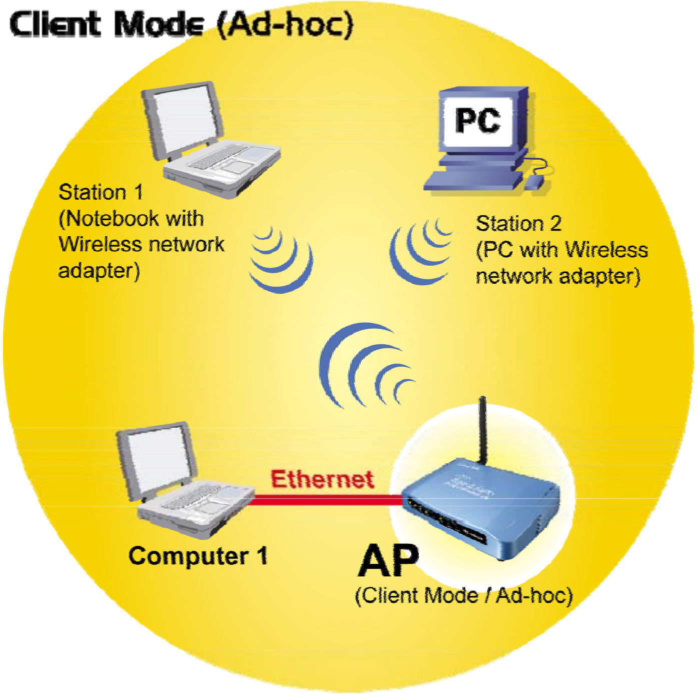
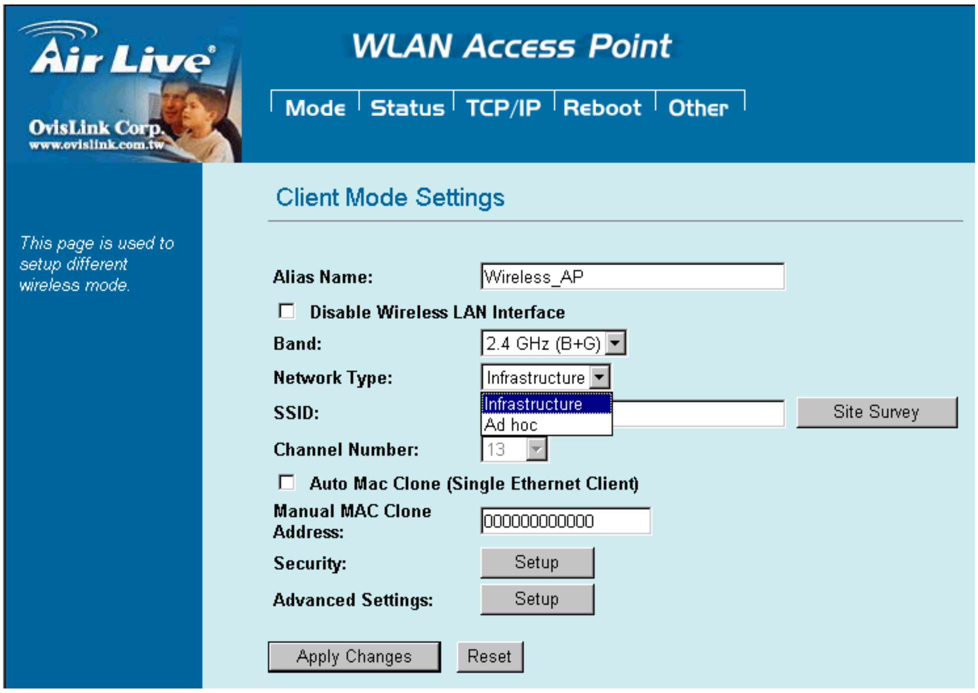
Client Mode (Ad-hoc)

If set to the Client (Ad-hoc) mode, this device can work like a wireless station when it is connected to a computer so that the computer can send packets from wired end to wireless interface. You can share files and printers between wireless stations (PC and laptop with wireless network adapter installed).

See the sample application below.



To set the operation mode to **"Client (Ad-Hoc)"**, Please go to **"Mode →Client"** and click the **Setup** button. In the **"Network Type"** field, select as **"infrastructure"** for configuration.



Client Mode Settings

This page is used to setup different wireless mode.

