “Wireless Site Survey Table” which shows all available Wi-Fi networks. Select which network the access point will connect to (see below).

Wireless Site Survey

The “Wireless Site Survey Table” displays available Wi-Fi networks. Select one and click “Done”.

Wireless Site Survey

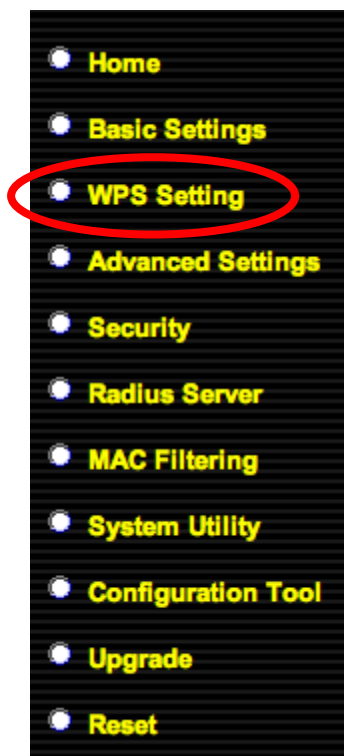
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

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



Note: If the SSID of the access point you wish to connect to is not listed, try clicking the “Refresh” button.

III-3. WPS Setting



WPS (Wi-Fi Protected Setup) is a simple way to establish connections between WPS compatible devices. WPS devices feature a WPS function which can be activated by pushing a WPS button on the device or from within the device's firmware/configuration interface. When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect.

The access point supports two types of WPS for wireless clients: PBC (Push Button Configuration) and PIN code. For PBC you can activate WPS on the wireless extender by pushing the WPS/Reset button on the access point or clicking the "Start PBC" button on the screen.

PIN code setup varies slightly in that it requires you to manually enter a PIN code into each device via the WPS

Settings before activating WPS.

WPS(Wi-Fi Protected Setup) Settings

This page allows you to change the setting for WPS(Wi-Fi Protected Setup).WPS can help your wireless client automatically connect to the Access Point.

☒ **Enable WPS**

• **Wi-Fi Protected Setup Information**

WPS Status	Configured
Self PinCode	24206747
SSID	Edimax AP
Authentication Mode	Disable
Passphrase Key	

• **Device Configure**

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

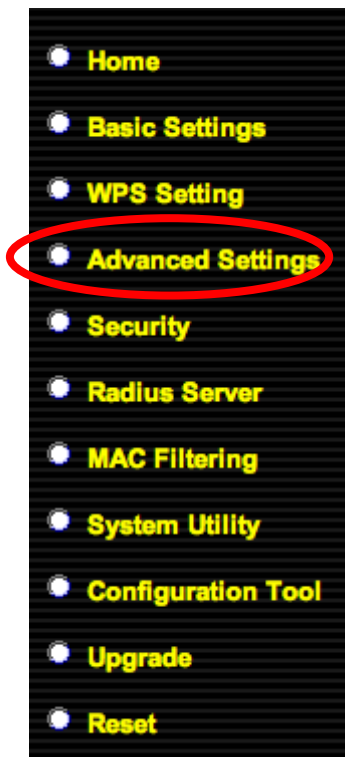
Enable WPS	Check this box to enable or disable WPS.
------------	--

Wi-Fi Protected Setup Information

WPS Status	Displays “Configured” or “unConfigured” depending on whether WPS Settings for the access point have been configured or not, either manually or using the WPS button.
Self PIN Code	This is the WPS PIN code of the wireless access point for use 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 the access point, this field will be blank.
Device Configuration	
Config Mode	There are two modes for the WPS connection, “Registrar” and “Enrollee”. 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 activate WPS. This access point will wait for WPS requests from wireless clients for 2 minutes.
Input Client PIN Code	Enter the PIN code of the wireless client, and click the “Start PIN” button to activate WPS. The “WLAN” LED on the access point will stay on while this access point waits for incoming WPS requests.

When WPS is activated on the access point, the “WLAN” LED will display on for two minutes. **Within two minutes**, activate WPS on your client device (refer to client device’s user manual for guidance on how to do so) in order to establish a connection.

III-4. Advanced Settings



In “Advanced Setting” you can configure the advanced features of the access point. Please do not modify these settings unless you know what effect the changes will have on your access point; advanced settings are for experienced users only.

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



Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(0-2347)
Beacon Interval	100	(20- 1024 ms)
DTIM Period	3	(1-10)
Data Rate	Auto	
N Data Rate	Auto	
Transmit Rate		
Channel Width	<input checked="" type="radio"/> Auto 20/40 MHZ	<input type="radio"/> 20 MHZ
Preamble Type	<input checked="" type="radio"/> Short Preamble	<input type="radio"/> Long Preamble
Broadcast ESSID	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
WMM	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
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. The default value is 2346 - please do not modify unless
--------------------	--

	you are familiar with this setting.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347 - please do not modify unless you are familiar with this setting.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100 - please do not modify unless you are familiar with this setting.
DTIM Period	Set the DTIM period of wireless radio. The default value is 3 - please do not modify unless you are familiar with this setting.
Data Rate	Set the wireless data transfer rate. The default is set to Auto - please do not modify unless you are familiar with this setting.
N Data Rate	Set the data rate of 802.11n. The default is set to Auto - please do not modify unless you are familiar with this setting.
Channel Width	Select wireless channel width (bandwidth used by wireless signals from the access point) – the recommended value is Auto 20/40MHz please do not modify unless you are familiar with this setting.
Preamble Type	Set the wireless radio preamble type. The default value is “Short Preamble” - please do not modify unless you are familiar with this setting.
Broadcast ESSID	Set if the access point will broadcast its own ESSID. To hide the ESSID of your access point select “Disable” - only users who know the ESSID of your access point will be able to connect.
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 WMM is enabled, the access point will prioritize different kinds of data and 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	Set the power output of the wireless radio. Unless you’re using the access point in a very large space, you

	may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
--	---

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

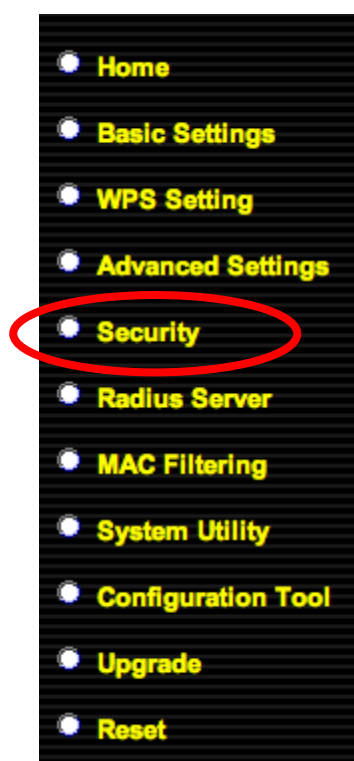
You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-5. Security



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

Note: It is important to configure security to prevent intruders from accessing your local network and causing damage to computers and servers. Use complicated, hard-to-guess security keys which include combinations of letters and numbers – and change your security key regularly.

A screenshot of the 'Security' configuration page. The title 'Security' is at the top. Below it is a paragraph: '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.' Under the heading 'Select SSID', there is a form with a label 'SSID choice' and a dropdown menu currently showing 'Edimax AP'.

Select SSID	
SSID choice	Select which SSID to configure security settings for.

A screenshot of the 'Security Settings' configuration page. Under the heading 'Security Settings', there is a form with a label 'Encryption' and a dropdown menu. The dropdown menu is open, showing options: 'Disable' (which is selected with a checkmark), 'WEP', 'WPA pre-shared key', and 'WPA RADIUS'. Below the dropdown, there is a checkbox labeled 'Enable 802.1x Authentication' which is currently unchecked.

Security Settings	
Encryption	Select an SSID from the drop down menu to configure security for. Refer to the next section for more details about each security type.

III-5-1. 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, and is not recommended.

Enable 802.1x Authentication	Check this box to enable 802.1x user authentication. See III-5-2. 802.1x Authentication.
------------------------------	--

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE	APPLY
----------	-------

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

III-5-2. Enable 802.1x Authentication

If you select “Disable” or “WEP” as your encryption type, you can check the “Enable 802.1x Authentication” box to enable 802.1x authentication based on a RADIUS user authentication server.

<input type="checkbox"/>	Use internal MD5/PEAP RADIUS Server
<input checked="" type="checkbox"/>	Enable 802.1x Authentication
RADIUS Server IP address	<input type="text"/>
RADIUS Server Port	<input type="text" value="1812"/>
RADIUS Server Password	<input type="text"/>

Use internal MD5/PEAP RADIUS Server	Check the box to use an internal MD5/PEAP RADIUS Server.
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.

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-5-3. WEP

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



Note: *Most wireless devices support WPA encryption, though some legacy wireless devices only support WEP encryption. WEP only supports up to 54Mbps transmission data rate.*

Encryption	WEP
Key Length	64-bit
Key Format	Hex (10 characters)
Default Tx Key	Key 1
Encryption Key 1	*****
Encryption Key 2	*****
Encryption Key 3	*****
Encryption Key 4	*****

☐ 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	Select a key format: ASCII or Hex. The key length will also be displayed here - ASCII and Hex keys vary in length according to “Key Length” (above)”.
Default Tx Key	You can set up to four sets of WEP keys, and you can decide which key is used the default. If you are unsure, leave the value as the default “Key 1”.
Encryption Key 1 to 4	Enter WEP key here, the number of characters must be the same as the number displayed in the “Key Format” field. For “ASCII” key format, you can use any alphanumerical characters (0-9, a-z, and A-Z). For “Hex” 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 enter multiple WEP keys, each should be unique.
Enable 802.1x Authentication	Check this box to enable 802.1x user authentication. See III-5-2. Enable 802.1x Authentication .

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

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

III-5-4. WPA Pre-Shared Key

WPA pre-shared key is the recommended and most secure encryption type.

Encryption	WPA pre-shared key ▼
WPA Unicast Cipher Suite	<input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key Format	Passphrase ▼
Pre-shared Key	<input type="text"/>

WPA Unicast Cipher	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed.
--------------------	---

Suite	AES is safer than TKIP, but not supported by all wireless clients. Please make sure your wireless client supports your selection. WPA2(AES) is recommended, or WPA2 Mixed if your client does not support AES.
Pre-shared Key Format	Select the pre-shared key format from “Passphrase” (8 to 63 alphanumerical characters) or “Hex (64 characters 0 to 9 and a to f.)
Pre-shared 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.



Note: *TKIP only supports up to 54Mbps transmission data rate.*

Click “APPLY” to save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-5-5. WPA Radius

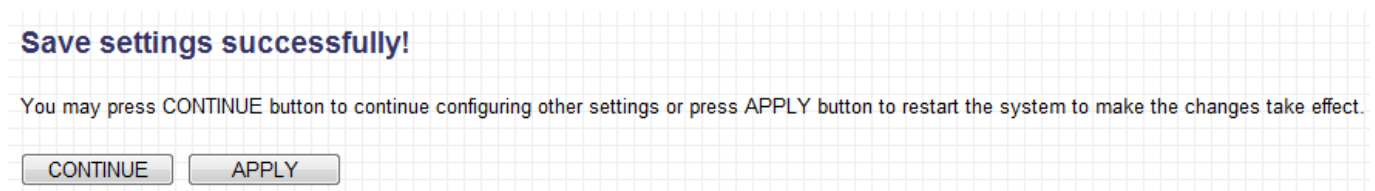
WPA RADIUS is a combination of WPA encryption and RADIUS user authentication. If you have a RADIUS authentication server, you can authenticate the identity of every wireless client against a user database.

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	Select from WPA (TKIP), WPA2 (AES) or WPA2 Mixed. AES is safer than TKIP, but not supported by all wireless
--------------------------	---

	clients. Please make sure your wireless client supports your selection. WPA2(AES) is recommended, or WPA2 Mixed if your client does not support AES.
Use internal MD5/PEAP RADIUS Server	Check the box to use an internal MD5/PEAP RADIUS Server.
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.

Click “APPLY” to save changes. The following message will appear:



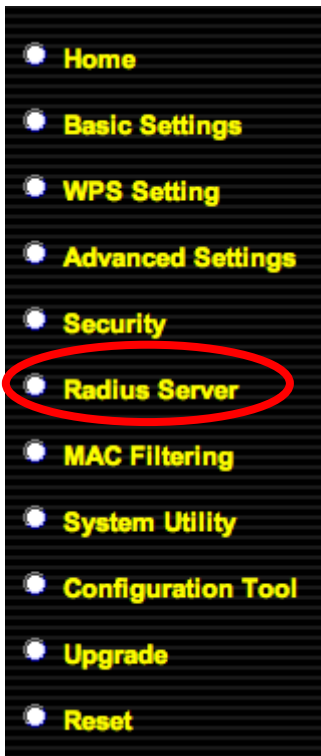
Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE APPLY

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

III-6. Radius Server



Radius server settings can be configured on this page. A Radius server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The access point's internal radius server only supports 96 users and 16 IP addresses – for more users and/or IP addresses please use an external radius server.

Radius Server

This page allows you to set the internal Radius Server. This server can be used as the Authentication server of other wireless devices.

