EDIMAX
NETWORKING PEOPLE TOGETHER

EW-7228APn

User Manual

08-2012 / v1.1

COPYRIGHT

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

Thank you for purchasing the Edimax EW-7228APn wireless access point. This product provides wireless access to an existing wired Ethernet network, at speeds up to 150Mbps for 802.11n compatible wireless devices. Its quick and easy installation process ensures that anybody can set up a network environment and share an Internet connection in a matter of minutes.

I-1. Package Contents

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

- Wireless Access Point
- CD containing setup wizard, multi language quick installation guide and user manual
- Power Adapter
- 3dBi Antenna
- Accessory Kit
- Quick installation guide

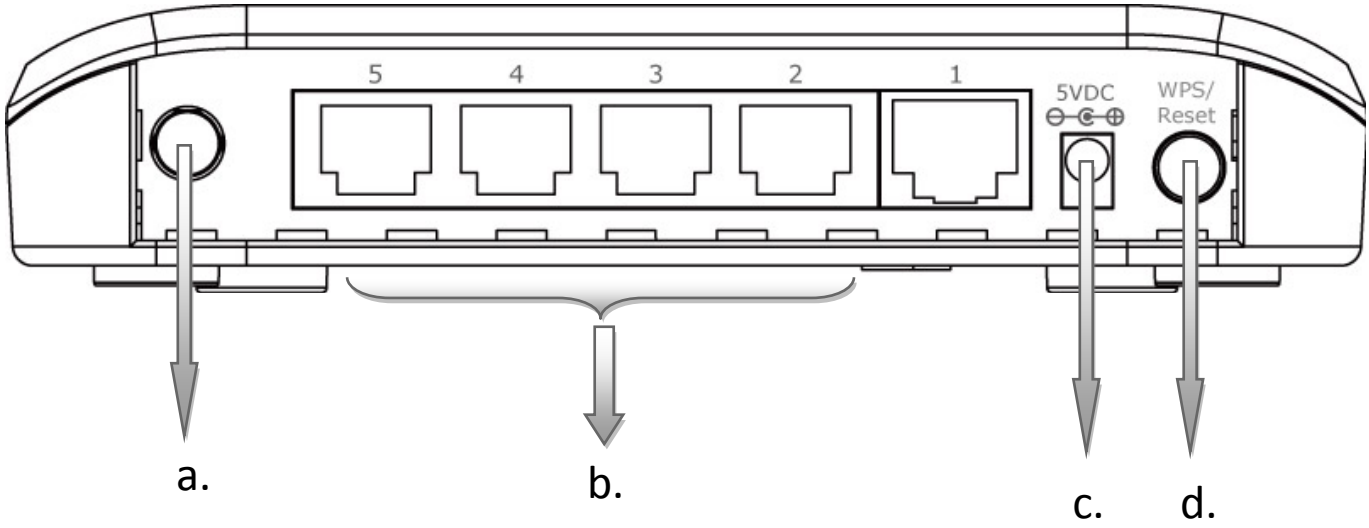
I-2. Description

Front panel:

Item	Color	Status	Description
PWR (Power)	Green	On	Device is on
		Off	Device is off
WLAN (Wireless LAN)	Orange	Flashing	Data is being transmitted wirelessly
		Off	Data is not being transmitted wirelessly
1 to 5	Green	On	Ethernet port is connected to a device

(LAN Ports 1 to 5)		Flashing	Data is being transmitted through the Ethernet cable
		Off	No connection

Back panel:



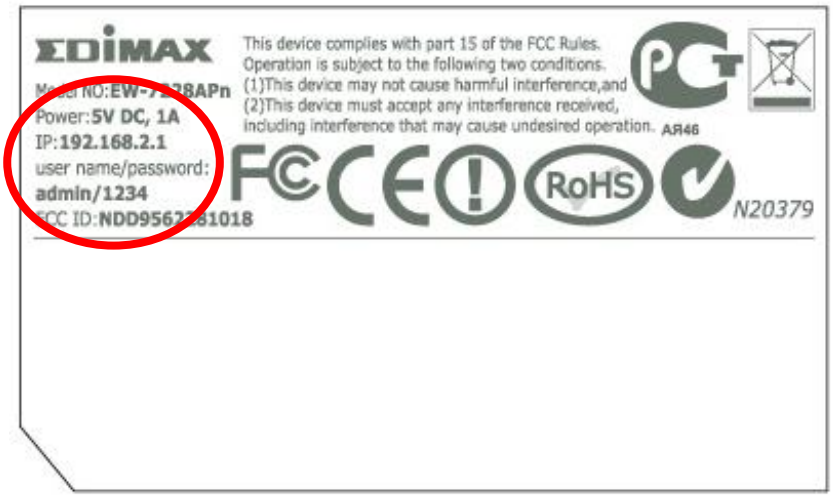
a. **Antenna Connector**
Connect the included 3dBi antenna here. It is a round connector (standard reverse SMA).

b. **10/100M LAN Ports**
Connect wired computers or other network devices to these ports..

c. **5V DC**
Connect the included power adapter here.

d. **WPS/Reset Button**
Press this button and hold for 20 seconds to reset the access point to factory default settings. Press this button for less than 5 seconds to start WPS functions.

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


EDIMAX
Model NO:EW-7228APn
Power:5V DC, 1A
IP:192.168.2.1
user name/password:
admin/1234
FCC ID:NDD9567281018
This device complies with part 15 of the FCC Rules.
Operation is subject to the following two conditions.
(1)This device may not cause harmful interference,and
(2)This device must accept any interference received,
including interference that may cause undesired operation.
AR46
RoHS
N20379

I-3. Safety Information

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

1. The travel router is designed for indoor use only; do not place the travel router outdoors.

2. Do not place the travel router 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 travel router.

4. Take care when moving and handling the travel router; accidental damage is not covered by the travel router's warranty.

5. The device contains small parts which are a danger to small children under 3 years old. Please keep the travel router out of reach of children.

6. Do not place the travel router on paper, cloth, or other flammable materials. The travel router will become hot during use.

7. There are no user-serviceable parts inside the travel router. If you experience problems with the travel router, please contact your dealer of purchase and ask for help.

8. The travel router 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 travel router, then disconnect the travel router 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 Windows98/2000/XP/Vista/7, Mac OS.
- Web Browser for software configuration (Internet Explorer 7 or above, Google Chrome, Firefox, Safari)

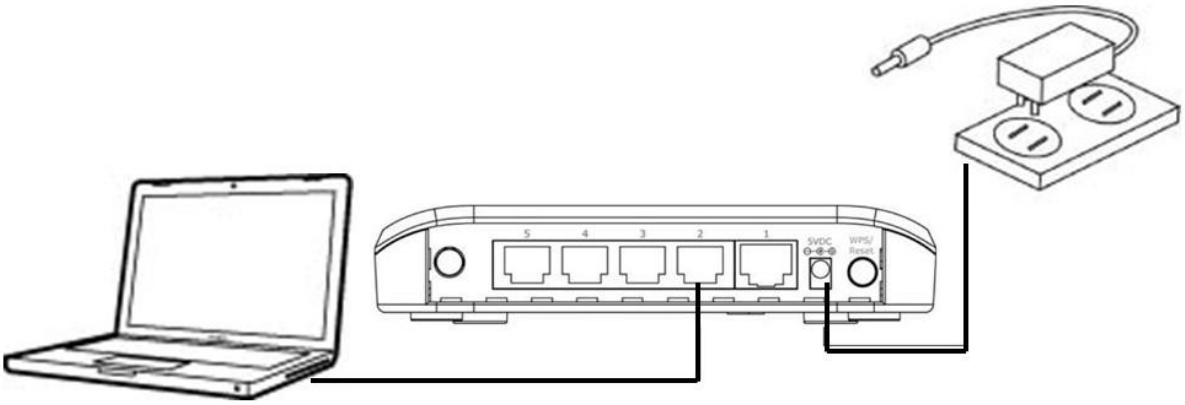
II. Quick Installation

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.

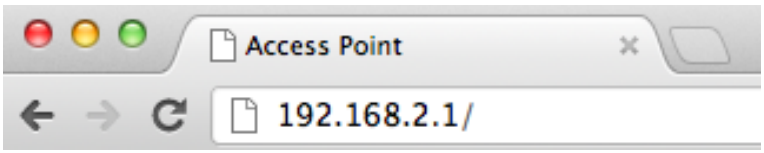


Refer to the following instructions appropriate for your operating system.

II-1. Mac

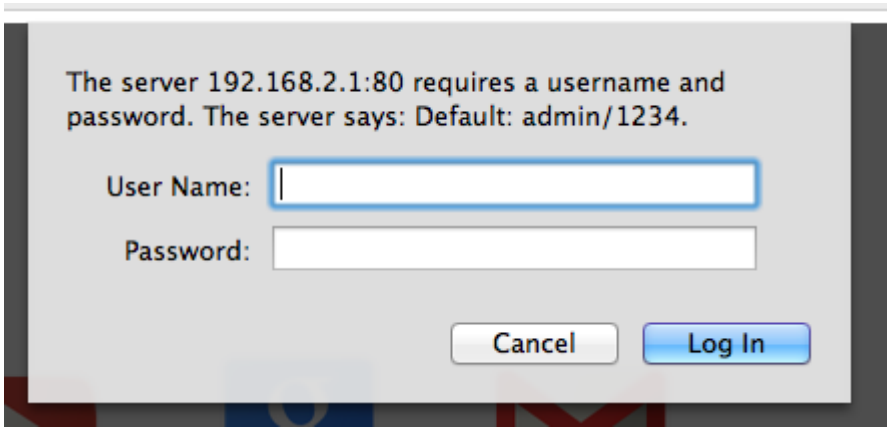
MAC USERS: You may need to modify the IP address of your computer before you can setup the access point. For guidance on how to do this, please see **Appendix IV-1. Configuring your IP Address**.

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.

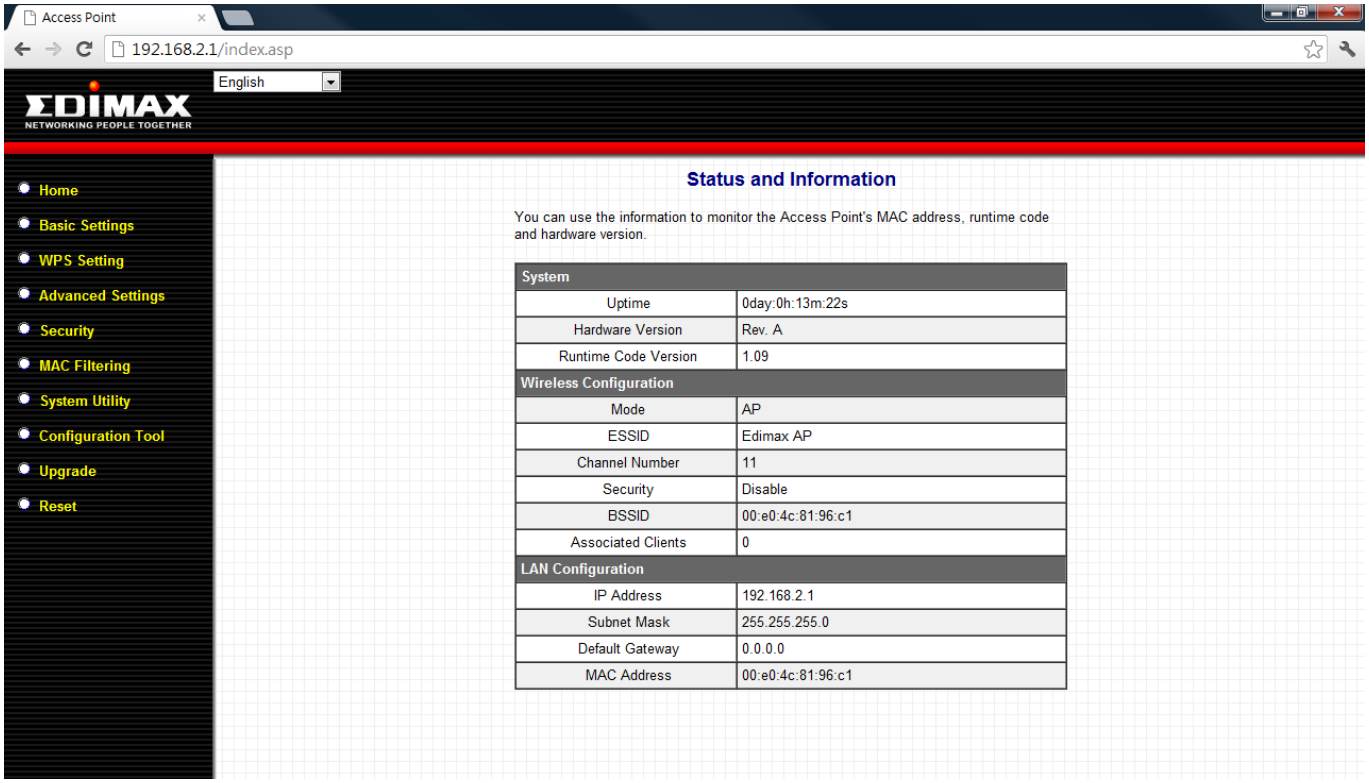


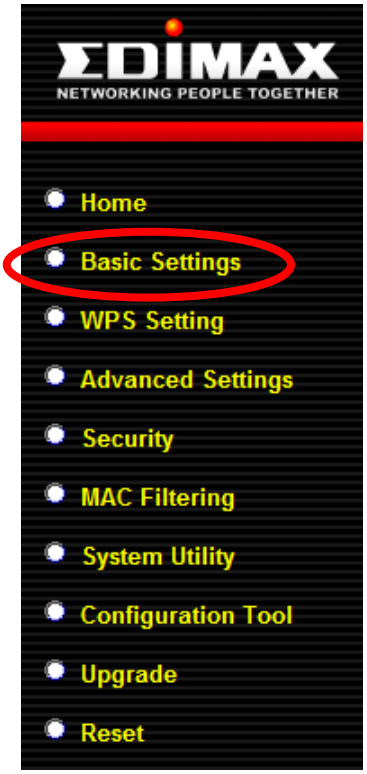
You will then be prompted to enter the device's username and password. The

default username is **admin** and the default password is **1234**.



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

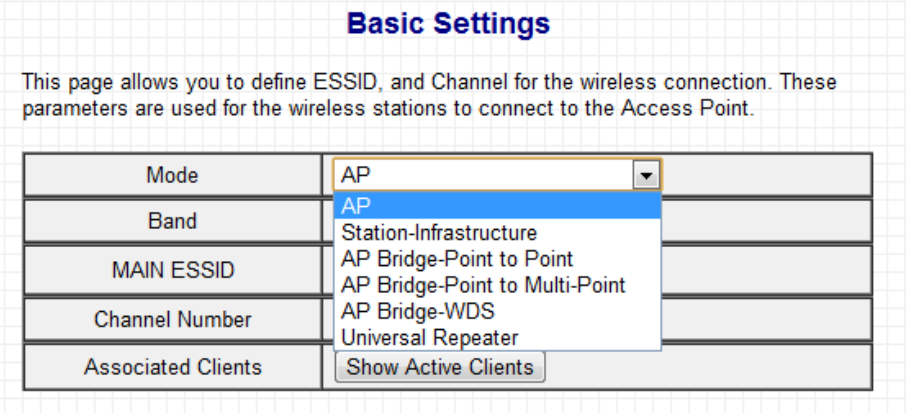




Select “Basic Settings” from the menu on the left side of the screen.

“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

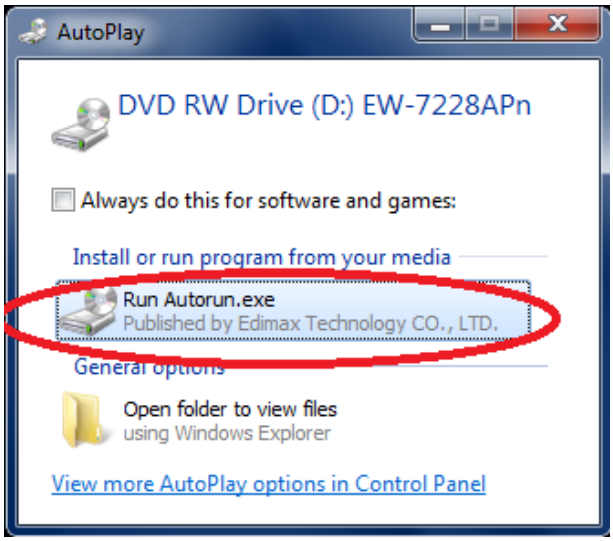
	Multi-Point", but the device is not in bridge-dedicated mode, and will be able to accept wireless clients while the device is working as a wireless bridge.
Universal Repeater	The device will act as a wireless range extender that will help you to extend your Wi-Fi network. The device acts as a client 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**

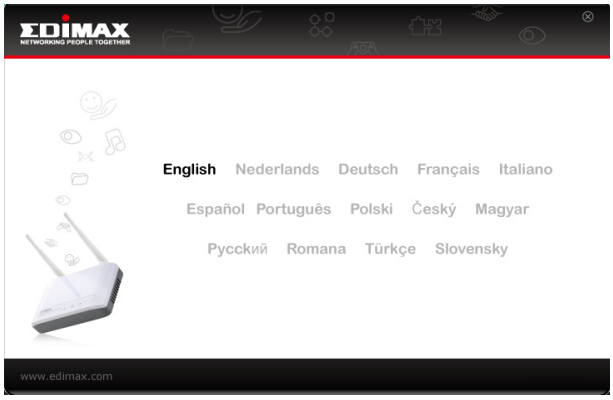
II-2. Windows

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."

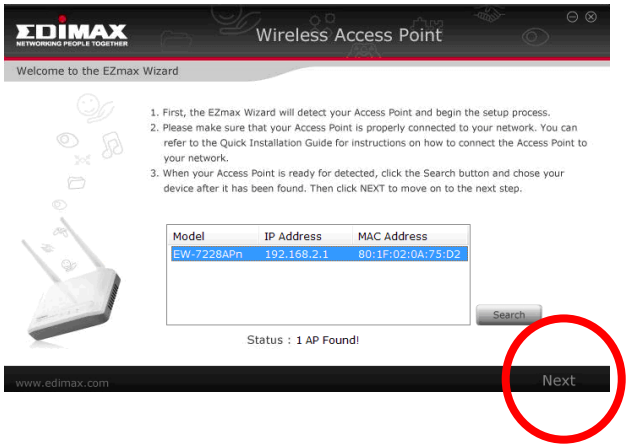


Note: If a popup window appears asking "Do you want to allow the following program to make changes to this computer", please click "Yes" to continue.

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



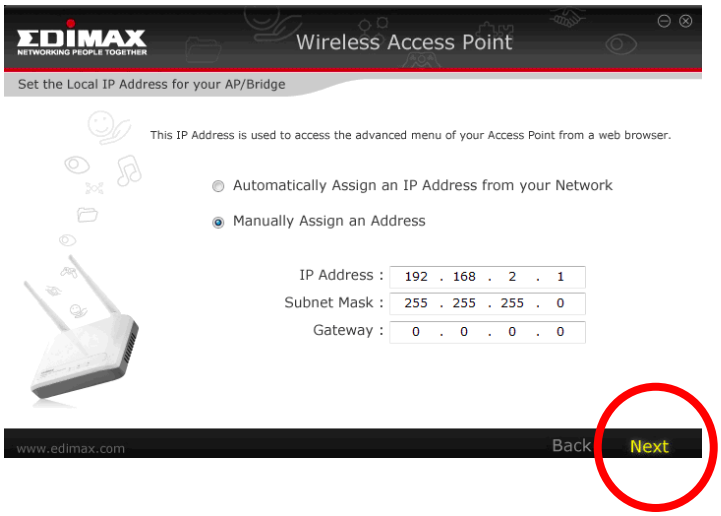
3. The setup wizard will search for the access point. When it has successfully found the device, click “Next” to continue.



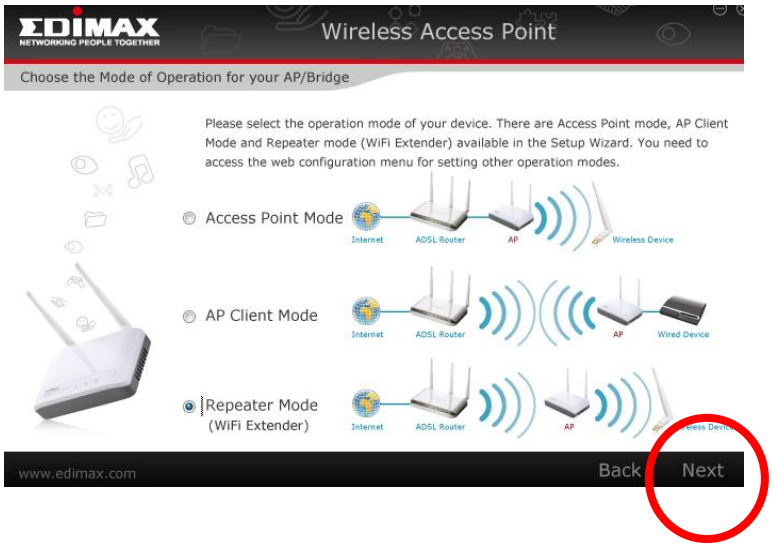
4. The setup wizard will prompt you for a password. Enter the default password, **1234**.

