Airdata 300 Access Point

11n Wireless 300 Mbps Access Point

manual

Version 1.0

Contents

1. Product Information

Crypto's Airdata 300 Access Point is a cost-effective wireless access point. Computers and wireless devices which are compatible with 802.11 Draft-N can connect to existing wired Ethernet network via this wireless access point, at the speed of 300Mbps. Easy install procedures allows any computer users to setup a network environment in very short time.

This wireless access point supports 64/128-bit WEP, WPA, and WPA2 wireless data encryption security features for home, office and enterprise use. It also supports the WPS feature that simplifies the wireless client setup procedures. Through the MAC filtering procedure it allows specific wireless devices of your choice to connect to this access point, adding another level of security to your Wireless Network.

1.1 Product Features

Other features of this access point include:

- Compatibility with IEEE 802.11b/g/Draft-N wireless network standard - works with other 802.11b/g/Draft-N wireless devices.
- High speed wireless network, six times faster than conventional 802.11g wireless network (up to 300Mbps).
- Allow wireless devices to connect to existing wired network and share network resources.
- Supports DHCP server function.
- Supports 64/128-bit WEP, WPA, and WPA2 wireless data encryption.
- Supports MAC address filtering (Only allow specific wireless device of your choice to connect to this access point).
- Supports RADIUS server; only allow users listed in your authorization server to use wireless network.
- Supports WPS (Wi-Fi Protected Setup), simplifies wireless client setup procedures.
- Easy to use web-based GUI (Graphical User Interface) for network configuration and management purposes.

1.2 Package Contents

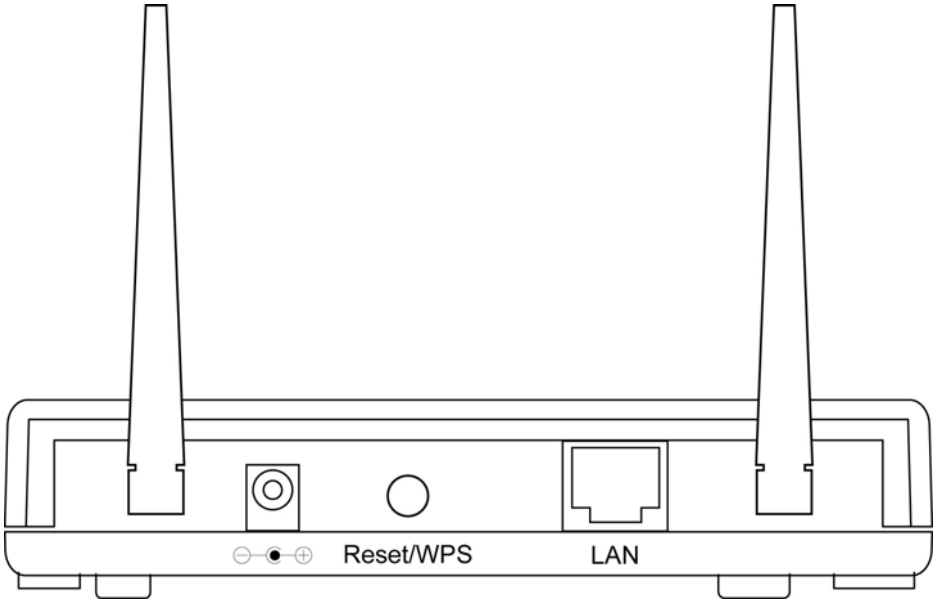
Before you starting to use this access point, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

1. Crypto Airdata 300 Access point
2. Detachable 3dBi Dipole Antenna
1. Quick Installation Guide (QIG)
1. RJ-45 Ethernet Cable
1. A/C power adapter
1. CD (with User's Manual)

1.3 Front Panel

LED Name	Light Status	Description
PWR	On	The access point is switched on and correctly powered.
WLAN	On	Wireless WPS mode is enabled.
	Off	Wireless network is switched off.
	Flashing	Wireless LAN activity (transferring or receiving data).
LAN	On	LAN port is connected
	Off	LAN port is not connected
	Flashing	LAN activity (transferring or receiving data)

1.4 Rear Panel



Item Name	Description
Antennas	Two reserve SMA antenna connectors for screwing 3dBi detachable antennas enclosed with the product.
Power	Power connector, connects to A/C power adapter.
Reset / WPS	Reset the access point to factory default settings (clear all settings) or start WPS function. Press this button and hold for 10 seconds to restore all settings to factory defaults, and press this button for less than 5 seconds to start WPS function.
LAN	Local Area Network (LAN) port.

2. System and Network Setup

2.1 Installing the access point to your Network

Please follow the instructions below to build the network connection between your new wireless access point and your computers or network devices:

1. Connect the access point to the ADSL modem, router, or switch/hub in your network through the LAN port of the access point by Ethernet cable.
2. Connect the A/C power adapter to the wall socket, and then connect it to the 'Power' socket of the access point.
   Please check all LEDs on the front panel. 'PWR' LED should be steadily on, LAN LEDs should be on if the access point is correctly connected to the ADSL modem, router or switch/hub.

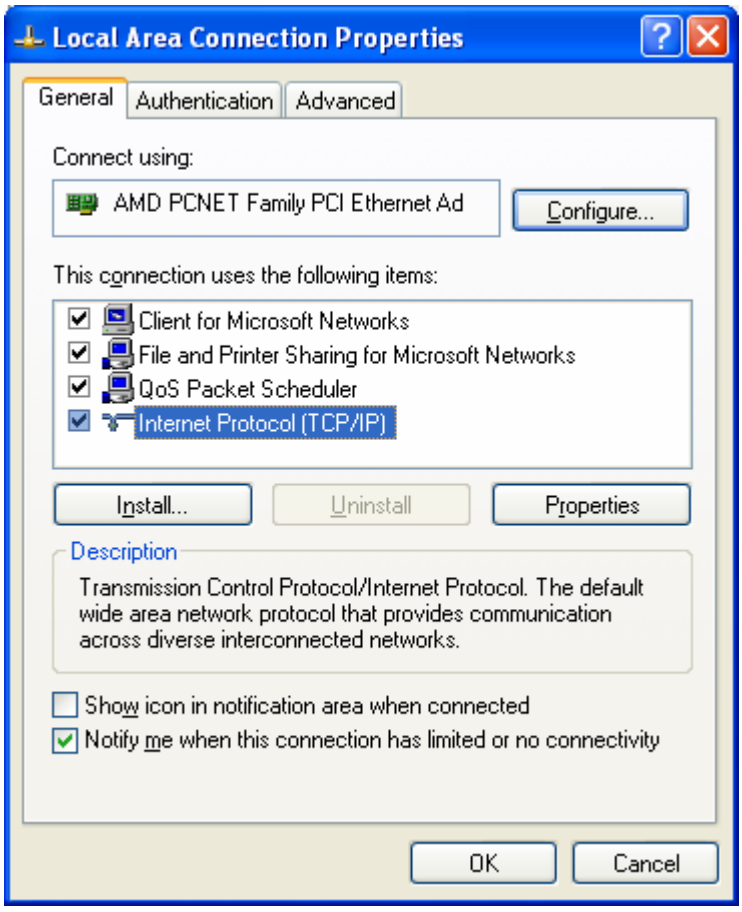
2.2 Connecting to wireless access point by web browser

After the network connection is built, the next step you should do is setup the access point with proper network parameters, so it can work properly in your network environment.

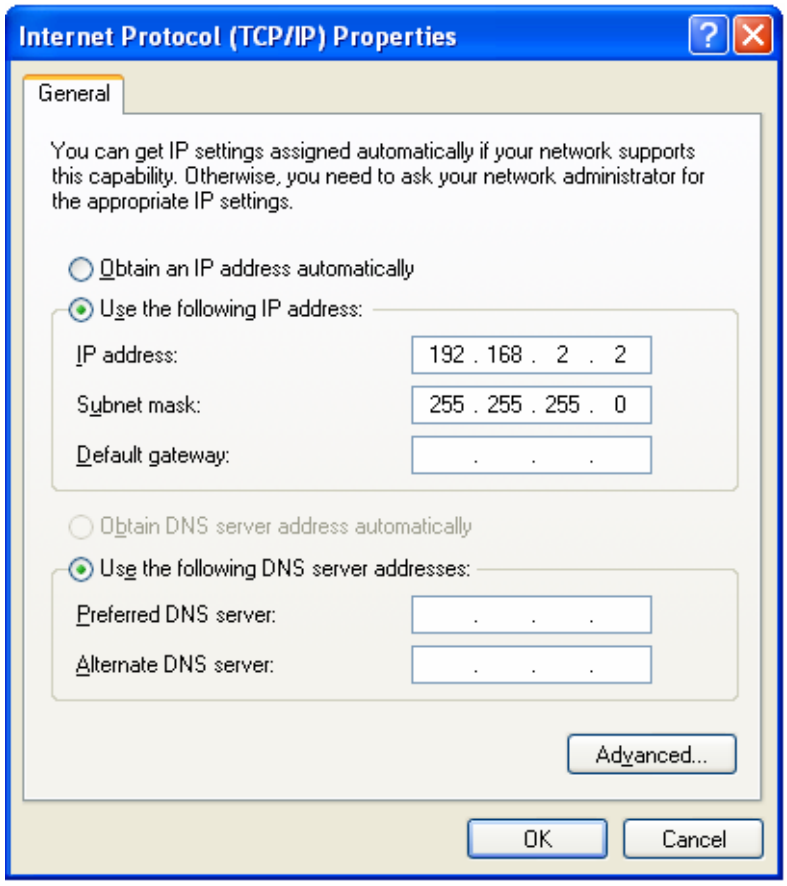
Before you can connect to the access point and initiate the configuration procedures, your computer must be able to get an IP address automatically (use dynamic IP address). If it's set to use static IP address, or you're unsure, please follow the following instructions to configure your computer to use dynamic IP address

2.2.1 Windows XP IP address setup

1. Click the 'Start' button, then click control panel. Double-click ***Network and Internet Connections*** icon, click ***Network Connections,*** and then double-click ***Local Area Connection, Local Area Connection Status*** window will appear, and then click 'Properties'. ***Local Area Connection Status*** window will appear, click 'Internet Protocol (TCP/IP)' and then click 'Properties'.

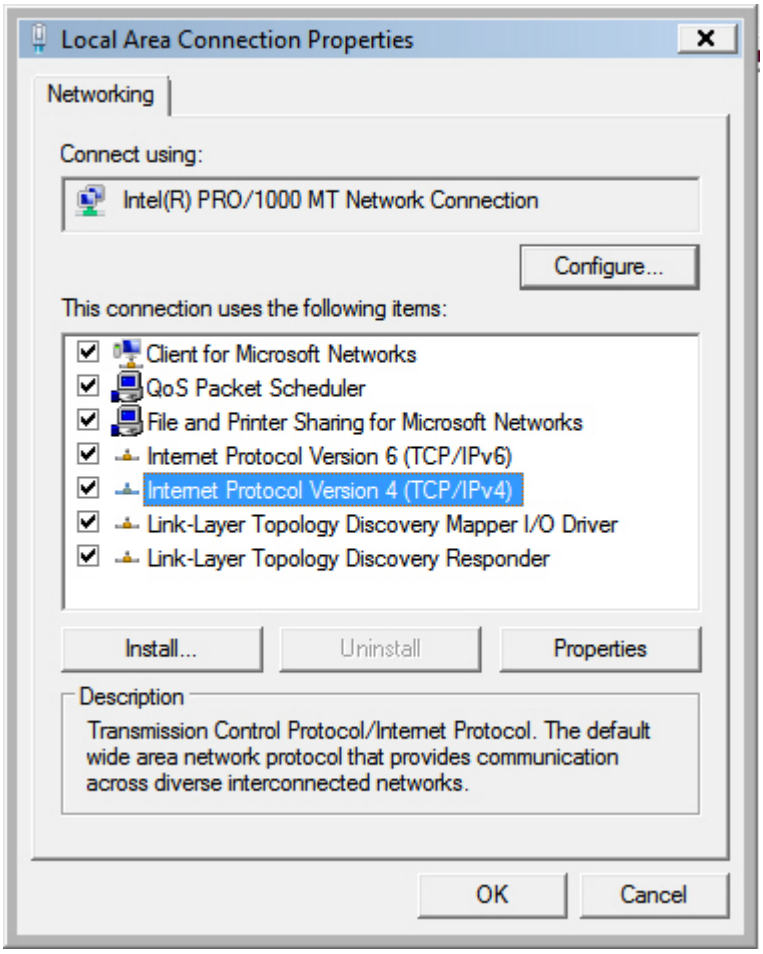


2. Select ‘Use the following IP address’, then input the following settings in respective fields:
IP address: 192.168.2.2
Subnet Mask: 255.255.255.0
click ‘OK’ when finish.

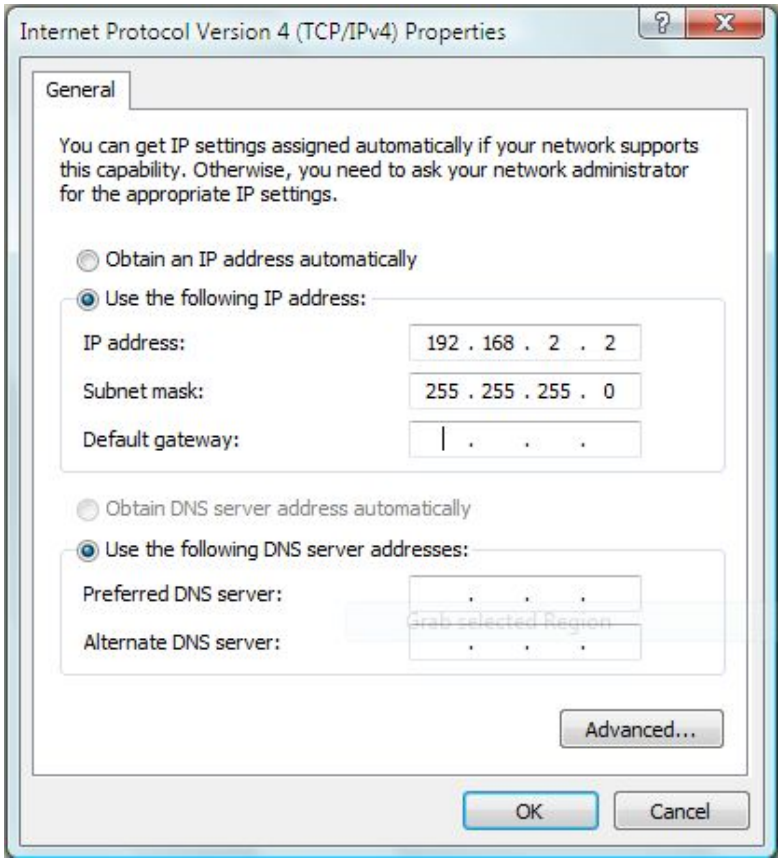


2.2.2 Windows Vista IP address setup

1. Click ‘Start’ button, then click control panel. Click ***View Network Status and Tasks***, and then click ***Manage Network Connections.*** Right-click ***Local Area Network, then select ‘Properties’. Local Area Connection Properties*** window will appear, select ‘Internet Protocol Version 4 (TCP / IPv4), and then click ‘Properties’



2. Select ‘Use the following IP address’, then input the following settings in respective field:
IP address: 192.168.2.2
Subnet Mask: 255.255.255.0
click ‘OK’ when finish.