Alias Name: Wireless_AP

□ **Disable Wireless LAN Interface**

Band: 2.4 GHz (B+G)

Network Type: Infrastructure (Infrastructure / Ad hoc)

SSID: Site Survey

Channel Number: 13

□ **Auto Mac Clone (Single Ethernet Client)**

Manual MAC Clone Address: 000000000000

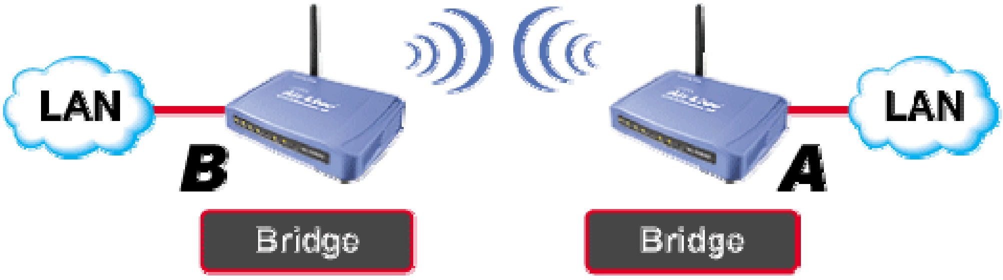
Security: Setup

Advanced Settings: Setup

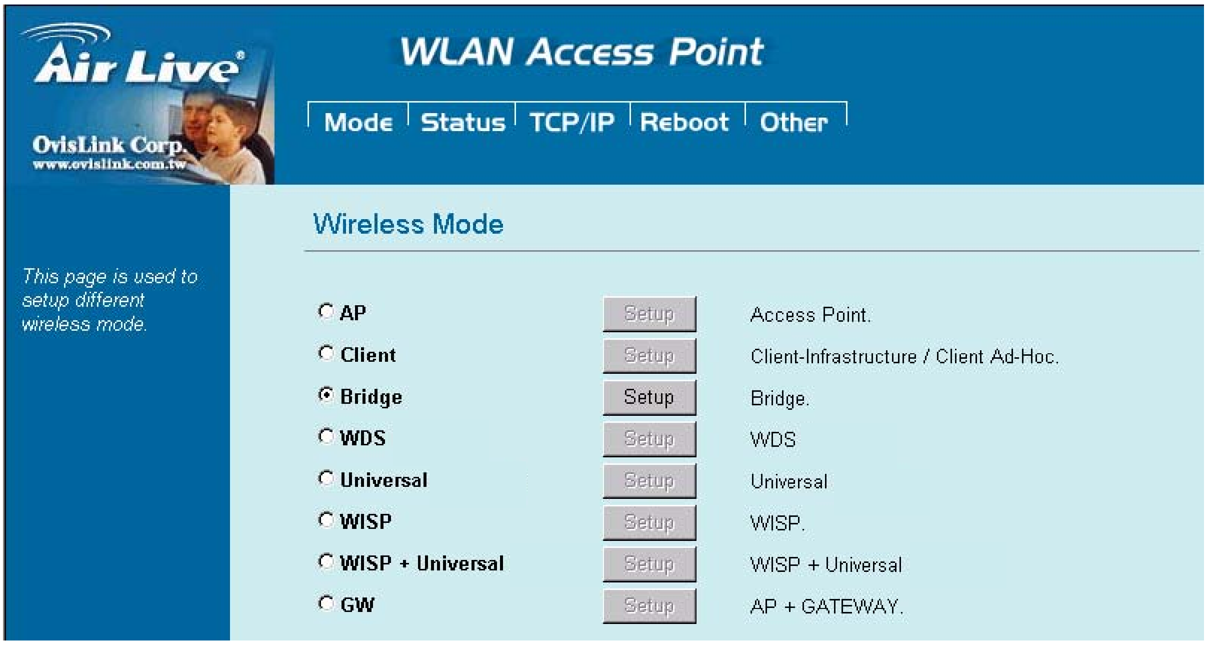
Apply Changes Reset

Bridge Mode

In this mode, 2 access points in two remote locations connect to each other to provide a wireless bridge between 2 remote LANs. It is mostly used by enterprise to connect 2 remote office's network together. The bridge modes are connected by using either the WDS (Wireless Distribution System) or Ad-Hoc topology. This feature is also useful when users want to bridge networks between buildings where it is impossible to deploy network cable connections between these buildings.



To set the operation mode to **"Bridge"**, Please go to **"Mode →Bridge"** and click the **Setup** button for configuration.



Wireless Mode

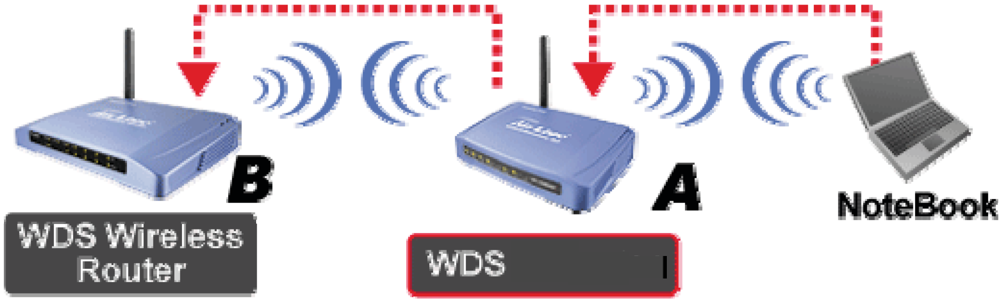
This page is used to setup different wireless mode.

○ AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
● Bridge	Setup	Bridge.
○ WDS	Setup	WDS
○ Universal	Setup	Universal
○ WISP	Setup	WISP.
○ WISP + Universal	Setup	WISP + Universal
○ GW	Setup	AP + GATEWAY.

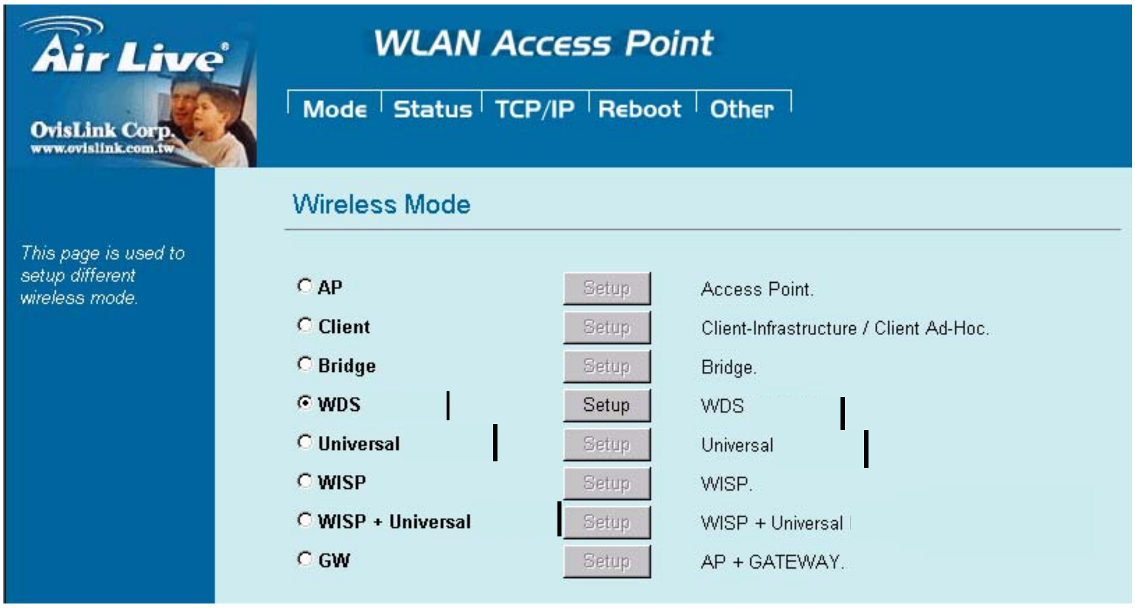
WDS Mode

A function is to extend the wireless coverage of another wireless AP or router.

For WDS to work, the remote wireless AP/Router must also support WDS function.



To set the operation mode to **“WDS ”**, Please go to **“Mode   WDS”** and click the **Setup** button for configuration.



Wireless Mode

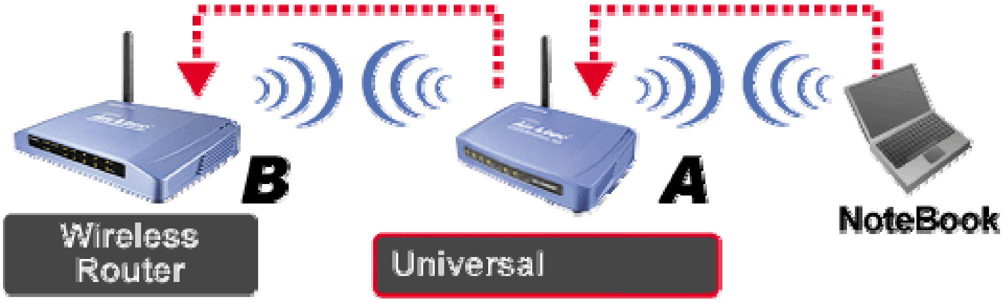
This page is used to setup different wireless mode.

○ AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
○ Bridge	Setup	Bridge.
● WDS	Setup	WDS
○ Universal	Setup	Universal
○ WISP	Setup	WISP.
○ WISP + Universal	Setup	WISP + Universal
○ GW	Setup	AP + GATEWAY.