5. 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.



6. Select which mode you wish to use and click “Next”.



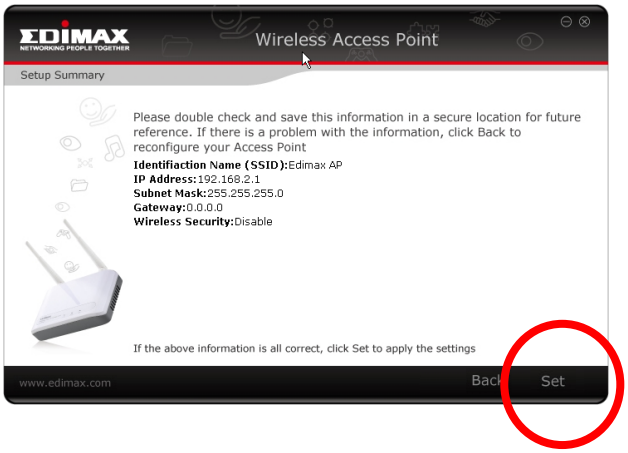
II-3. Access Point Mode

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

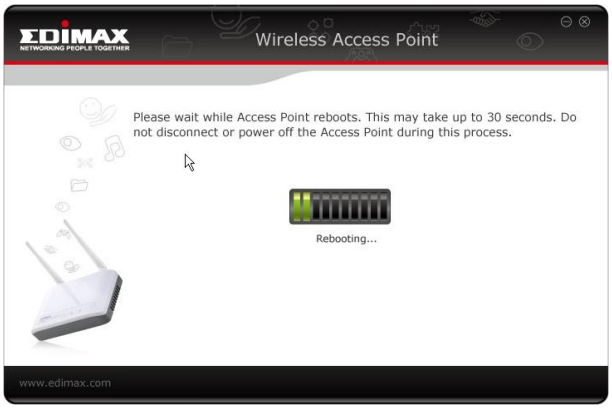
2. You will be prompted to set the SSID of this access point. The SSID will be the name of the access point when you connect to it wirelessly. The default SSID is **Edimax AP**. This page also offers the option to change the password used to access the device’s browser based configuration interface. 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. For security reasons, it is recommended that you use an encryption method.

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.



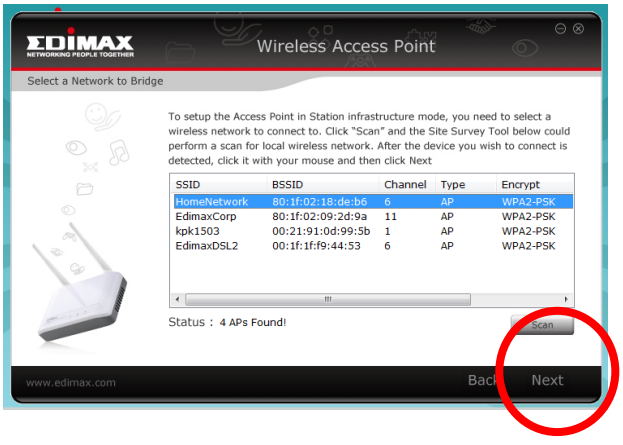
6. After the device reboots, you will see a final congratulation screen. Click “Finish” to complete the setup.

II-4. AP Client Mode

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

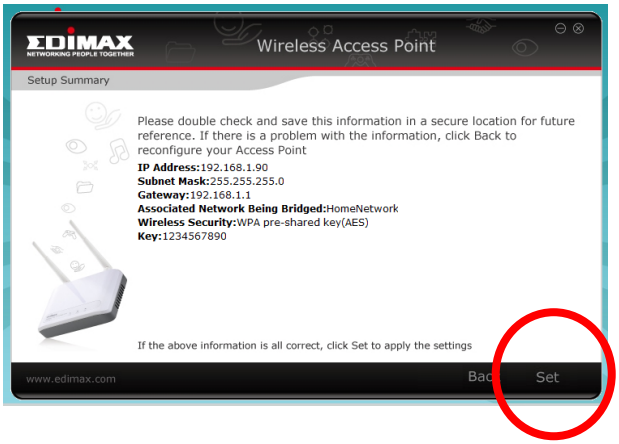
2. You have the option to change the password used to access the device’s browser based configuration interface. For first time setup, please simply click “Next” without changing anything.

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.

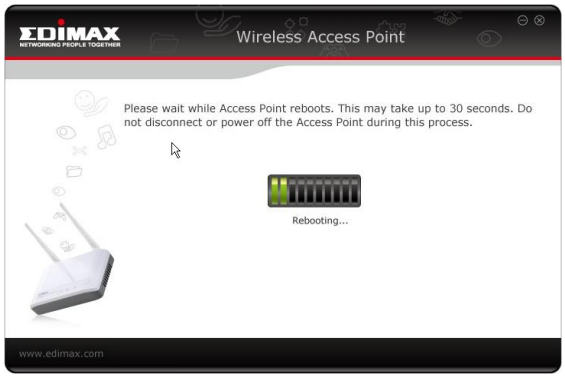


4. If the wireless network you selected requires a network security key, enter it here. If you do not know the network security key then please refer to **IV-2. Appendix How to Find Your Network Security Key**. Click “Next” to continue when finished.

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.

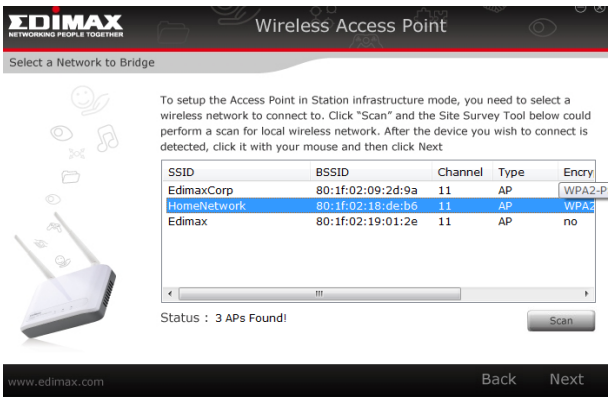

EDIMAX
NETWORKING PEOPLE TOGETHER
Wireless Access Point
Congratulation, your setup is now complete.
www.edimax.com
Back
Finish

II-5. 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 browser based configuration interface.

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.



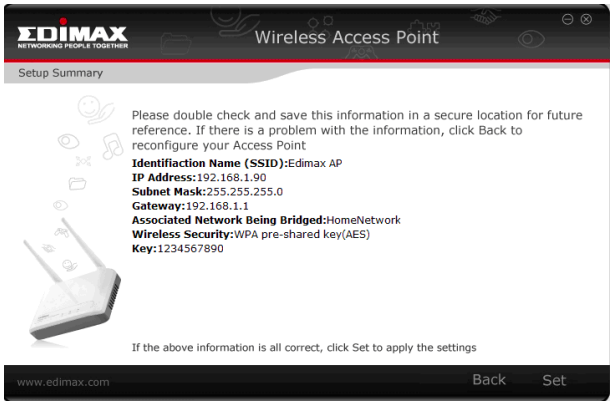
Note: Note the channel number used by the wireless router or access point you select. If the router or AP uses “Auto” for its channel selection, then this repeater will disconnect from the router or AP as soon as it switches channels. For best results, check the wireless settings for your router

and set the channel to a fixed number, such as 1, 6, or 11.

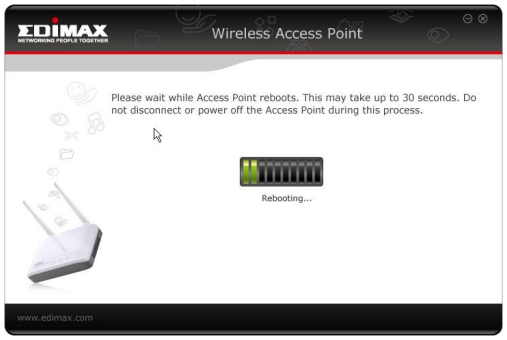
7. If the wireless network you selected requires a network security key, enter it here. If you do not know the network security key then please refer to **IV-2. Appendix How to Find Your Network Security Key**. Click “Next” to continue when finished.

Note: If the network you select shows that it uses WPA-PSK/WPA2-PSK encryption, then please use WPA2 AES here. Please do not use WPA2 mixed mode.

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.

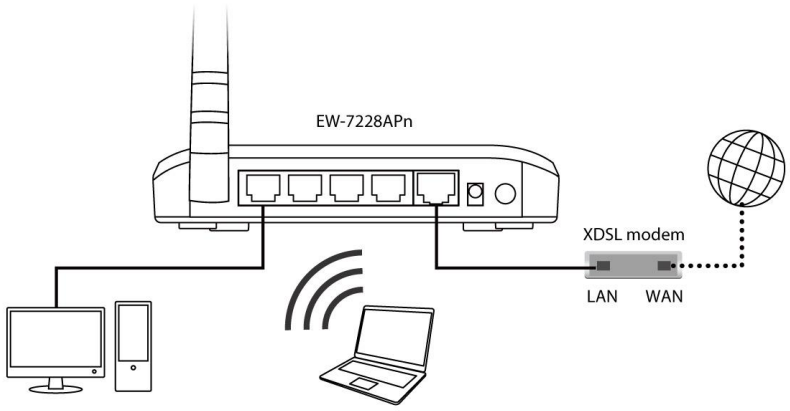

EDIMAX
NETWORKING PEOPLE TOGETHER
Wireless Access Point
Congratulation, your setup is now complete.
www.edimax.com
Back
Finish

II-6. Hardware Installation

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

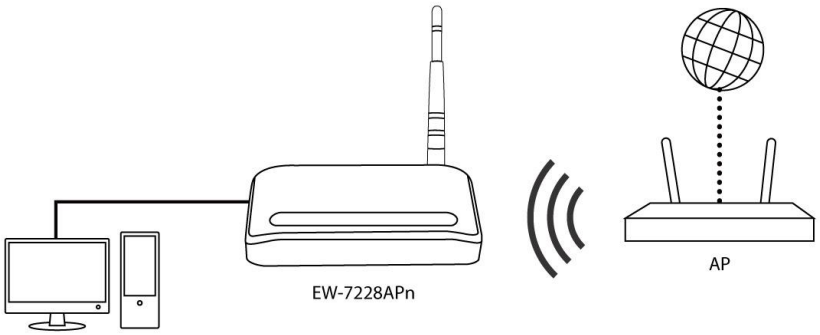
Access Point Mode

Connect one port of the device to your router or xDSL modem. You can now connect a computer or other network device to the access point wirelessly by locating and connecting to its SSID. Or you can connect a computer/device to the access point using an Ethernet cable.



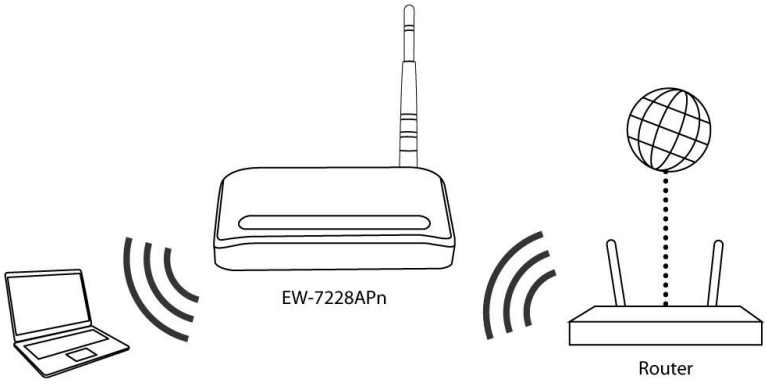
AP Client Mode

Connect one port of the access point to the network device you wish to connect to the Internet wirelessly, e.g. a games console or smart TV. Your network device should now be connected to your existing wireless network.



Repeater Mode

Position the device in a location for optimal wireless extension; usually a central location in your house or roughly an equal distance between your router and the furthest wireless client. You can connect to the access point wirelessly by locating and connecting to its SSID.


EW-7228APn
Router

III. Browser Based Configuration Interface

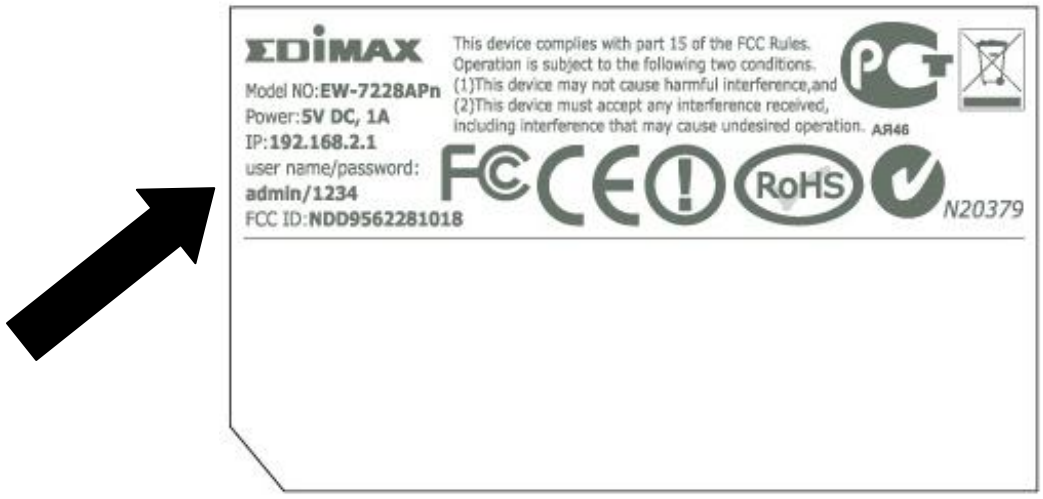
Once you have setup the access point in its desired operating mode as detailed in **II. Quick Setup**, you can further configure the settings of the access point anytime using the browser based configuration interface.

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, please enter the access point's default IP address "**http://192.168.2.1**" into the URL bar of a web browser.

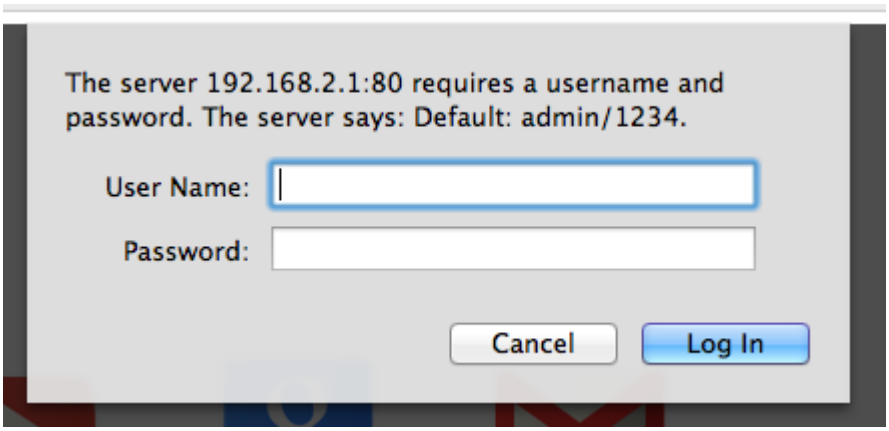
Note: For your reference, the access point's default IP address, username and password are all displayed on the product label on the underneath of the device, as shown below.



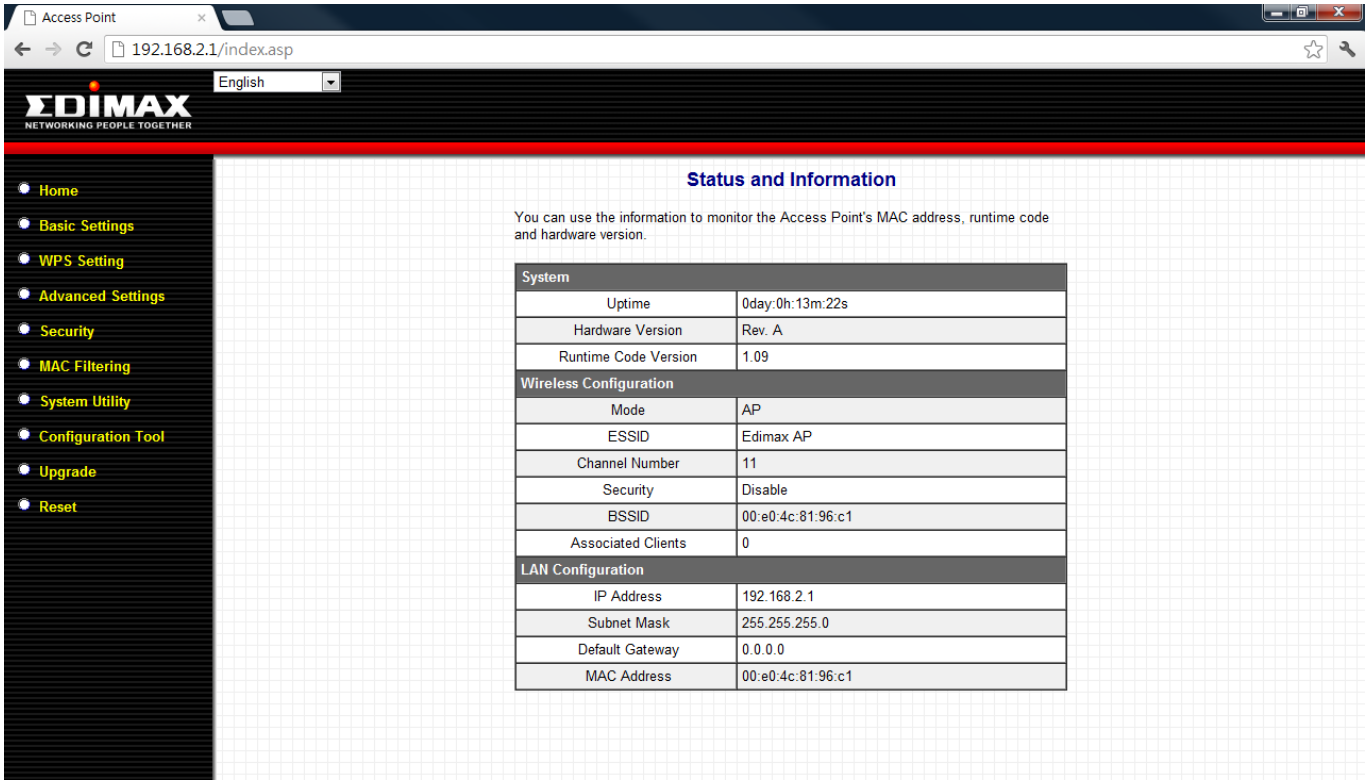
You will then be prompted to enter the device's username and password. The default username is **admin** and the default password is **1234**.

Windows:

Mac:

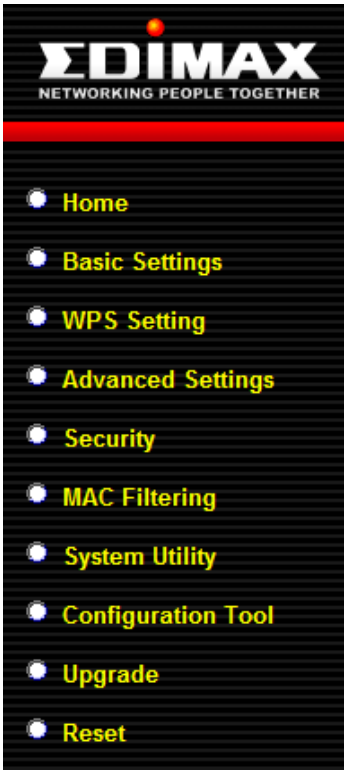


From here, you will see the browser based configuration interface home screen.