☐ **Enable Radius Server**

Username	Password	Re-Type Password	Configure
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Reset"/>

NO.	Username	Select
<div><input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/></div>		

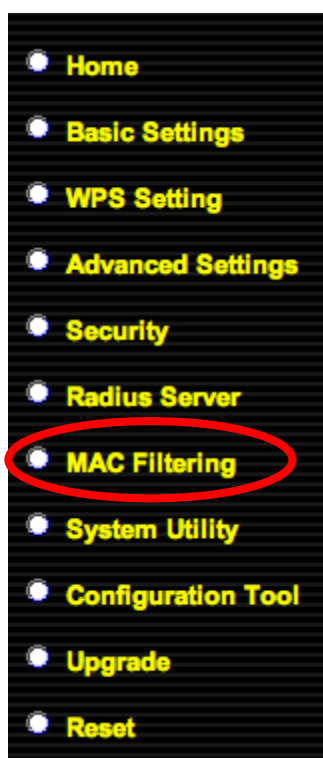
Authentication Client (up to 16 clients)

Client IP	Secret Key	Re-Type Secret Key	Configure
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/> <input type="button" value="Reset"/>

NO.	Client IP	Select
<div><input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/></div>		

Enable Radius Server	Check the box to enable the Radius server.
Username	Enter a username for a Radius user profile.
Password	Enter a password for a Radius user profile.
Re-Type Password	Confirm the password.
Configure	Select “Add” to add the user profile – all user profiles will be displayed underneath once they have been added. Select “Reset” to clear all fields.
Select	Check this box to select Radius user(s).
Delete Selected	Click this button to delete selected Radius user(s).
Delete All	Delete all Radius user(s) in the table.
Reset	Uncheck all selected Radius user(s).
Authentication Client (up to 16 clients)	
Client IP	Enter the IP address of the client to be authorized.
Secret Key	Enter a secret key for the client.
Re-Type Secret Key	Confirm the secret key.
Configure	Select “Add” to add the client to the list of authorized clients – all authorized clients will be displayed underneath once they have been added. Select “Reset” to clear all fields.
Select	Check this box to select client(s).
Delete Selected	Click this button to delete selected client(s).
Delete All	Delete all Radius client(s) in the table.
Reset	Uncheck all selected client(s).

III-7. MAC Filtering



The MAC filtering feature allows you to define a list of wireless devices permitted to connect to this access point, identified by their unique MAC address. When devices not on the 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 AP ▾

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

NO.	MAC Address	Comment	Select
Delete Selected Delete All Reset			

☐ **Enable Wireless Access Control**

New	MAC Address: <input type="text"/>	Comment: <input type="text"/>	Add Clear
-----	--------------------------------------	----------------------------------	-------------------------------------

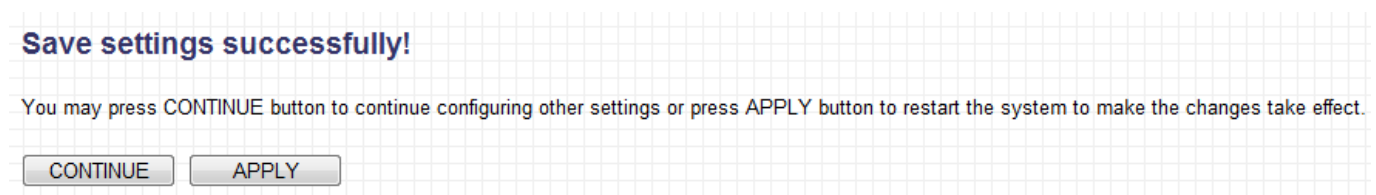
Select SSID	
SSID choice	Select which SSID to configure MAC address filtering.

MAC Address Filtering Table	Displays MAC addresses which have been added to the list of permitted devices.
Select	Check this box to select MAC address(es).

Delete Selected	Click this button to delete 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.
MAC address	Enter a MAC address permitted to connect to the access point. Only enter characters 0 to 9 or a to f.
Comment	Enter an optional comment associated with the specified MAC address for reference/identification, consisting of up to 16 alphanumerical characters.
Add	Add the MAC address entry to the list.
Clear	Remove all characters in the “MAC address” and “Comments” fields.

Click “APPLY” to save changes. The following message will appear:



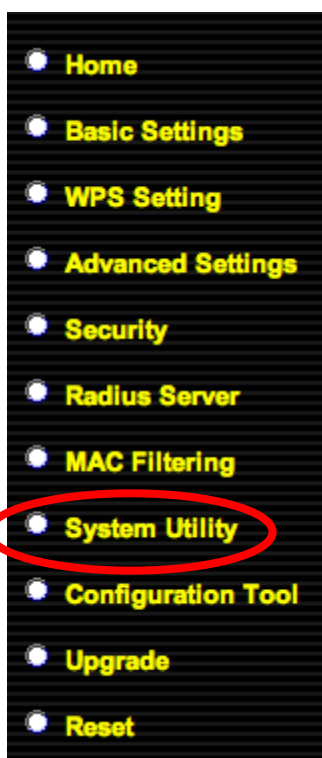
Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE APPLY

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

III-8. System Utility



In “System Utility” you can configure basic system and administrative parameters.

System Utility
Enter the IP Address of the Access Point. If you want to use DHCP server service, you should enter a unique IP for the Access Point.

III-8-1. 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"/>

Password Settings	
Current Password	Enter your current password. The default password is 1234 .
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 save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-8-2. 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, input the IP address, subnet mask and gateway address into the corresponding fields.

Management IP

IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Gateway Address	0.0.0.0
DHCP Server	Disabled

Management IP	
IP Address	Specify an IP address here. This IP address will be assigned to your access point, and will replace the default IP address 192.168.2.1.
Subnet Mask	Input the subnet mask of the new IP address.
Gateway Address	Input the network’s gateway IP address.
DHCP Server	Select “Enabled” if you wish to use the DHCP function of the access point, as detailed below.

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 may

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 192.168.2.1, press and hold the WPS/Reset 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 save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-8-3. DHCP Server

The access point can be configured to act as a DHCP server for your network. By default DHCP is disabled. Enable DHCP by selecting “Enable” in the field “DHCP Server” of “Management IP” as detailed in the previous section.

DHCP Server	
Default Gateway IP	<input type="text" value="0.0.0.0"/>
Domain Name Server IP	<input type="text" value="0.0.0.0"/>
Start IP :	<input type="text" value="192.168.2.100"/>
End IP	<input type="text" value="192.168.2.200"/>
Domain Name	<input type="text"/>
Lease Time	<input type="text" value="Forever"/>

DHCP Server

Default Gateway IP	Specify 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	Choose 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 save changes. The following message will appear:

Save settings successfully!

You may press CONTINUE button to continue configuring other settings or press APPLY button to restart the system to make the changes take effect.

CONTINUE

APPLY

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

III-9. Configuration Tool

- Home
- Basic Settings
- WPS Setting
- Advanced Settings
- Security
- Radius Server
- MAC Filtering
- System Utility
- Configuration Tool**
- Upgrade
- Reset

The access point's configuration tool enables you to back up the current settings, restore the settings to a previously backed up version or reset the access point back to its original factory settings.

Configuration Tool

Use the "Backup" tool to save the Access Point's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Access Point. Alternatively, you can use the "Restore to Factory Default" tool to force the Access Point to perform System Reset and restore the original factory settings.


Backup Settings :	<input type="button" value="Save..."/>
Restore Settings	<input type="button" value="Choose File"/> no file selected <input type="button" value="Upload"/>
Restore to Factory Default	<input type="button" value="Reset"/>

Backup Settings	Click "Save" to save the current settings on your computer as a .bin file. The default filename is config.bin.
Restore Settings	Click the browse button to locate a previously saved configuration file and then click "Upload" to upload the file and 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.



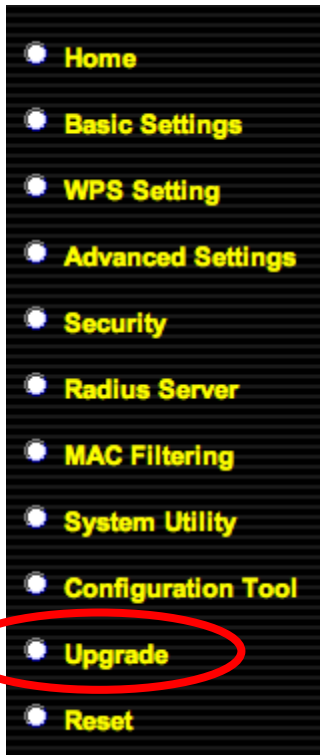
Note: Restoring settings to the factory default will restore all settings, configurations and passwords back to the factory default.



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.

III-10. Upgrade



The access point's upgrade feature allows you to update the system firmware to a more recent version. You can download the latest firmware from the Edimax website.

Selecting "Upgrade" from the menu on the left side will bring you to the following screen.

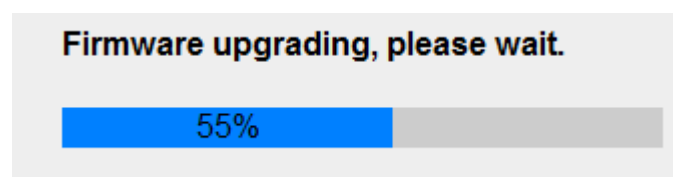
Note: Do not turn off or disconnect the access point during a firmware upgrade, as this could damage the device.



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

A screenshot of the 'WEB Upgrade' page. The title 'WEB Upgrade' is at the top. Below it, there is a paragraph of text: 'This tool allows you to upgrade the Access Point's system firmware. It is recommended that upgrading the firmware from wired stations. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.' Below the text is a 'Choose File' button and the text 'no file selected'.

Click on the "Choose file" button to open a window and locate the downloaded firmware file. Confirm your selection and click "APPLY". A firmware upgrade may take several minutes. The following message will appear:



Please wait for the upgrade to complete. When it is complete, you will see the following message.

Upgrade Accomplished.

You should be able to reconnect to the router by refreshing the web page now. If not, please restart the router by reconnecting the power line manually.

Refresh your browser to return to the “Status and Information” homepage of the browser based configuration device.

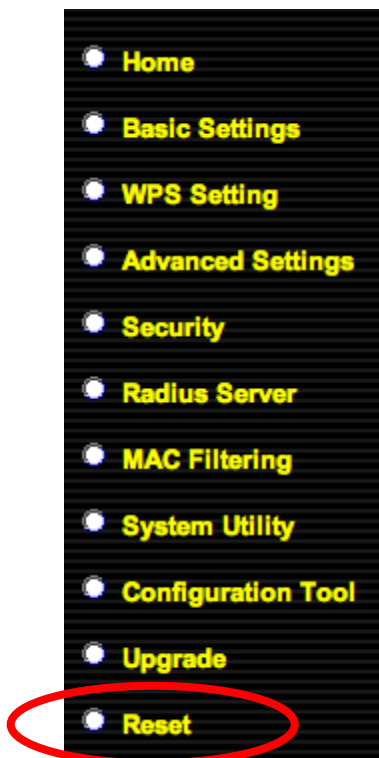
III-11. Reset

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

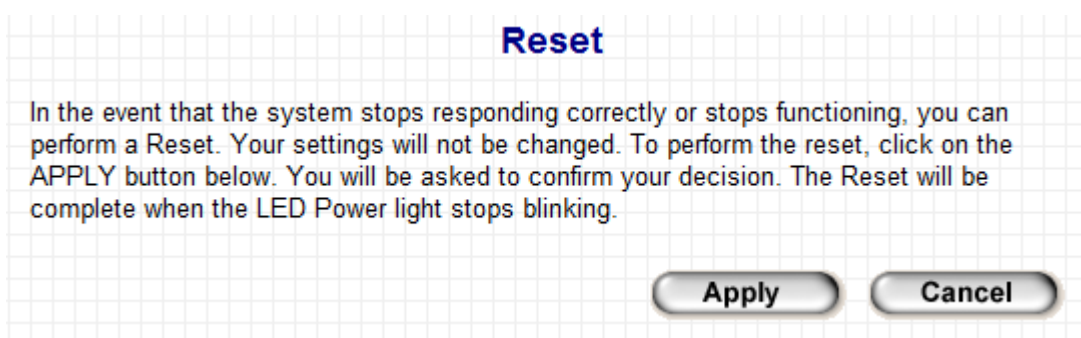
Note: If the access point is still not responding after a reset, then switch off the device by disconnecting the power supply and wait for 10 seconds before reconnecting the power.



Note: Resetting the device will not affect the current settings and configuration.

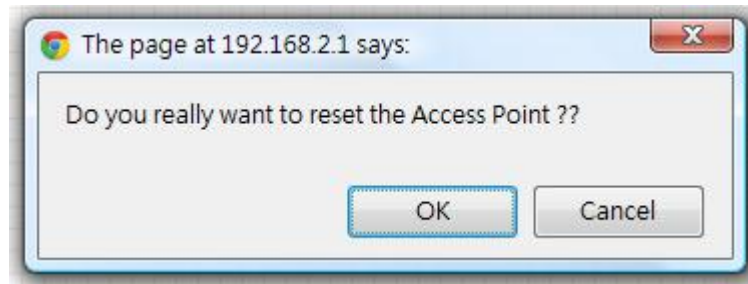


To reset the access point, click “Reset” in the menu on the left side of the browser based configuration interface and the following screen will be displayed.

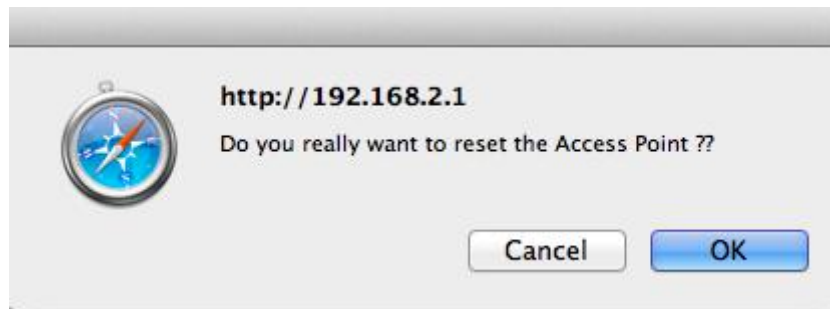


Please click “Apply” to reset the device. A new window will ask you to confirm, as shown below.

Windows:



Mac:

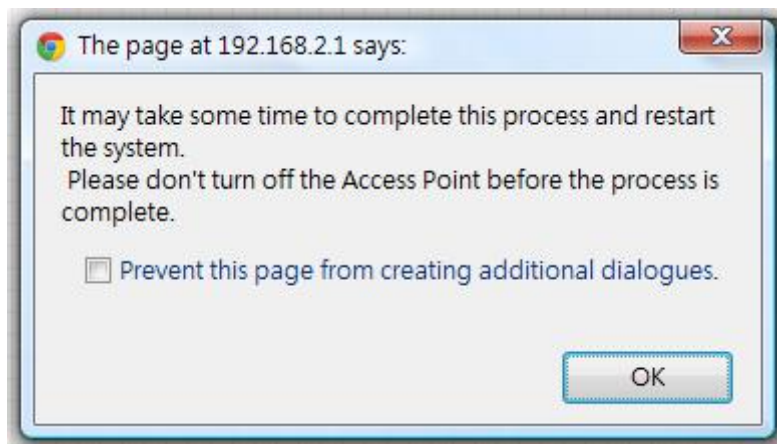


Click "OK" to continue, or "Cancel" to abort. You will see a warning that it may take a while for the access point to reset.