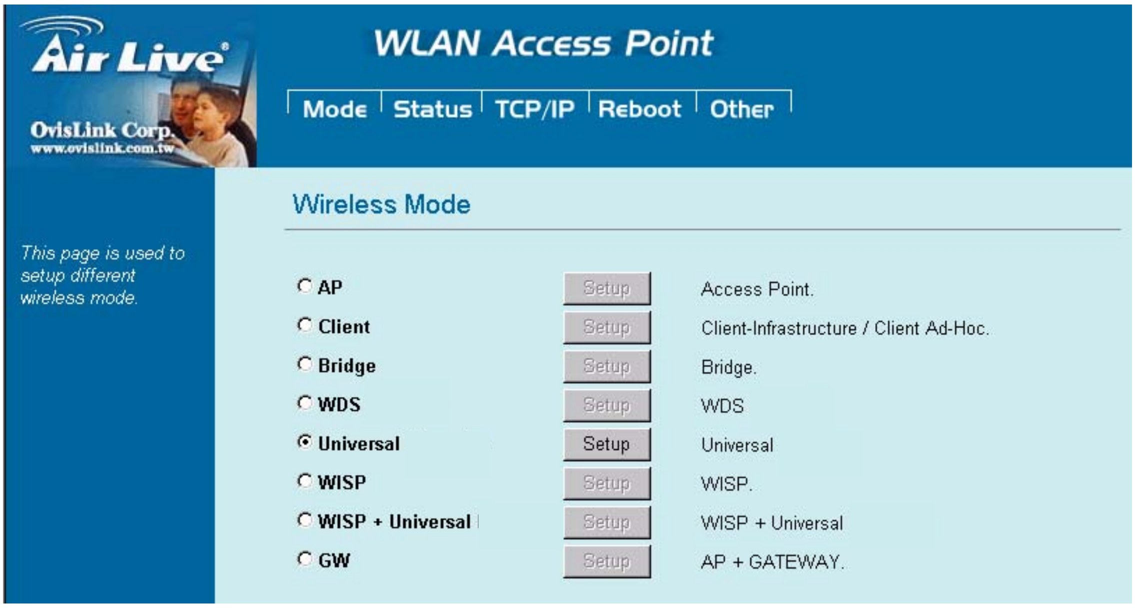
Universal Mode

A universal can also extend the wireless coverage of another wireless AP or router. But the universal does not require the remote device to have WDS function. Therefore, it can work with almost any wireless device.

Note: When you are using the universal mode, please make sure the remote AP/Router's WDS function is turned off.



To set the operation mode to **"Universal"**, Please go to **"Mode →Universal"** and click the **Setup** button for configuration.



Wireless Mode

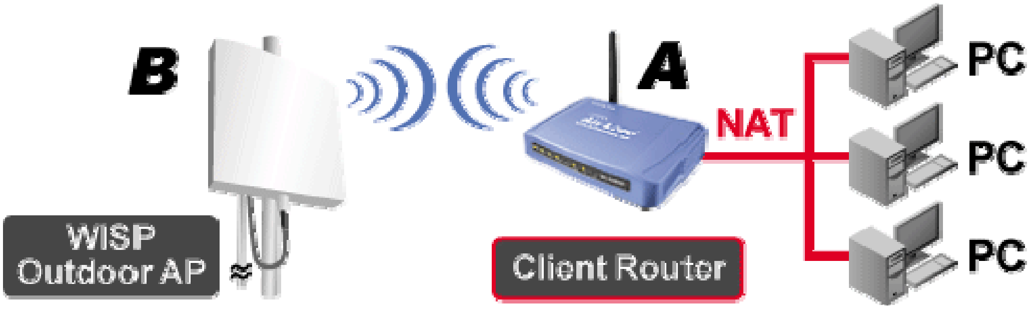
This page is used to setup different wireless mode.

○ AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
○ Bridge	Setup	Bridge.
○ WDS	Setup	WDS
● Universal	Setup	Universal
○ WISP	Setup	WISP.
○ WISP + Universal	Setup	WISP + Universal
○ GW	Setup	AP + GATEWAY.

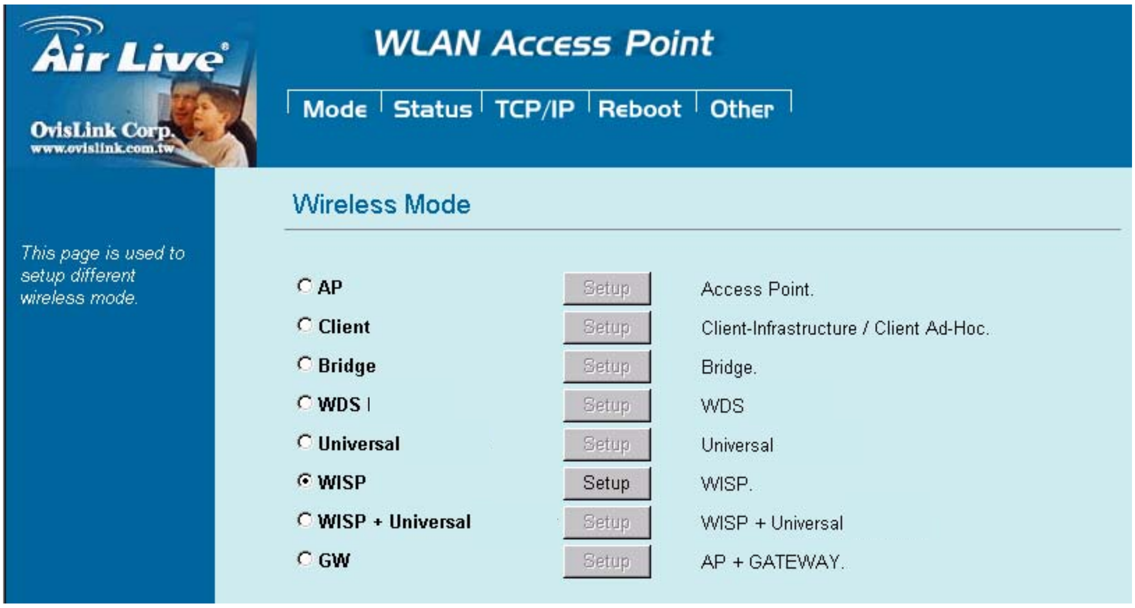
WISP (Client Router) Mode

WISP (Client Router) mode

In WISP mode, the AP will behave just the same as the Client mode for wireless function. However, Router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, The WISP subscriber can share the WISP connection without the need for extra router.