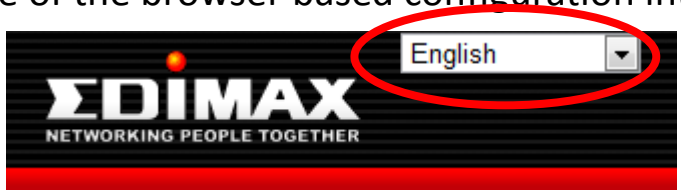

Access Point
192.168.2.1/index.asp
English
EDIMAX
NETWORKING PEOPLE TOGETHER
Home
Basic Settings
WPS Setting
Advanced Settings
Security
MAC Filtering
System Utility
Configuration Tool
Upgrade
Reset
Status and Information
You can use the information to monitor the Access Point's MAC address, runtime code and hardware version.
System
Uptime 0day: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

III-1. Home

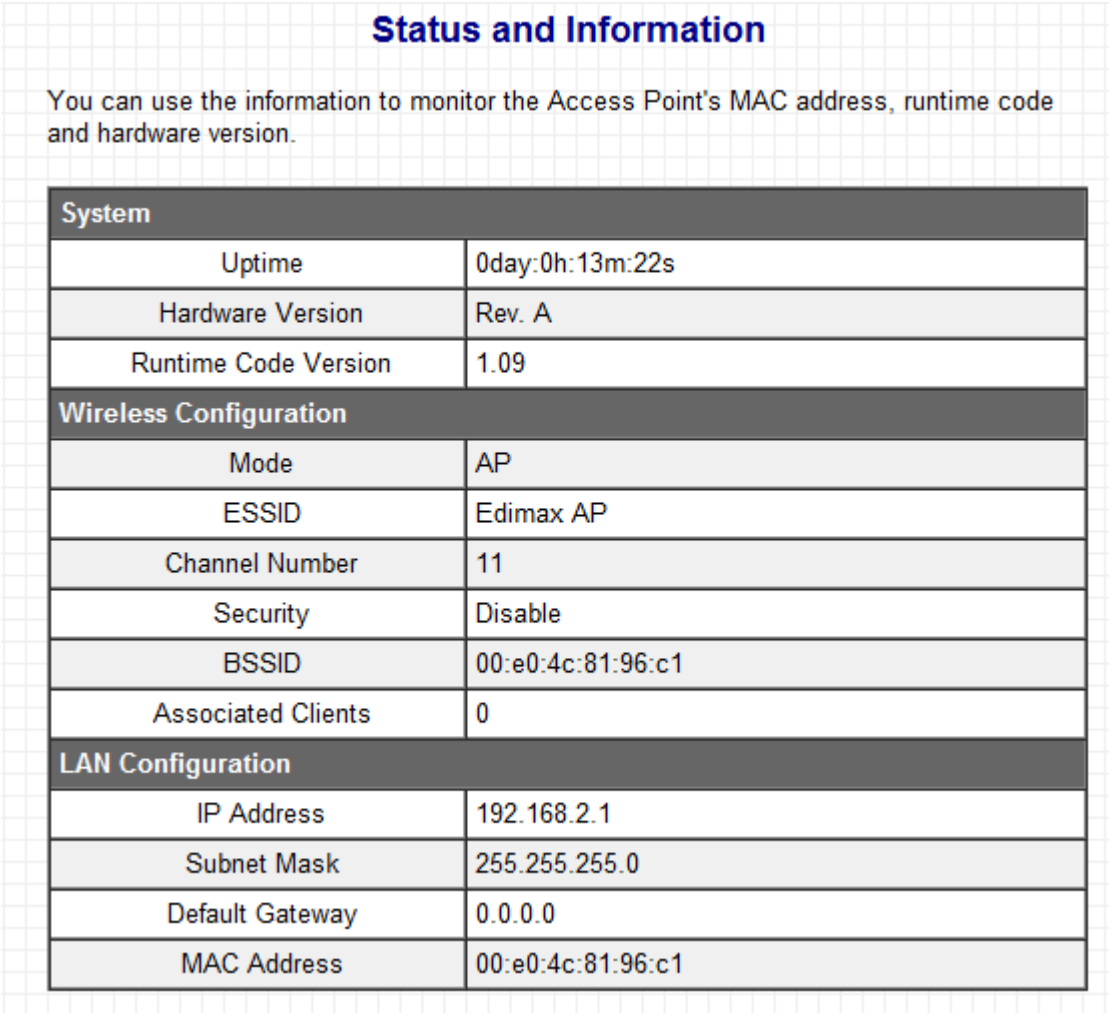
The Home page displays 10 categories in the left panel which you can select:



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



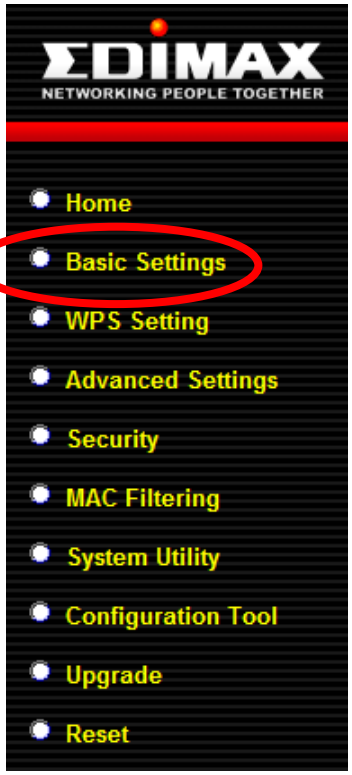
The “Status and Information” screen is displayed in the main window. This shows basic system information about the access point for reference, such as firmware version, wireless mode and SSID, and the access point’s IP and MAC address.



System	
Uptime	Displays the total time the access point has been operational since it was last powered 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.

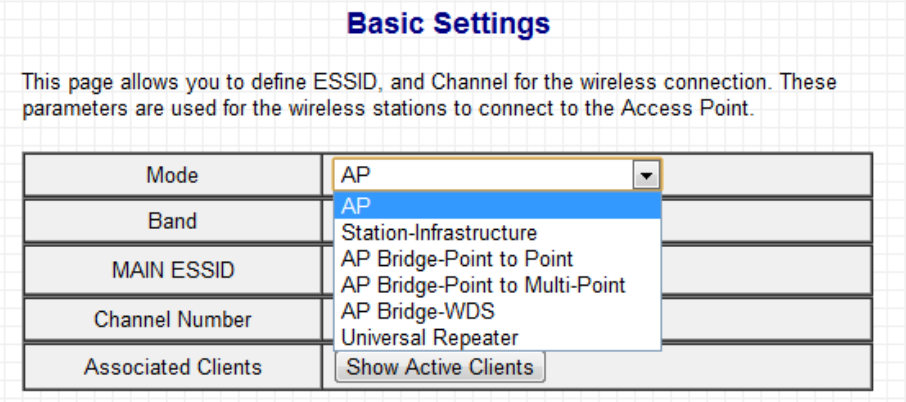
Security	Displays the current wireless security setting.
BSSID	Displays the current BSSID (a unique ID of the access point, which cannot be modified).
Associated Clients	Displays the number of connected wireless clients.
LAN Configuration	
IP Address	Displays the IP address of the access point.
Subnet 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:

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

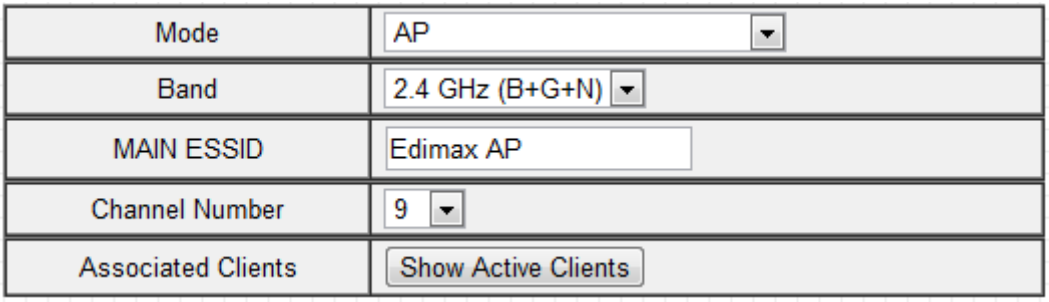
	game consoles to connect to a wireless network
AP Bridge-Point to Point	Establishes a wireless connection with another wireless access point using the same mode, and links any wired networks connected to these two wireless access points together. Only one access point can be connected in this mode.
AP 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 follow the appropriate chapter of the user manual for your desired operating mode:

III-2-1. AP Mode

In AP mode the device acts as a bridge between IEEE 802.11b/g/n wireless devices and a wired Ethernet network.

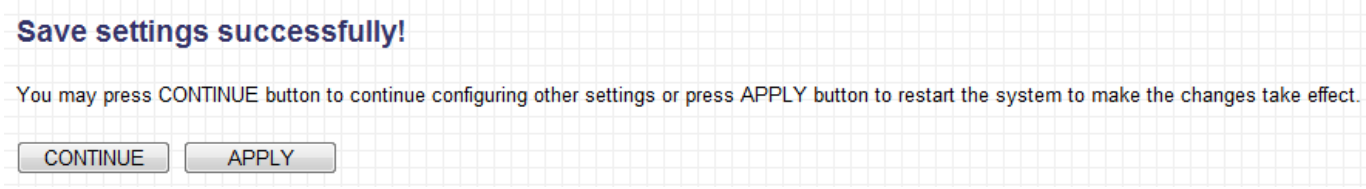
When you select AP Mode, the following appears:



Band	Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny wireless clients using certain bands. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using the 802.11b and 802.11g bands will be able to connect to this access point. If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 2.4GHz (B+G+N).
MAIN ESSID	Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **Please note that the ESSID is case sensitive.**
Channel Number	Please select a channel number you wish to use. If you know a certain channel number is being used by other wireless access points nearby, please refrain from using the same channel number
Associated	Click the "Show Active Clients" button and a

Clients	new window will appear, which contains information about all wireless clients connected to this access point. You can click the “Refresh” button in the popup window to keep the information up-to-date.

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

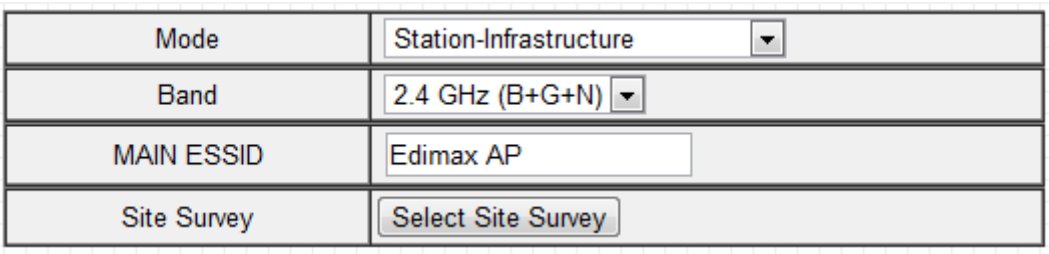


Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

III-2-2. Station Infrastructure Mode

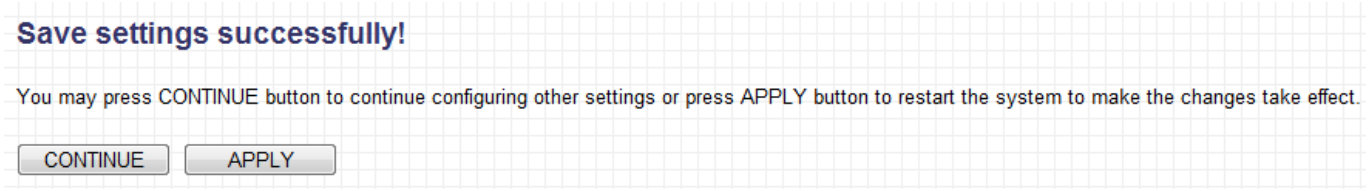
In Station-Infrastructure mode, the device acts as a wireless client and can be connected to Ethernet-only Internet devices, such as smart televisions or video game consoles. This gives these devices the capability to connect to the Internet wirelessly.



Band	Please select the wireless band you wish to use. By selecting different band settings, you’ll be able to allow or deny access points using certain bands. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only access points using the

	wireless band you select (802.11b, 802.11n, or 802.11g) will be able to connect to this device. If you select 2.4GHz (B+G), then only access points using the 802.11b and 802.11g bands will be able to connect to this device. If you want to allow 802.11b, 802.11g, and 802.11n access points to connect to this device, select 2.4GHz (B+G+N).
MAIN ESSID	Please input the ESSID (the name used to identify the wireless device) of the access point you want to connect to here. You can input up to 32 alphanumerical characters. **Please note that the ESSID is case sensitive.**
Site Survey	When you use this device to give an Ethernet network device wireless capability, you have to associate it with a working access point. Click the “Select Site Survey” button and a “Wireless Site Survey Table” will appear. It will list all available access points nearby. Select one access point in the table for this device to connect to (please see below).

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

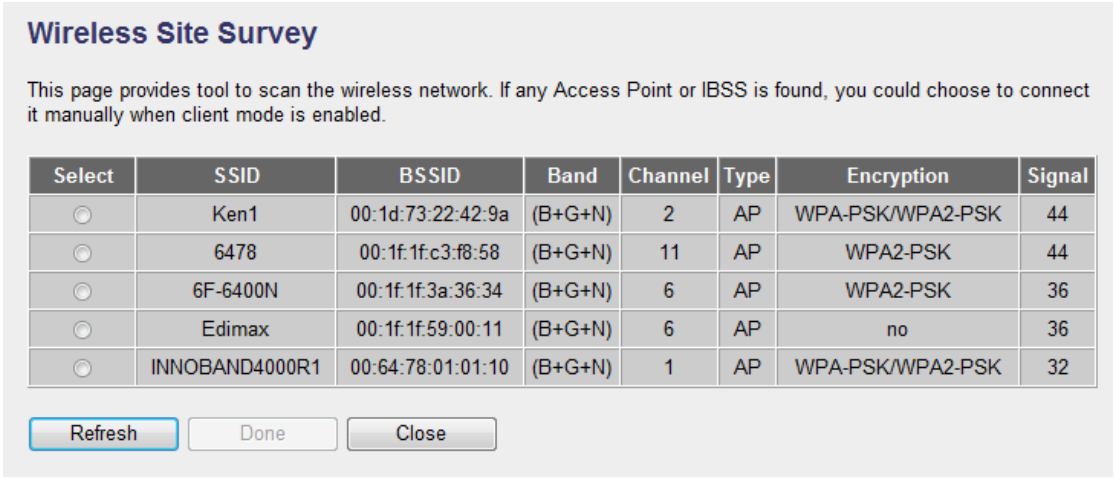


Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

Wireless Site Survey

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



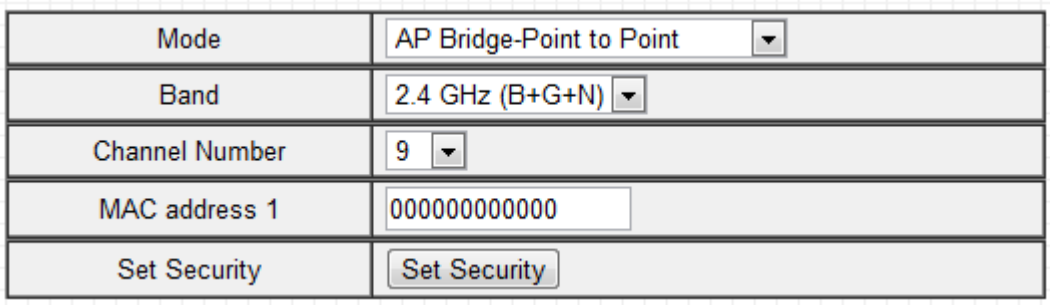
Note: If the SSID of the access point you wish to connect to is not listed, try clicking the “Refresh” button.

Note: The access point you wish to connect to may have hidden its SSID, in which case it will not be listed. You will need to manually enter the SSID in the “MAIN SSID” field of the previous page.

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

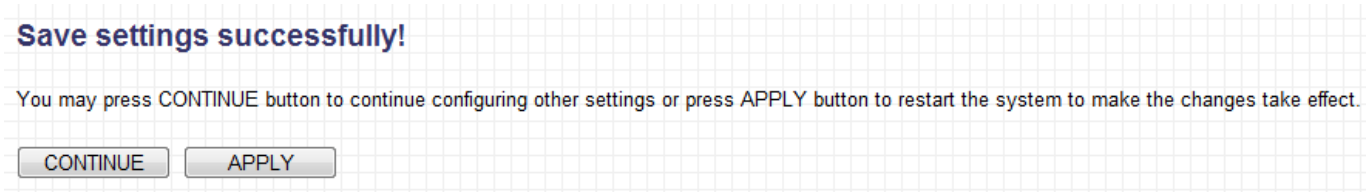
In this mode, the access point connects to another wireless access point in the same mode, and all connected Ethernet clients of both devices will be connected together. This allows two physically isolated networks to communicate with each other.

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



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

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



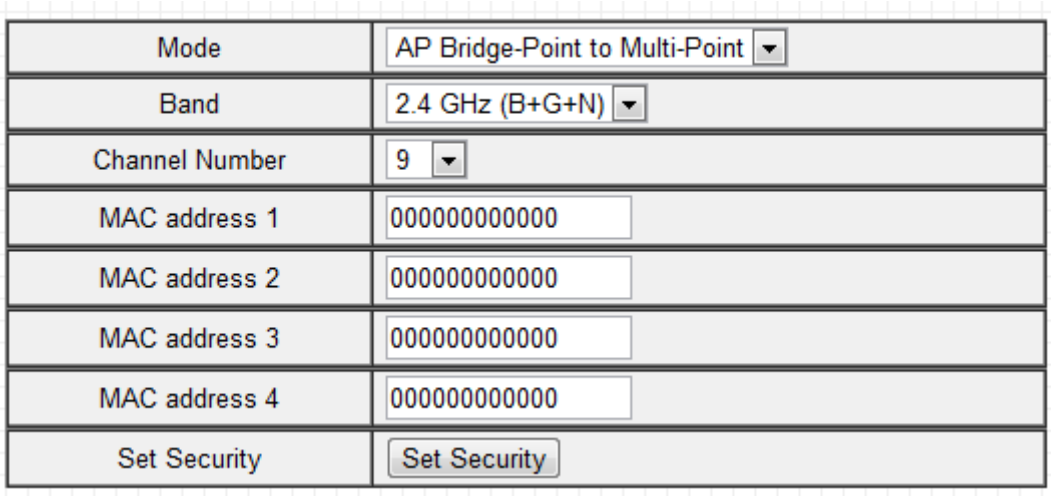
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

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

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

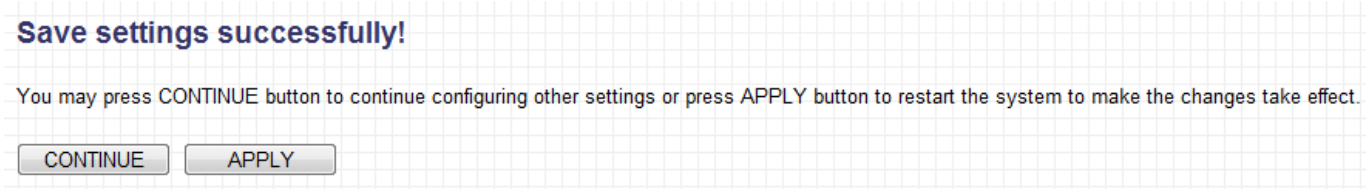
Note: When you set the device to this mode, it will not accept regular wireless clients any more.



Band	Please select the wireless band you wish to use. By selecting different band settings, you’ll be able to allow or deny access points using certain bands. If you select 2.4GHz (B), 2.4GHz (N), or

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

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



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

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

III-2-5. AP Bridge-WDS

In this mode, this access point will connect to up to four other wireless access

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

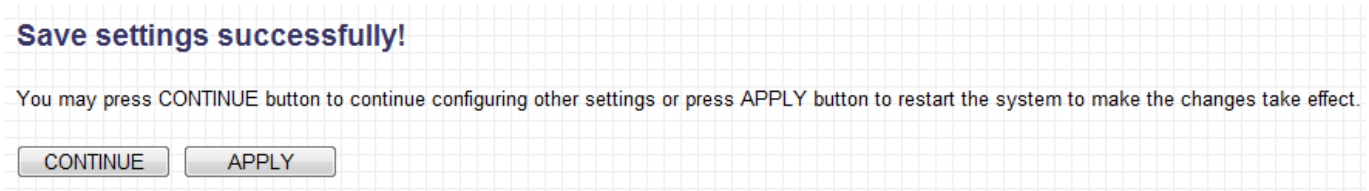
Note: When you set the device to this mode, it will still be able to accept regular wireless clients.

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

MAIN ESSID	Please input the ESSID (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **Please note that the ESSID is case sensitive.**
Channel Number	Please select a channel number you wish to use. The channel number must be same as the other wireless access points you wish to connect to.
Associated Clients	Click the “Show Active Clients” button and a new window will appear, which contains information about all wireless clients connected to this access point. You can click the “Refresh” button in the popup window to keep the information up-to-date.
MAC address 1-4	Please input the MAC addresses of the wireless access point you wish to connect to.
Set Security	Click this button to select an encryption mode for this wireless link. A popup window with security options will appear.