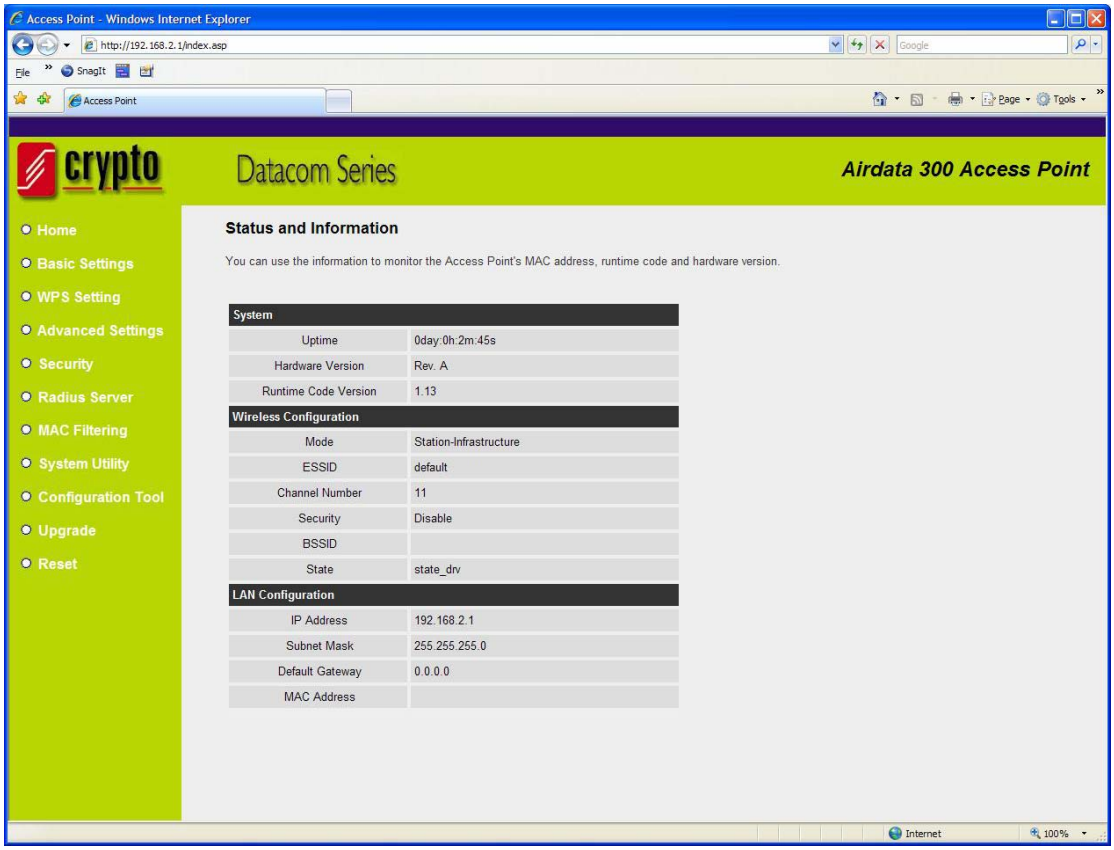


2.2.3 Connecting to Web Management Interface

All functions and settings of this access point must be configured via the web management interface. Please start your web browser, and input '192.168.2.1' in address bar, then press 'Enter' key. The following message should be shown:

Please input user name and password in the field respectively, default user name is

'admin', and default password is 'admin', then press 'OK' button, and you can see the web management interface of this access point:

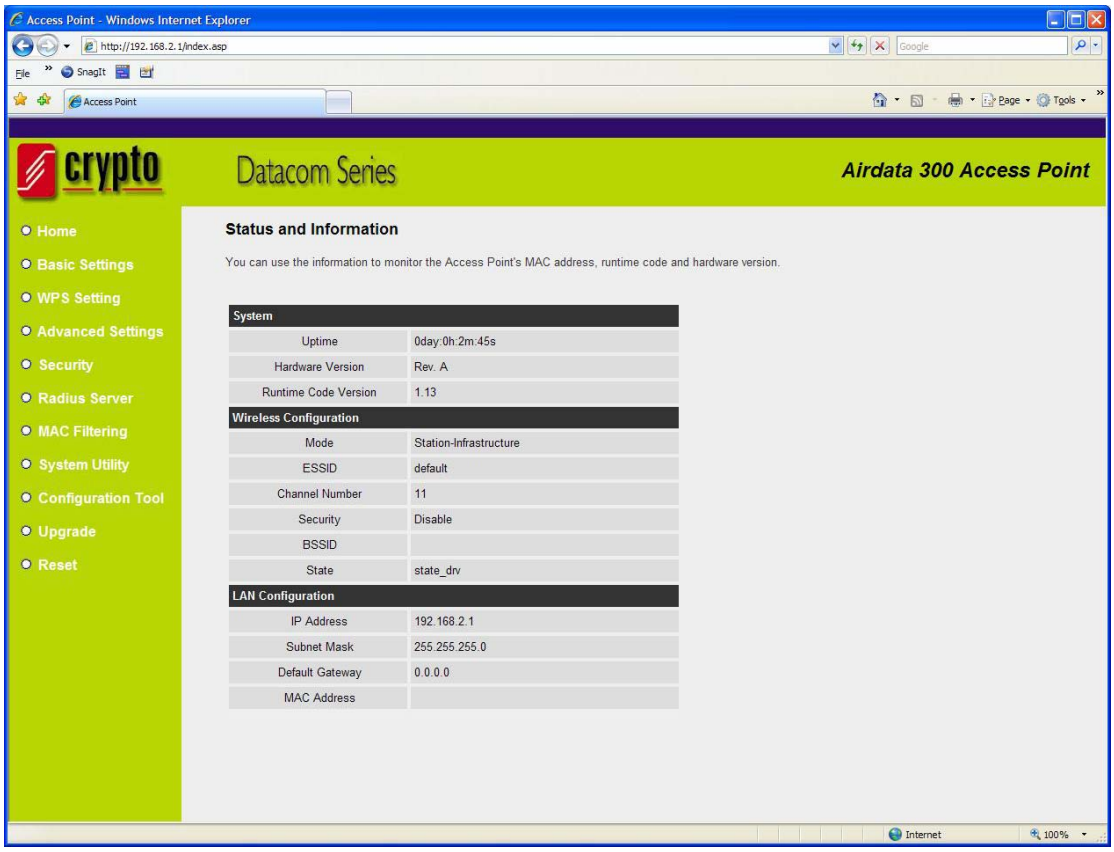


NOTE: If you can't see the web management interface, and you're being prompted to input user name and password again, it means you didn't input username and password correctly. Please retype user name and password again.

2.3 View System Status and Information

After you have successfully connected to the access point by web browser, the first thing you see is the 'Status and Information' page. All system and network related information of this access point will be displayed here. The information is very helpful when you want to know the detailed information of your access point, and when you try to fix the communication problem between this access point and other wired / wireless computer / devices.

You can click 'Home' on the left, and the system status and information will be displayed, as shown below:



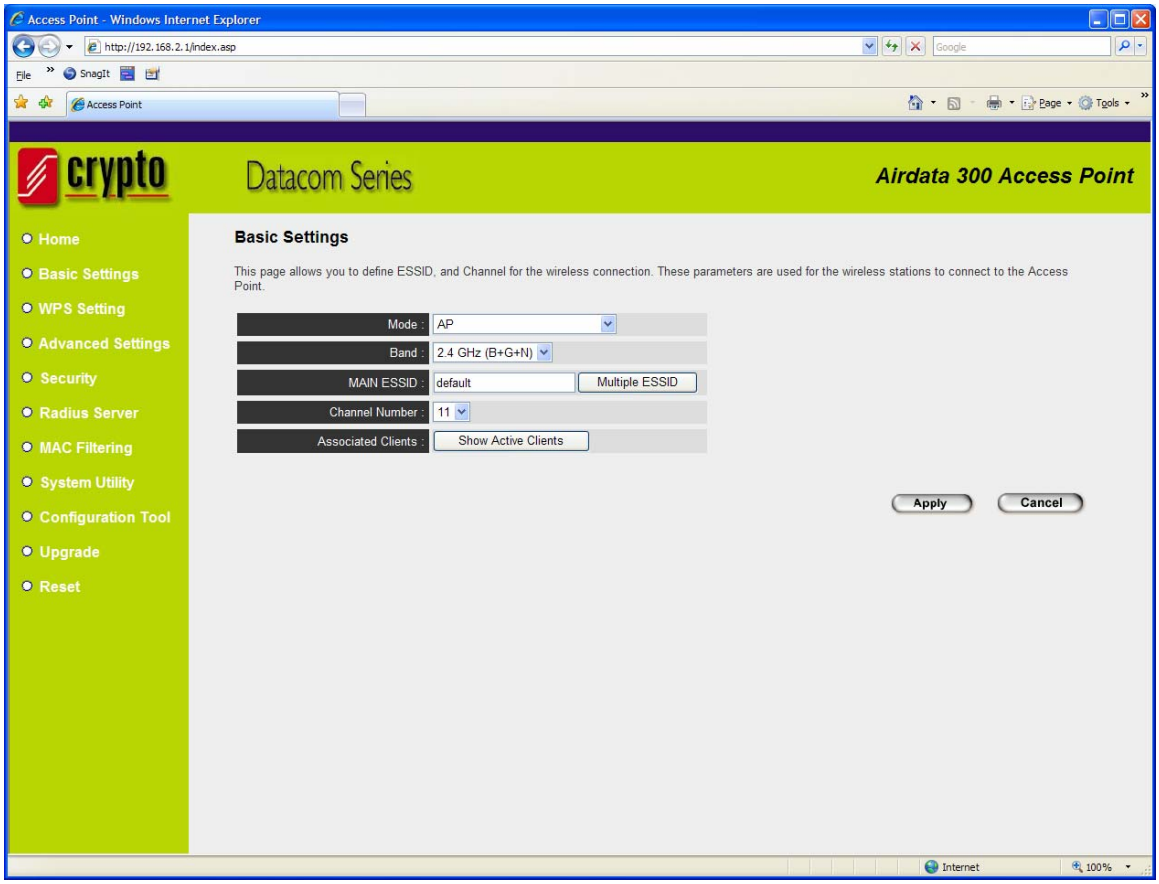
Here are descriptions of every item:

Up time	Displays the total passed time since the wireless access point is powered.
Hardware Version	Displays hardware version. This information is helpful when you need online help from the dealer of purchase.
Runtime Code Version	Displays current firmware version. If you want to perform firmware upgrade, this number will help you to determine if you need such upgrade.
Mode	Displays current wireless operating mode (see next Section)
ESSID	Displays current ESSID (the name used to identify this wireless access point)
Channel Number	Displays current wireless channel number
Security	Displays current wireless security setting
BSSID	Displays current BSSID (a set of unique identification name of this access point, it can not be modified by user)
Associated Clients	Displays the number of connected wireless client
IP Address	Displays the IP address of this wireless access point
Subnet Mask	Displays the net mask of IP address

Default Gateway	Displays the IP address of default gateway
MAC address	Displays the MAC address of LAN interface

2.4 Select an Operating Mode for Wireless Access Point

This access point can be operated in different modes; you can click 'Basic Setting' on the left of the web management interface to select an operating mode you want to meet for different needs:



You can click the 'Mode' dropdown menu to select the operating mode. There are 6 operating modes available:

AP	Access point mode, allows wireless clients to connect to access point and exchange data with the devices connected to the wired network.
Station-Infrastructure	Enable the Ethernet device such as TV and Game player connected to the access point to a wireless client.

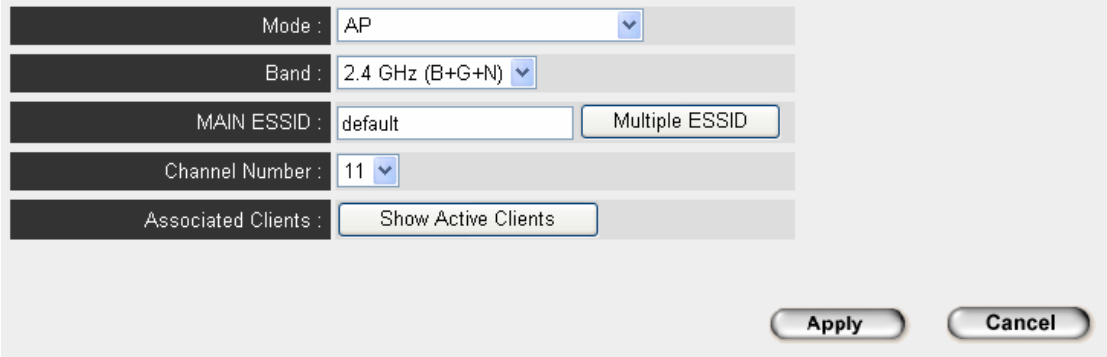
AP Bridge-Point to Point	Establish wireless connection with another wireless access point using the same mode, and link the wired network which these two wireless access points connected together. Only one access point can be connected in this mode.
AP Bridge-Point to Multi-Point	Establish wireless connection with other wireless access points using the same mode, and link the wired network which these wireless access points connected to 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 access point is not work in bridge-dedicated mode, and will be able to accept wireless clients while the access point is working as a wireless bridge.
Universal Repeater	This product can act as a wireless range extender that will help you to extend the networking wirelessly. The access point can act as Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless clients within its coverage.

Please select one wireless operating mode, for detailed descriptions of every operating mode; please refer to Section 2.4.1 to 2.4.6 listed below.

2.4.1 AP Mode

This is the most common mode. When in AP mode, this access point acts as a bridge between 802.11b/g/Draft-N wireless devices and wired Ethernet network, and exchange data between them.

When you select 'AP', the following options will be displayed:

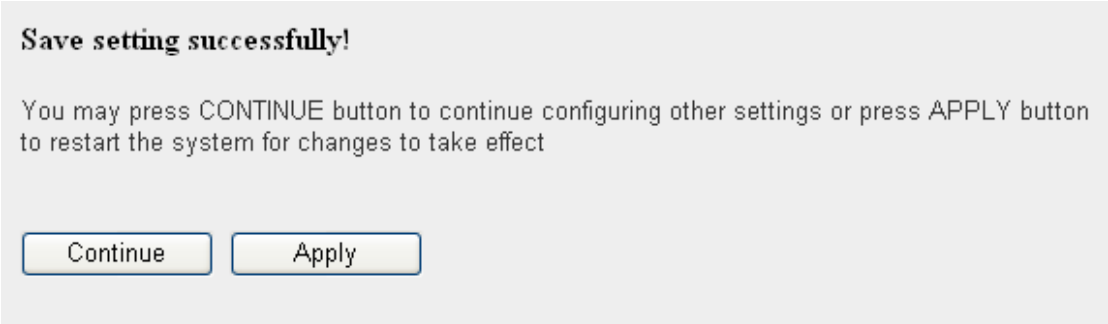


Here are descriptions of every setup item:

Band	Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. If you want to allow 802.11b, 802.11g, and 802.11 Draft-N 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 ESSID IS CASE SENSITIVE.**

Multiple ESSID	The access point supports multiple SSID function; up to four SSIDs can be set. If you want to configure additional SSIDs, please click this button. For detailed descriptions of the function, please refer to Section 2.4.1.1.
Channel Number	Please select a channel number you wish to use. If you know a certain channel number is being used by other wireless access points nearby, please refrain from using the same channel number
Associated Clients	Click 'Show Active Clients' button and a new popup window will appear which contains the information about all wireless clients connected to this access point. You can click 'Refresh' button in popup window to keep information up-to-date.