Note: Do not turn off the Access point during the reset process.

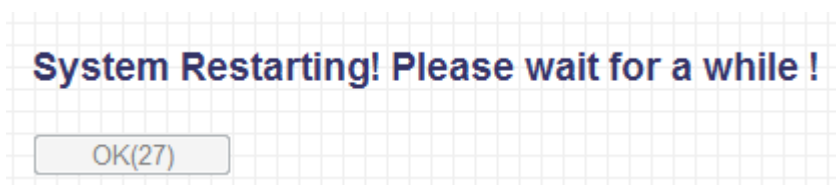
Windows:



Mac:



Please click “OK” to start the reset process. You will see the following screen while the system resets, the timer will count down from 30 seconds.



When the timer reaches zero and the reset is complete, please click “OK”. You will return to the “Reset” page of the browser based configuration interface.

IV. APPENDIX

IV-1. Configuring your IP address

Before you use this access point, you may need to **modify the IP address of your PC or Macintosh**. The procedure for doing so varies across different operating systems; please follow the appropriate guide:

- [IV-1-1. Windows XP](#)
- [IV-1-2. Windows Vista](#)
- [IV-1-3. Windows 7](#)
- [IV-1-4. Windows 8](#)
- [IV-1-5. Mac OS](#)

This is since the access point's default IP address 192.168.2.1 may not be in the same IP address subnet of your network; meaning you are unable to access the browser based configuration interface. In order to access the browser based configuration interface, your computer's IP must be **192.168.2.x** where **x** is a number in the range 1-254, meaning the access point's default IP address is in the same IP address subnet of your network. So if it isn't already, then you need to **modify the IP address of your computer to 192.168.2.10**.

After you access the browser based configuration interface, you can change the IP address of the access point as shown in [III-8-2. Management IP](#), to one that is within the same IP address subnet of your network; meaning you will not have to modify the IP address of your computer again in future when you wish to access the browser based configuration interface.

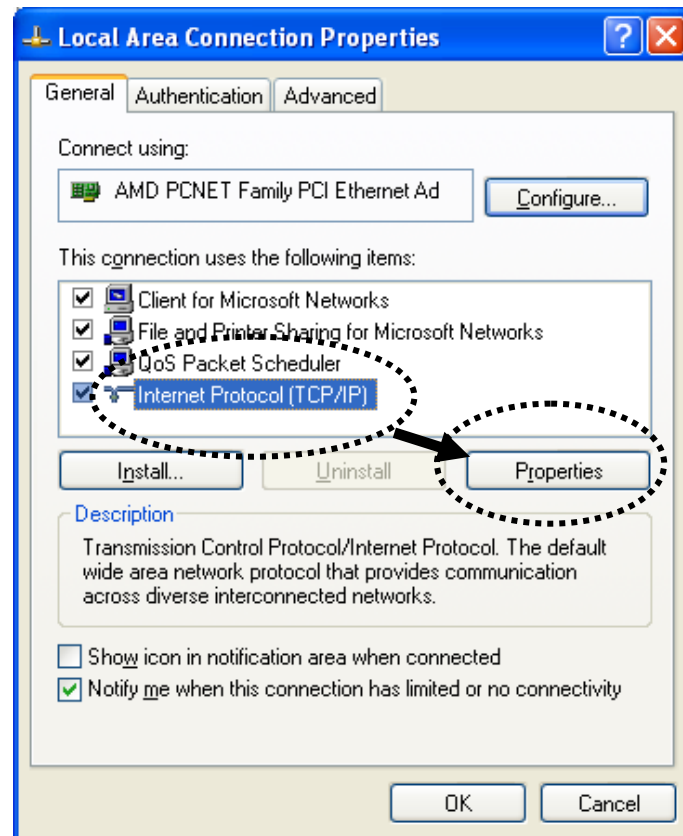


Note: Please ensure that your access point is switched on and connected to your computer via Ethernet cable before you begin.

IV-1-1. Windows XP

1. Click the "Start" button, located in the lower-left corner of your computer, and then click "Control Panel". Double-click the "Network and Internet Connections" icon, followed by "Network Connections" and then double-click "Local Area Connection".

The “Local Area Connection Status” window will appear, click “Properties”.



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

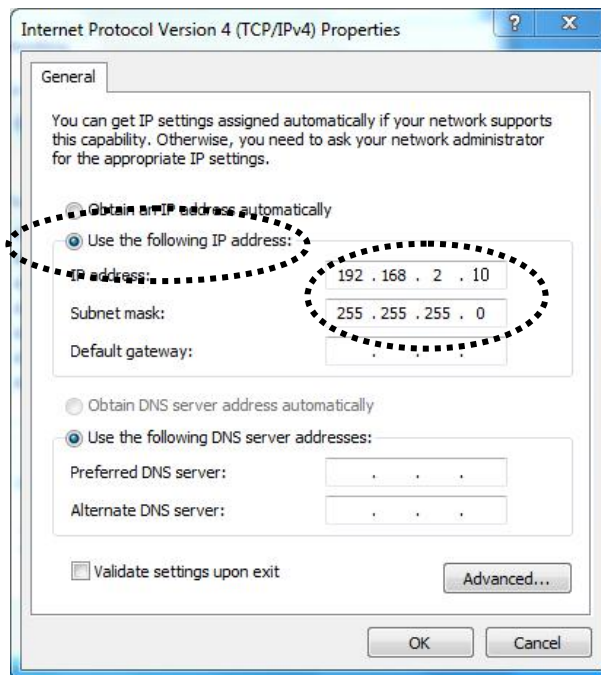


Note: Please note your existing setting before changing it. After you have finished using the browser based configuration interface, change this setting back to its original value.

IP address: 192.168.2.10

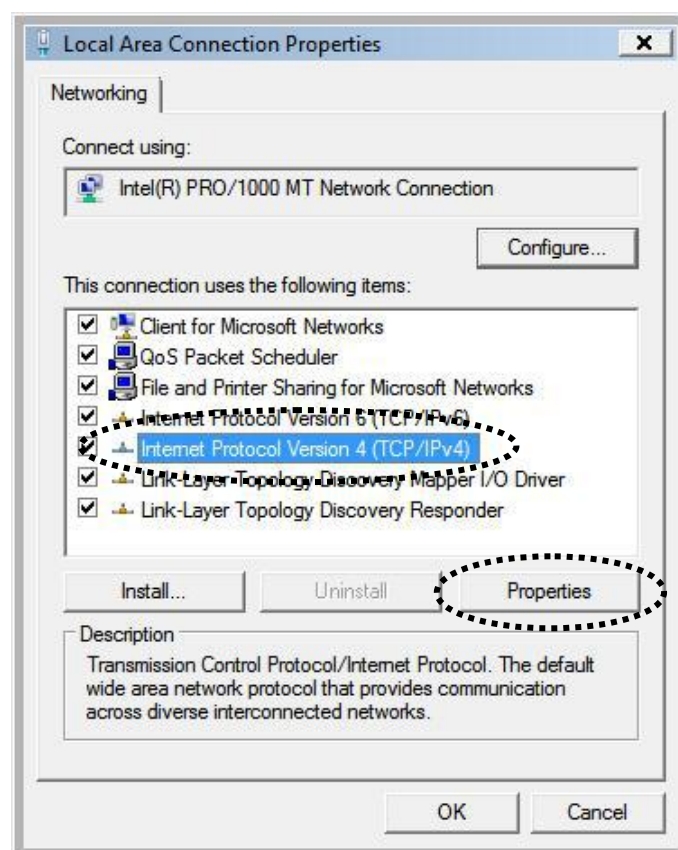
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



IV-1-2. Windows Vista

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



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

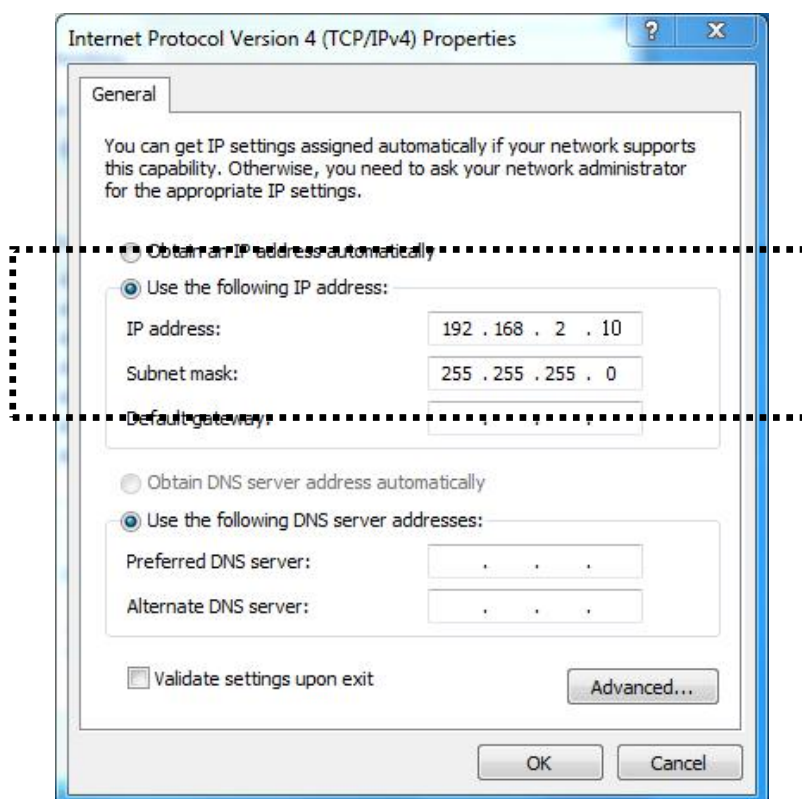
IP address: 192.168.2.10

Subnet Mask: 255.255.255.0



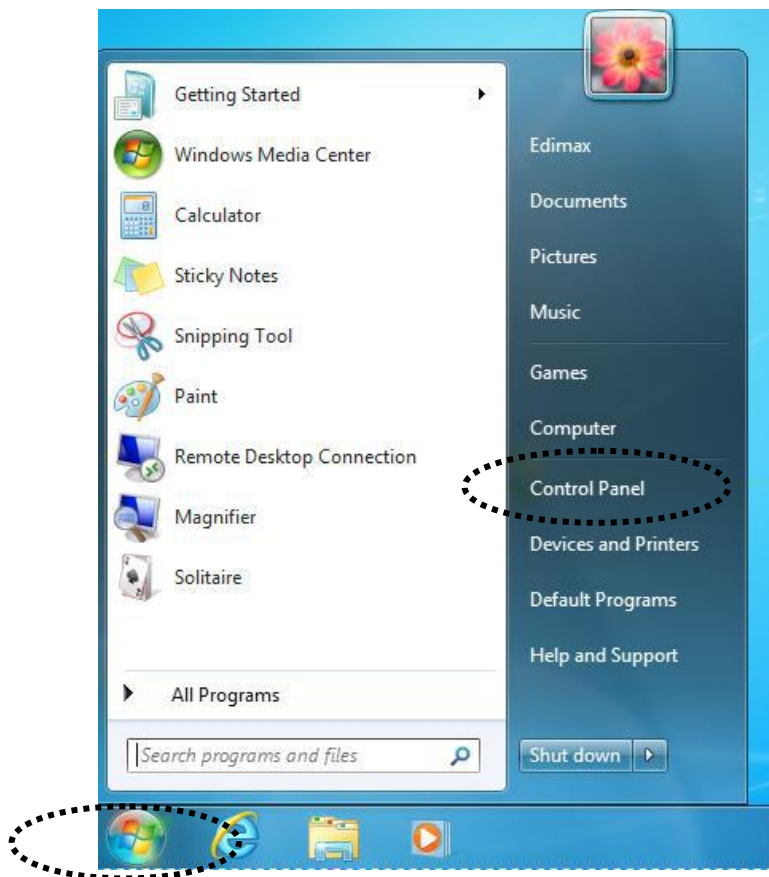
Note: Please note your existing setting before changing it. After you have finished using the browser based configuration interface, you can change this setting back to its original value.

Click ‘OK’ when finished.