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



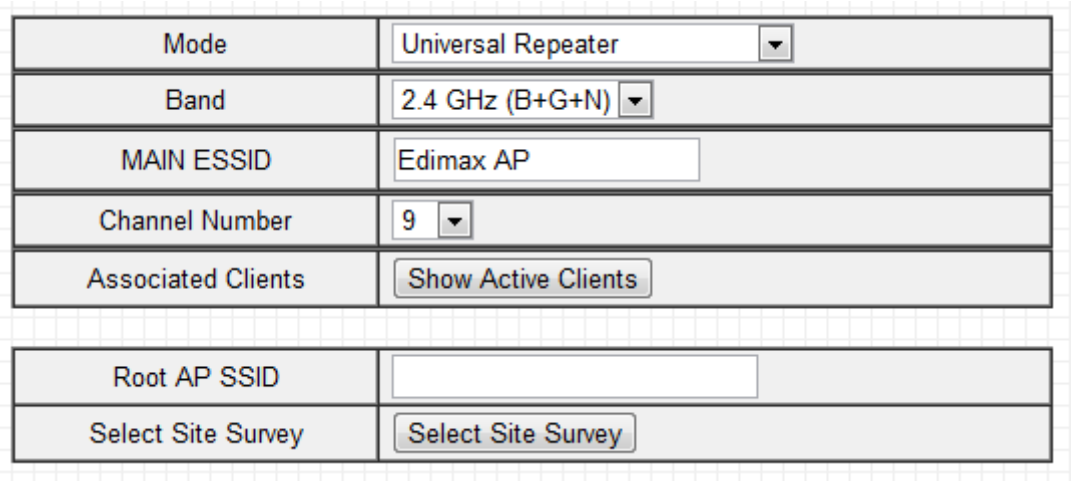
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

III-2-6. Universal Repeater Mode

In this mode, this device 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 dead spots.

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

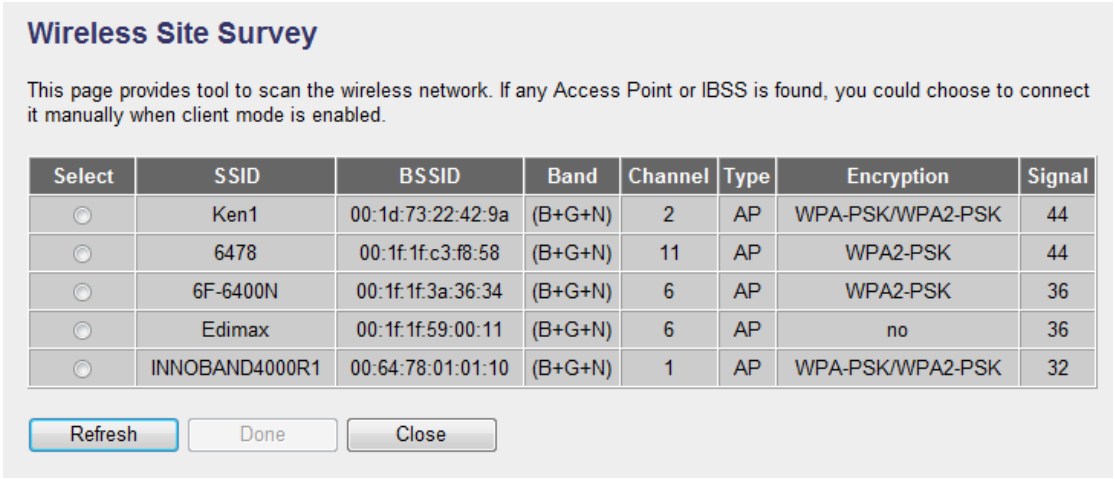


Band	Please select the wireless band you wish to use. By selecting different band settings, you'll be able to allow or deny devices using certain bands. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only devices using the wireless band you select (802.11b, 802.11n, or 802.11g) will be able to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

Channel Number	Please select a channel number you wish to use. The channel number must be same as the other wireless access points you wish to connect to.
Associated Clients	Click the “Show Active Clients” button and a new window will appear, which contains information about all wireless clients connected to this access point. You can click the “Refresh” button in the popup window to keep the information up-to-date.
Root AP SSID	In Universal Repeater mode, this device will act as a station and connect to a root AP. Enter the SSID of the root AP here, or click the “Select Site Survey” button to choose a root AP.
Select Site Survey	Click the “Select Site Survey” button, and a “Wireless Site Survey Table” will pop up. It will list all available access points nearby. Select one access point in the table for this device to connect to (please see below).

Wireless Site Survey

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

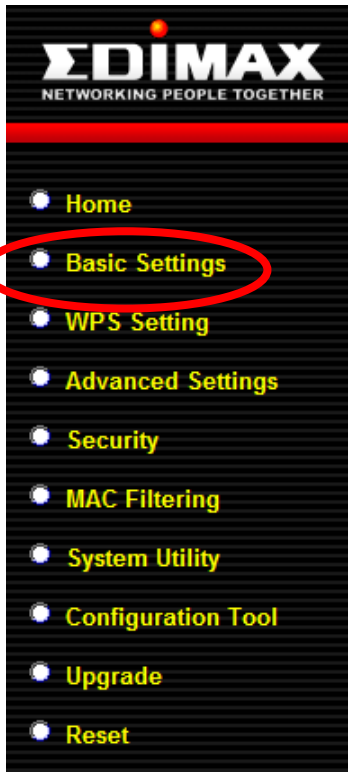


Note: If the SSID of the access point you wish to connect to is not listed, try clicking the “Refresh” button.

Note: The access point you wish to connect to may have hidden its SSID, in which case it will not be listed. You will need to manually enter the SSID in

the “MAIN SSID” field of the previous page.

III-3. WPS Setting

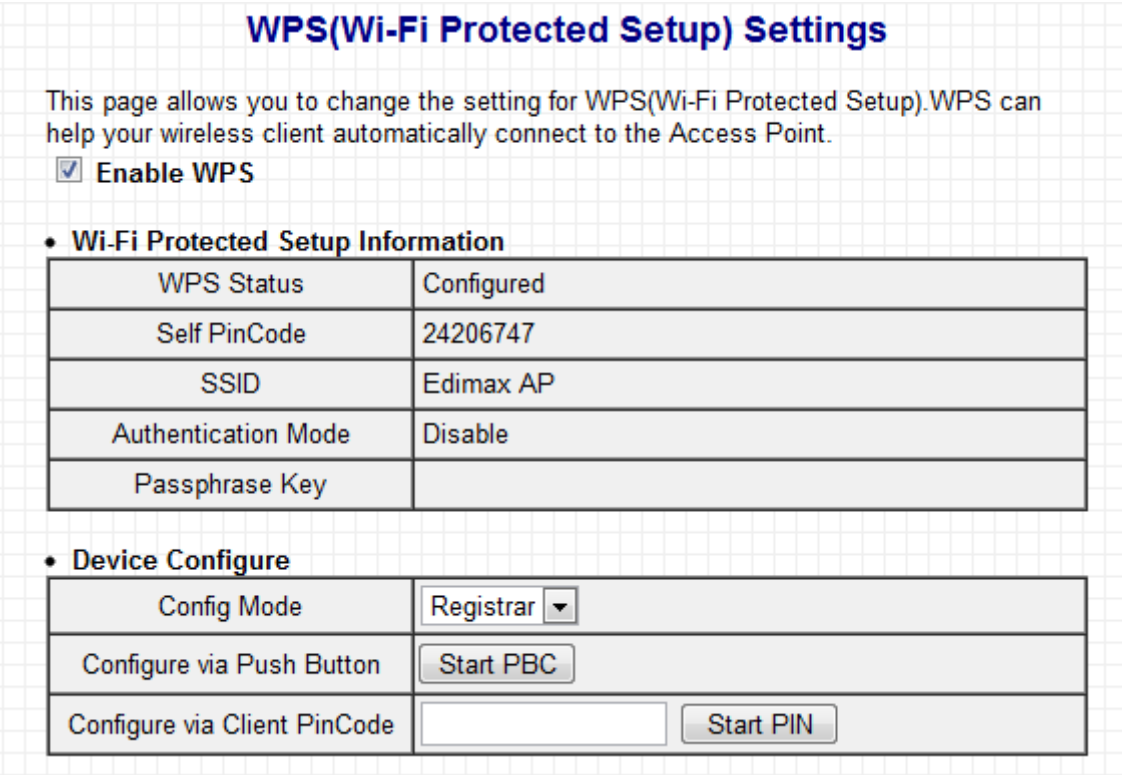


Wi-Fi Protected Setup (WPS) is a simple and convenient way to build a connection between the travel router and wireless network clients. This function eliminates the need to select an encryption mode and enter an encryption passphrase each time you want to set up a connection. You can build a connection simply by pressing a button on both the travel router and the wireless client.

This router supports two types of WPS: **Push-Button Configuration (PBC)** and **PIN code**.

To use **PBC** you will need to activate WPS by pushing the Reset/WPS button, or by clicking “Start PBC” in the “WPS” screen; and to activate WPS in the wireless client by pushing a WPS button.

To use **PIN code**, you will need to enter the PIN code of the wireless client you wish to connect to, and then activate WPS in the wireless client.

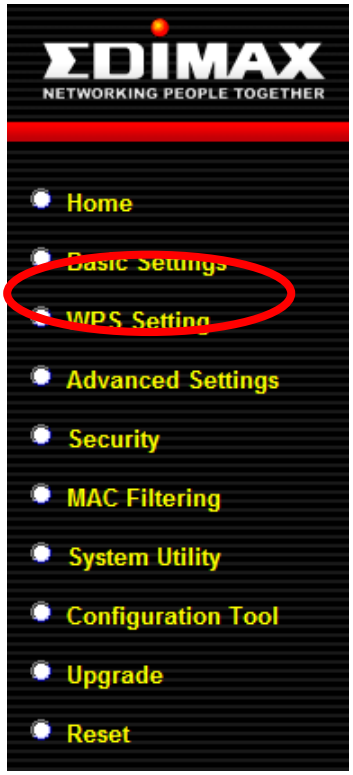


Enable WPS	Check this box to enable or disable WPS.
Wi-Fi Protected Setup Information	
WPS Status	Displays WPS status. If data encryption settings for this access point have never been set, “unConfigured” will be shown here. If data encryption settings have been set, “Configured” will be shown here.
Self PIN Code	This is the WPS PIN code of this access point. This code is used when you need to build a wireless connection by WPS with other WPS-enabled wireless devices.
SSID	Displays the SSID (ESSID) of this access point.
Authentication Mode	The wireless security authentication mode of this access point will be shown here. If you don’t enable the security functions of the access point before WPS is activated, the access point will automatically set the security to WPA (AES) and generate a passphrase key for WPS connection.
Passphrase Key	Shows the WPA passphrase here, though all characters will be replaced by asterisks for security reasons. If encryption is not set on this access point, this field will be blank.
Device Configuration	
Config Mode	There are “Registrar” and “Enrollee” modes for the WPS connection. When “Registrar” is enabled, the wireless clients will follow the access point’s wireless settings for WPS connections. When “Enrollee” mode is enabled, the access point will follow the wireless settings of wireless client for WPS connections.
Configure via Push Button	Click “Start PBC” to start Push-Button style WPS setup. This access point will wait for WPS requests from wireless clients for 2 minutes. The “WLAN” LED on the access point will stay on for 2 minutes while this access point waits for incoming WPS requests.
Input Client PIN	Please input the PIN code of the wireless

Code	client you wish to connect, and click the “Start PIN” button. The “WLAN” LED on the access point will stay on while this access point waits for incoming WPS requests.

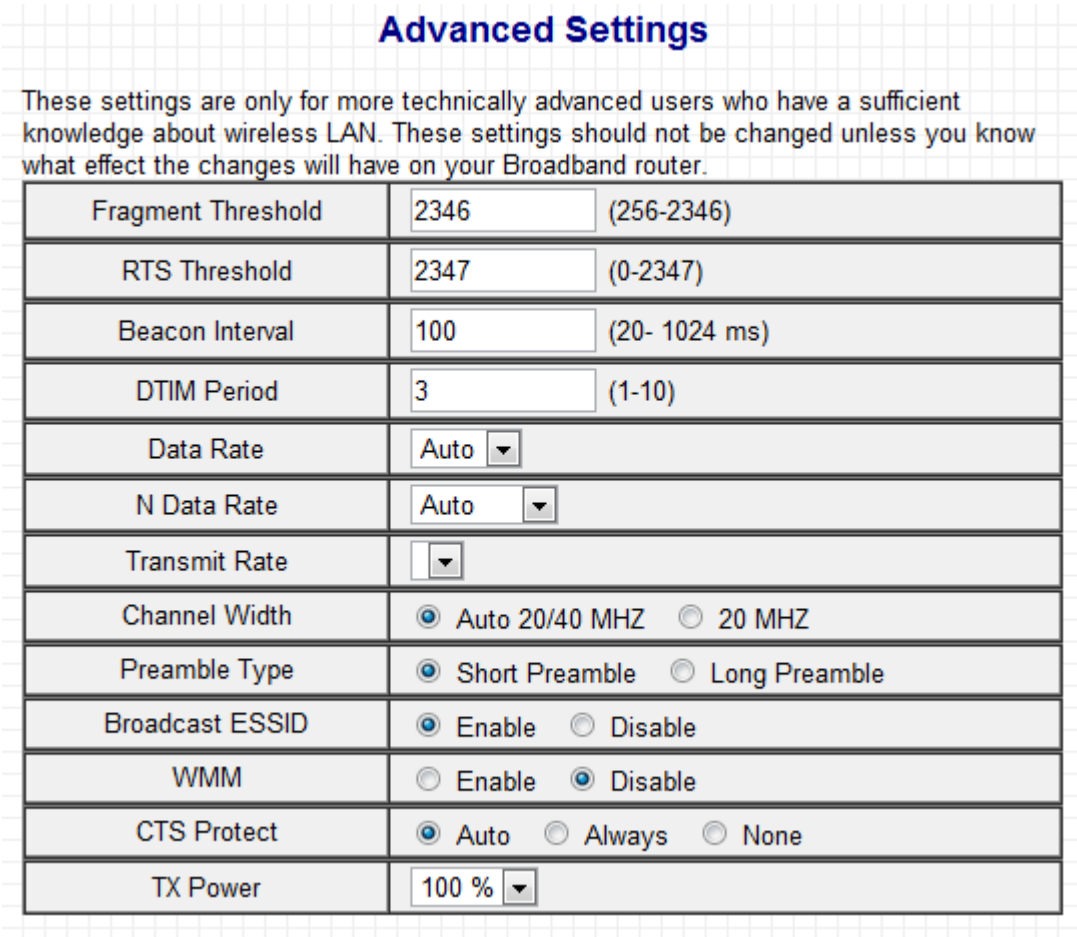
Note: When using PBC-type WPS setup, you must press the hardware or software WPS button on the wireless client within 120 seconds. If you do not do so in time, you will need to activate WPS on the access point again.

III-4. Advanced Setting



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.

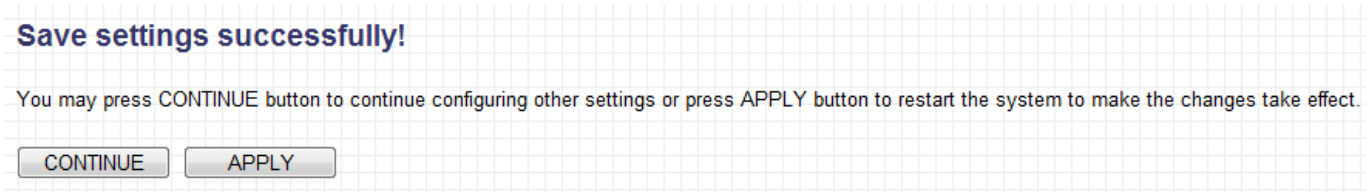
Note: Changing these settings can adversely affect the performance of your access point.



Fragment Threshold	Set the Fragment threshold of the wireless radio. **Please do not modify the default value if you don't know what this does, the default value is 2346**
RTS Threshold	Set the RTS threshold of the wireless radio. **Please do not modify the default value if you don't know what this does, the default value is 2347**
Beacon Interval	Set the beacon interval of the wireless radio. **Please do not modify the default value if you don't know what this does, the default value is 100**
DTIM Period	Set the DTIM period of wireless radio. **Please do not modify default value if you don't know what it is, the default value is 3**
Data Rate	Set the wireless data transfer rate. Since most wireless devices will negotiate with each other and pick a proper data transfer rate automatically, **it's not necessary to change this value unless you know what will happen after modification.**

N Data Rate	Set the data rate of 802.11n clients, available options are MCS 0 to MCS 7. It's safe to set this option to "Auto" and **it's not necessary to change this value unless you know what will happen after modification.**
Channel Width	Select wireless channel width (bandwidth used by wireless signals from the travel router). It's suggested you select "Auto 20/40MHz". **Do not change to "20 MHz" unless you know what effect that will have.**
Preamble Type	Set the wireless radio preamble type. **Please do not modify the default value if you don't know what this does, the default value is "Short Preamble".**
Broadcast ESSID	Decide if the device will broadcast its own ESSID. You can hide the ESSID of your access point (set the option to "Disable"), so only people who know the ESSID of your access point can connect to it.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It's recommended to set this option to "Auto".
TX Power	You can set the output power of the wireless radio. Unless you're using the access point in a very large space, you may not require 100% output power. **This will enhance security (malicious/unknown users in distant areas will not be able to reach your access point).**
WMM	WMM (Wi-Fi Multimedia) technology can improve the performance of certain network applications, such as audio/video streaming, network telephony (VoIP), and others. When you enable WMM, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responses. This improves the performance of such network applications.

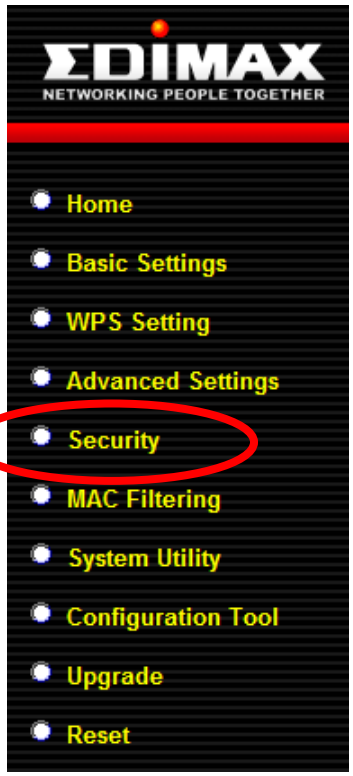
Click “APPLY” to save changes. The following message will appear:



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

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

III-5. Security



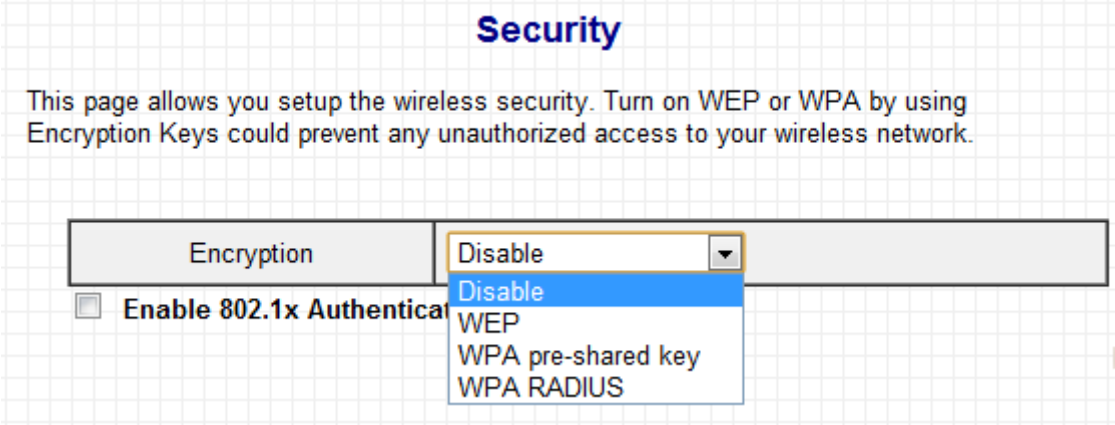
The access point provides a variety of wireless security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the encryption key.

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

Note: There are several things you can do to improve wireless security.

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

Open the drop down menu labeled encryption and select the type of encryption you would like to use.