After you finish with setting, please click 'Apply', and the following message will be displayed:

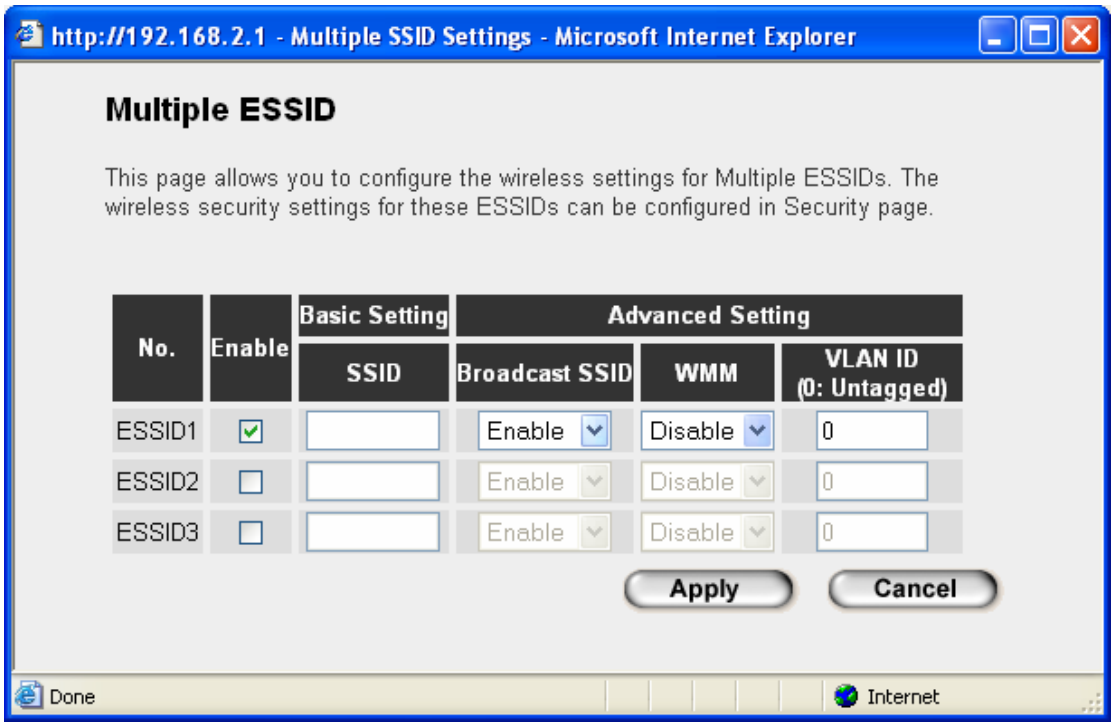


When you see this message, the settings you made are successfully saved. You can click the 'Continue' button to go back to the previous page and continue on other setting items, or click the 'Apply' button to restart the wireless access point. The changes will take effect after 30 seconds.

2.4.1.1 Multiple ESSID

This access point supports four SSIDs. Except from the main SSID (It can be configured in the Basic Setting page), you can configure another three of SSIDs here. With different SSIDs, you can separate the wireless networks with different SSID name, wireless security, WMM, and VLAN settings.

NOTE: If you want to configure the wireless security for different SSID, please go to '2.7 Wireless Security' for more information.



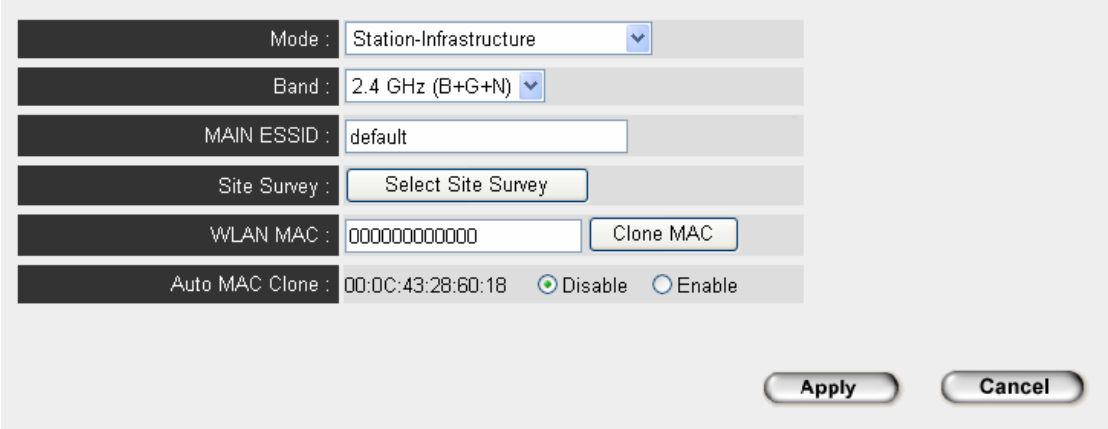
Here are descriptions of every setup item:

No.	Except Main SSID, you can configure additional three ESSID here.
Enable	Select the box to enable the different additional ESSID.
SSID	Please input the SSID name (the name used to identify this wireless access point) here. You can input up to 32 alphanumerical characters. **PLEASE NOTE THAT ESSID IS CASE SENSITIVE.**

Broadcast SSID	Decide if the wireless access point will broadcast its own ESSID or not. You can hide the ESSID of your wireless access point (set the option to 'Disable'), so only people those who know the ESSID of your wireless access point can get connected.
WMM	WMM (Wi-Fi Multimedia) technology, can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When you enable WMM function, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.
VLAN ID (0:Untagged)	If your network uses VLANs, you can assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. The VLAN ID range is from 1 to 4094. The VLAN ID is 0 by default.

2.4.2 Station-Infrastructure

In this mode, you can connect the access point to Ethernet device such us TV and Game player to enable the Ethernet device be a wireless station and join to a wireless network through an access point or AP router.

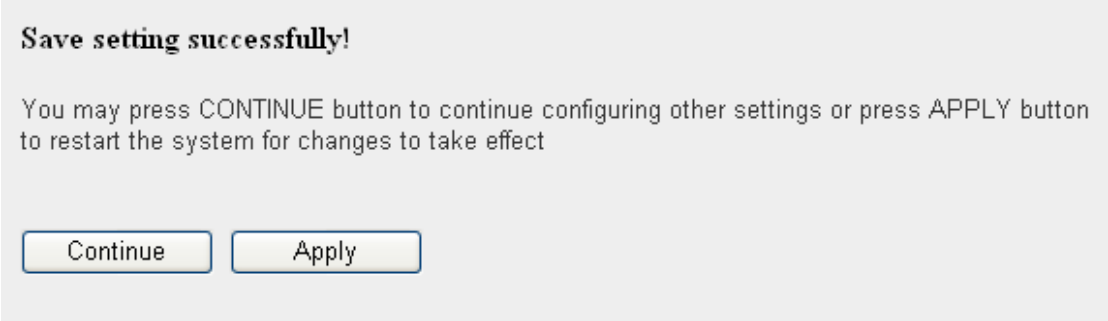


Here are descriptions of every setup item:

Band	Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. If you want to allow 802.11b, 802.11g, and 802.11 Draft-N 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 ESSID IS CASE SENSITIVE.**
Site Survey	When you use this access point as a wireless station for Ethernet network device to have wireless capability, you have to associate it with a working access point. Click the 'Select Site Survey' button, then a "Wireless Site Survey Table" will pop up. It will list all available access points near by. You can select one access point in the table and it will join wireless LAN through this access point. Please go to Section 2.4.2.1 for more information about the 'Wireless Site Survey Table'.
WLAN MAC	For some applications, you may need to designate a specific MAC address for the access point. Please enter the MAC address here. If you are connecting the access point to a computer, you can simply press 'Clone Mac address' button to fill the MAC address field with the MAC address of your computer.

Auto MAC Clone	If this function is enabled, the access point will automatically clone the MAC address of the wireless clients which is the first one to associate to the access point while the access point is powered on.

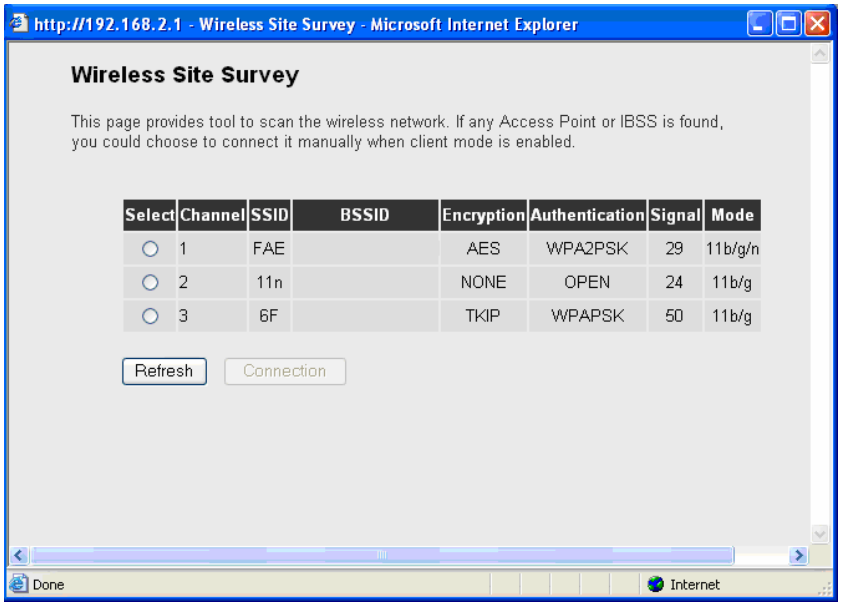
After you finish with the settings, please click ‘Apply’, and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click the ‘Continue’ button to go back to the previous page and continue on other setting items, or click the ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.4.2.1 Wireless Site Survey

The table will list the access points nearby as the access point is set to Station mode; you can select one of the access points to associate.



Here are descriptions of every setup item:

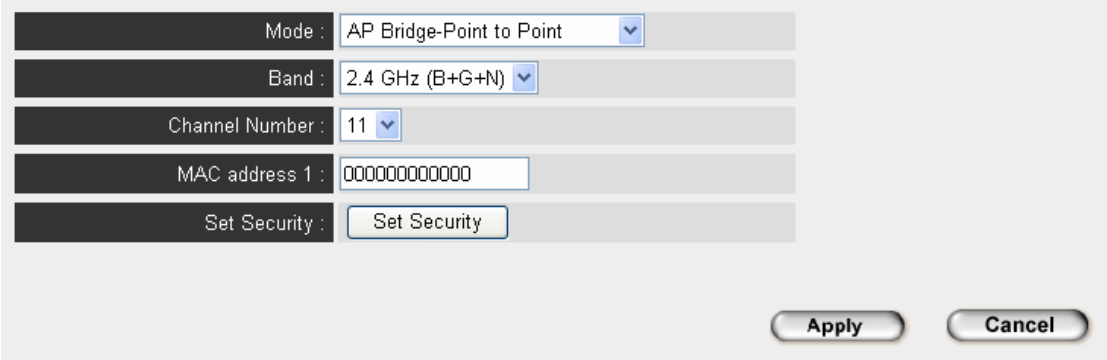
Select	Click the radio button to select the access point.
Channel	Display to channel number of the access point.
SSID	Display the SSID name of the access point.
BSSID	Display the BSSID (MAC Address) of the access point.
Encryption	Display the encryption setting of the access points. If you have selected the access point with security setting, you have to go to '2.7 Wireless Security' to set the same security with the access point you want to associate.
Authentication	Display the authentication type of the access point.
Signal	The signal strength of each access point will be displayed here. The signal strength is stronger, the connection quality is better.
Mode	Display the wireless modes including 11b, 11b/g or 11b/g/n or 11n only of the access points.
Refresh	Click this button to refresh the table.
Connection	Select an access point and click this button to choose the network. The SSID name of the access point you have selected will be displayed in the Main SSID in the Basic Setting page.

2.4.3 AP Bridge-Point to Point Mode

In this mode, this wireless access point will connect to another wireless access point which uses the same mode, and all wired Ethernet clients of both wireless access points will be connected together. You can use this mode to connect a network to another network which is physically isolated.

Please note that when you set your access point to this mode, it will not accept regular wireless clients anymore.

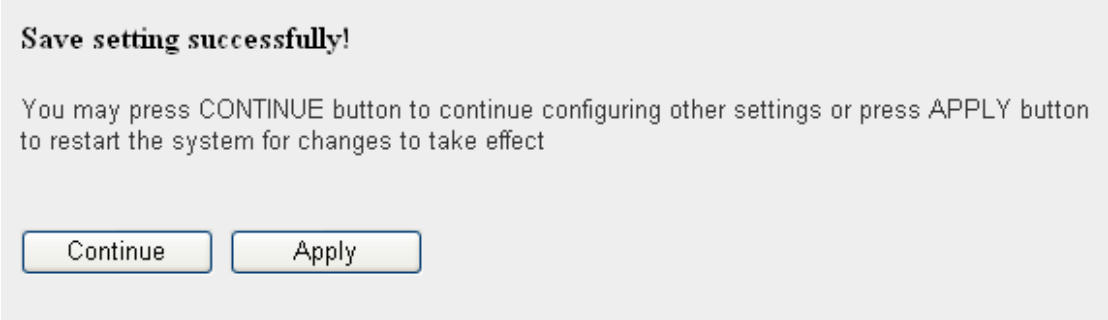
When you select 'AP Bridge-Point to Point', the following options will be displayed:



Here are descriptions of every setup item:

Band	Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. If you want to allow 802.11b, 802.11g, and 802.11 Draft-N clients to connect to this access point, select 2.4GHz (B+G+N).
Channel Number	Please select a channel number you wish to use. The channel number must be same with another wireless access point you wish to connect
MAC address 1	Please input the MAC address of the wireless access point you wish to connect
Set Security	Click this button to select an encryption mode for this wireless link; a new popup window will appear. Please refer to Section 2.7 for detailed descriptions.