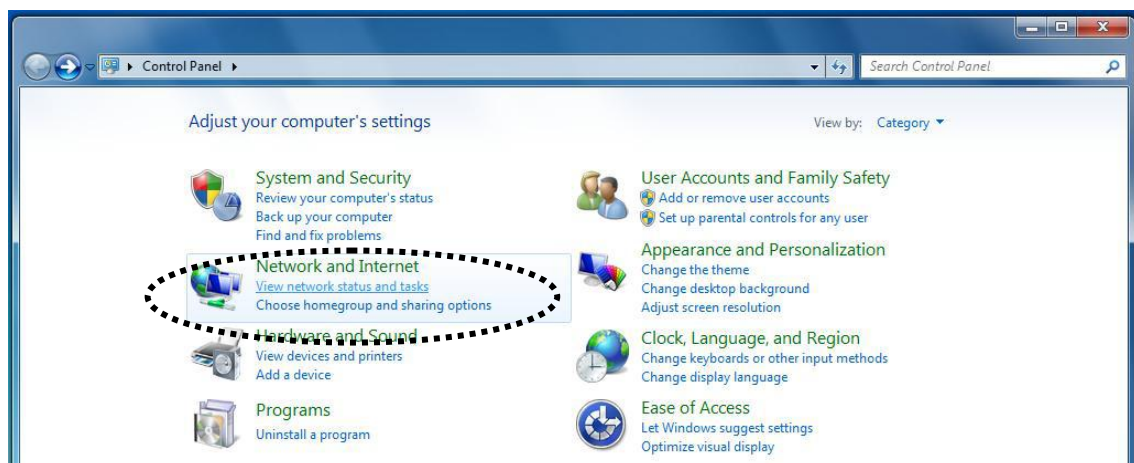


IV-1-3. Windows 7

1. Click the “Start” button, located in the lower-left corner of your computer, and then click “Control Panel”.

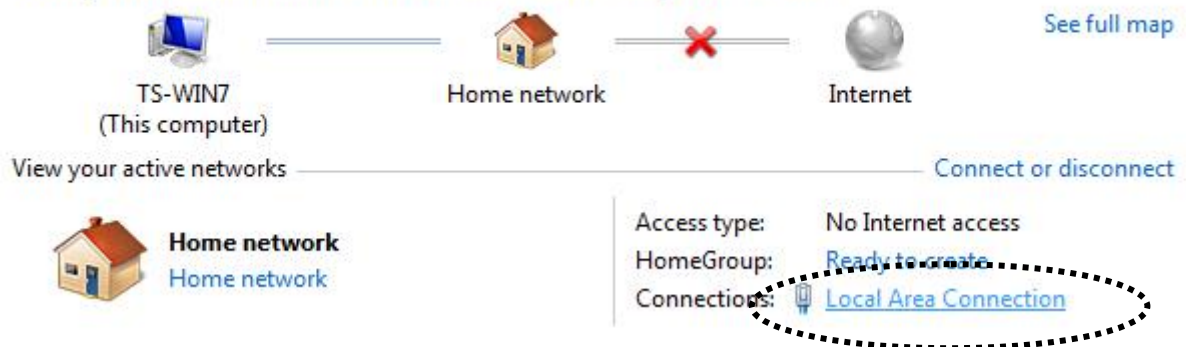


1. Under “Network and Internet” click “View network status and tasks”.

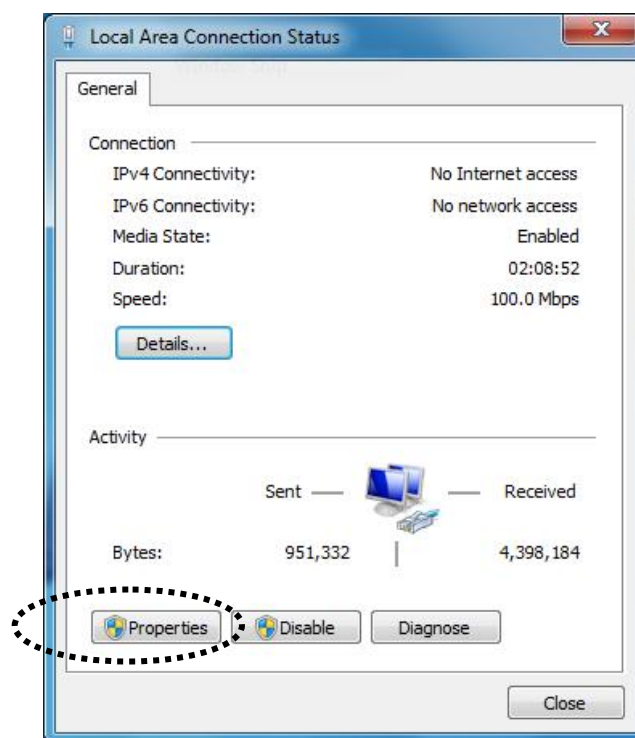


2. Click “Local Area Connection”.

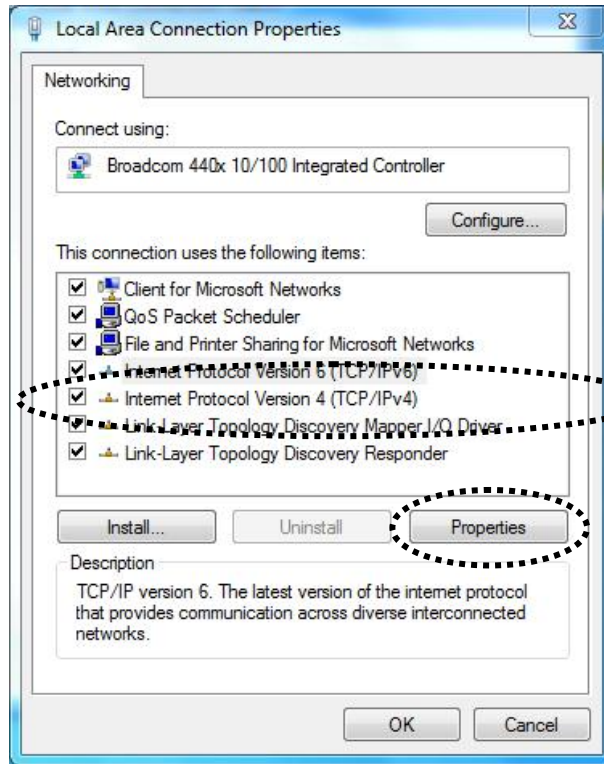
View your basic network information and set up connections



3. Click “Properties”.



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



5. Select “Use the following IP address”, and input the following values:

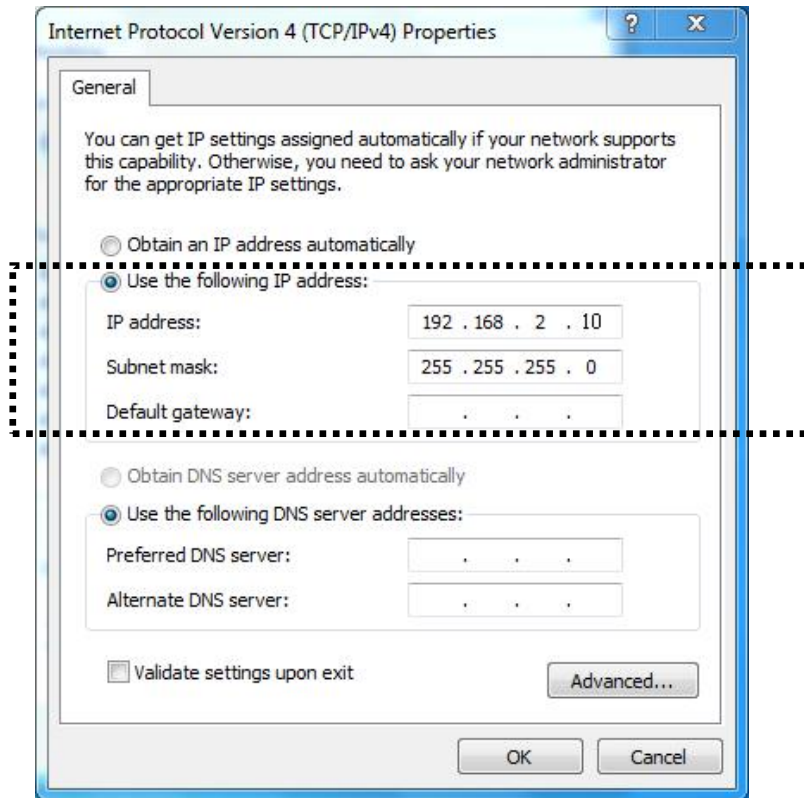


Note: Please note your existing setting before changing it. After you have finished using the browser based configuration interface, you can change this setting back to its original value.

IP address: 192.168.2.10

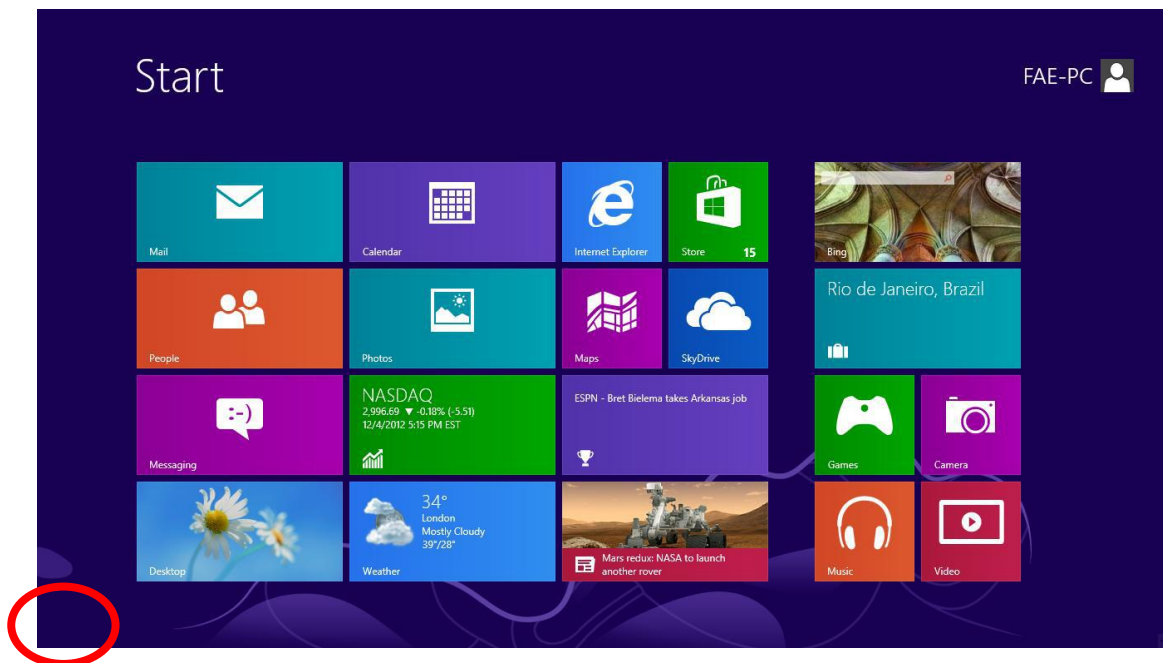
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.

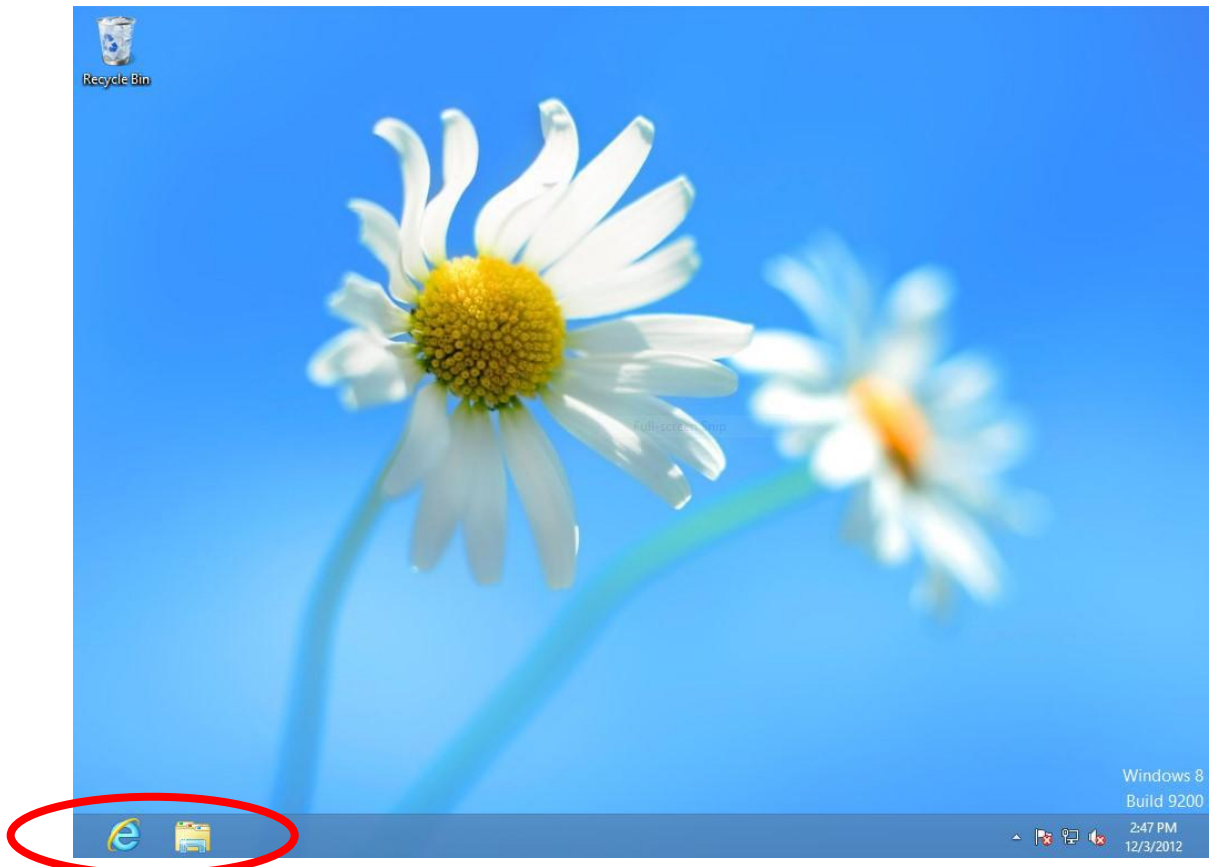


IV-1-4. Windows 8

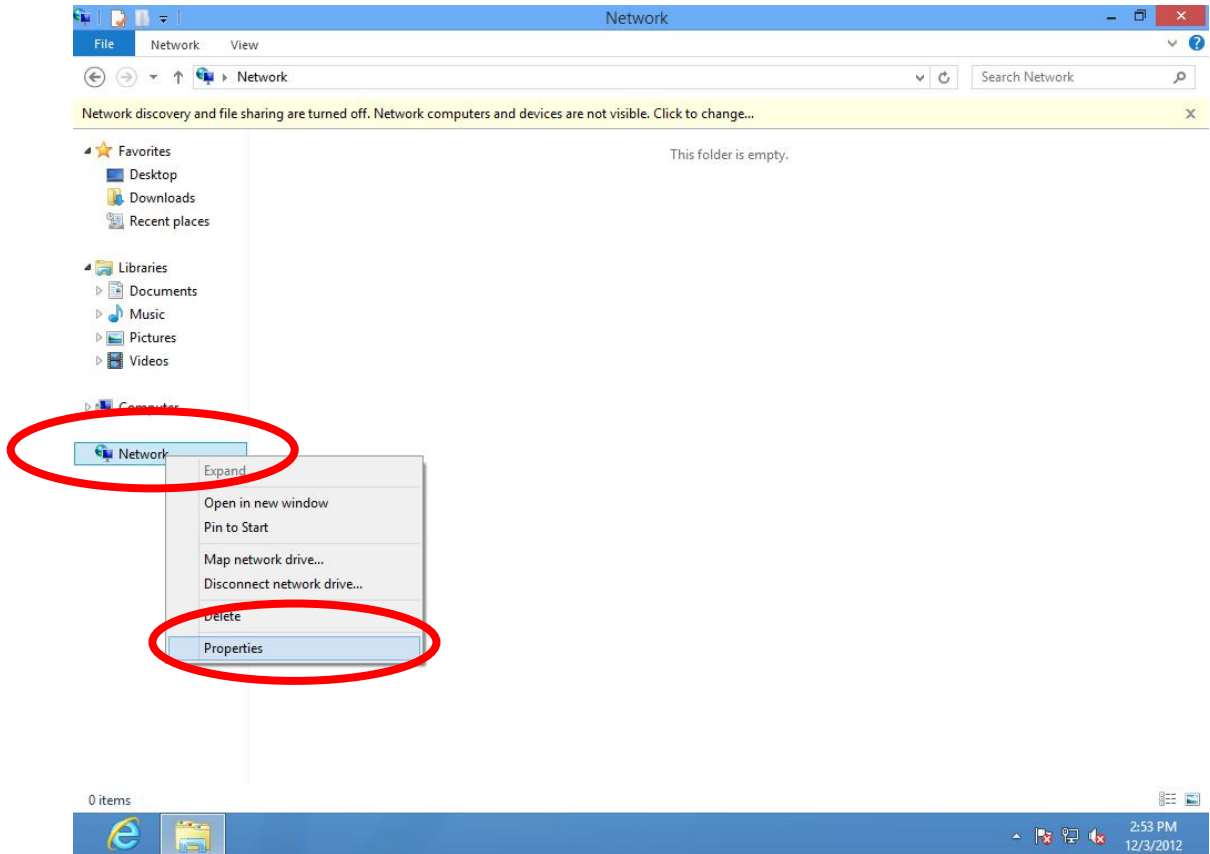
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your cursor to the bottom left of the screen and click.