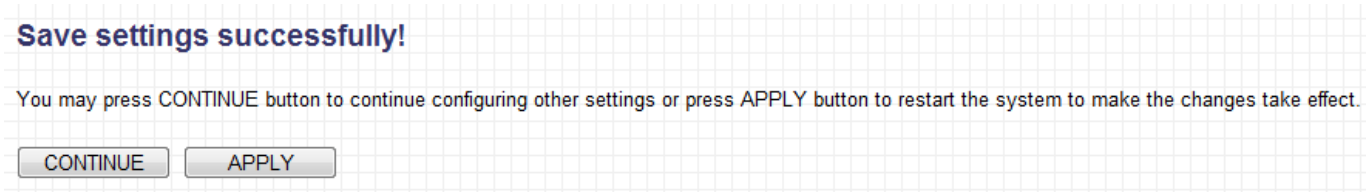


III-5-1. Disable

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:

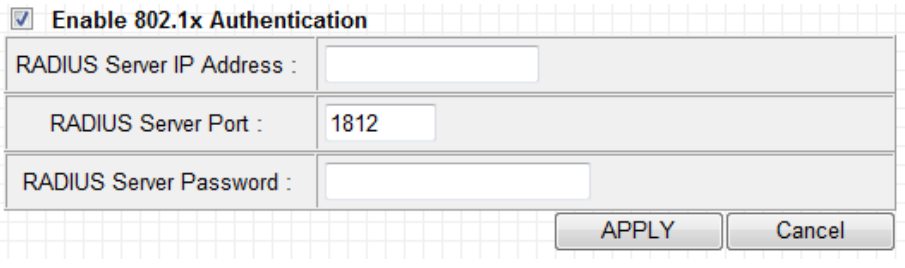


Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

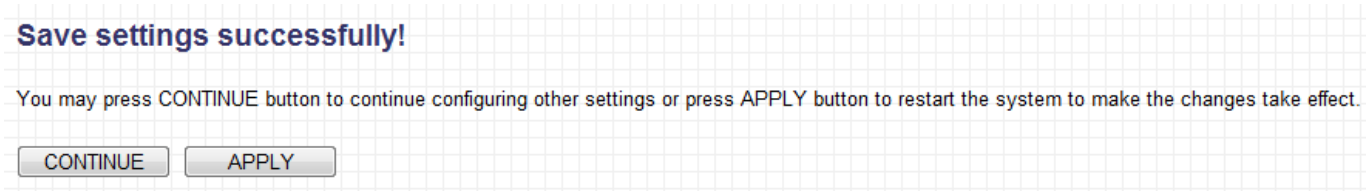
III-5-2. Enable 802.1x Authentication

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



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:



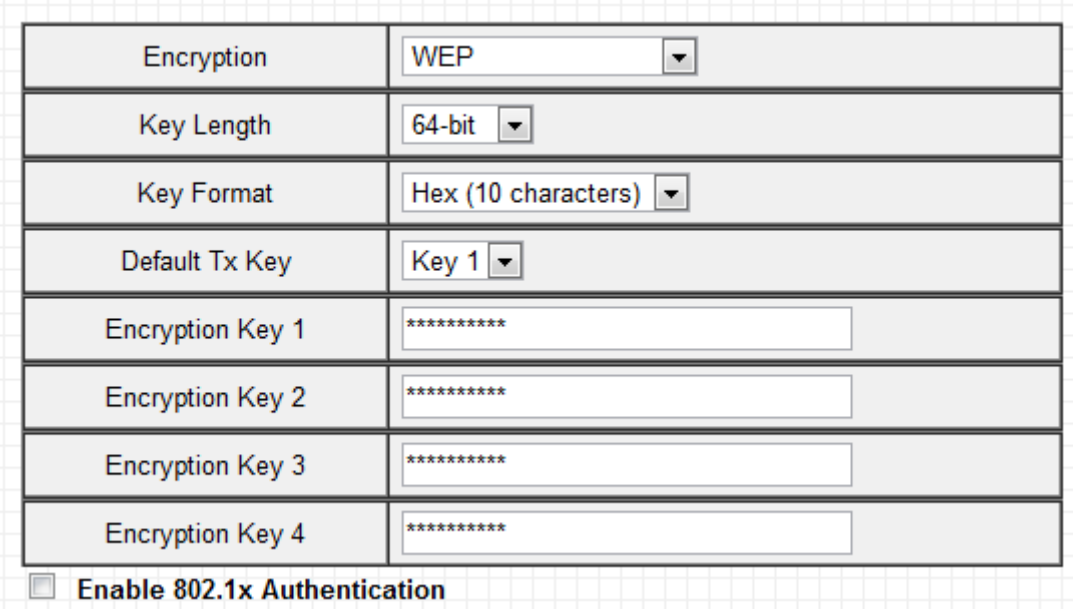
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

III-5-3. WEP

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

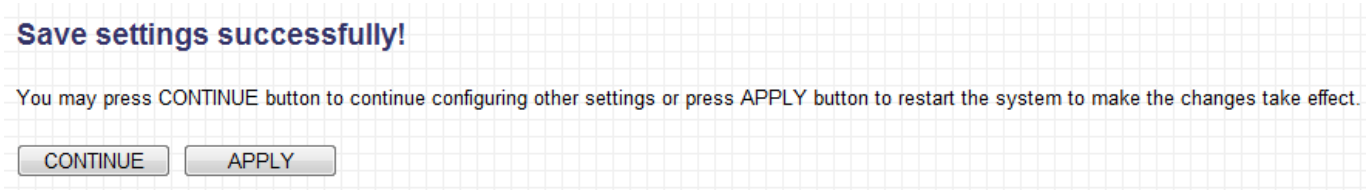
Note: Most wireless devices support WPA encryption, though some legacy wireless devices only support WEP encryption. **WEP only supports up to 54Mbps transmission data rate.**



Key Length	There are two types of WEP key length: 64-bit and 128-bit. Using “128-bit” is safer than “64-bit”, but will reduce some data transfer performance.
Key Format	There are two types of key format: ASCII and Hex. When you select a key format, the number of characters of the key will be displayed. For example, if you select a “64-bit” key length, and “Hex” as the key format, you’ll see the message “Hex (10 characters)” to the right, which means the length of the WEP key is 10 characters.
Default Tx Key	You can set up to four sets of WEP keys, and you can decide which key is used the default. **If you don’t know which one you should use, select “Key 1”.**
Encryption Key 1 to 4	Input WEP key characters here, the number of characters must be the same as the number displayed in the “Key Format” field. If you select the “ASCII” key format, you can use any alphanumerical characters (0-9, a-z, and A-Z). If you select “Hex” as the key format, you can use the characters 0-9, a-f, and A-F. You must enter at least one encryption key here, and if you entered multiple WEP keys, they should not be same as each other.

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

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

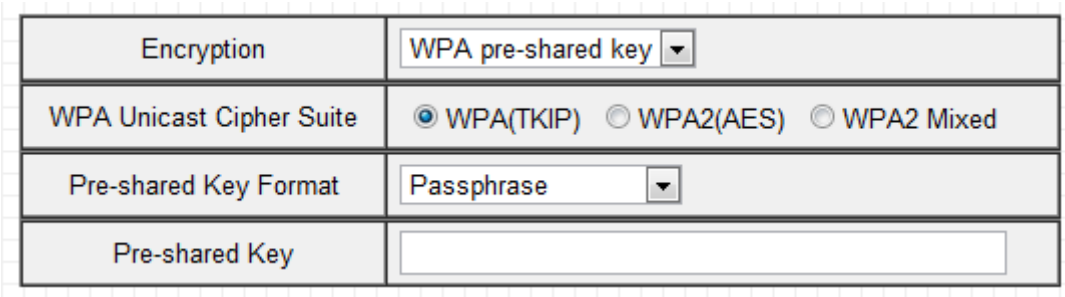


Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

III-5-4. WPA Pre-Shared Key

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

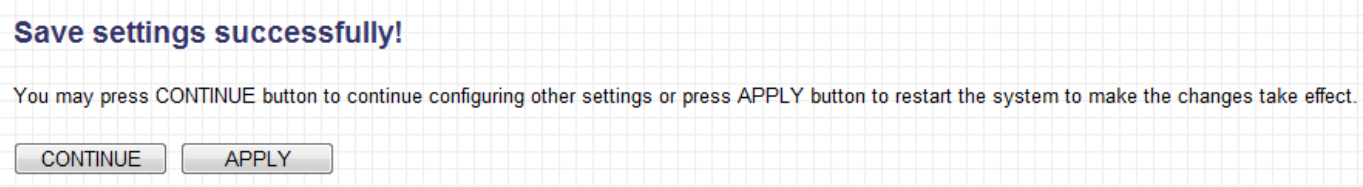


WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. AES is safer than TKIP, but not all wireless client support it. Please make sure your wireless client supports the cipher you selected. **We recommend WPA2(AES). If your wireless device does not support AES, then select WPA2 Mixed.**
Pre-shared Key Format	Please select the format of the pre-shared key here, available options are “Passphrase” (8 to 63 alphanumerical characters) and “Hex (64 characters)” – 0 to 9 and a to f.

Root AP Security 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:

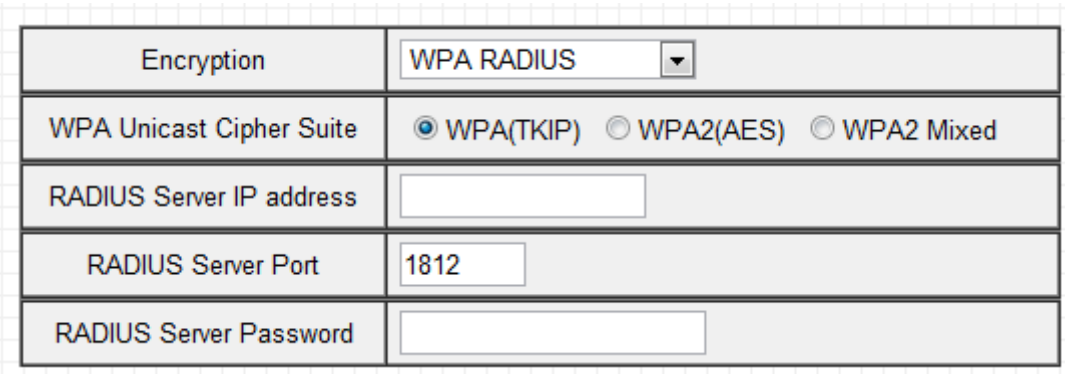


Click "CONTINUE" to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

III-5-5. WPA Radius

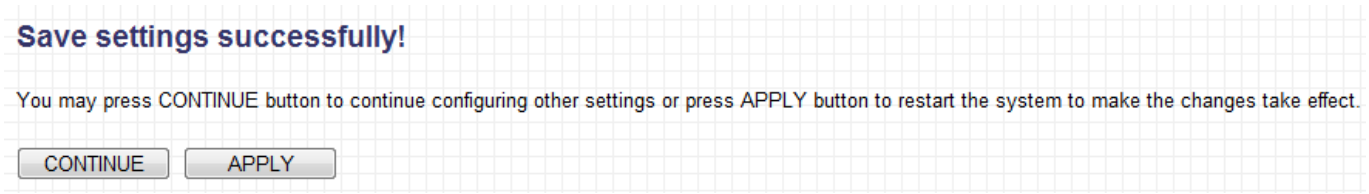
WPA RADIUS is a combination of WPA encryption and RADIUS user authentication. If you have a RADIUS authentication server, you can check the identity of every wireless client by using a user database.



WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. AES is safer than TKIP, but not every wireless client supports it. Please make sure your wireless client supports the cipher you selected.
RADIUS Server	Enter the IP address of the RADIUS

IP address	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:

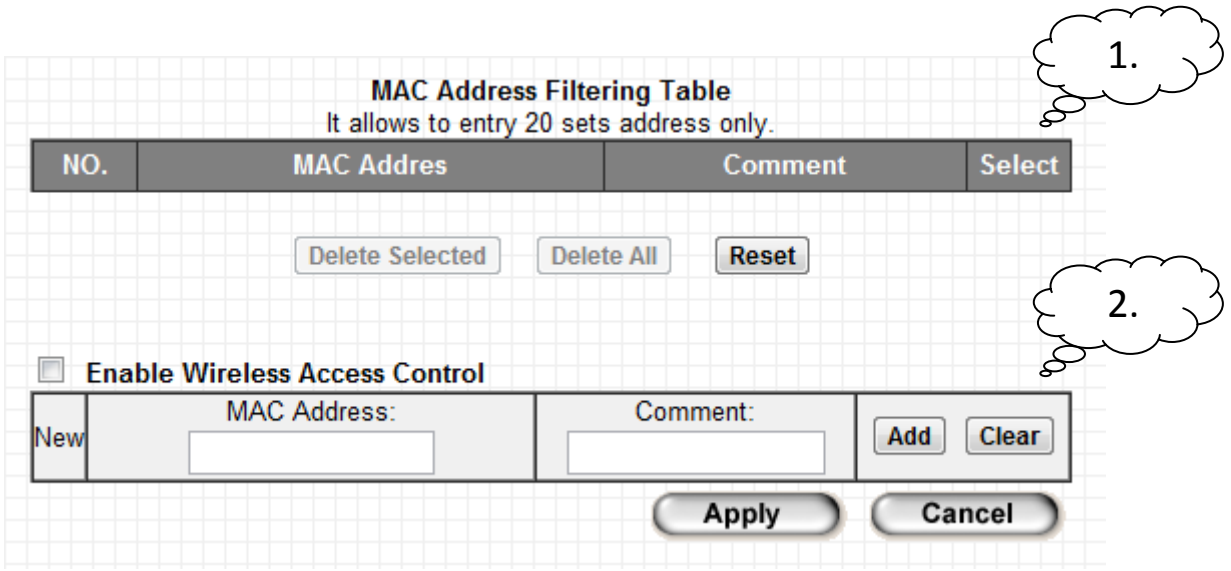


Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

III-6. MAC Filtering

The MAC filtering feature allows you to define a list of wireless devices permitted to connect to this access point. Devices are 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.



1. MAC Address Filtering Table

This table displays MAC addresses which have been added to the list of

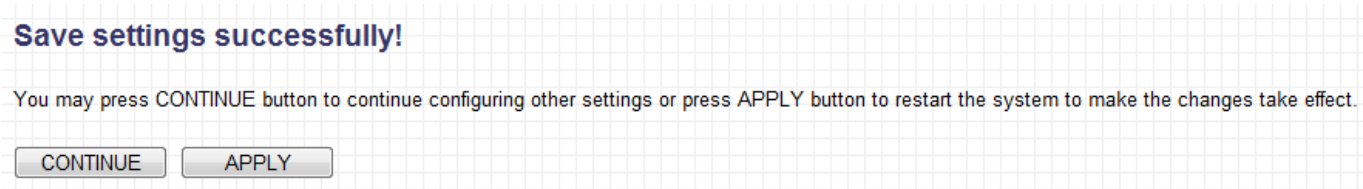
permitted devices.

Select	Check this box to select MAC address(es) for deletion.
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.

2. **Add new entries** to the MAC Filtering Table here.

Enable Wireless Access Control	Check this box to enable MAC address filtering. **If unchecked, no MAC restrictions will be enforced**, and any wireless client with proper encryption settings will be able to connect to this wireless access point.
MAC address	Input a MAC address allowed using this wireless access point here. Do not add any colons (:) or hyphens (-) only enter 0 to 9 and a to f here, such as “112233445566” or “aabbccddeeff”.
Comment	You can input an optional comment unique to this MAC address for reference, e.g. “ROOM 2A Computer”. You can enter up to 16 alphanumerical characters.
Add	After entering the MAC address and (optional) comment, click this button to add the MAC address entry to the list.
Clear	Remove all characters in the “MAC address” and “Comments” fields.

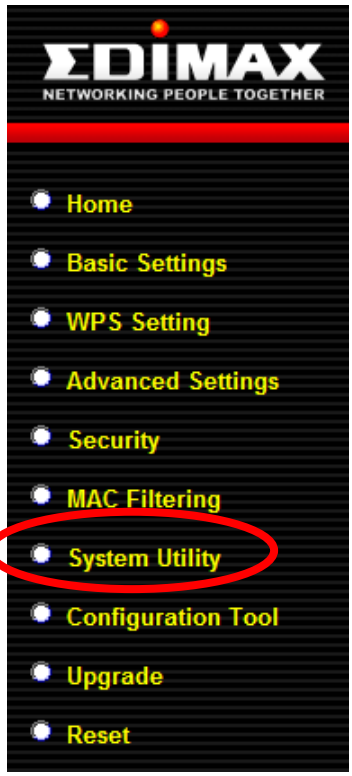
Click “APPLY” to save changes. The following message will appear:



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

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

III-7. System Utility

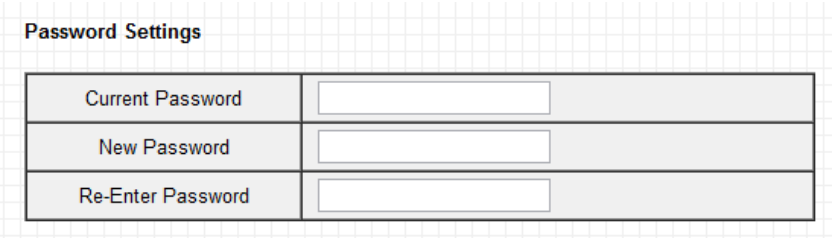


In “System Utility” you can configure basic system and administrative parameters.

On the main screen on the right there are 3 categories you can configure, **Password Settings, Management IP and DHCP Server.**

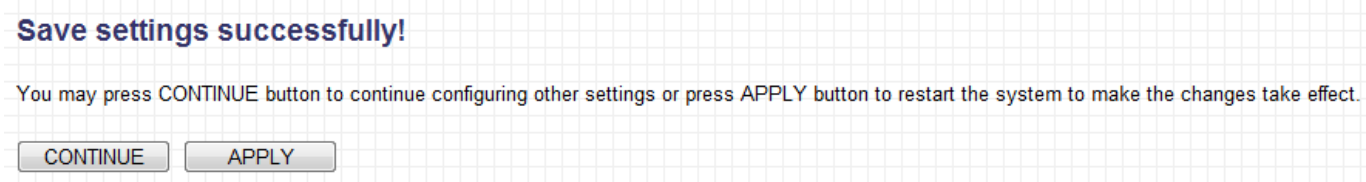
III-7-1. Password Settings

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



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:



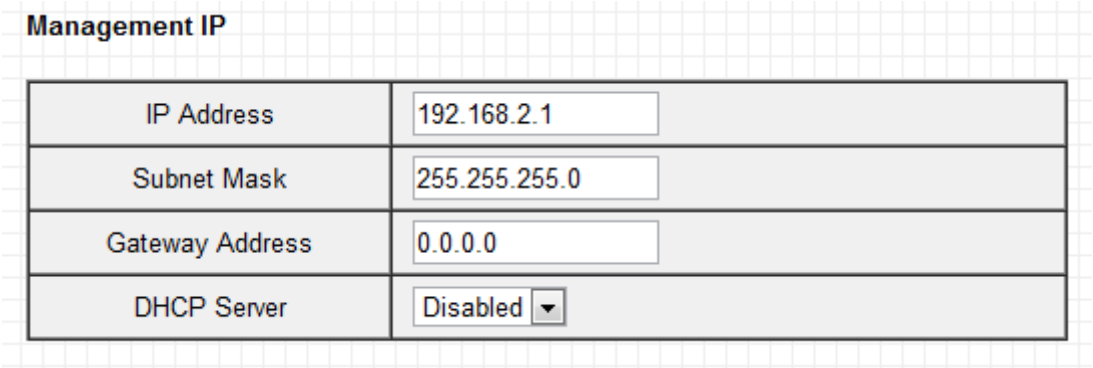
Click “CONTINUE” to save the changes but not apply them yet. This allows you

to make further changes in the browser-based management interface, before applying them all at once.

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

III-7-2. 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.



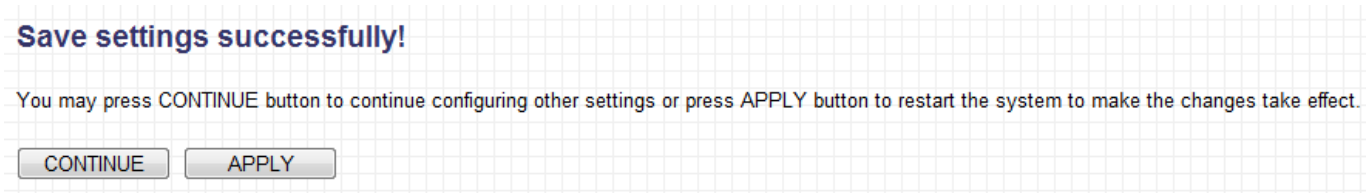
IP Address	Specify an IP address here. This IP address will be assigned to your access point, and will replace the default IP address 192.168.2.1.
Subnet Mask	Input the subnet mask of the new IP address.
Gateway Address	Input the network’s gateway IP address.
DHCP Server	Select “Enabled” if you wish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



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

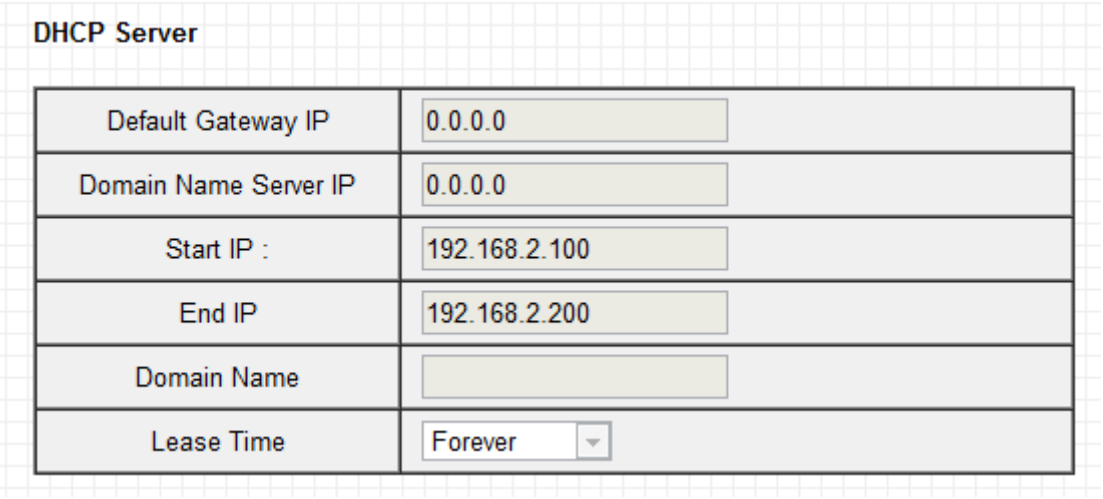
Click “APPLY” to restart the device and implement any changes. The device will restart itself.