After you finish with setting, please click 'Apply', and the following message will be displayed:



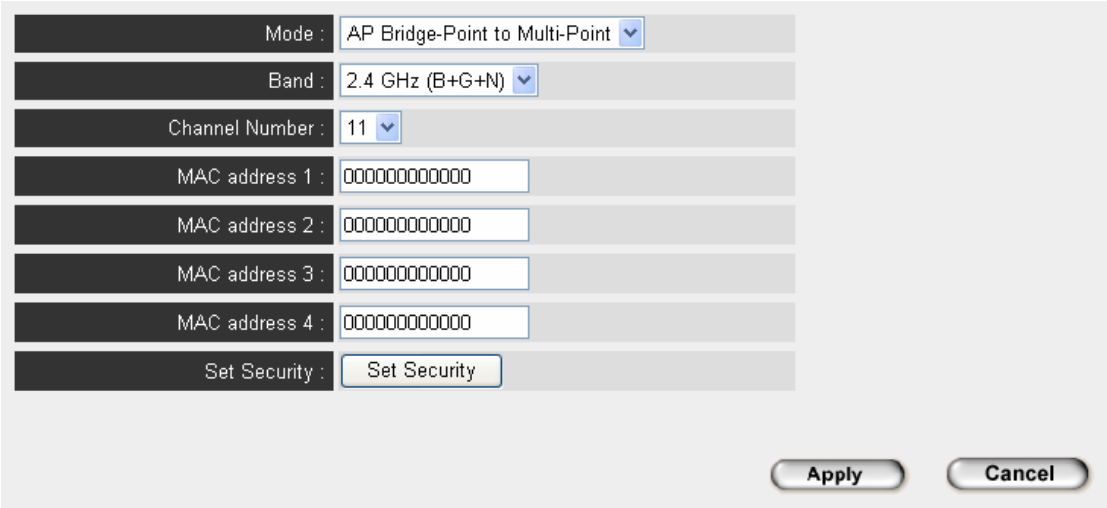
When you see this message, the settings you made are successfully saved, you can click the ‘Continue’ button to go back to the previous page and continue on other setting items, or click the ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.4.4 AP Bridge-Point to Multi-Point Mode

In this mode, this wireless access point will connect to up to four wireless access points that use the same mode, and all wired Ethernet clients of every wireless access points will be connected together. You can use this mode to connect a network to other networks which is physically isolated.

Please note that when you set your access point to this mode, it will not accept regular wireless clients anymore.

When you select 'AP Bridge-Point to Multi-Point', the following options will be displayed:

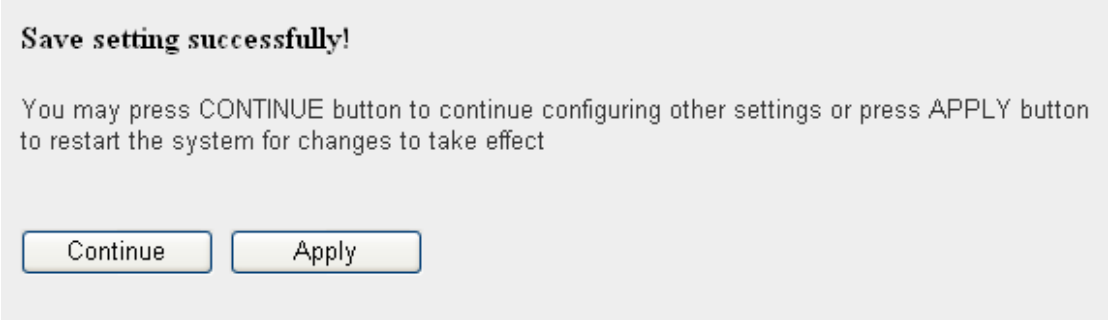


Here are descriptions of every setup item:

Band	Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point.

	If you want to allow 802.11b, 802.11g, and 802.11 Draft-N clients to connect to this access point, select 2.4GHz (B+G+N).
Channel Number	Please select a channel number you wish to use. The channel number must be same with another wireless access point you wish to connect
MAC address 1-4	Please input the MAC address of the wireless access point you wish to connect
Set Security	Click this button to select an encryption mode for this wireless link, a new popup window will appear. Please refer to Section 2-7 for detailed descriptions.

After you finish with setting, please click 'Apply', and the following message will be displayed:



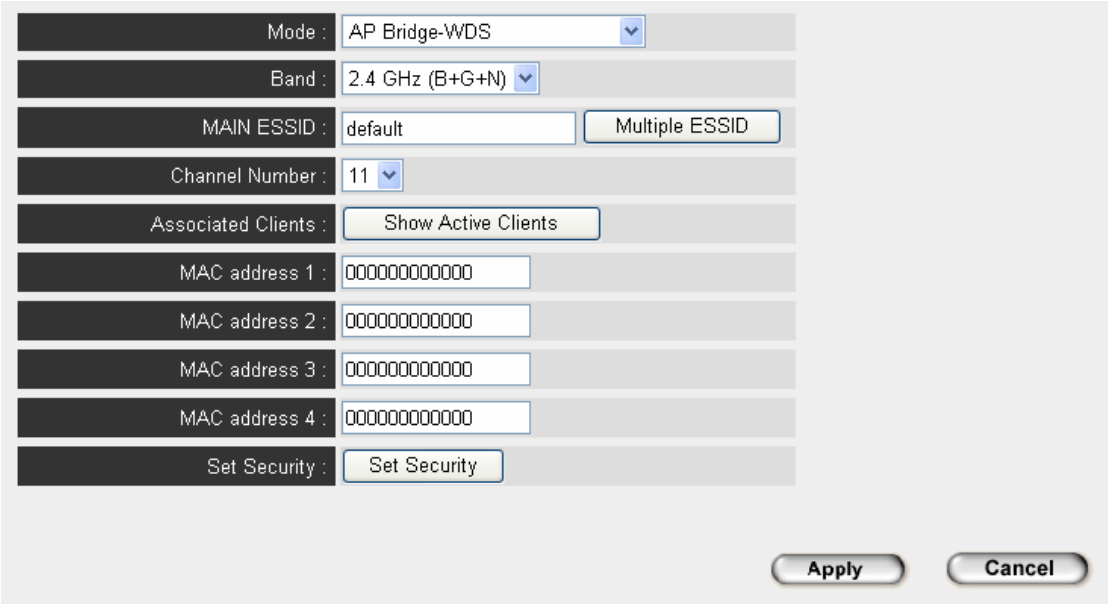
When you see this message, the settings you made are successfully saved. You can click the 'Continue' button to go back to the previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.4.5 AP Bridge-WDS Mode

In this mode, this wireless access point will connect to up to four wireless access points which uses the same mode, and all wired Ethernet clients of every wireless access points will be connected together. You can use this mode to connect a network to other networks which is physically isolated.

When you use this mode, this access point is still able to accept wireless clients.

When you select 'AP Bridge-WDS', the following options will be displayed:

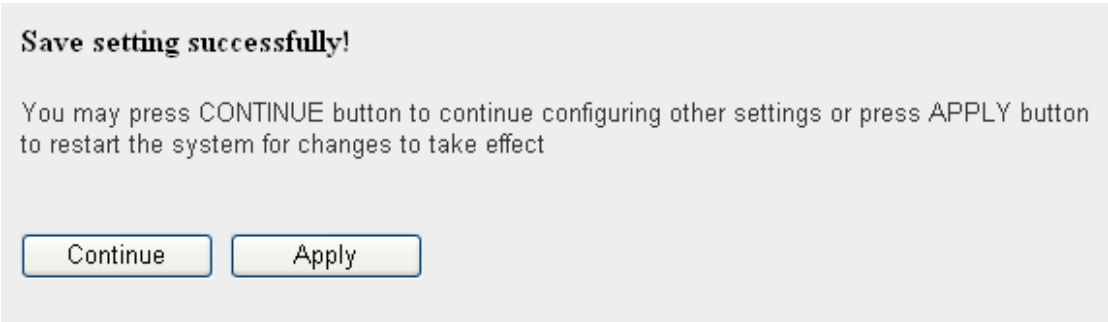


Here are descriptions of every setup item:

Band	Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point.

	If you want to allow 802.11b, 802.11g, and 802.11 Draft-N 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 ESSID IS CASE SENSITIVE.**
Multiple ESSID	The access point supports multiple SSID function; up to four SSIDs can be set. If you want to configure additional SSIDs, please click this button. For detailed descriptions of the function, please refer to Section 2-4-1-1.
Channel Number	Please select a channel number you wish to use. The channel number must be same with another wireless access point you wish to connect
Associated Clients	Click 'Show Active Clients' button and a new popup window will appear which contains the information about all wireless clients connected to this access point. You can click 'Refresh' button in popup window to keep information up-to-date.
MAC address 1-4	Please input the MAC address of the wireless access point you wish to connect
Set Security	Click this button to select an encryption mode for this wireless link; a new popup window will appear. Please refer to Section 2.7 for detailed descriptions.

After you finish with the settings, please click 'Apply', and the following message will be displayed:



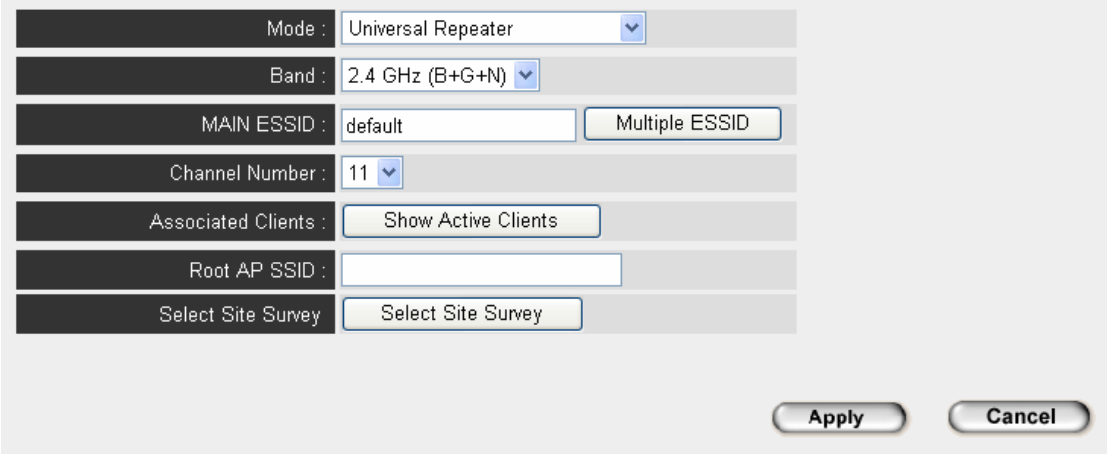
When you see this message, the settings you made are successfully saved. You can click the 'Continue' button to go back to the previous page and continue on other

setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.4.6 Universal Repeater

In this mode, the access point can act as a wireless repeater; it can be Station and AP at the same time. It can use Station function to connect to a Root AP and use AP function to service all wireless stations within its coverage.

NOTE: For Repeater Mode, this access point will demodulate the received signal, checking if this signal is noise for the operating network then have the signal modulated and amplified again. The output power of this mode is the same as that of WDS and normal AP mode.

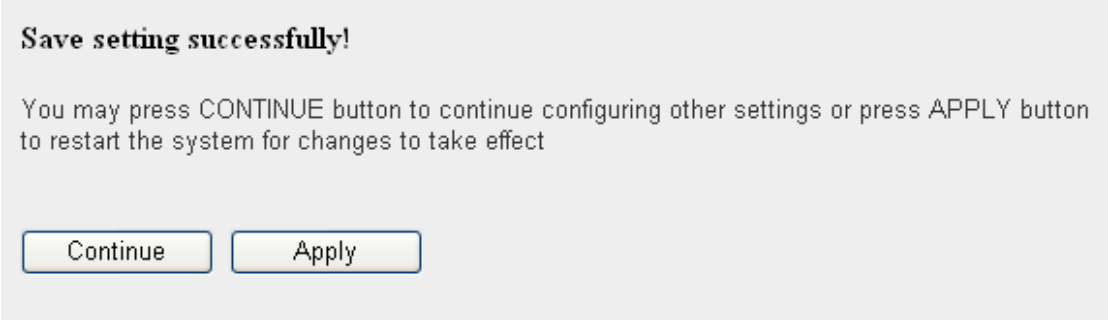


Here are descriptions of every setup item:

Band	Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band. If you select 2.4GHz (B), 2.4GHz (N), or 2.4GHz (G), only wireless clients using the wireless band you select (802.11b, 802.11 Draft-N, or 802.11g) will be able to connect to this access point. If you select 2.4GHz (B+G), then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. If you want to allow 802.11b, 802.11g, and 802.11 Draft-N

	clients to connect to this access point, 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 ESSID IS CASE SENSITIVE.**
Multiple ESSID	The access point supports multiple SSID function; up to four SSIDs can be set. If you want to configure additional SSIDs, please click this button. For detailed descriptions of the function, please refer to Section 2-4-1-1.
Channel Number	Please select a channel number you wish to use. The channel number must be same with another wireless access point you wish to connect
Associated Clients	Click 'Show Active Clients' button and a new popup window will appear which contains the information about all wireless clients connected to this access point. You can click 'Refresh' button in popup window to keep information up-to-date
Root AP SSID	In 'Universal Repeater' mode, this device can act as a station to connect to a Root AP. You should assign the SSID of the Root AP here or click 'Select Site Survey' button to choose a Root AP.
Select Site Survey	Click 'Select Site Survey' button, then a "Wireless Site Survey Table" will pop up. It will list all available access points near by. You can select one access point in the table and the access point will join wireless LAN through this access point. Please go to Section 2.4.2.1 for more information about the 'Wireless Site Survey Table'.

After you finish with the setting, please click 'Apply', and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click ‘Continue’ button to go back to the previous page and continue on other setting items, or click the ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

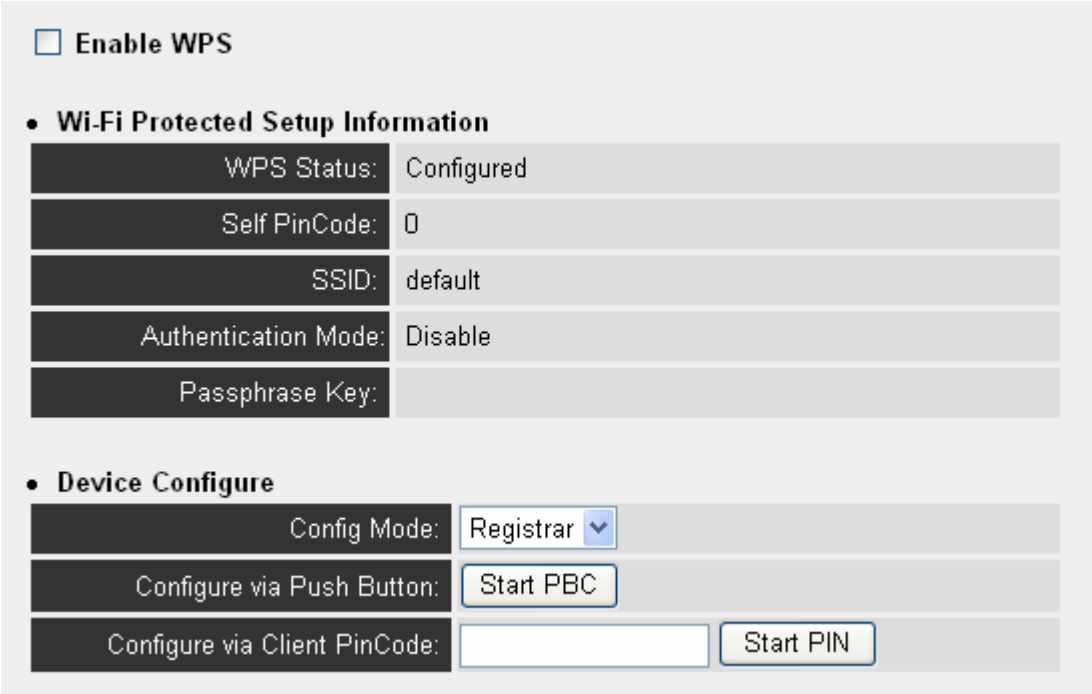
2.5 WPS Setting

Wi-Fi Protected Setup (WPS) is the simplest way to build a connection between wireless network clients and this access point. You don’t have to select encryption mode and input a long encryption passphrase every time when you need to setup a wireless client, you only have to press a button on wireless client and this access point, and the WPS will do the setup for you.