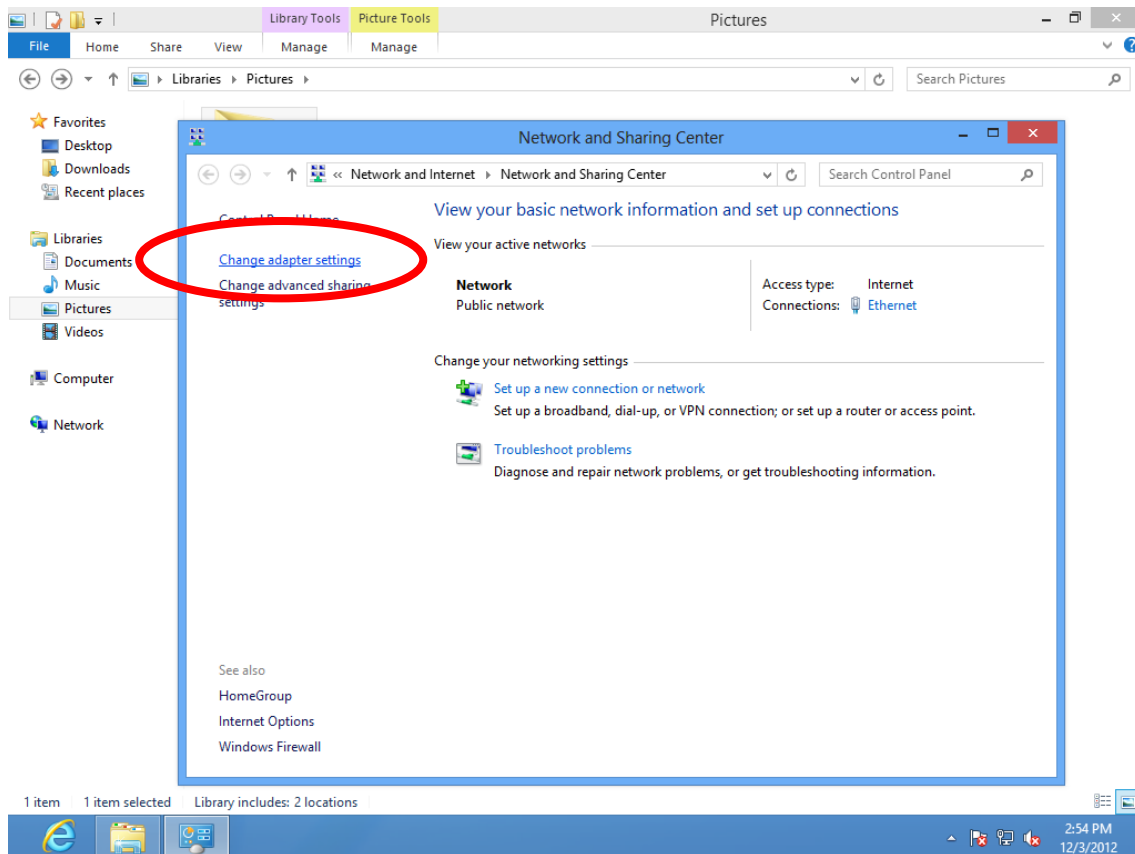
2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



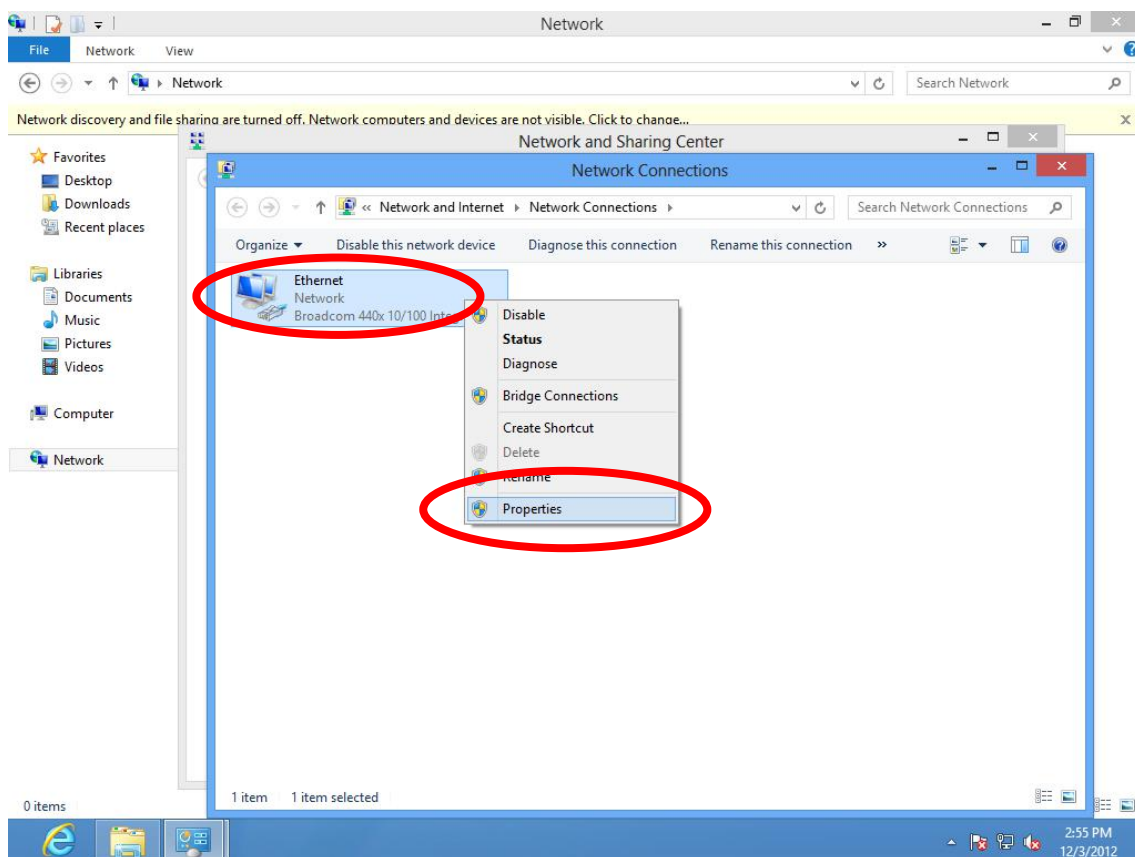
3. Right click “Network” and then select “Properties”.



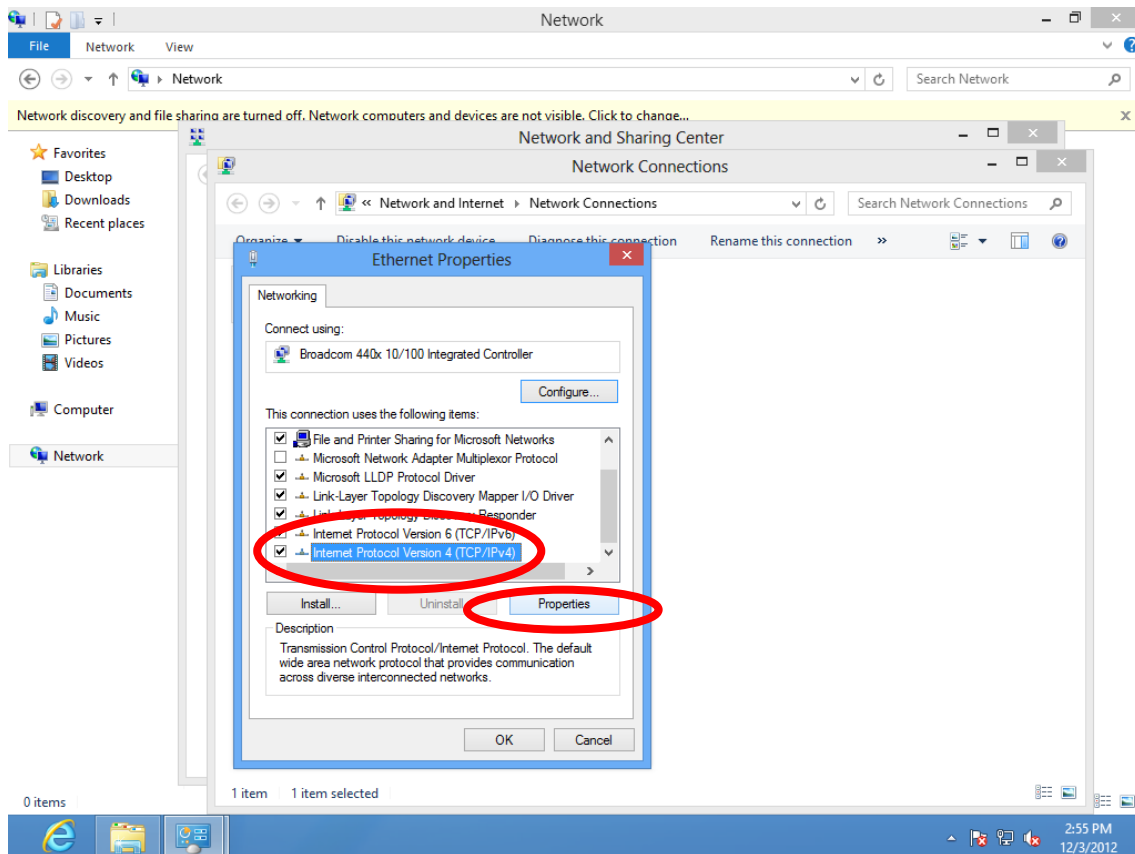
4. In the window that opens, select “Change adapter settings” from the left side.



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



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



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

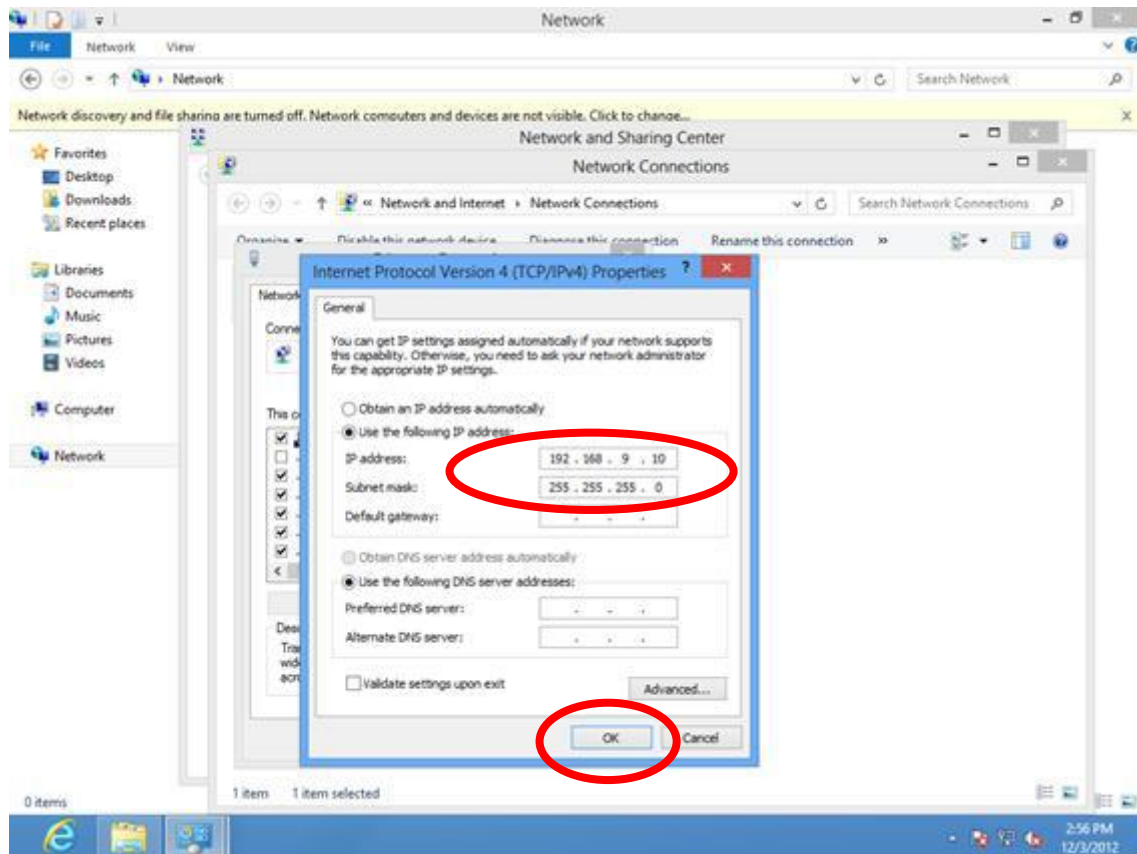


Note: Please note your existing setting before changing it. After you have finished using the browser based configuration interface, you can change this setting back to its original value.