III-7-3. DHCP Server

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

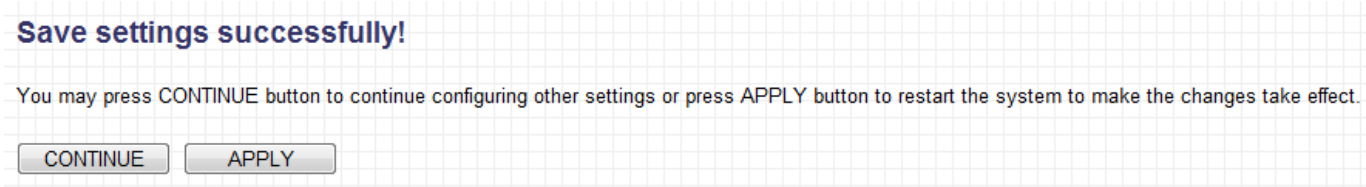
Note: This option will be unavailable unless you enable this function by selecting “Enabled” from the drop down menu labeled “DHCP Server”, under the heading “Management IP” as detailed above

Enter the appropriate information as shown below.



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.

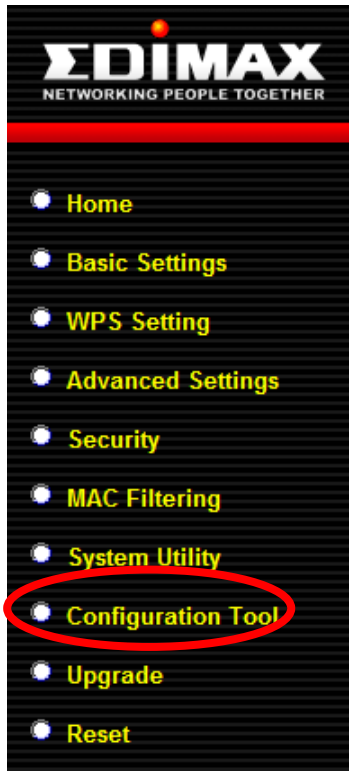
Click “APPLY” to save changes. The following message will appear:



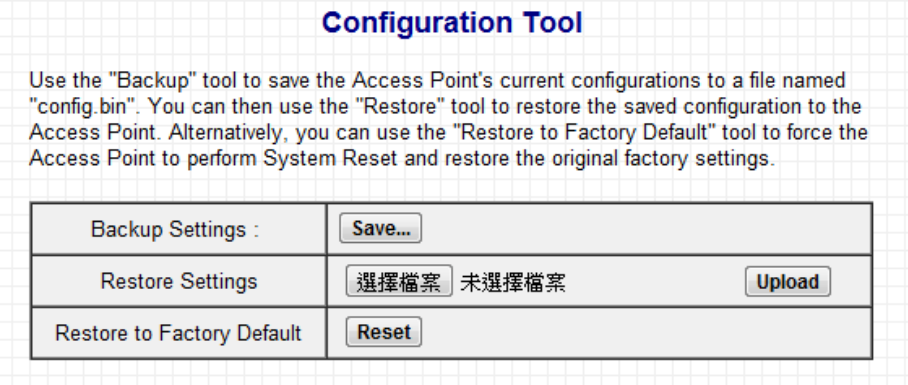
Click “CONTINUE” to save the changes but not apply them yet. This allows you to make further changes in the browser-based management interface, before applying them all at once.

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

III-8. Configuration Tool



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.



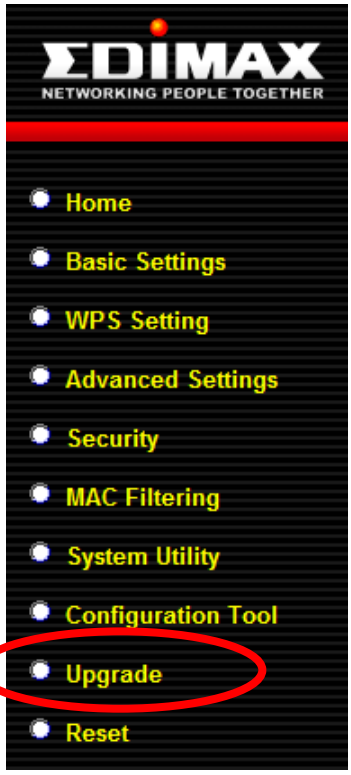
Backup Settings	Click "Save" to save the current settings on your computer as a .bin file. The default filename is config.bin.
Restore Settings	Click the browse button to locate a previously saved configuration file and then click "Upload" to upload the file and replace your current settings.
Restore 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-9. Upgrade



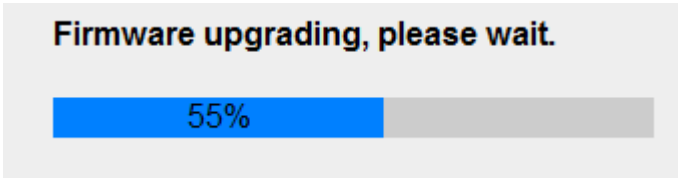
The access point's upgrade feature allows you to update the system firmware to a more recent version. You can download the latest firmware from the Edimax website.

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

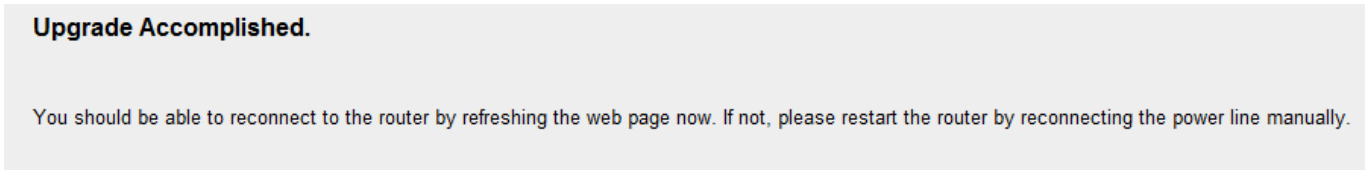
Note: Do not turn off or disconnect the access point during a firmware upgrade, as this could damage the device.

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

Click on the browse 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:

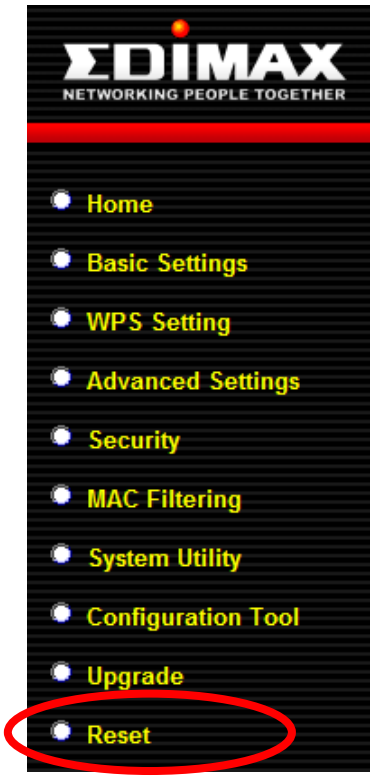


Please wait for the upgrade to complete. When it is complete, you will see the following message.



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

III-10. Reset

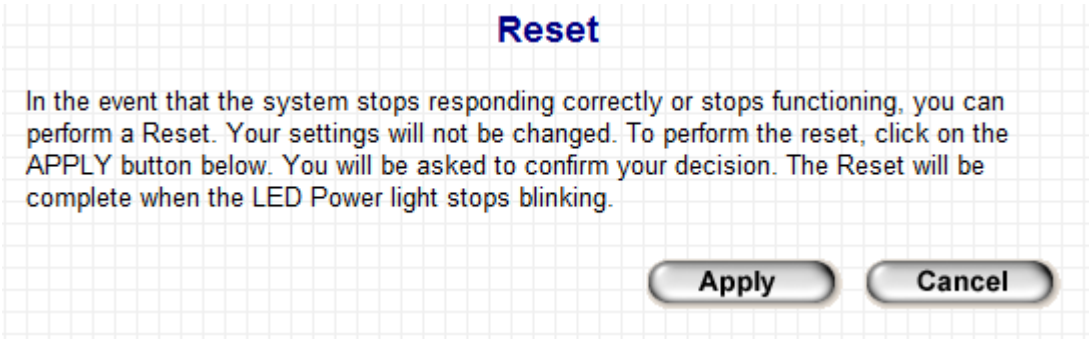


If the access point malfunctions or is not responding, then it is recommended that you reset the device. This feature is useful if the location of the access point is not convenient.

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.

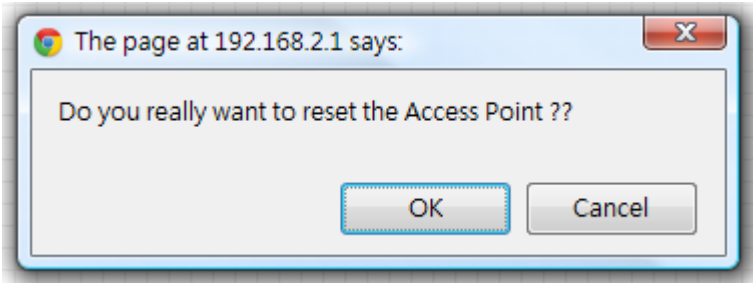
Note: Resetting the device will not affect the current settings and configuration.

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.

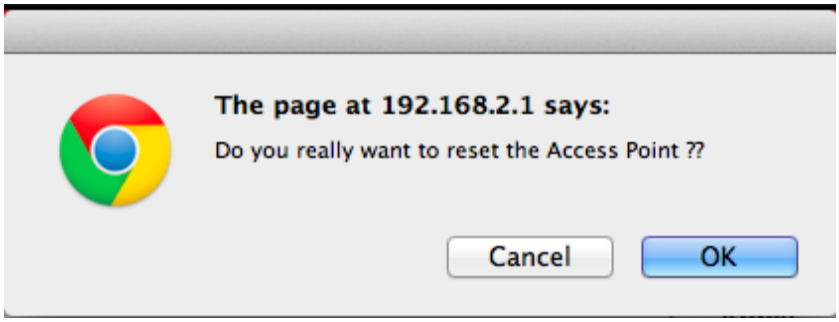


Please click “Apply” to reset the device. A pop up window will ask you to confirm, as shown below.

Windows:



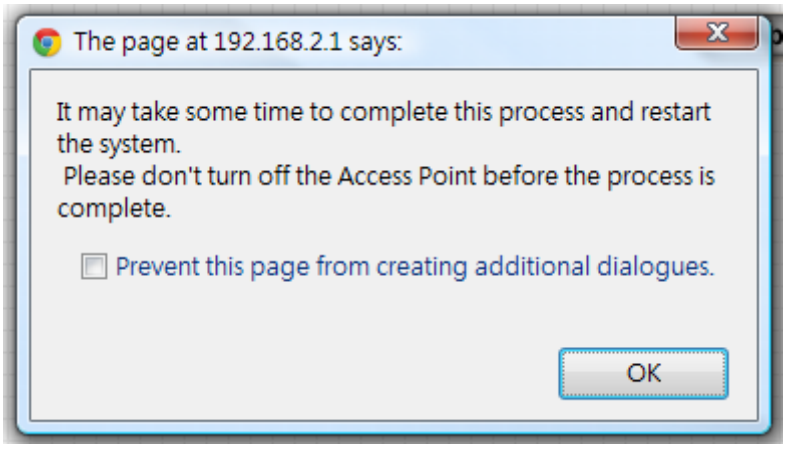
Mac:



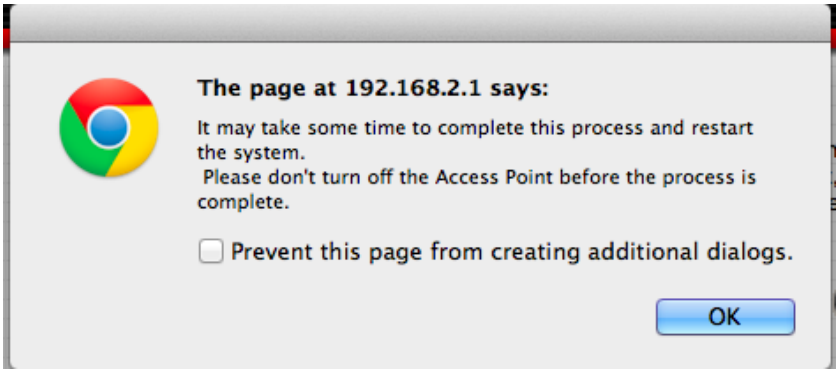
Click “OK” to continue, or “Cancel” to abort. You will see a warning that it may take a while for the access point to reset.

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:

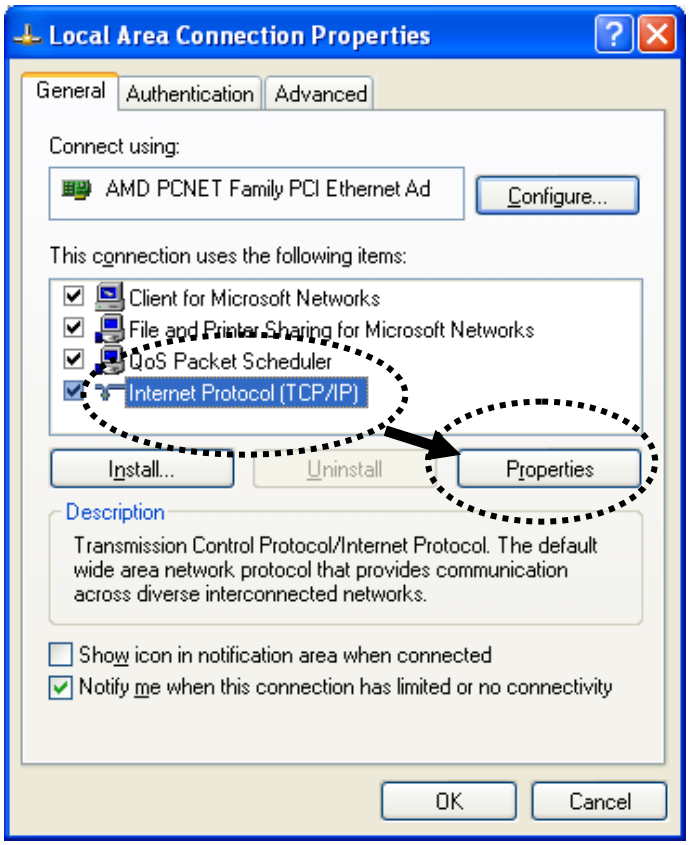
This is since the access point's default IP address 192.168.2.1 may not be in the same IP address subnet of your network; meaning you are unable to access the browser based configuration interface. In order to access the browser based configuration interface, your computer's IP must be **192.168.2.x** 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-7-2. 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.

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".

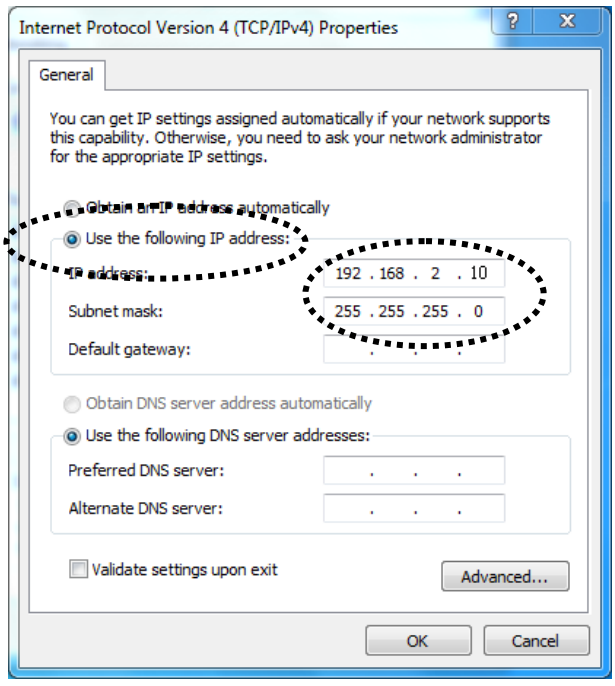
   The "Local Area Connection Status" window will appear, click "Properties".



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

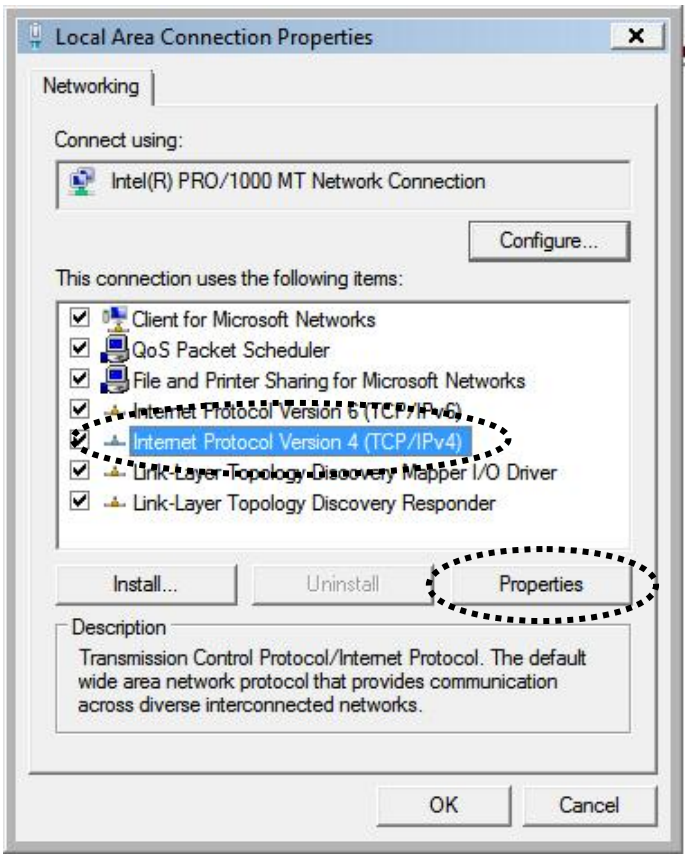
   IP address: 192.168.2.10
   Subnet Mask: 255.255.255.0

   Click ‘OK’ when finished.



IV-1-2. Windows Vista

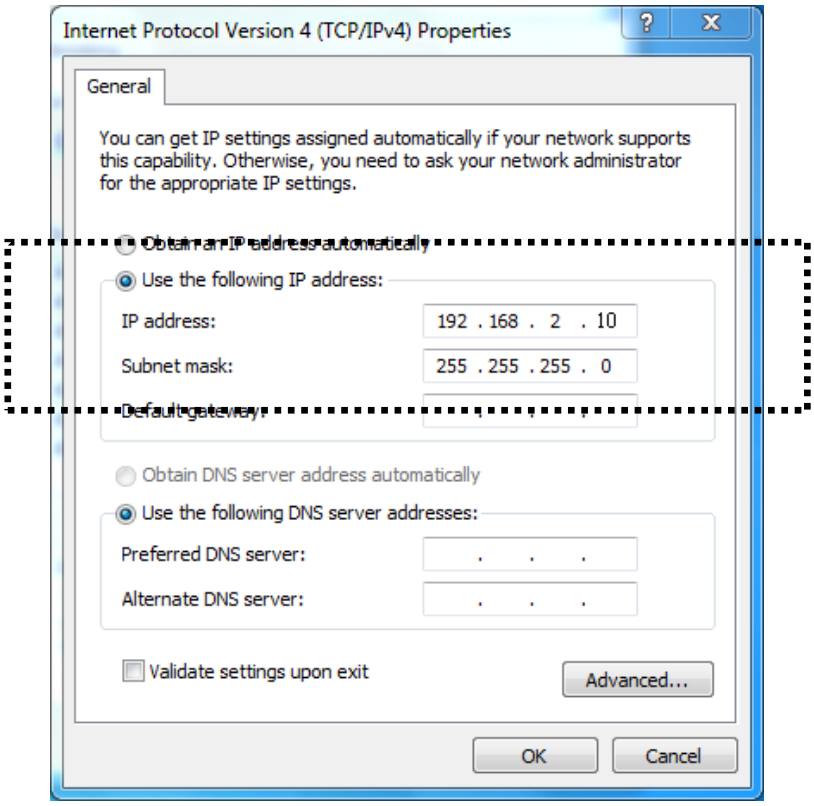
1. Click the “Start” button, located in the lower-left corner of your computer, and then click “Control Panel”. Click “View Network Status and Tasks” and then click “Manage Network Connections”. Right-click “Local Area Network”, and select “Properties”. The “Local Area Connection Properties” window will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



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

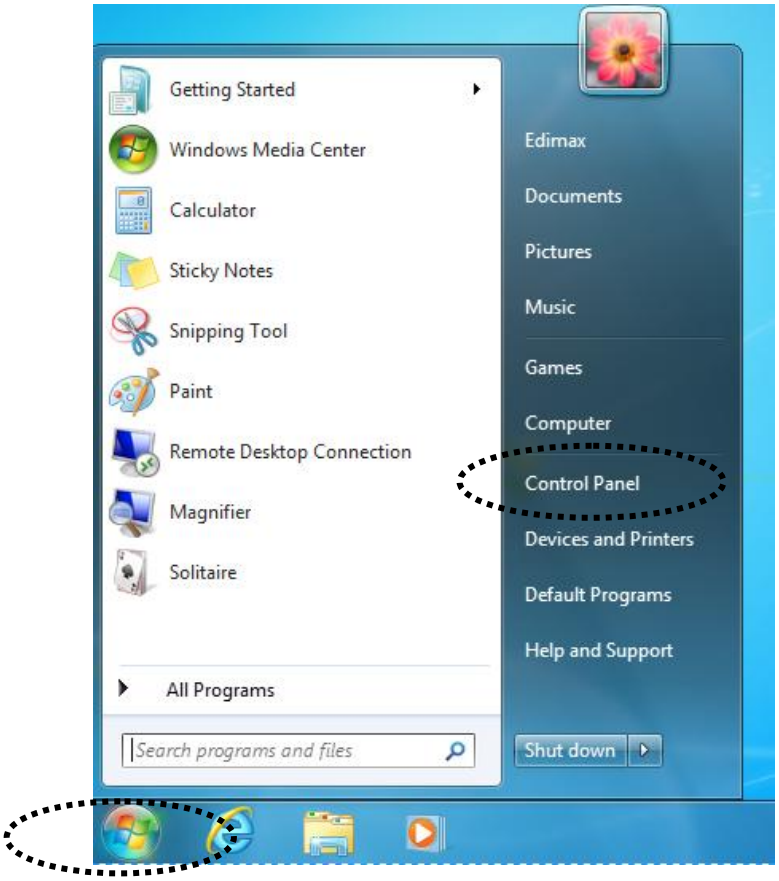
   IP address: 192.168.2.10
   Subnet Mask: 255.255.255.0

   Click ‘OK’ when finished.