This access point supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to switch this access point to WPS mode and push a specific button on the wireless client to start WPS mode. You can push Reset/WPS button of this access point, or click ‘Start PBC’ button in the web configuration interface to do this; if you want to use PIN code, you have to provide the PIN code of the wireless client you wish to connect to this access point and then switch the wireless client to WPS mode. The detailed instructions are listed follow:

Note: WPS function of this access point will not work for those wireless clients do not support WPS.

To use WPS function to set encrypted connection between this access point and WPS-enabled wireless client by WPS, click ‘WPS Setting’ on the left of web management menu, and the following information will be displayed:



Here are descriptions of every setup item:

Enable WPS	Check this box to enable or disable WPS function
Wi-Fi Protected Setup Information	All information related to WPS will be displayed here, they're helpful when you're setting up connections by WPS. WPS Status: Displays WPS status. If data encryption settings of this access point has never been set, 'unConfigured' message will be displayed here. (see Section 2.7 for detailed information); if data encryption settings has been set before, 'Configured' message will be displayed here. Self PinCode: This is the WPS PIN code of this access point. This code is useful when you need to build 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 displayed here. If you don't enable security function of the access point before WPS is activated, the access point will automatically set the security to WPA (AES) and generate a set of passphrase key

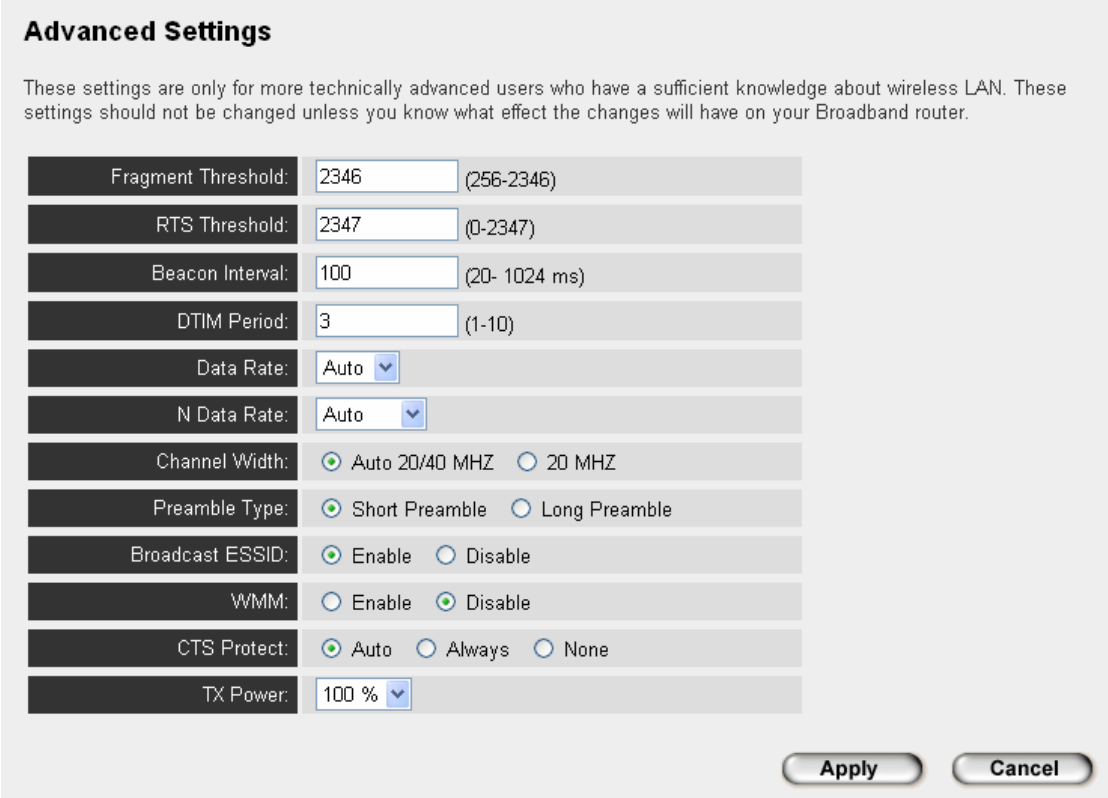
	for WPS connection. Passphrase Key: Displays the WPA passphrase here, all characters will be replaced by asterisk for security reason. If encryption is not set on this access point, nothing will be displayed here.
Config Mode	There are ‘Registrar’ and ‘Enrollee’ modes for the WPS connection. When ‘Registrar’ is enabled, the wireless clients will follow the access point’s wireless settings for WPS connection. When ‘Enrolle’ mode is enabled, the access point will follow the wireless settings of wireless client for WPS connection.
Start PBC	Click ‘Start PBC’ to start Push-Button style WPS setup procedure. This access point will wait for WPS requests from wireless clients for 2 minutes. The ‘WLAN’ LED on the access point will be steady on for 2 minutes when this access point is waiting for incoming WPS request.
Start PIN	Please input the PIN code of the wireless client you via client wish to connect, and click ‘Start PIN’ button. The ‘WLAN’ LED on the access point will be steady on when this access point is waiting for incoming WPS request.

NOTE: When you’re using PBC type WPS setup, you must press ‘PBC’ button (hardware or software) of wireless client within 120 seconds; if you didn’t press PBC button of wireless client within this time period, please press ‘PBC’ button (hardware or software) of this access point again.

2.6 Advanced Wireless Settings

This wireless access point has many advanced wireless features. Please note that all settings listed here are for experienced users only, if you're not sure about the meaning and function of these settings, please don't modify them, or the wireless performance will be reduced.

You can click 'Advanced Setting' on the left to enter advanced settings menu, and the following message will be displayed:



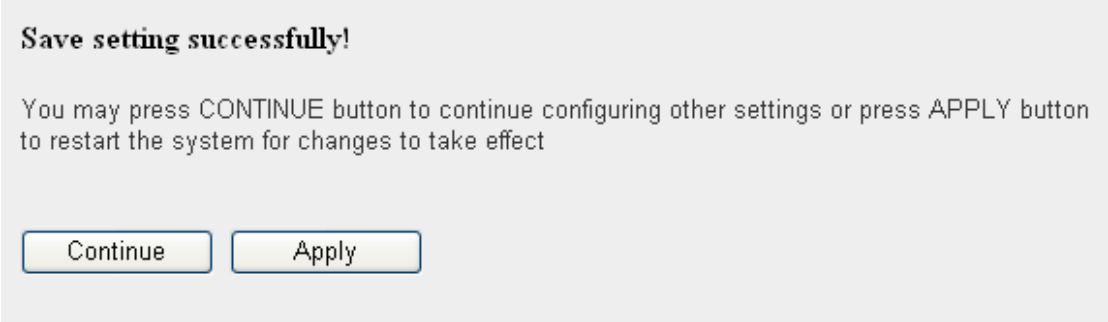
Here are descriptions of every setup item:

Fragment Threshold	Set the Fragment threshold of wireless radio. **Do not modify default value if you don't know what it is, default value is 2346**
RTS Threshold	Set the RTS threshold of wireless radio. **Do not modify default value if you don't know what it is, default value is 2347**
Beacon Interval	Set the beacon interval of wireless radio. **Do not modify default value if you don't know what it is, default value is 100**

DTIM Period	Set the DTIM period of wireless radio. **Do not modify default value if you don't know what it is, default value is 3**
Data Rate	Set the wireless data transfer rate to a certain value. Since most of 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 802.11 Draft-N clients, available options are MCS 0 to MCS 15, 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 taken by wireless signals of this access point). It's suggested to select 'Auto 20/40MHz'. Do not change to '20 MHz' unless you know what it is.
Preamble Type	Set the type of preamble of wireless radio, **Do not modify default value if you don't know what it is, default setting is 'Short Preamble'.**
Broadcast ESSID	Decide if the wireless access point will broadcast its own ESSID or not. You can hide the ESSID of your wireless access point (set the option to 'Disable'), so only people those who know the ESSID of your wireless access point can get connected.
WMM	WMM (Wi-Fi Multimedia) technology, can improve the performance of certain network applications, like audio/video streaming, network telephony (VoIP), and others. When you enable WMM function, the access point will define the priority of different kinds of data, to give higher priority to applications which require instant responding. Therefore you can improve the performance of such network applications.
CTS Protect	Enabling this setting will reduce the chance of radio signal collisions between 802.11b and 802.11g wireless access points. It's recommended to set this option to 'Auto'.
TX Power	You can set the output power of wireless radio. Unless you're using this wireless access point in a really big space, you may not have to set output power to 100%. **This will**

	enhance security (malicious / unknown users in distance will not be able to reach your wireless access point).

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



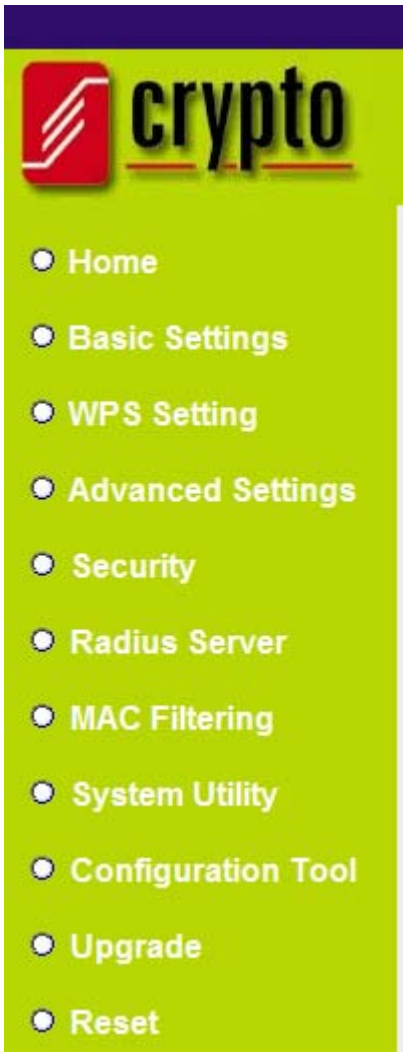
When you see this message, the settings you made are successfully saved. You can click ‘Continue’ button to go back to the previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.7 Wireless Security

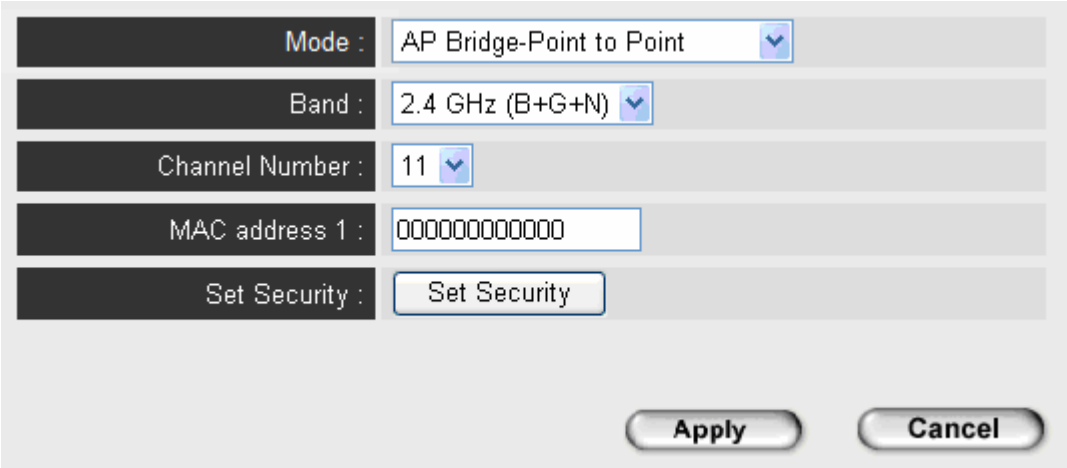
This wireless access point provides many types of wireless security (wireless data encryption). When you use data encryption, data transferred by radio signals in the air will become unreadable for those people who don’t know correct encryption key (encryption password).

There are two ways to set wireless security:

1. Click ‘Security’ on the left of web management interface.



2. Click ‘Set Security’ button when the wireless operating mode you selected is ‘AP Bridge-Point to Point’, ‘AP Bridge-Point to Multi-Point’, or ‘AP Bridge-WDS’.



There are four types of security level you can select: Disable (no security - data

encryption disabled), WEP, WPA Pre-shared Key, and WPA Radius. Please refer to the following sections for detailed instructions.

NOTE: If you have enabled Multiple SSID function, please select the SSID network you wish to configure in advance.

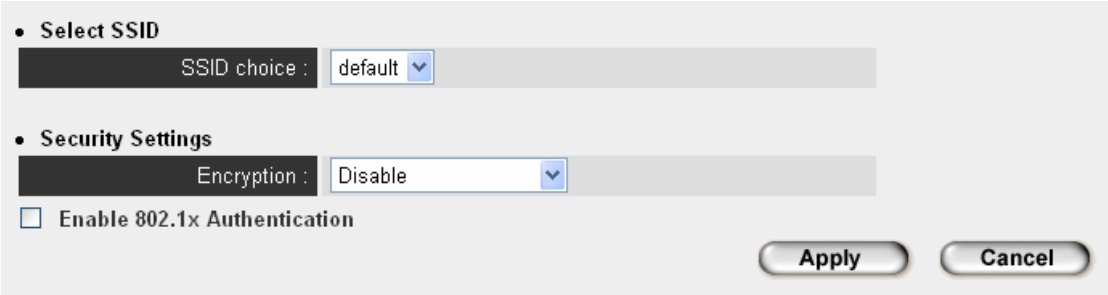
Please remember it's very important to set wireless security settings properly! Without a proper setting, hackers and intruders may gain access to your local network and perform malicious actions to your computers and servers, which could cause serious problems.

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

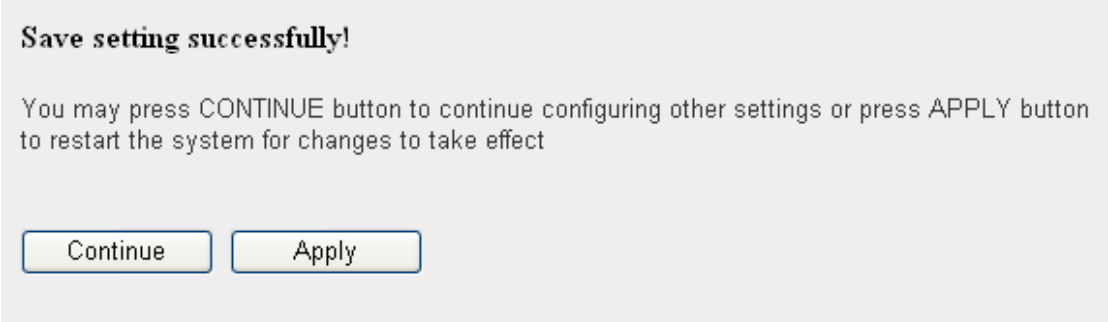
1. Always enable data encryption. Only disable it when you want to open your wireless access point to the public.
2. Never use simple words as encryption password. Using a random combination of symbols, numbers, and alphabets will greatly improve security.
3. Use WPA when possible - it's much safer than WEP.
4. Change encryption password when you've used it for too long time.