To set the operation mode to **"WISP"**, Please go to **"Mode →WISP"** and click the **Setup** button for configuration.



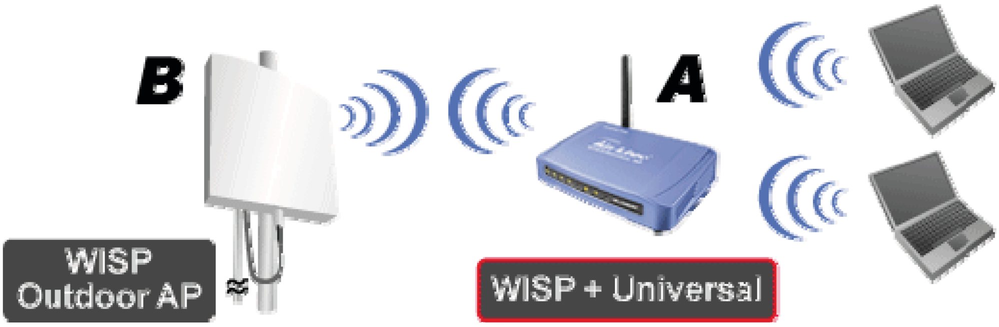
Wireless Mode

This page is used to setup different wireless mode.

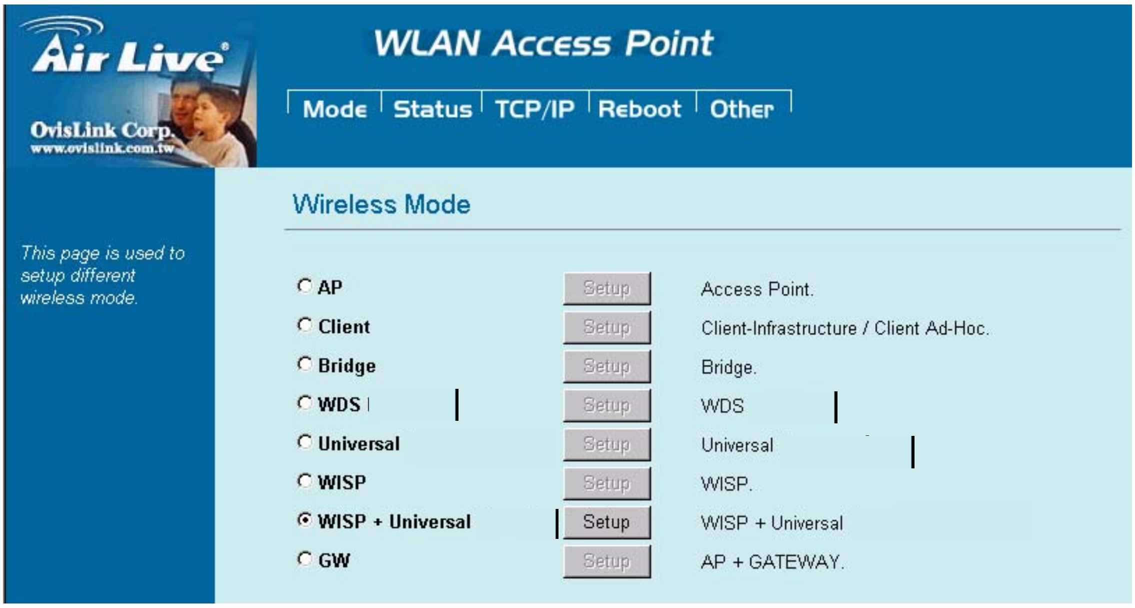
○ AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
○ Bridge	Setup	Bridge.
○ WDS I	Setup	WDS
○ Universal	Setup	Universal
● WISP	Setup	WISP.
○ WISP + Universal	Setup	WISP + Universal
○ GW	Setup	AP + GATEWAY.

WISP + Universal Mode

In this mode, the AP behaves virtually the same as the WISP mode, except one thing: the AP can also send wireless signal to the LAN side. That means the AP can connect with the remote WISP AP and the indoor wireless card, and then provide IP sharing capability all at the same time! However, the output power is divided between 2 wireless sides and proper antenna installation can influence the performance greatly.



To set the operation mode to **“WISP + Universal”**, Please go to **“Mode WISP + Universal ”** and click the **Setup** button for configuration.