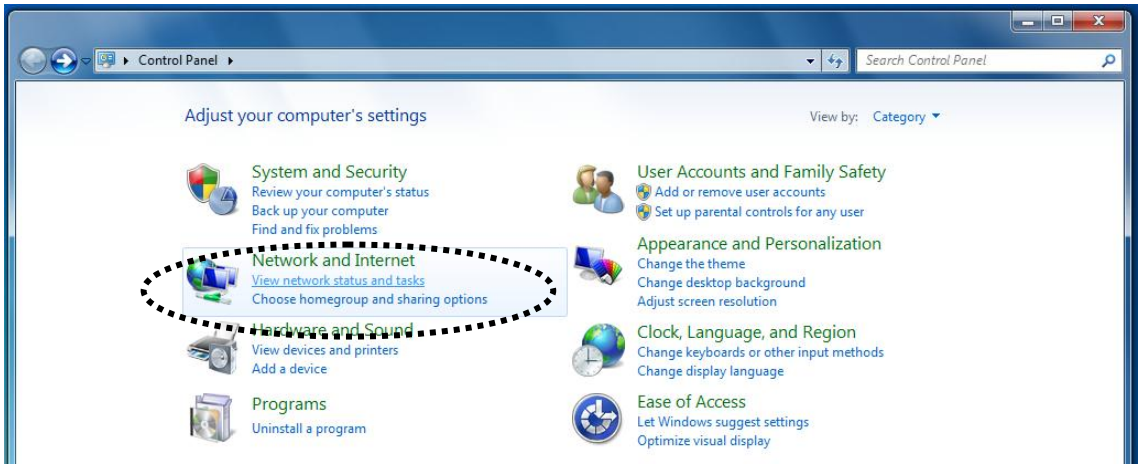


IV-1-3. Windows 7

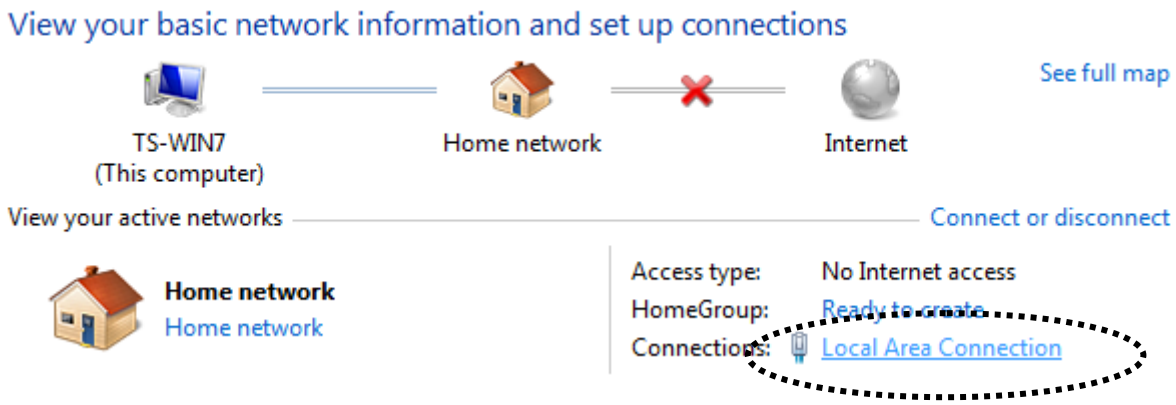
1. Click the “Start” button, located in the lower-left corner of your computer, and then click “Control Panel”.



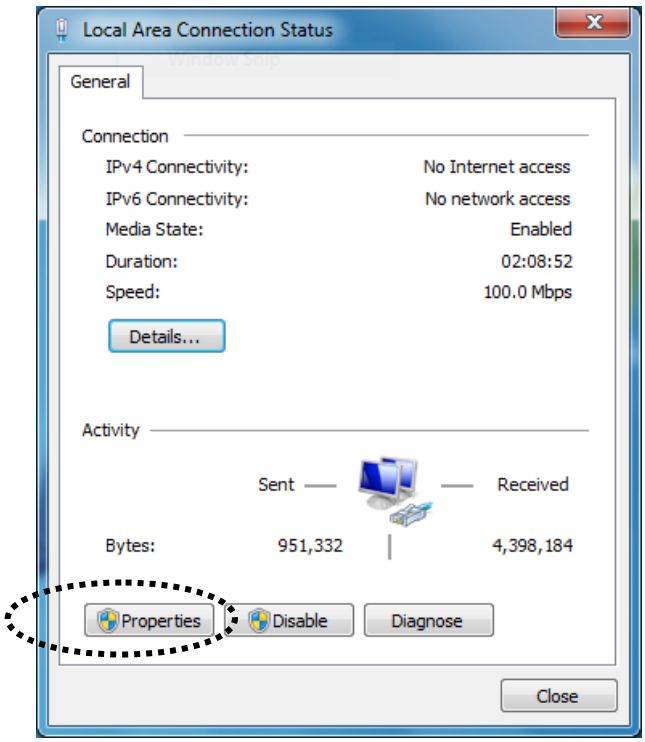
1. Under “Network and Internet” click “View network status and tasks”.



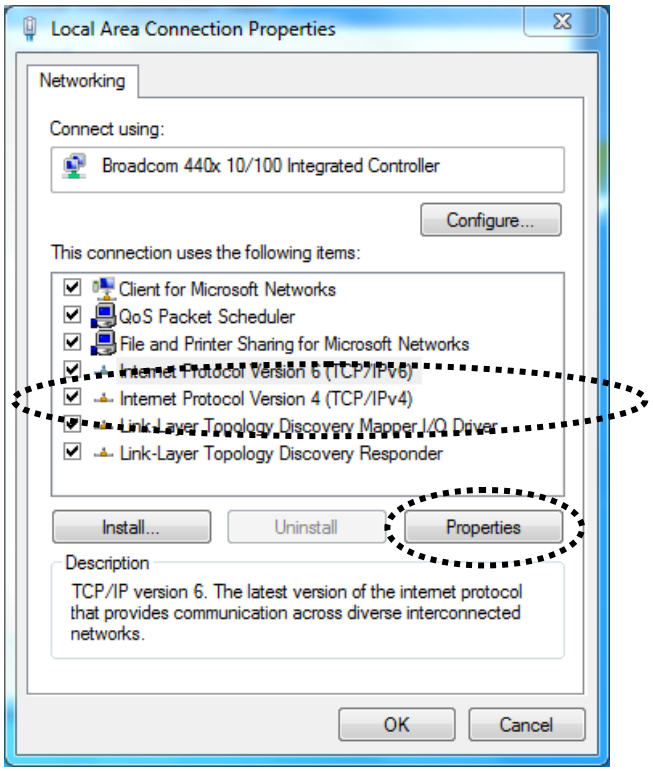
2. Click “Local Area Connection”.



3. Click “Properties”.



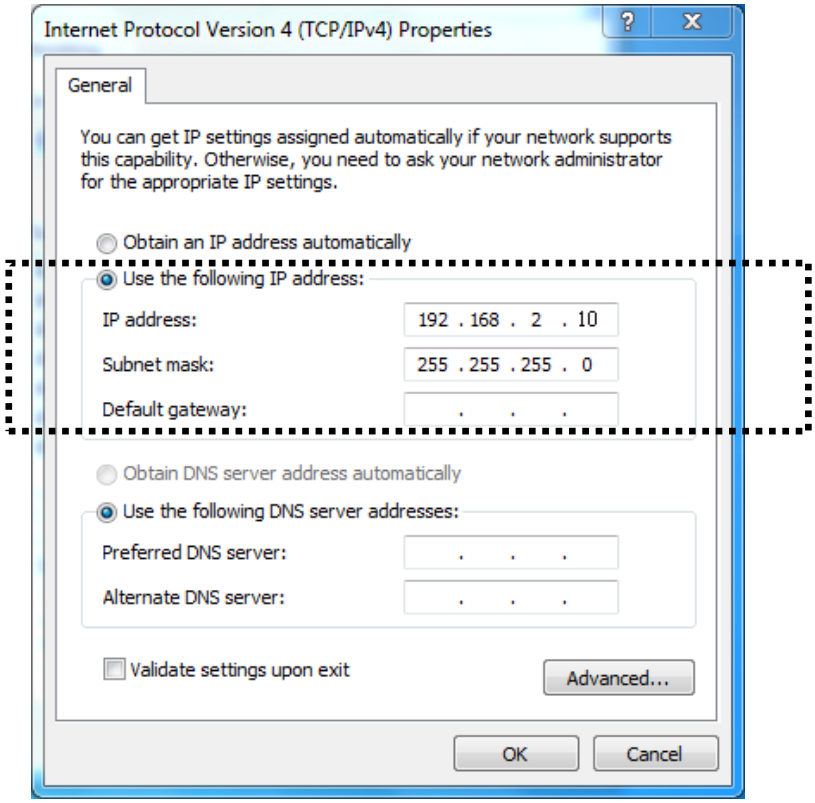
4. Select “Internet Protocol Version 4 (TCP/IPv6) and then click “Properties”.



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

   IP address: 192.168.2.10
   Subnet Mask: 255.255.255.0

   Click ‘OK’ when finished.

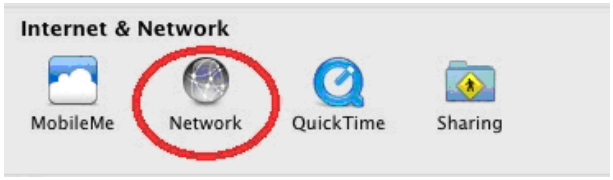


IV-1-4. Mac OS

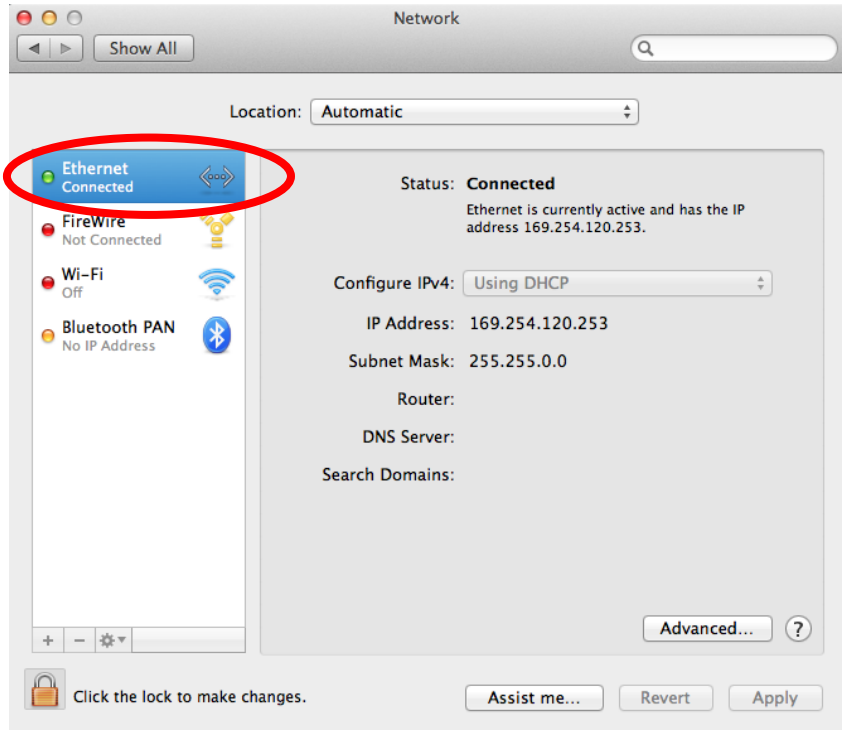
Note: Please ensure that your access point is switched on and connected to your Macintosh via Ethernet cable before you begin.

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

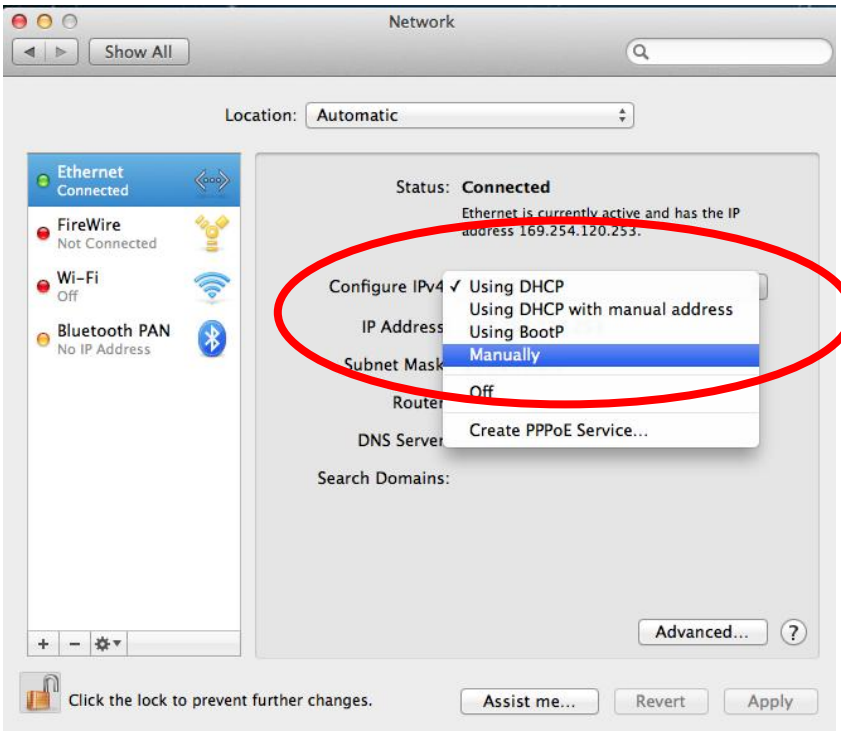
2. In System Preferences, click on “Network”.



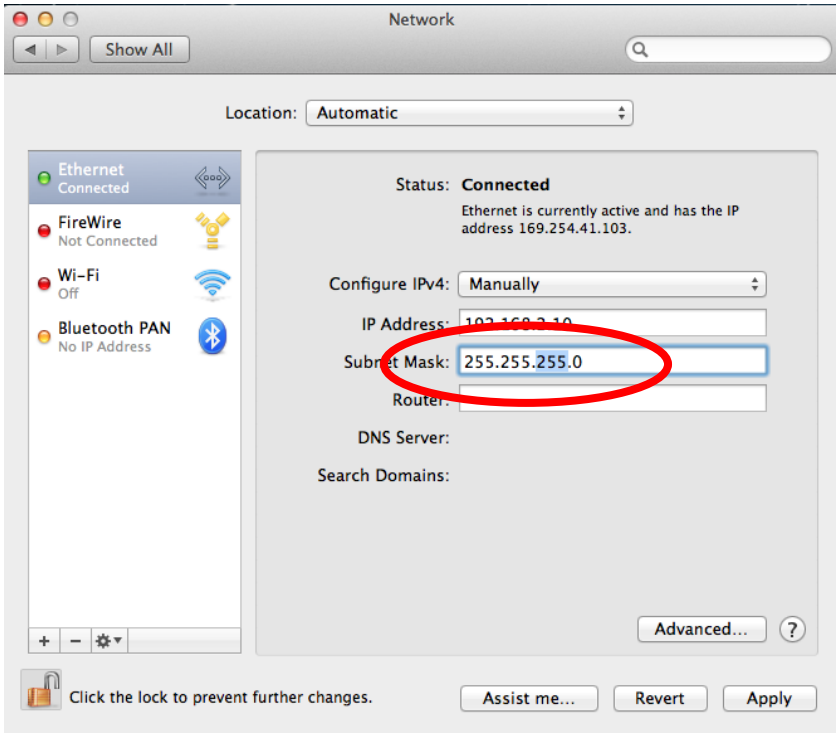
3. Here you will see all of your network connections. Network Preferences will now display an Ethernet adapter, as shown below. The status of “Ethernet” should be “Connected”.



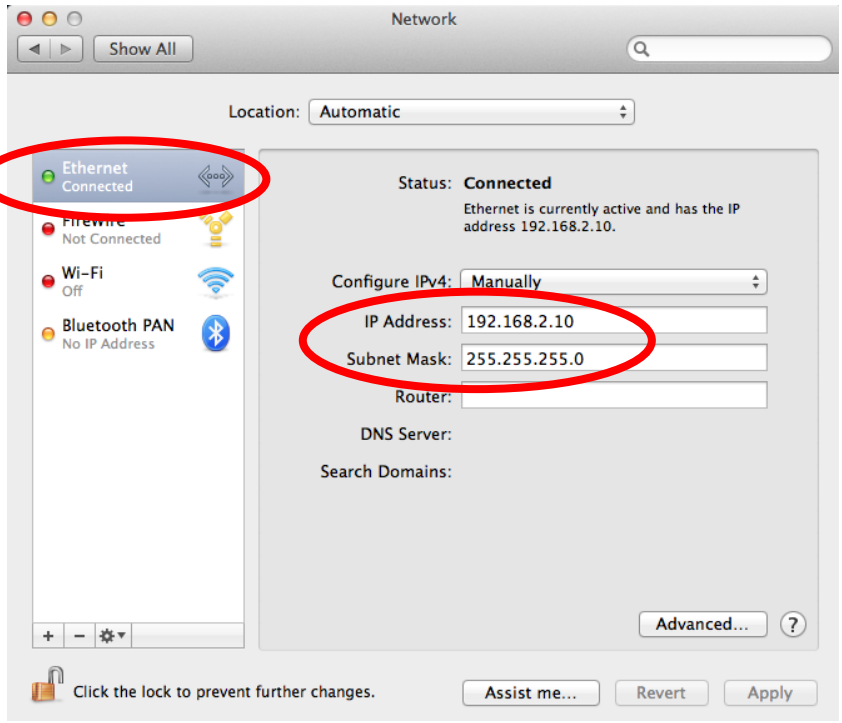
4. Click on “Ethernet” in the left panel and then click the drop down arrow for the menu labeled “Configure IPv4” in the right panel. From the drop down menu, select “Manually”.



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.