2.7.1 Disable Security

Select the SSID you wish to configure. When you select 'Disable', wireless encryption for the network is disabled.



After you finish with setting, please click 'Apply', and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can

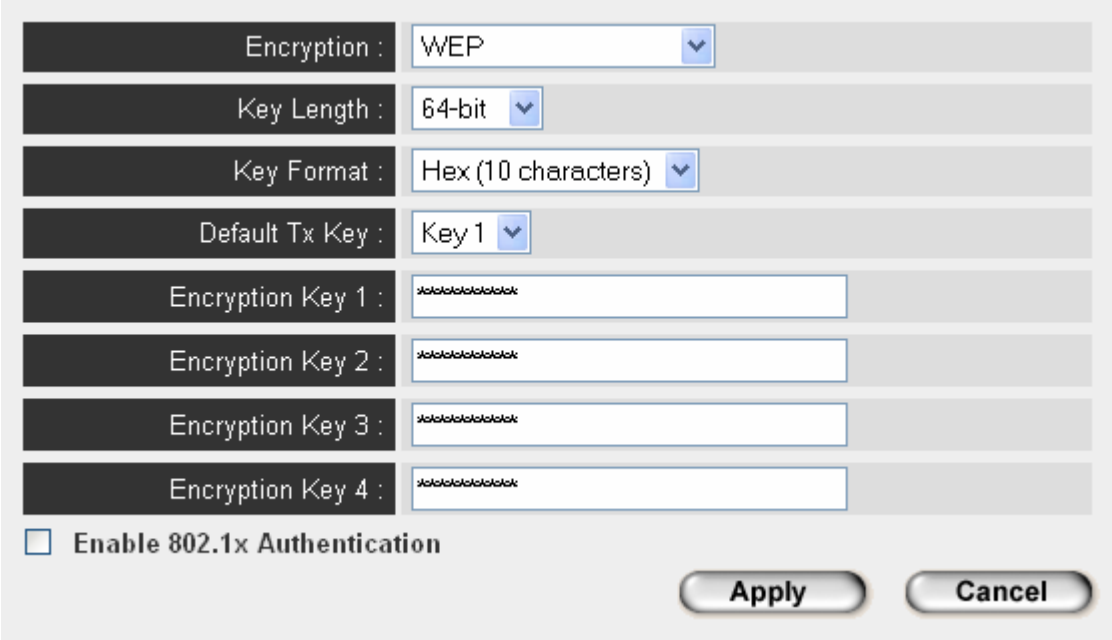
click ‘Continue’ button to go back to the previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.7.2 WEP

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

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

When you select ‘WEP’ as encryption type, the following messages will be displayed:

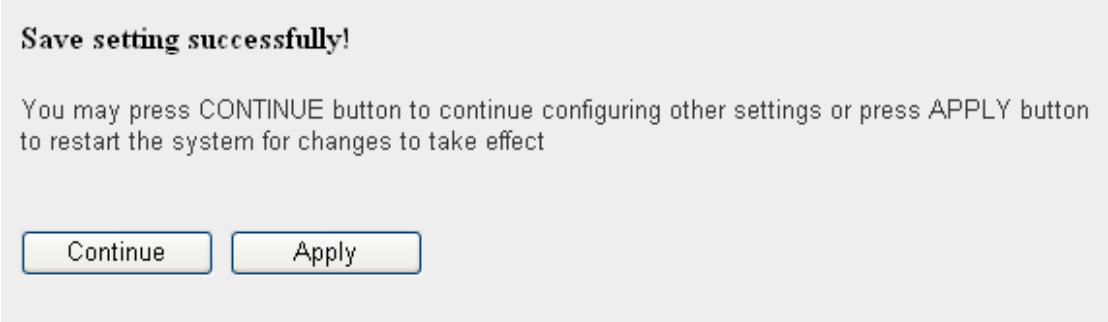


Here are descriptions of every setup item:

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 key will be displayed. For example, if you select ’64-bit’ as key length, and ‘Hex’ as key format, you’ll see the message at the right of ‘Key Format’ is ‘Hex (10 characters), which means the length of WEP key is 10 characters.

Default Tx Key	You can set up to four sets of WEP key, and you can decide which key is being used by default here. **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 at 'Key Format' field. You can use any alphanumerical characters (0-9, a-z, and A-Z) if you select 'ASCII' key format, and if you select 'Hex' as key format, you can use 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 with each other.
Enable 802.1x Authentication	Check this box to enable 802.1x user authentication. Please refer to Section 2.7.5 for detailed instructions.

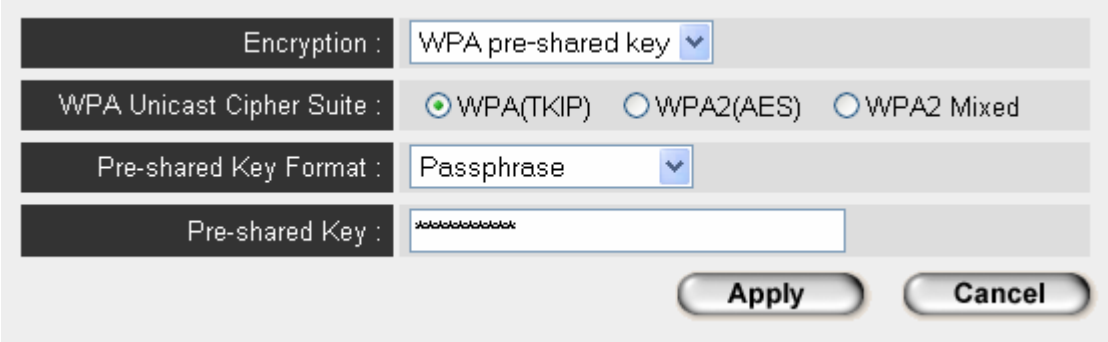
After you finish with setting, please click 'Apply', and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click 'Continue' button to go back to the previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.7.3 WPA Pre-shared Key

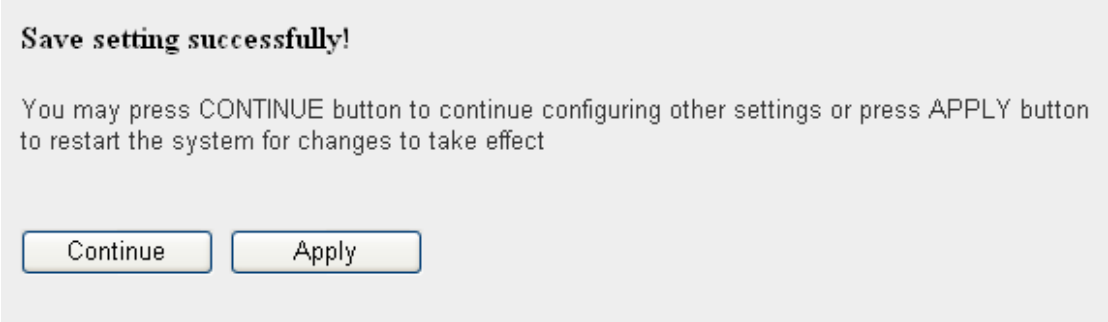
WPA Pre-shared key is the safest encryption method currently, and it's recommended to use this encryption method to ensure the safety of your data.
When you select 'WPA pre-shared key' as encryption type, the following messages will be displayed:



Here are descriptions of every setup item:

WPA Unicast Cipher Suite	Available options are: WPA (TKIP), WPA2 (AES), and WPA2 Mixed. You can select one of them, but you have to make sure your wireless client support the cipher you selected.
Pre-shared Key Format	Please select the format of pre-shared key here, available options are 'Passphrase' (8 to 63 alphanumerical characters) and 'Hex (64 hexadecimal characters – 0 to 9 and a to f).
Pre-shared Key	Please input pre-shared key according to the key format you selected here. For security reason, don't use simple words).

After you finish with setting, please click 'Apply', and the following message will be displayed:

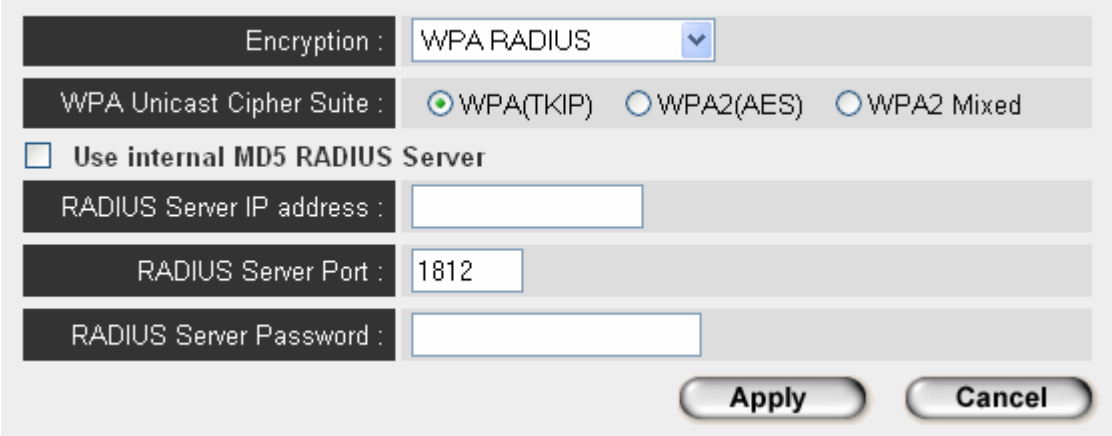


When you see this message, the settings you made is successfully save. You can click 'Continue' button to back to previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.7.4 WPA RADIUS

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

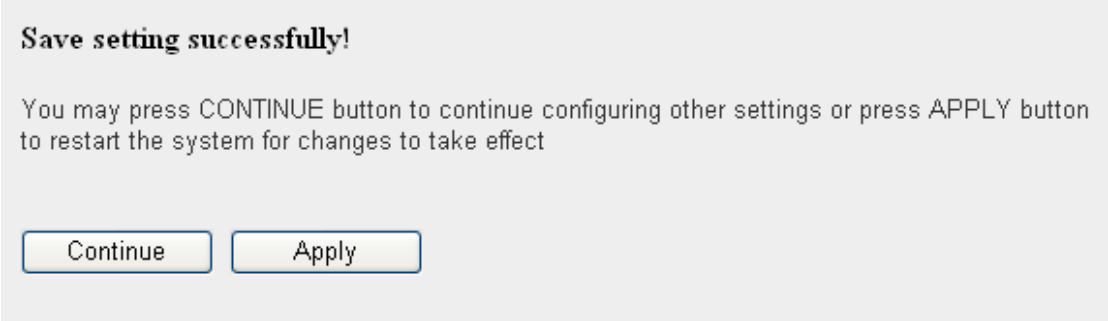
When you select 'WPA RADIUS' as encryption type, the following messages will be displayed:



Here are descriptions of every setup item:

WPA Unicast Cipher Suite	You can select WPA encryption type here. AES is safer than TKIP, but not every wireless client supports it. Please refer to the specification of your wireless client to decide which encryption type you should use.
Use internal MD5 RADIUS Server	Uses built-in RADIUS Server (refer to Section 2-8) instead of external RADIUS server. If you check this box, the value in following three fields will be ignored.
RADIUS Server IP address	Please input the IP address of RADIUS authentication server here.
RADIUS Server Port	Please input the port number of RADIUS authentication server here. Default value is 1812.
RADIUS Server Password	Please input the password of RADIUS authentication server here.

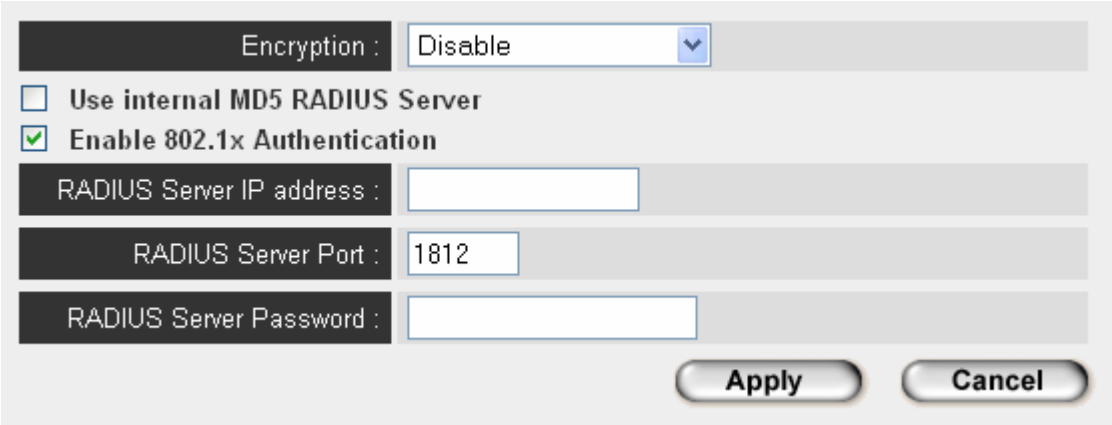
After you finish with setting, please click 'Apply', and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click the 'Continue' button to go back to the previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.7.5 802.1x Authentication

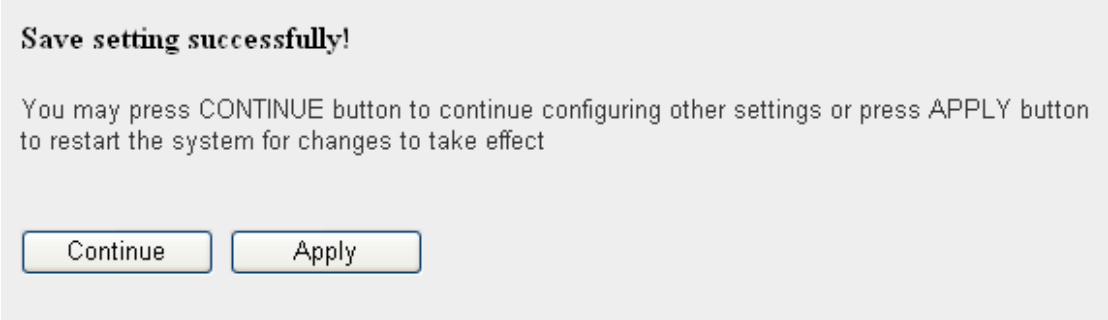
You can enable 802.1x user identification (based on RADIUS user authentication server) by checking 'Enable 802.1x Authentication' box when you select 'Disable' or 'WEP' as encryption type, and the following message will be displayed:



Here are descriptions of every setup item:

Use internal MD5 RADIUS Server	Uses built-in RADIUS Server (refer to next Section) instead of external RADIUS server. If you check this box, the value of internal RADIUS server fields will be ignored.
Enable 802.1x Authentication	Enable or disable the use of 802.1x user authentication.
RADIUS Server IP address	Please input the IP address of RADIUS authentication server here.
RADIUS Server Port	Please input the port number of RADIUS authentication server here. Default value is 1812.
RADIUS Server Password	Please input the password of RADIUS authentication server here.