IP address: 192.168.2.10

Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



IV-1-5. Mac OS

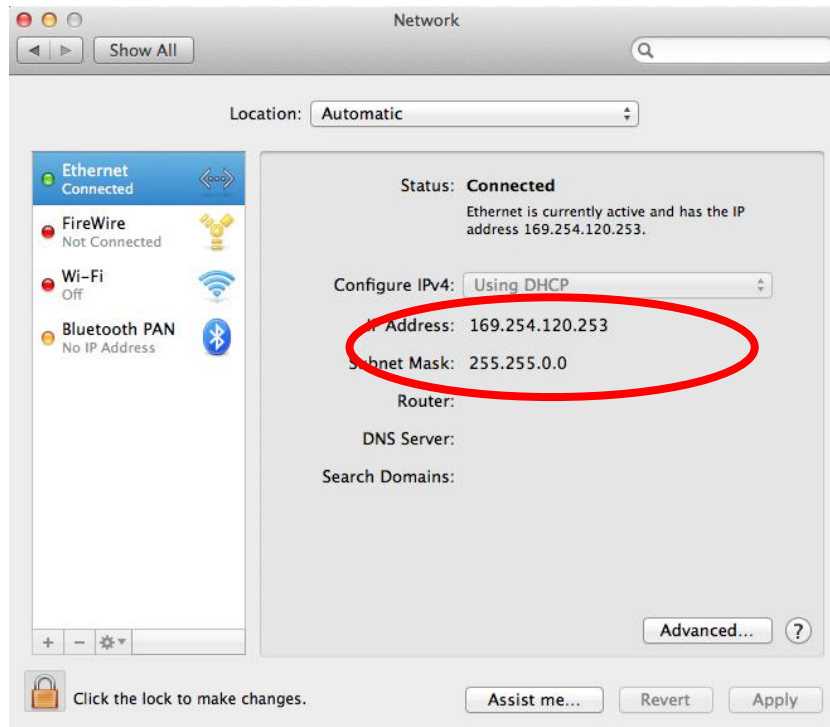
1. Have your Macintosh computer operate as usual, and click on “System Preferences”.



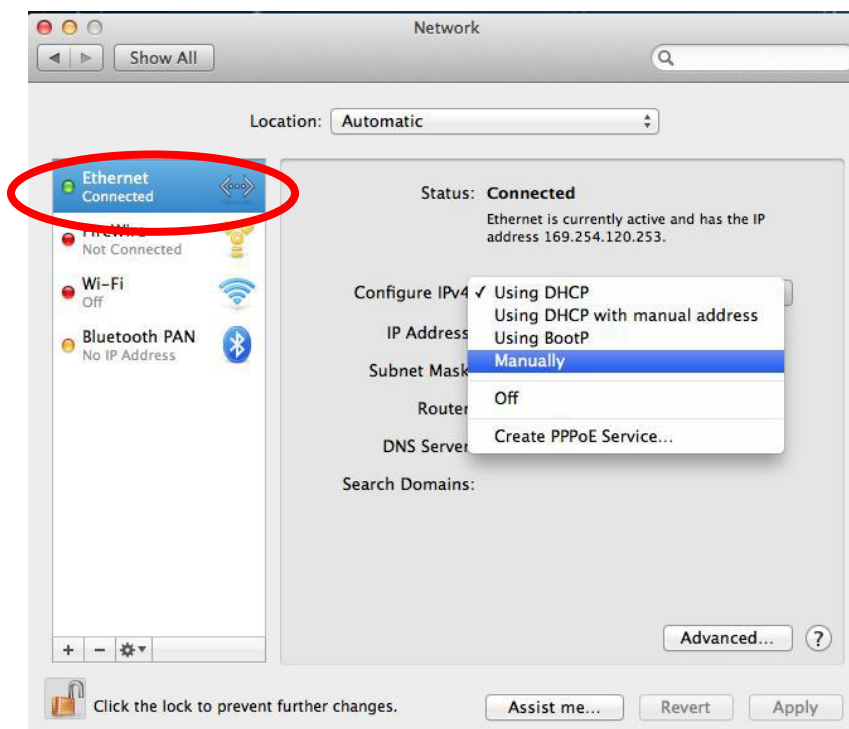
2. In System Preferences, click on “Network”.



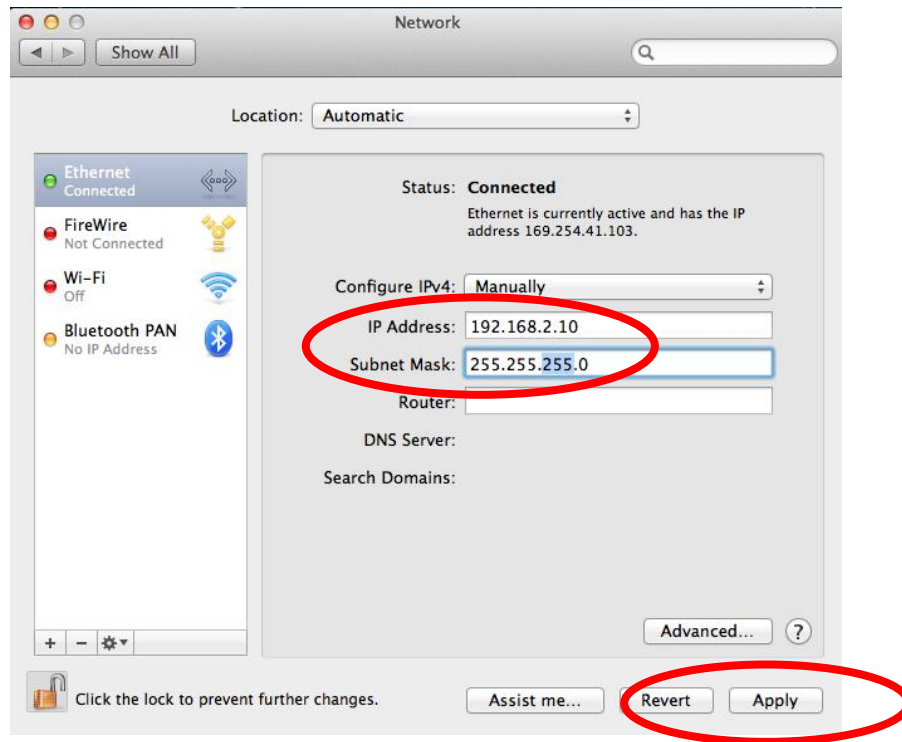
3. Here you will see all of your network connections. Network Preferences will now display an Ethernet adapter, as shown below. The status of “Ethernet” should be “Connected”.



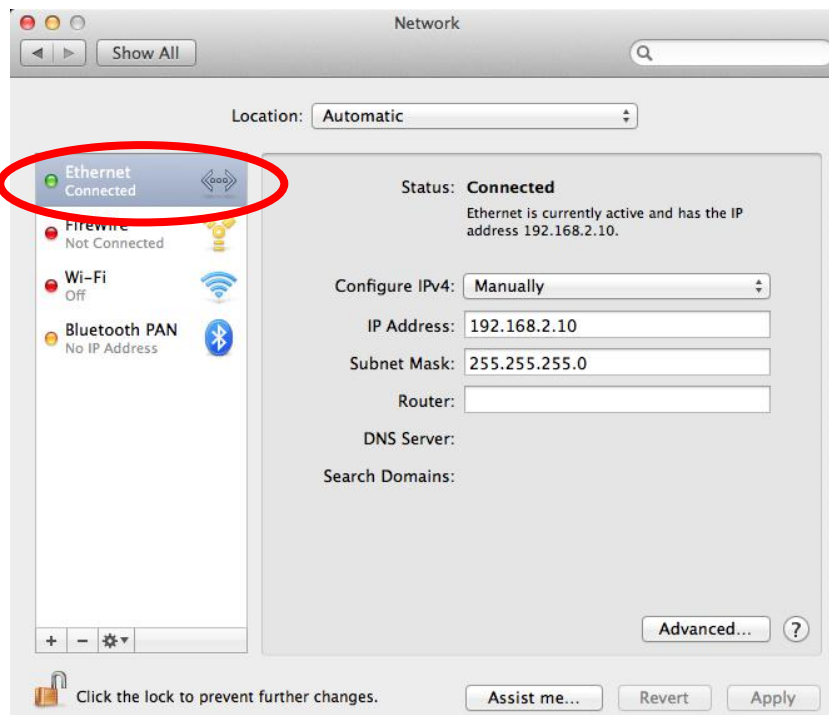
4. Click on “Ethernet” in the left panel and then click the drop down arrow for the menu labeled “Configure IPv4” in the right panel. From the drop down menu, select “Manually”.



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



6. 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. How to Find your Network Security Key

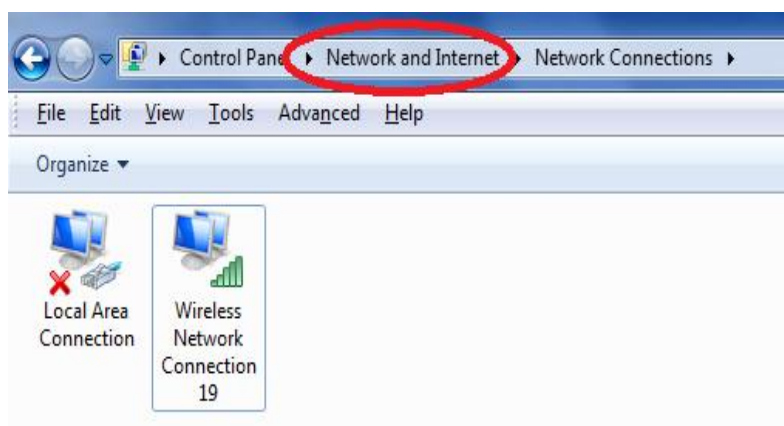
To find your network security key, please follow the instructions appropriate for your operating system.



Note: *If you are using Windows XP or earlier, please contact your ISP or router manufacturer to find your network security key.*

IV-2-1. Windows 7 & Windows Vista

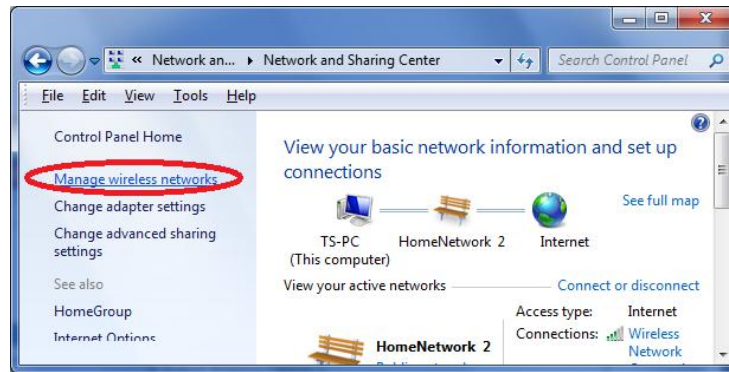
1. Open “Control Panel” and click on “Network and Internet” in the top menu.



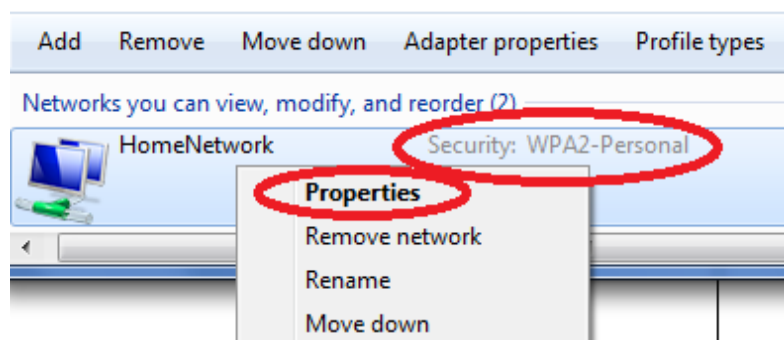
2. Click on “View network status and tasks” which is under the heading “Network and Sharing Center”.



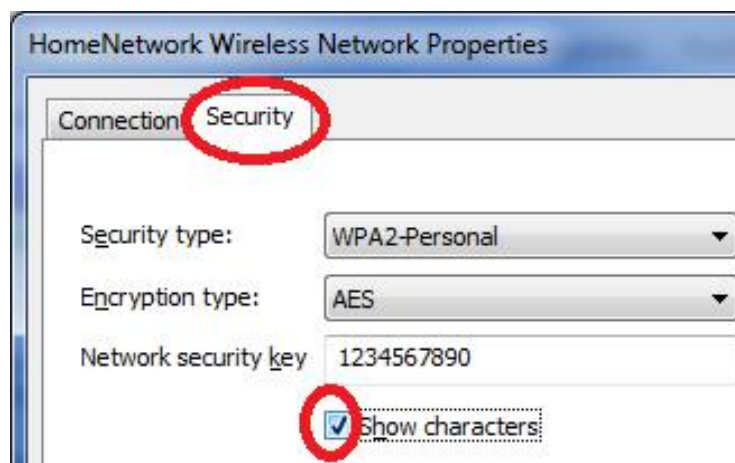
3. Click on “Manage wireless networks” in the left menu.



4. You should see the profile of your Wi-Fi network in the list. Right click on your Wi-Fi network and then click on “Properties”.