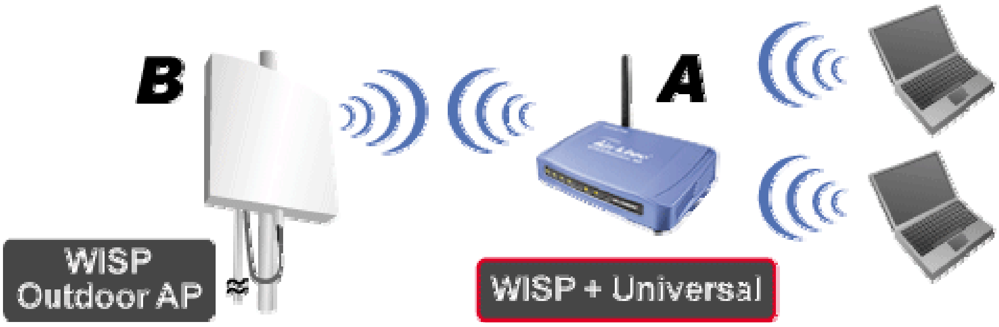
Wireless Mode

This page is used to setup different wireless mode.

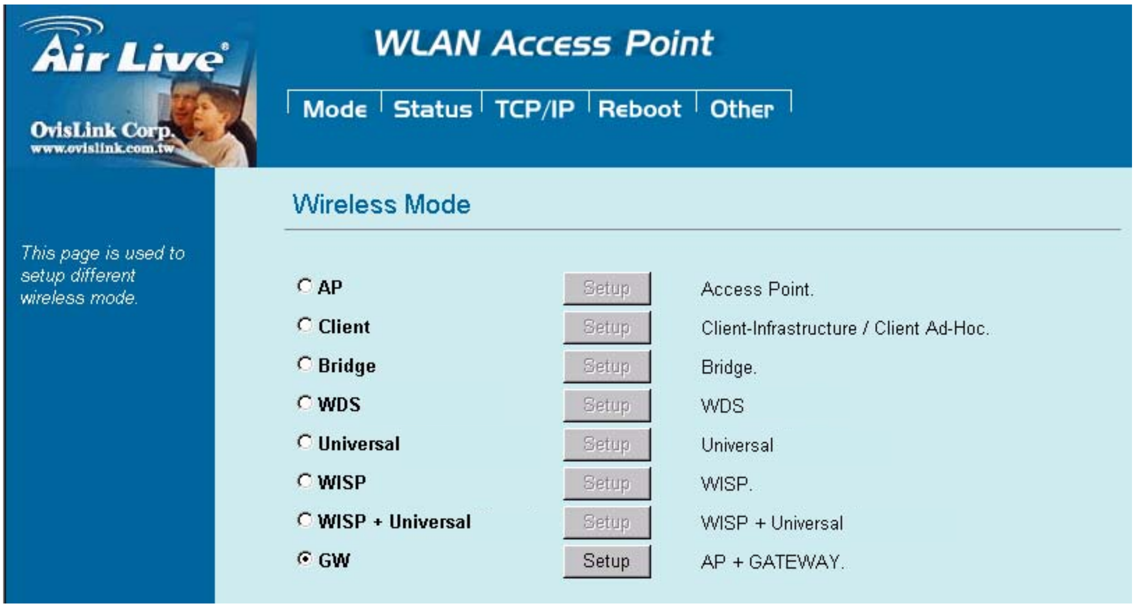
○ AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
○ Bridge	Setup	Bridge.
○ WDS	Setup	WDS
○ Universal	Setup	Universal
○ WISP	Setup	WISP.
● WISP + Universal	Setup	WISP + Universal
○ GW	Setup	AP + GATEWAY.

GW Mode

In this mode, the AP behaves virtually the same as the WISP mode, except one thing: the AP can also send wireless signal to the LAN side. That means the AP can connect with the remote WISP AP and the indoor wireless card and then provide IP sharing capability all at the same time! However, the output power is divided between 2 wireless sides, and proper antenna installation can significantly improve the performance.



To set the operation mode to **"GW Mode"**, Please go to **"Mode →GW"** and click the **Setup** button for configuration.



Wireless Mode

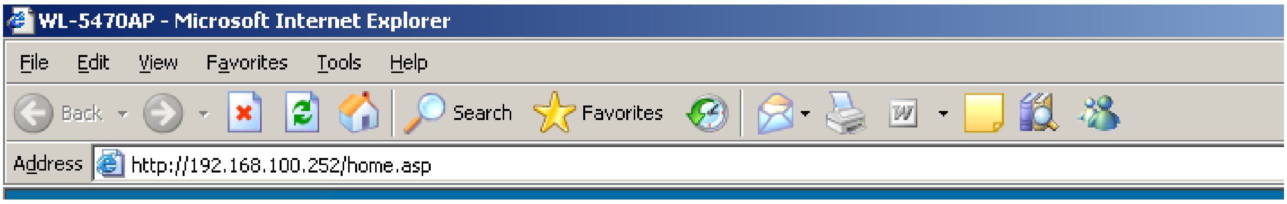
This page is used to setup different wireless mode.

○ AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
○ Bridge	Setup	Bridge.
○ WDS	Setup	WDS
○ Universal	Setup	Universal
○ WISP	Setup	WISP.
○ WISP + Universal	Setup	WISP + Universal
● GW	Setup	AP + GATEWAY.

Configuration

1. Start your computer. Connect an Ethernet cable between your computer and the Wireless Access Point.
2. Make sure your wired station is set to the same subnet as the Wireless Access Point, i.e. 192.168.100.X
3. Start your WEB browser. In the *Address* box, enter the following:

http://192.168.100.252/

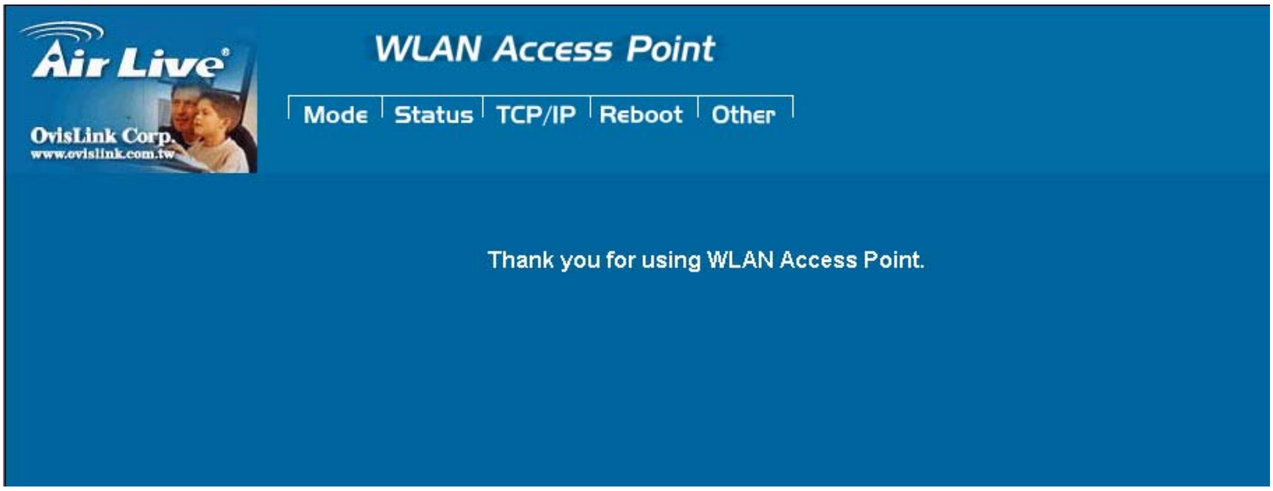


http://192.168.100.252/home.asp

The configuration menu is divided into five categories:

Mode, Status, TCP/IP, Reboot and **Other.**

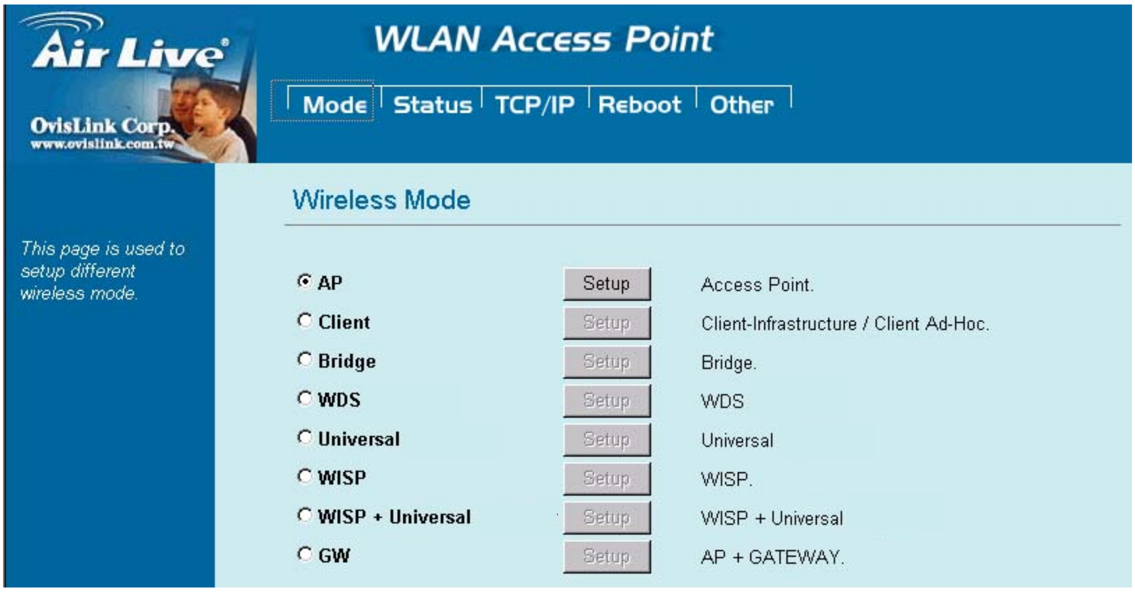
Click on the desired setup item to expand the page in the main navigation page. The setup pages covered in this utility are described below.