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



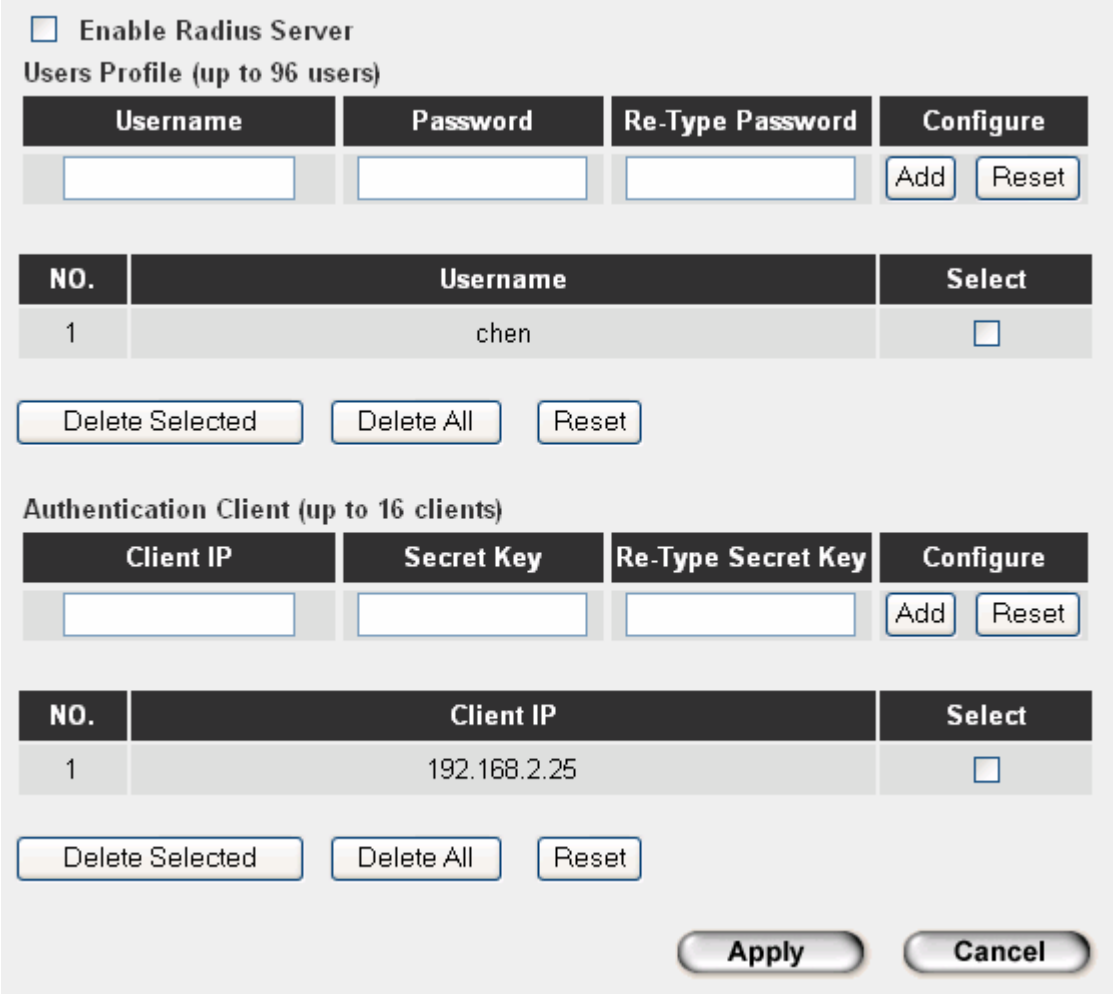
When you see this message, the settings you made are successfully saved. You can click the ‘Continue’ button to go back to the previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.8 Radius Server

Comparing to other wireless security measures, radius server provides user-based authentication. If your wireless client supports 802.1x user authentication, you can use the ‘Radius Server’ function to use the internal mini radius server to improve security and wireless user control.

The internal radius server only supports 96 users and 16 IP addresses. If the number of user and/or IP address you need is more than this, please use external radius server.

To setup internal radius server, click ‘Radius Server’ on the left of web management interface, and the following information will be displayed:

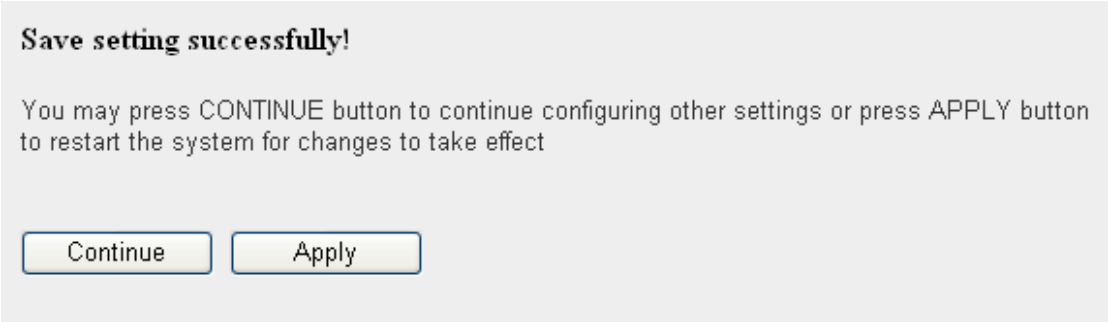


Here are descriptions of every setup item:

Enable Radius Server	Check this box to enable internal radius server function.
User Profile	You can add or delete radius user here. Please input username, password, re-type password in corresponding field, and click ‘Add’ button to add the user to radius server database. You can click ‘Reset’ to clear the text you typed in above three fields. All current radius users will be listed here. If you want to delete one or more users, check ‘Select’ box of that user, and click ‘Delete Selected’ button; you can click ‘Delete All’ button to delete all users in radius server database. You can also click ‘Reset’ button to uncheck all ‘Select’ boxes.
Authentication Client	You can add allowed radius client IP address here. Please input client IP, secret key, re-type secret key in corresponding field, and click ‘Add’ button to add the IP

	address to radius server database. You can click ‘Reset’ to clear the text you typed in above three fields. All current IP addresses will be listed here. If you want to delete one or more addresses, check ‘Select’ box of that address, and click ‘Delete Selected’ button; you can click ‘Delete All’ button to delete all addresses in radius server database. You can also click ‘Reset’ button to uncheck all ‘Select’ boxes.

After you finish with setting, please click ‘Apply’, and the following message will be displayed:

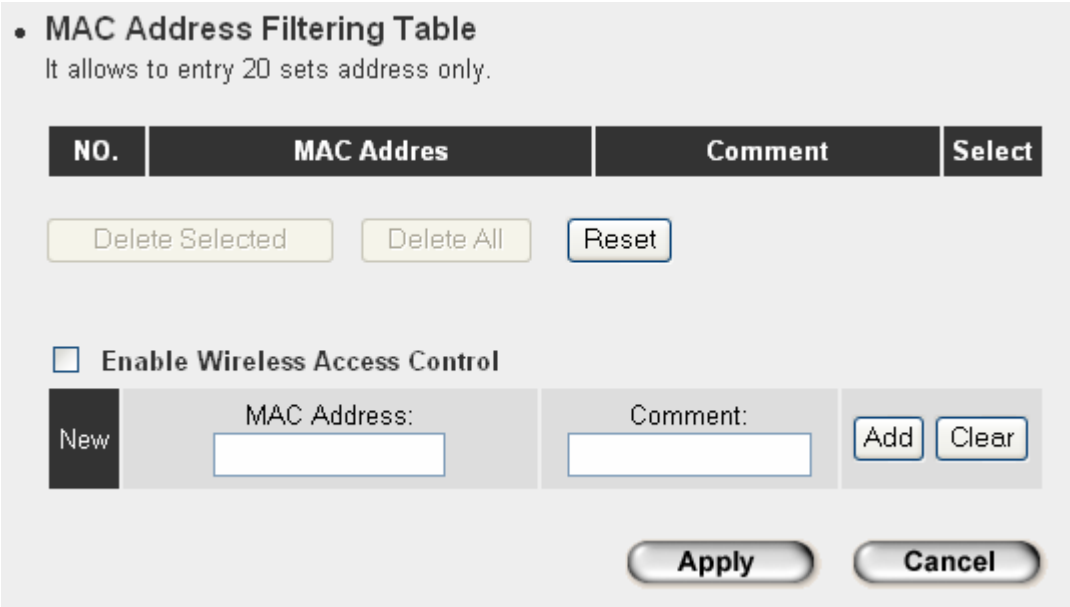


When you see this message, the settings you made are successfully saved. You can click the ‘Continue’ button to go back to the previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.9 MAC Filtering

Another security measure you can use to keep hackers and intruders away is ‘MAC filtering’. You can pre-define a so-called ‘white-list’, which contains MAC addresses of the wireless clients you trust. All other wireless client with the MAC address which is not in your list will be denied by this wireless access point.

To setup MAC filtering, please click ‘MAC Filtering’ on the left of web management interface and the following messages will be displayed:

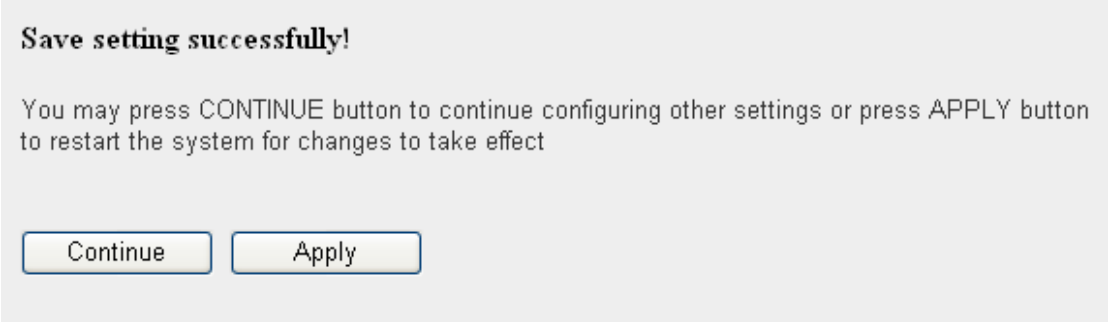


This page contains two parts of MAC filtering information. All allowed MAC addresses will be listed in upper part (1), and you can add new MAC addresses by components in lower part (2).
Here are descriptions of every setup item:

Select	Check this box to select one or more MAC address(es) to delete.
Delete Selected	Click this button to delete all selected MAC address(es).
Delete All	Delete all MAC address entries.
Reset	Uncheck all selected MAC address entries.
Enable Wireless Access Control	Check this box to enable MAC address restriction, if unchecked, no restriction will be enforced (any wireless client with proper encryption setting will be able to connect to this wireless access point).
MAC address	Input MAC address allowed using this wireless access point here. You don't have to add colon (:) or hyphen (-) by yourself, just input 0 to 9 and a to f here, like 112233445566 or aabbccddeeff.
Comment	You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory

	aid. This is optional.
Add	When you finish inputting MAC address and (optional) Comment, click this button to add the MAC address to the list.
Clear	Remove all characters in ‘MAC address’ and ‘Comments’ field.

After you finish with setting, please click ‘Apply’, and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

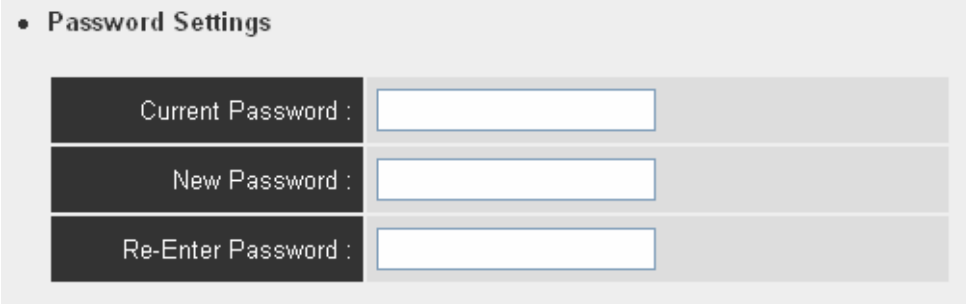
2.10 System Utilities

This access point provides some control functions including password, IP address management, and DHCP server function. Please click ‘System Utility’ on the left of the web management interface to access these functions. Below are detailed descriptions of every control function.

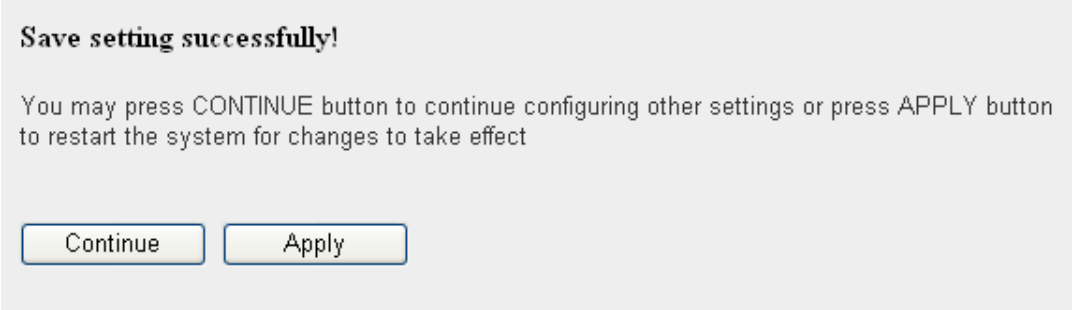
2.10.1 Change Password

You can change the password used to enter the web configuration menu of this wireless access point.

Please click ‘System Utility’ on the left, and the following message will be displayed:



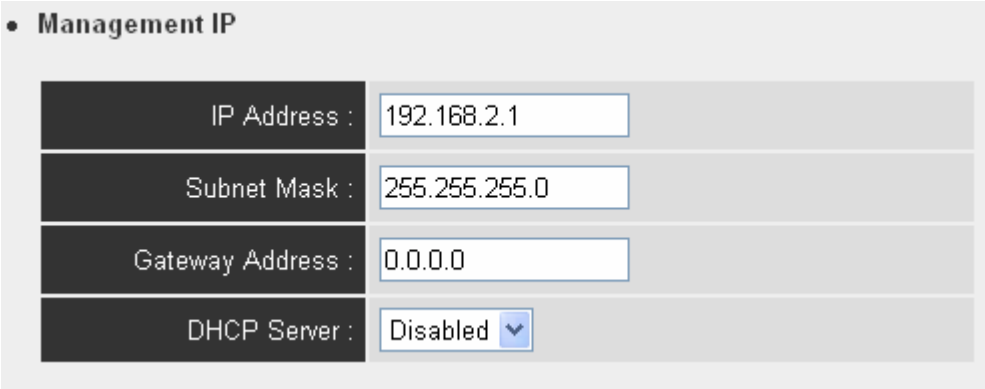
Please input current password in ‘Current Password’ field, then input new password in both ‘New Password’ and ‘Re-Enter Password’ field. After you finish, please go to the bottom of this page and click ‘Apply’, and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click the ‘Continue’ button to go back to the previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.10.2 IP Address of the Wireless Access Point

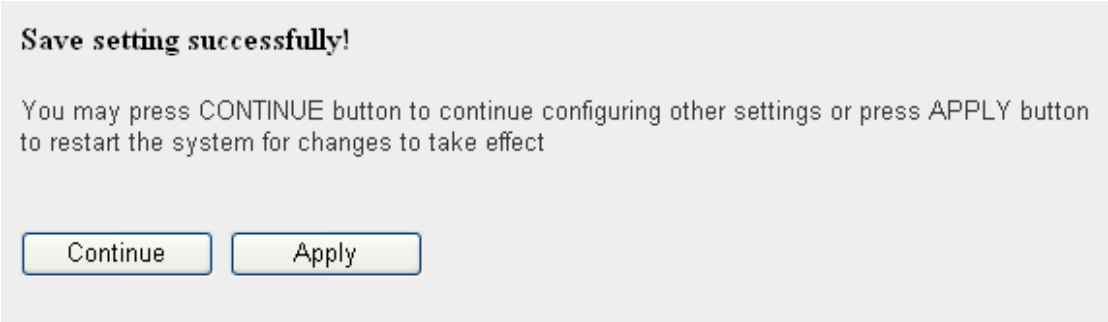
You can change the IP address of this wireless access point, so it can become a part of your local network. Please remember this address or you will not be able to connect the configuration menu of this wireless access point.
Default IP address is: 192.168.2.1 / Subnet Mask 255.255.255.0, you can press and hold ‘Reset/WPS’ button over 10 seconds to change the IP address back to default value if you forget the IP address you set.
To change IP address, please click ‘System Utility’ on the left, and the following message will be displayed:



Please input IP address and Subnet Mask in corresponding field, and you can input the IP address of gateway in 'Gateway Address' field, if you need to manage this wireless access point from other network (like Internet).