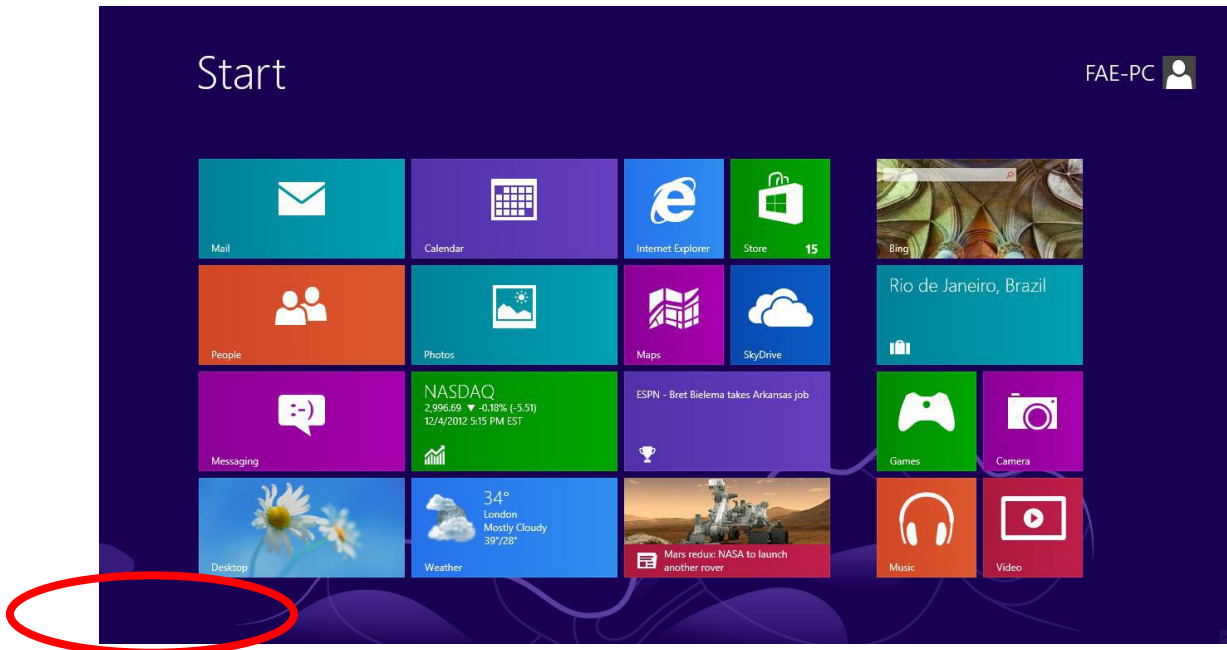


5. Click on the “Security” tab, and then check the box labeled “Show characters”. This will show your network security key. Click the “Cancel” button to close the window.

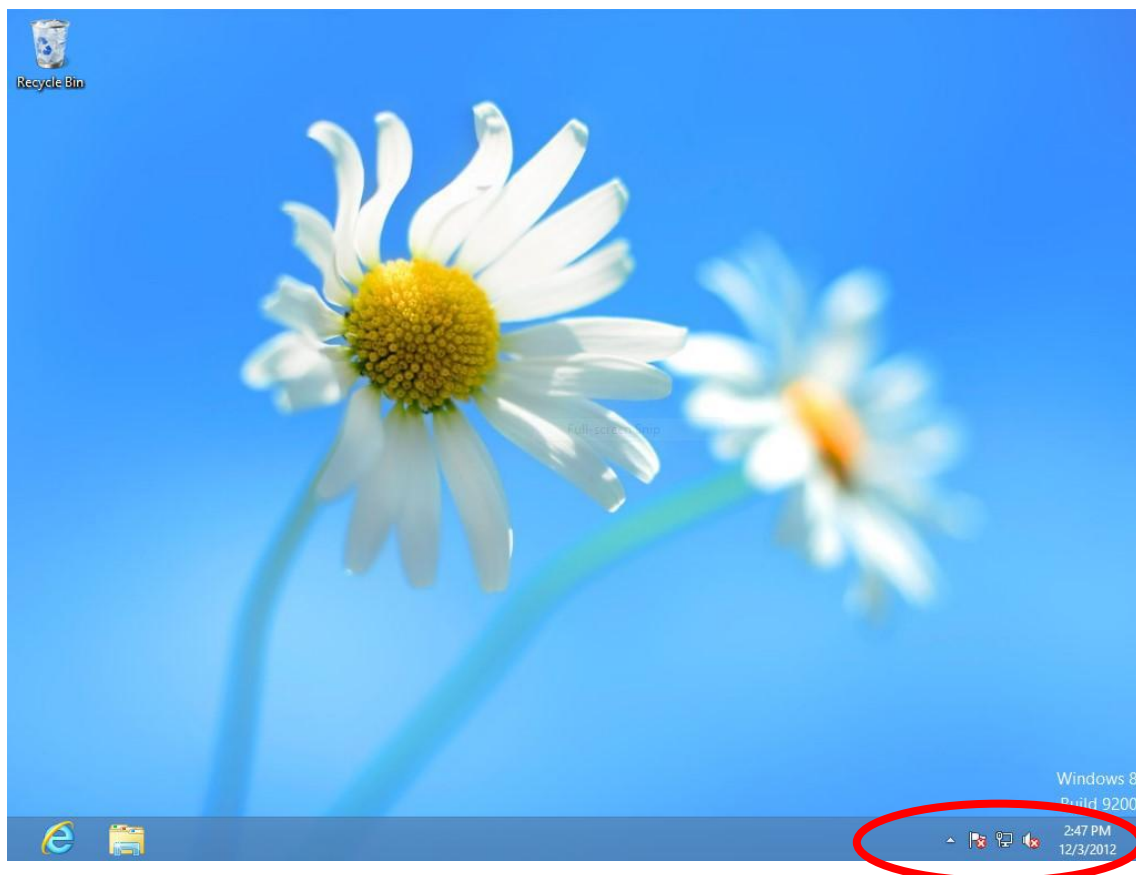


IV-2-2. Windows 8

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

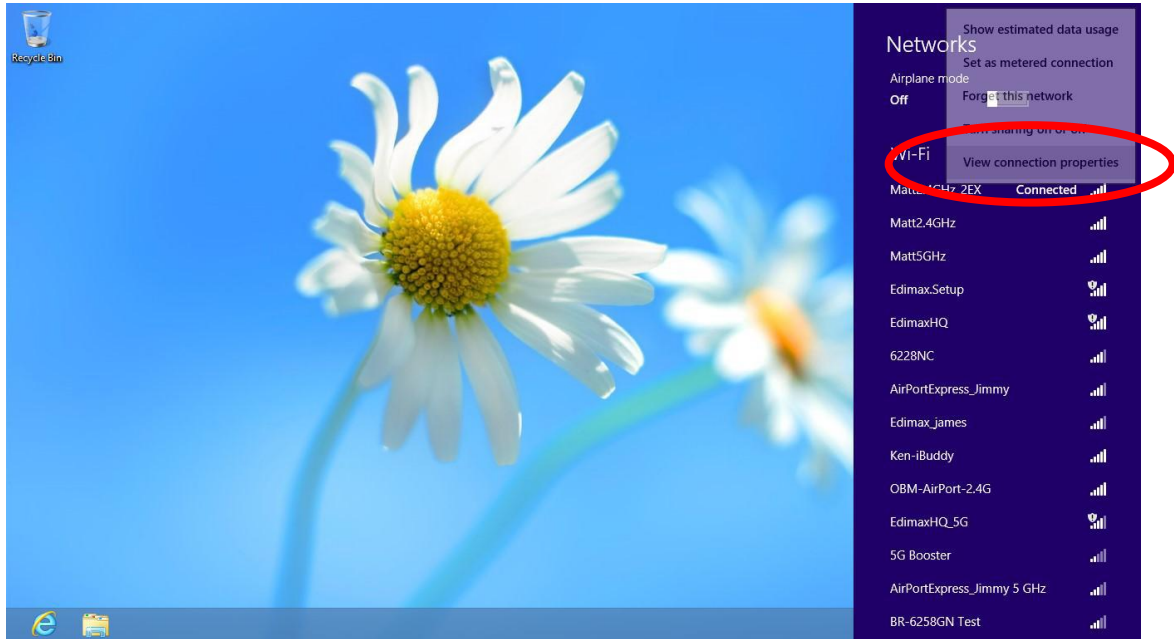


2. In desktop mode, click the network icon in the bottom right corner.

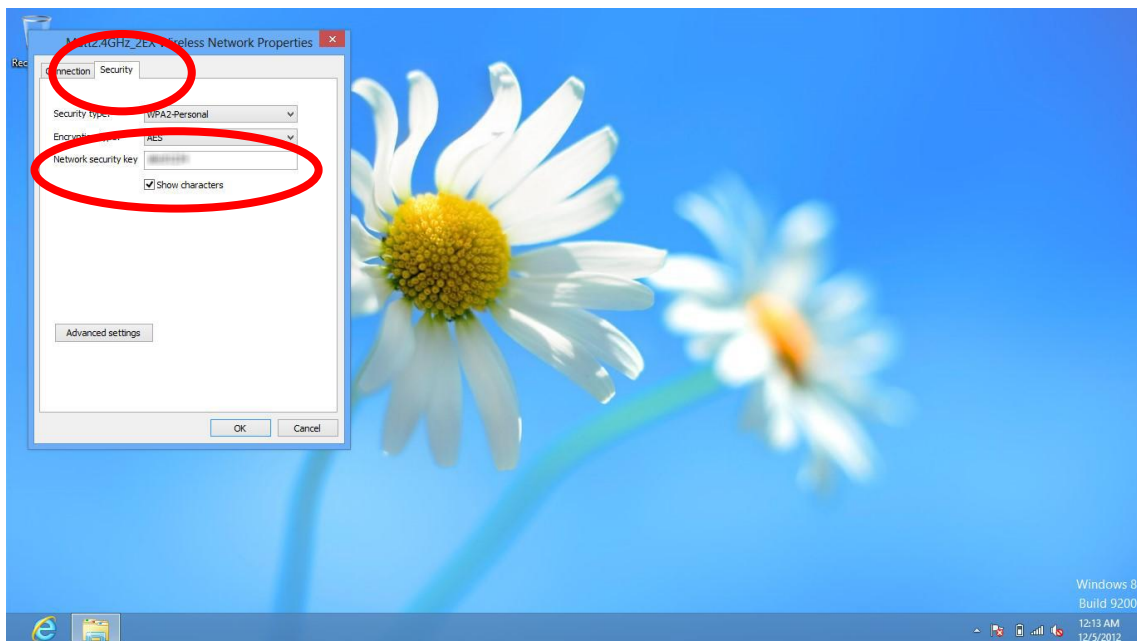


3. Select your Wi-Fi connection from the list and right click. Select "View

connection properties”.

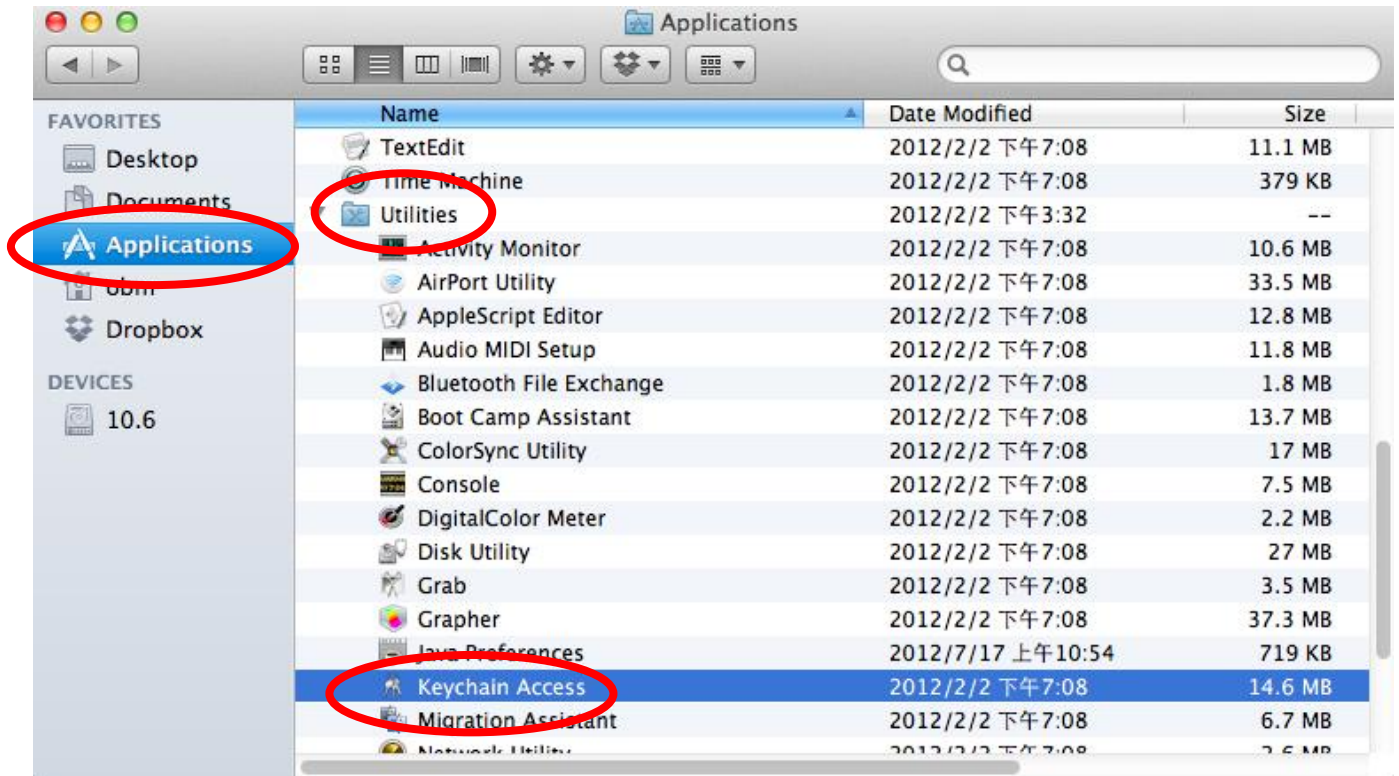


4. In the window that opens, click the “Security” tab and check the box labeled “Show characters”. Your network security key will be displayed in the field “Network security key”.