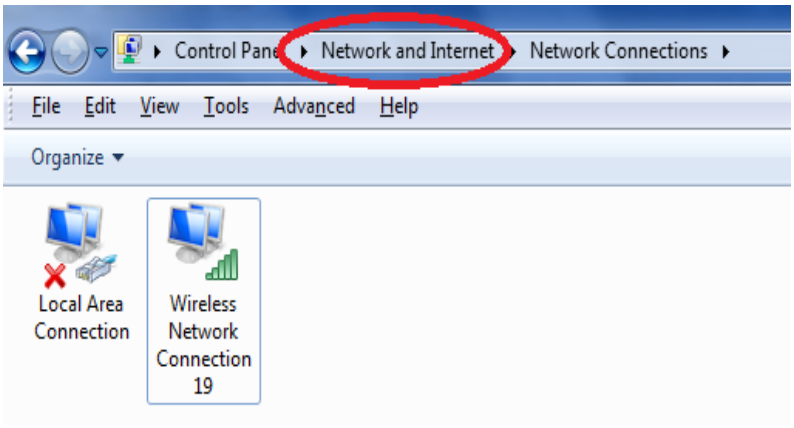
IV-2. How to Find your Network Security Key

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

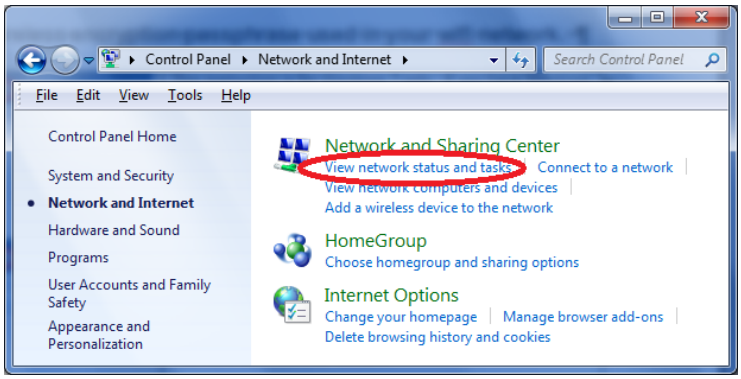
Note: If you are using Windows XP or earlier, please contact your ISP or router manufacturer to find your network security key.

IV-2-1. Windows 7 & Windows Vista

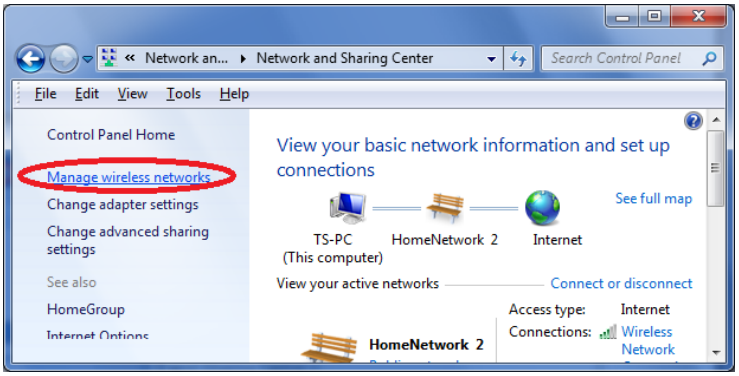
1. Open “Control Panel” and click on “Network and Internet” in the top menu.



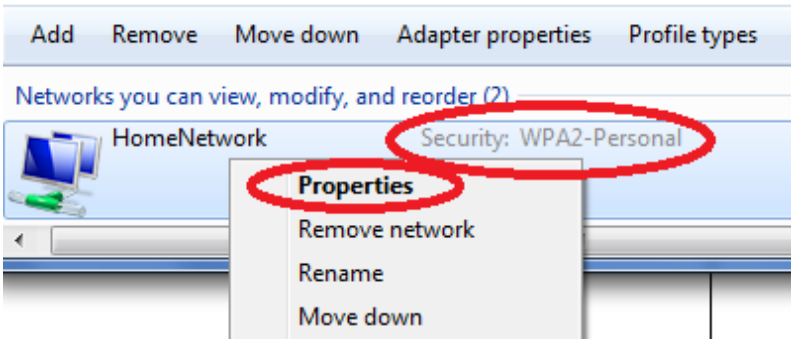
2. Click on “View network status and tasks” which is under the heading “Network and Sharing Center”.



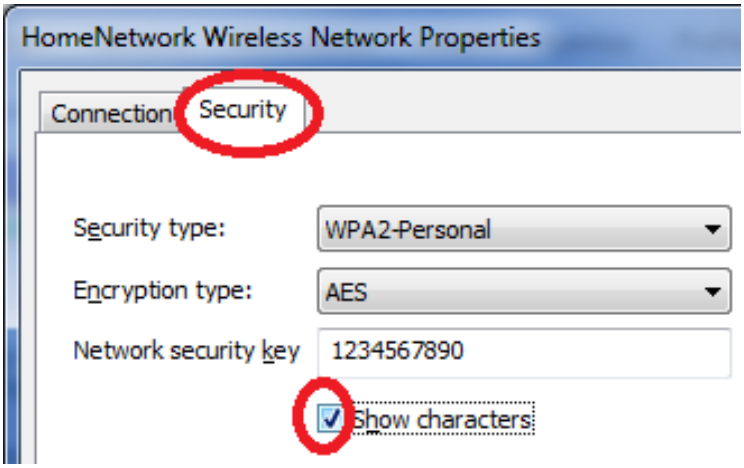
3. Click on “Manage wireless networks” in the left menu.



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”.

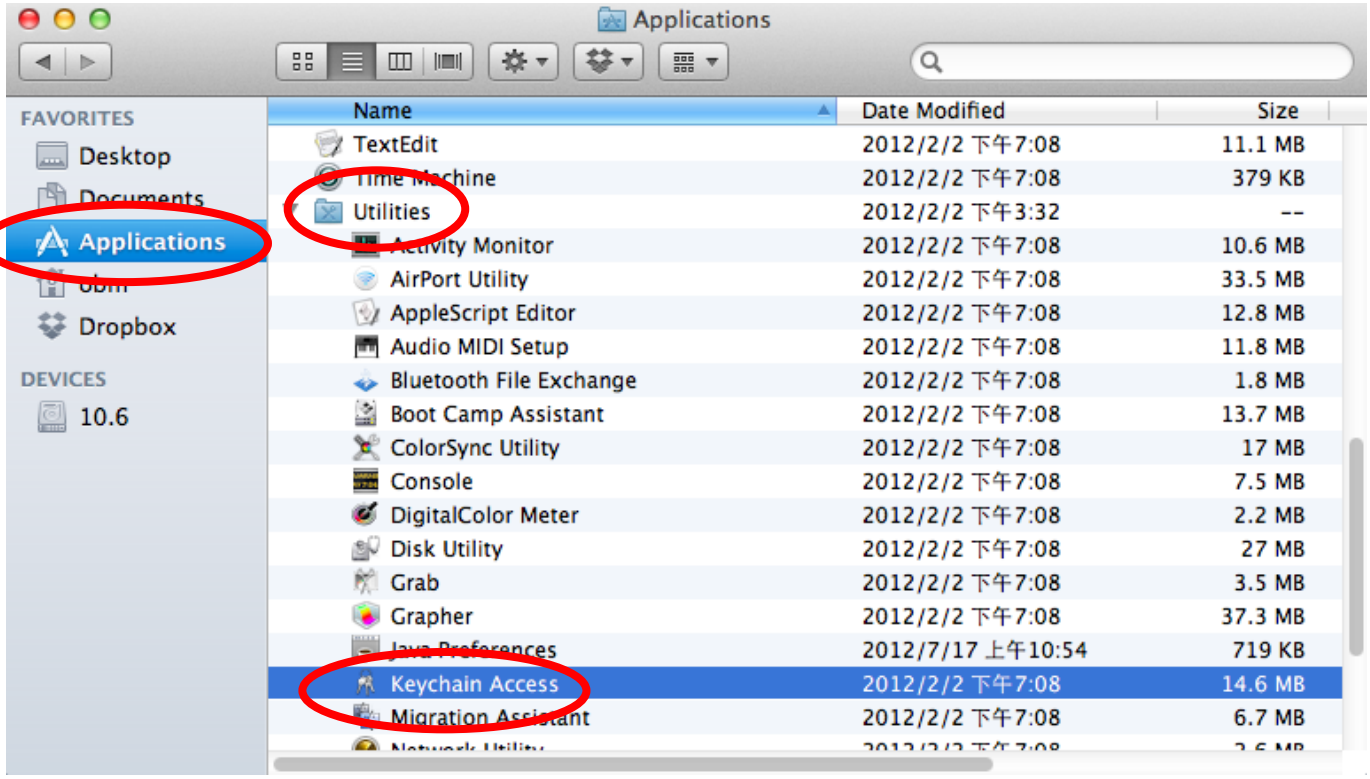


5. Click on the “Security” tab, and then check the box labeled “Show characters”. This will show your network security key. Click the “Cancel” button to close the window.

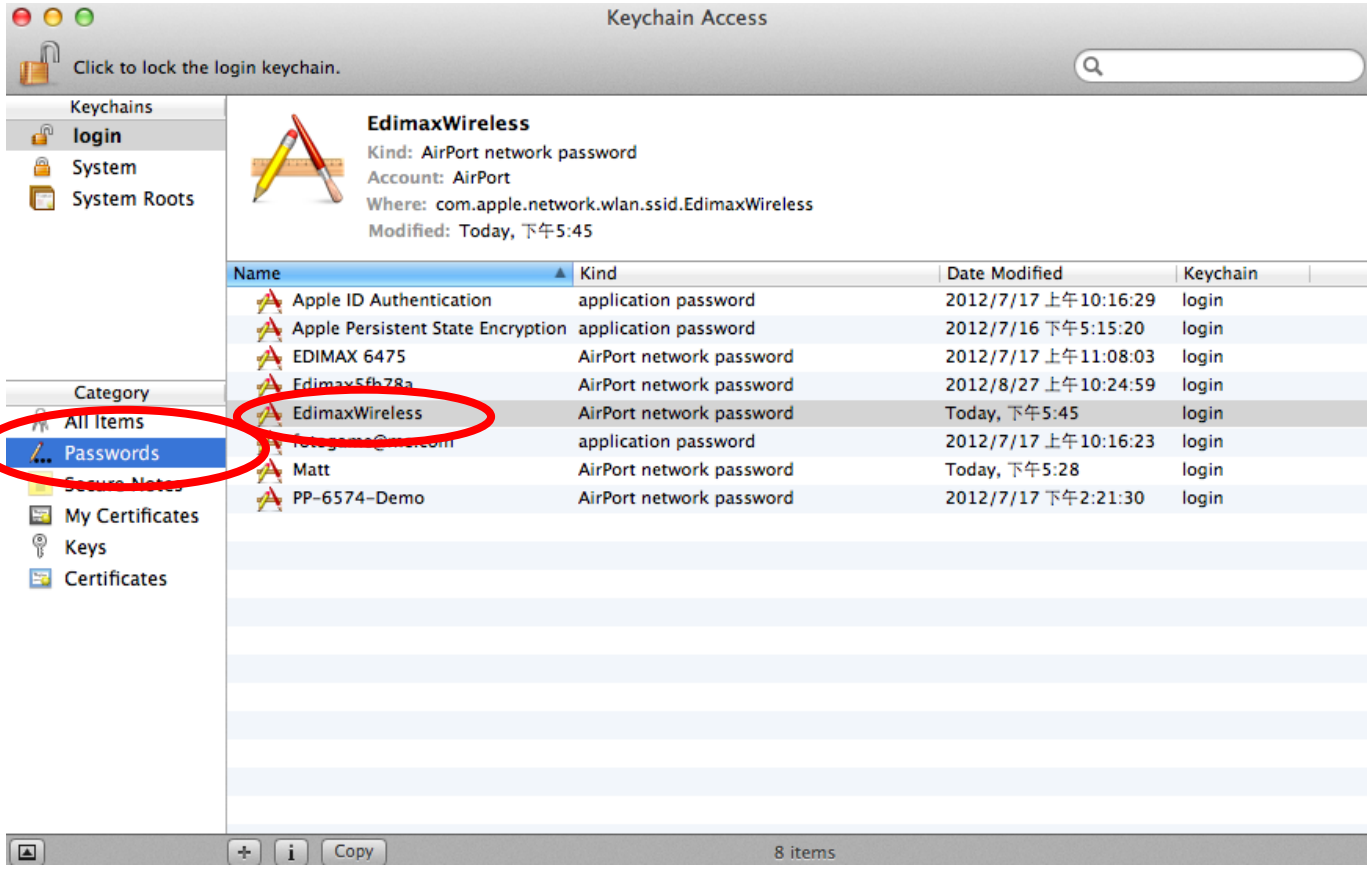


IV-2-2. Mac

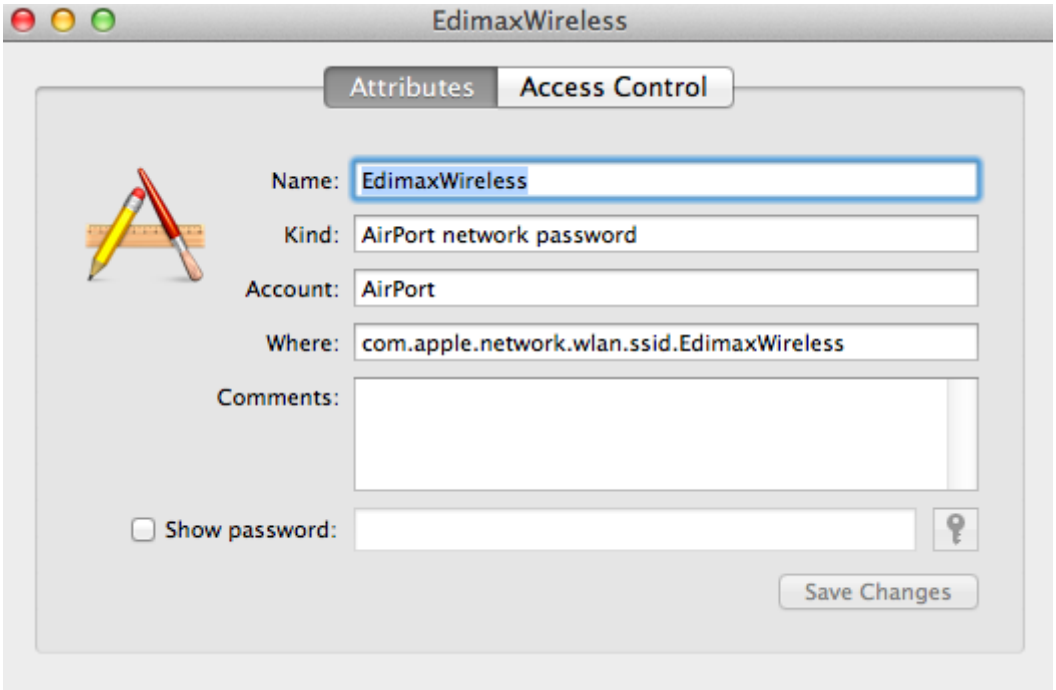
1. Open a new Finder window, and select “Applications” from the menu on the left side. Open the folder labeled “Utilities” and then open the application “Keychain Access”.



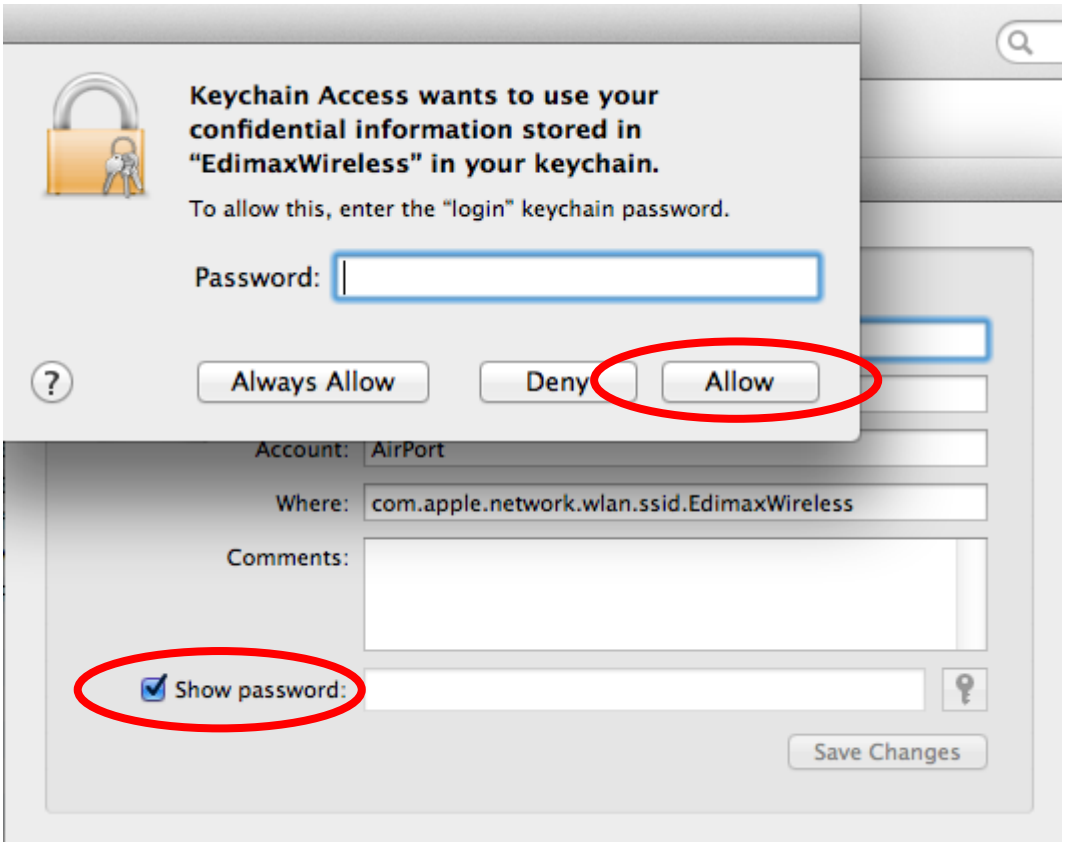
2. Select “Passwords” from the sub-menu labeled “Category” on the left side, as shown below. Then search the list in the main panel for the SSID of your network. In this example, the SSID is “EdimaxWireless” – though your SSID will be unique to your network.



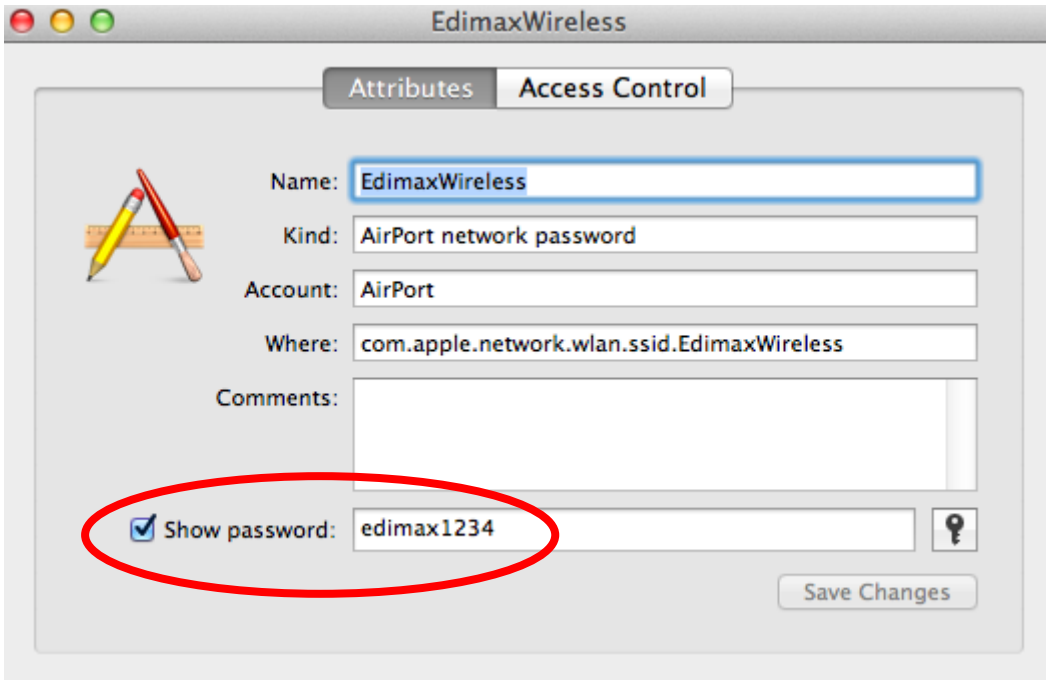
3. Double click the SSID of your network and you will see the following window.



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 travel router, 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.	a. Click "Rescan" several more times and see if the wireless access point/device appears. b. Adjust the position of the access point, or move closer to a known wireless access point. c. 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.	a. Click "Connect" several more times and see if you can establish a connection. b. Ensure that you input the correct passphrase/security key if connecting to an access point with encryption. c. 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.	a. Make sure access point is powered on. Check the LED on the front panel. If the LED is out, then check the USB connection. b. Use your wireless device connects to this travel router wirelessly. c. Make sure you are using the correct IP address. d. If you are using a MAC or IP address

	filter, try to connect the access point to another computer. e. Set your computer to obtain an IP address automatically (DHCP), and see if your computer can obtain an IP address. f. 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 client.	a. Check if "Broadcast ESSID" (in the "Wireless Advanced" section of the browser-based 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.Broadbandaccess point.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 "Broadbandaccess point.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

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

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

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

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

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by ".": aaa.aaa.aaa.aaa, where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by ".": bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each "b" can either be 0 or 1.
A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as "x" number of leading 1's.
When both are represented side by side in their binary forms, all bits in the IP address

that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000
It means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

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

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

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

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

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

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

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110

H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

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

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

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

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer 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

NETWORKING PEOPLE TOGETHER

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