If you want to activate the DHCP server function of this wireless access point, please select 'Enabled' in 'DHCP Server' option, and see next Section for detailed instructions; if you don't want to use DHCP server function of this wireless access point, or there's another DHCP server on the network this access point connects to, please select 'Disable'.

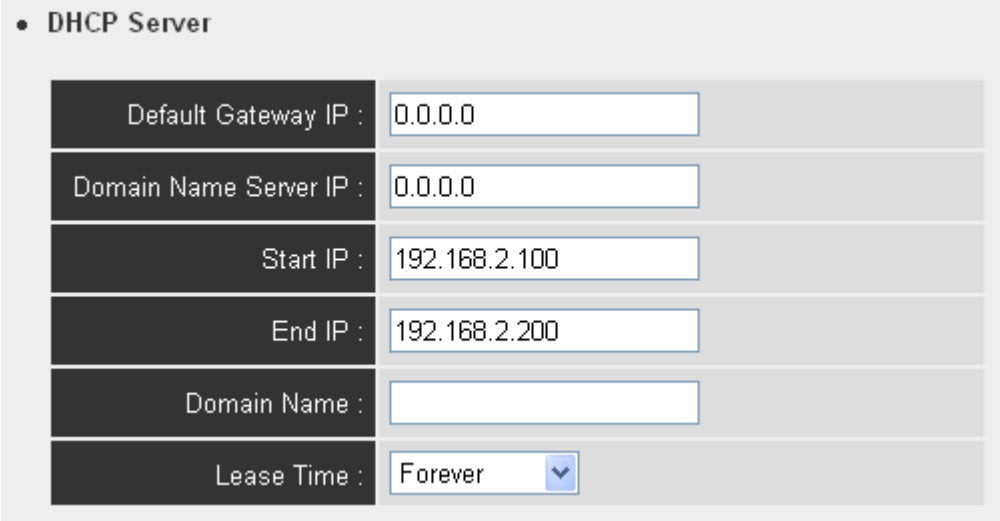
After you finish, please go to the bottom of this page and click 'Apply', and the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click the 'Continue' button to go back to the previous page and continue on other setting items, or click 'Apply' button to restart the wireless access point and the changes will take effect after about 30 seconds.

2.10.3 DHCP Server

This wireless access point is capable to act as a DHCP server for your network, and it's disabled by default. If you want to activate this function, please click 'System Utility' on the left, and the following message will be displayed:

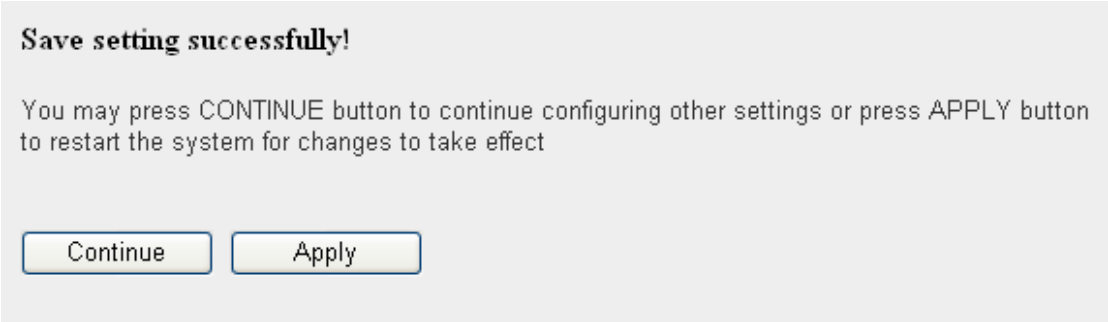


NOTE: Please remember to select 'Enable' in 'DHCP Server' option as described in last Section or all DHCP-related fields will be grayed out, and you will not be able to input any DHCP parameter.

Here are descriptions of every setup item:

Default Gateway IP	Please input the IP address of default gateway of your network here.
Domain Name Server IP	Please input the IP address of domain name server (DNS) here.
Start IP	Please input the start IP address of the IP range.
End IP	Please input the end IP address of the IP range.
Domain Name	If you wish, you can also optionally input the domain name for your network. This is optional.
Lease Time	Please choose a lease time (the duration that every computer can keep a specific IP address) of every IP address assigned by this access point from dropdown menu.

After you finish, please click 'Apply', the following message will be displayed:



When you see this message, the settings you made are successfully saved. You can click ‘Continue’ button to back to previous page and continue on other setting items, or click ‘Apply’ button to restart the wireless access point and the changes will take effect after about 30 seconds.

3. Advanced Configuration

3.1 Configuration Backup and Restore

You can backup all configurations of this access point to a file, so you can make several copies of access point configurations for security reasons.
To backup or restore access point configuration, please follow the instructions below:
Please click ‘Configuration Tool’ on the left of web management interface, and the following message will be displayed on your web browser:

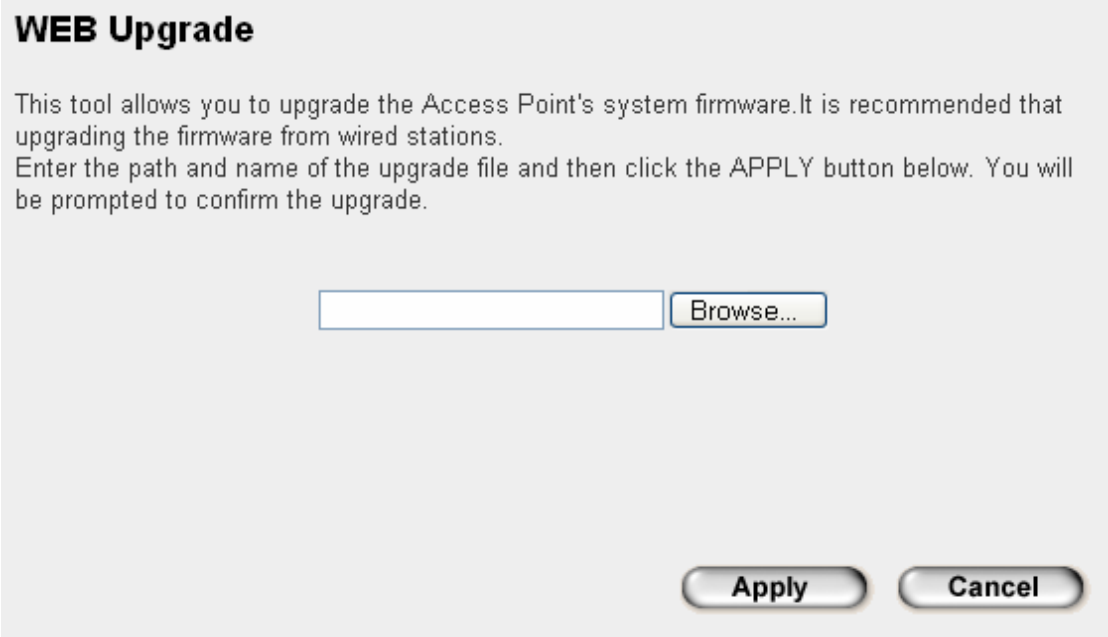
Here are descriptions of every buttons:

Backup Settings	Press ‘Save...’ button, and you’ll be prompted to download the configuration as a file, default filename is ‘config.bin’, you can save it as another filename for different versions, and keep it in a safe place.
Restore Settings	Press ‘Browse…’ to pick a previously-saved configuration file from your computer, and then click ‘Upload’ to transfer the configuration file to access point. After the configuration is uploaded, the access point’s configuration will be replaced by the file you just uploaded.
Restore to Factory Default	Click this button to remove all settings you made, and restore the configuration of this access point back to factory default settings.

3.2 Firmware Upgrade

If there are new firmware of this wireless access point available, you can upload the firmware to the access point to change the firmware with new one, to get extra functions or problem fix.

To perform firmware upgrade, please click ‘Upgrade’ on the left of web management interface, and the following message will be displayed:

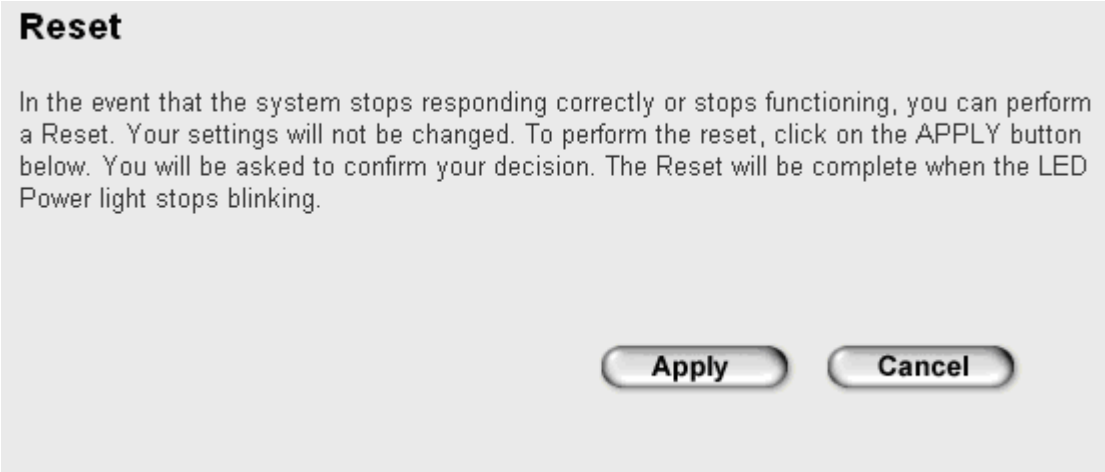


Click ‘Browse’ button first, you’ll be prompted to provide the filename of firmware upgrade file. Please download the latest firmware file from our website, and use it to upgrade your access point.

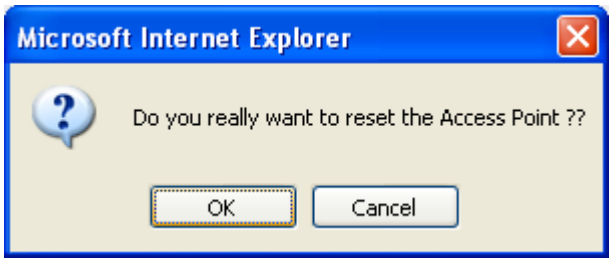
After a firmware upgrade file is selected, click ‘Apply’ button, and the access point will start firmware upgrade procedure automatically. The procedure may take several minutes, please be patient.

3.3 System Reset

When you think the access point is not working properly, you can use this function to restart the access point; this may help and solve the problem.
This function is useful when the access point is far from you or unreachable. However, if the access point is not responding, you may have to switch it off by unplugging the power plug and plug it back again after 10 seconds.
To reset your access point, please click ‘Reset’ on the left, and the following message will be displayed:



Please click ‘Apply’, and a popup message will ask you again, to make sure you really want to reset the access point:



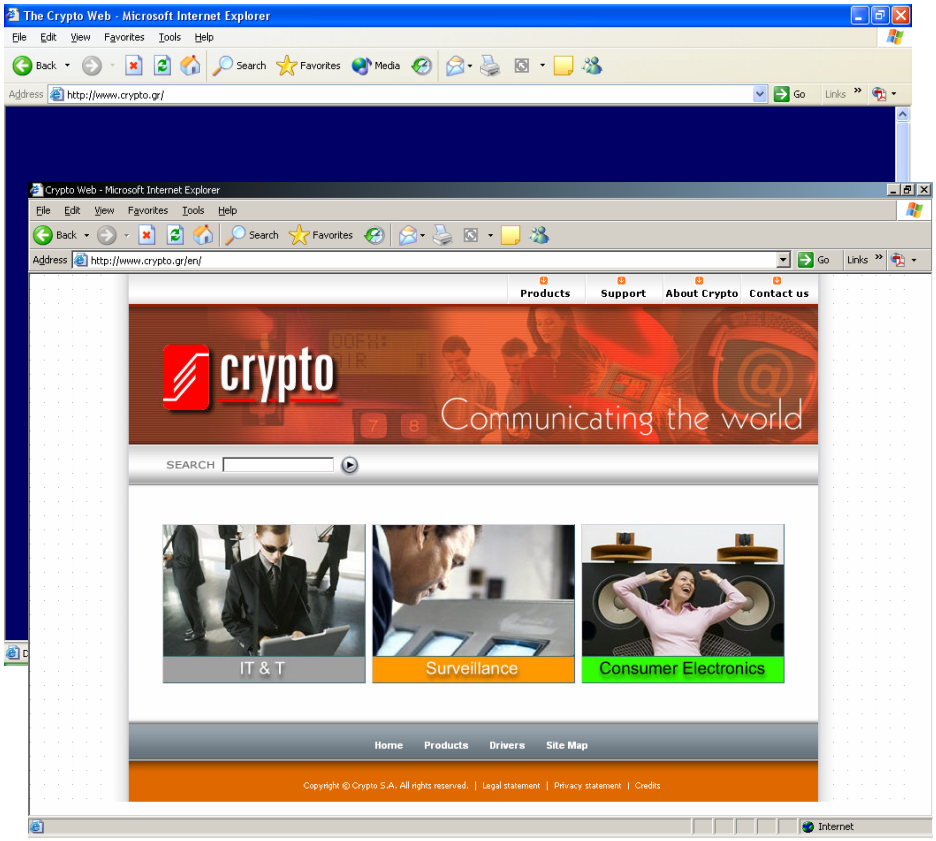
Click ‘OK’ to reset the access point, or click ‘Cancel’ to abort. Please remember all connections between wireless client and this access point will be disconnected.

4. Technical Support

For technical information and support please contact us:

Web Site: www.crypto.gr

E-mail: support@crypto.gr



Disposal of old electrical and electronic equipment

If you see this symbol on the product or on its packaging, you should hand the product over to the applicable collection point for the recycling of electrical and electronic equipment. Do not throw it away with household wastes.

The improper disposal of these products may have negative consequences for the environment and human health.

For more information about the recycling of this product, please contact your local city office, your household waste disposal service or the shop where you purchased it.