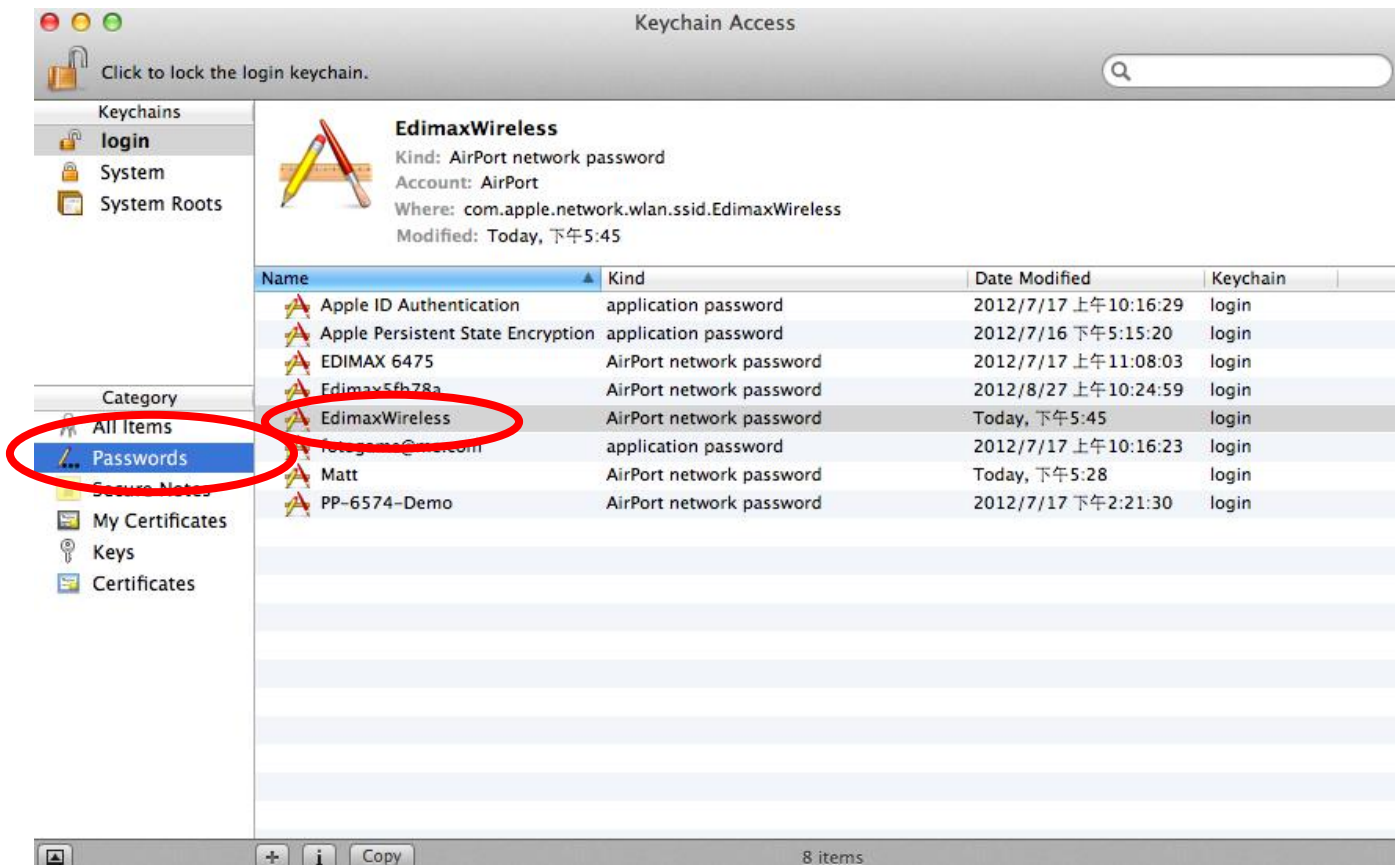


IV-2-3. Mac

1. Open a new Finder window, and select “Applications” from the menu on the left side. Open the folder labeled “Utilities” and then open the application “Keychain Access”.



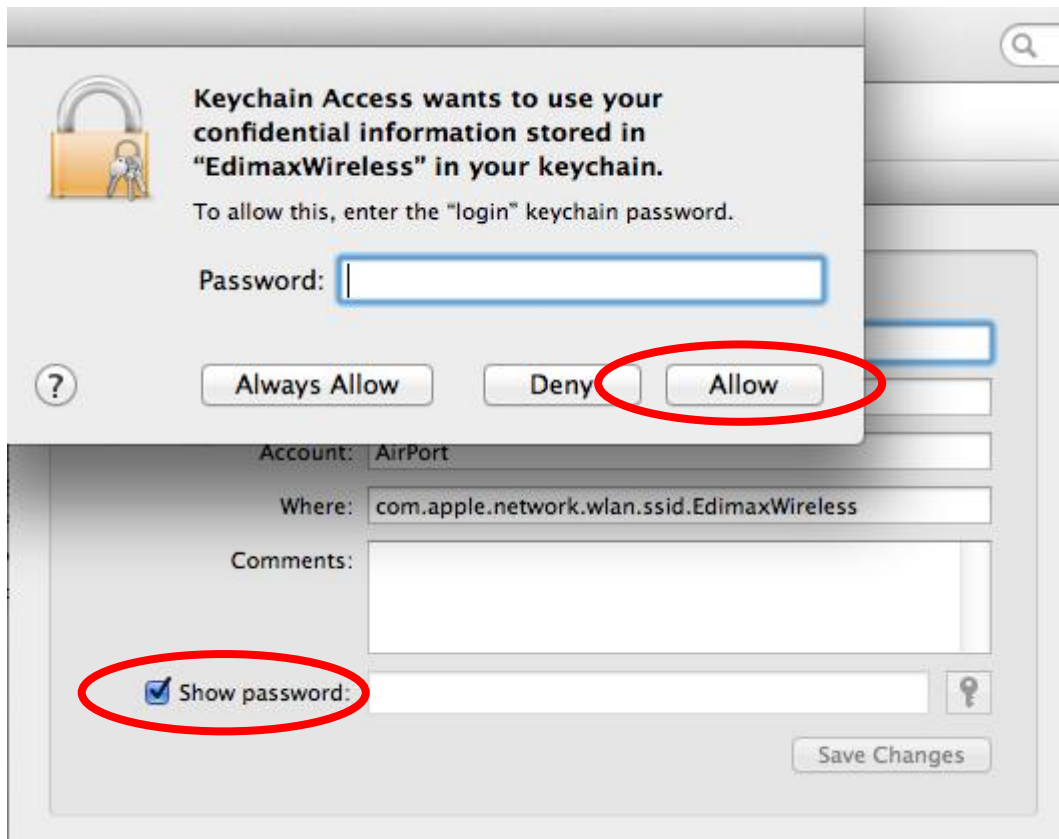
2. Select “Passwords” from the sub-menu labeled “Category” on the left side, as shown below. Then search the list in the main panel for the SSID of your network. In this example, the SSID is “EdimaxWireless” – though your SSID will be unique to your network.



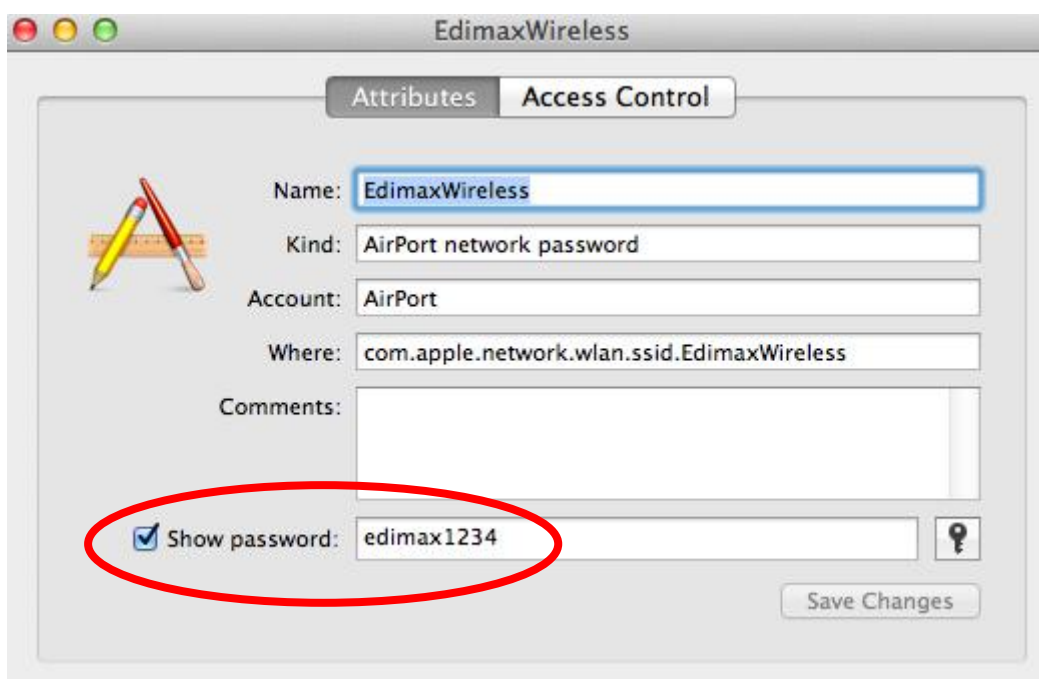
3. Double click the SSID of your network and you will see the following window.



4. Check the box labeled “Show password” and you will be asked to enter your administrative password, which you use to log into your Mac. Enter your password and click “Allow”.



Your network security password will now be displayed in the field next to the box labeled "Show password". In the example below, the network security password is "edimax1234". Please make a note of your network security password.



IV-3. 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
My access point can't locate a wireless access point/wireless device when using the "Site Survey" function.	<ol style="list-style-type: none">Click "Rescan" several more times and see if the wireless access point/device appears.Adjust the position of the access point, or move closer to a known wireless access point.If the SSID of the access point you wish to connect to is hidden (nothing displayed in the "SSID" field in the "Site Survey" function), then you need to input the SSID manually. Ensure that you input the correct SSID.
My access point can't establish a connection with a particular wireless access point.	<ol style="list-style-type: none">Click "Connect" several more times and see if you can establish a connection.Ensure that you input the correct passphrase/security key if connecting to an access point with encryption.It is possible that the access point you wish to connect to only allows network cards with specific MAC address's to establish connections. Request that the owner/administrator of the access point add your MAC address to the list.
I can't log onto the browser-based configuration interface: the access point is not responding.	<ol style="list-style-type: none">Make sure access point is powered on. Check the LED on the front panel. If the LED is out, then check the USB connection.Use your wireless device connects to this access point wirelessly.Make sure you are using the correct IP address.If you are using a MAC or IP address filter, try to connect the access point to another computer.Set your computer to obtain an IP address automatically (DHCP), and see if your computer can obtain an IP address.If you are experiencing problems after a firmware upgrade, please contact your dealer of purchase for help.
I can't locate the access point with my wireless	<ol style="list-style-type: none">Check if "Broadcast ESSID" (in the "Wireless Advanced" section of the browser-based

client.	configuration interface) is “Enabled” or “Disabled”. If “Disabled” you need to input the ESSID into your wireless client manually. b. Try moving closer to the access point
File transfers are slow or frequently interrupted.	a. Try to move closer to where the wireless access point is located. b. Try again later. Your local network may be experiencing technical difficulties or very high usage. c. Change channel number.
I can't log onto the browser-based configuration interface: incorrect password.	a. Password is case-sensitive. Make sure the “Caps Lock” light is not illuminated. b. If you do not know your password, restore the device to factory settings.
The access point is extremely hot.	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. 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.

IV-4. 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 “.”:

bbbbbbbbb.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 protocol. 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.

IV-5. Technical Support

Support documentation is available on the enclosed CD and on our global websites.

Headquarters

Tel: +886-2-77396888

Fax: +886-2-77396887

Support: support@edimax.com.tw

European Headquarters

Tel: +31-499-377344

Fax: +31-499-372647

Support: support@edimax.nl

French Office

Tel: +33-160535680

Fax: +33-160535689

Support: support@edimax.fr

German Office

Tel: +49-215488-77334

Fax: +49-215488-77339

Support: support@edimax-de.eu

Poland Office

Tel: +48-22-6079480

Fax: +48-22-6079481

Support: support@edimax.pl

Romania Office

Tel: +40-31-4250126

Fax: +40-31-4250125

Support: support@edimax.ro

Russia Office

Tel: +7-499-7266678

Email: sales@edimax.ru

Support: support@edimax.ru

Ukraine Office

Tel: +38 (044) 4983091, +38 (044) 4983092

Fax: +38 (044) 4983093

Support: support@edimax.ua

United Kingdom Office

Tel: +44-845-1238307

Fax: +44-845-1238306

Support: support@edimax.co.uk

USA Office

Tel: +1-408-4961105

Fax: +1-408-9801530

Support: support@edimax.com

Australia Office

Tel: +61-3-95431888

Fax: +61-3-98992746

Tech Support: 1300 540 833

Email: sales@edimax-au.com

Support: support@edimax-au.com

China Office

Tel: +8610-82665815

Fax: +8610-82665795

Support: service@edimax.com.cn

Hong Kong Office

Tel: +852-2169 6311

Fax: +852-2169 6300

Support: service@edimax.com.cn

India Office

Technical & RMA Support: +91 9867520529 / 9888060206

Bulk & Corporate Enquiries: +91 9818029555

Working Hours: 10am ~ 7pm (IST) Monday ~ Saturday (except national holidays)

Email: support_india@edimax.com.tw

MEA Office

Tel: +971-4-804-1888

Support: +971 800 334629 [800-EDIMAX]

Fax: +971-4-883-4079

Support: technical.support@edimax-me.com

South East Asia Office

Singapore Authorized Service Centre

Tel: +65 6334 2298 (11am ~ 8pm, Monday ~ Sunday)

Technical Support Hotline: 31062273

(9am~6pm, Monday ~ Friday except national holidays)

Support: support@edimax.com.sg

Cambodia Service Centre

Sales & Technical Hotline: +855 (23) 996 638

(9am ~ 5:30pm, Monday ~ Friday except national holidays)

(9am ~ 12:30pm Saturday)

Support: service@i-qlick.com

Malaysia - Kuala Lumpur Authorized Service Centre

Technical Hotline: 03 2052 4288; 03 9130 7728

(11am ~ 8pm, Monday ~ Friday except national holidays)

Email: sales@edimax.com.sg

Support: support@edimax.com.sg

Indonesia - Jakarta Authorized Service Centre

Sales & Technical Hotline: 021 70777 629

(9am ~ 6pm, Monday ~ Sunday except national holidays)

Support: idsupport@edimax.com.sg



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