Thank you for using WLAN Access Point.

Mode

You can choose and setup different wireless mode for detail configurations



WLAN Access Point

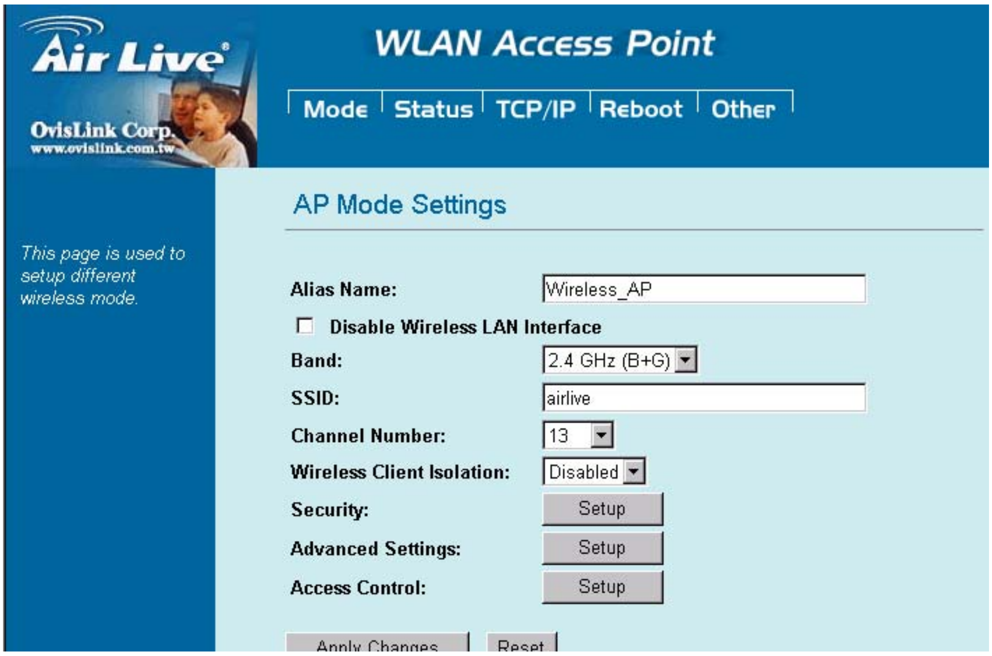
Wireless Mode

This page is used to setup different wireless mode.

● AP	Setup	Access Point.
○ Client	Setup	Client-Infrastructure / Client Ad-Hoc.
○ Bridge	Setup	Bridge.
○ WDS	Setup	WDS
○ Universal	Setup	Universal
○ WISP	Setup	WISP.
○ WISP + Universal	Setup	WISP + Universal
○ GW	Setup	AP + GATEWAY.

Wireless Mode	
AP	Select the AP and press Setup button for Wireless AP mode configuration.
Client	Select the Client and press Setup button for Wireless Client mode configuration.
Bridge	Select the Bridge and press Setup button for Wireless Bridge mode configuration.
WDS	Select the WDS and press Setup button for Wireless WDS mode configuration.
Universal	Select the Universal and press Setup button for Wireless Universal mode configuration.
WISP	Select the WISP and press Setup button for WISP (Client Router) mode configuration.
WISP + Universal	Select the WISP + Universal and press Setup button for WISP + Universal mode configuration.
GW	Select the GW and press Setup button for GW mode configuration.

AP Mode Setting



AP Mode Settings

This page is used to setup different wireless mode.

Alias Name: Wireless_AP

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

SSID: airlive

Channel Number: 13

Wireless Client Isolation: Disabled

Security: Setup

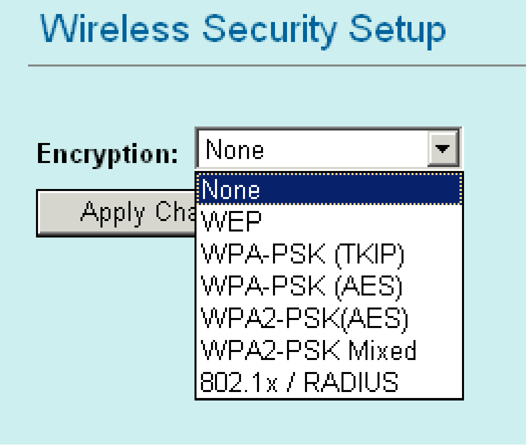
Advanced Settings: Setup

Access Control: Setup

Apply Changes Reset

Alias Name	You can set the alias name for this device. Limited not exceed 32 characters.
□ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing; you won't be able to make wireless connection with this Access Point in your located network. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network. The default SSID is **airlive**.
Channel Number	Allow user to set the channel **manually** or **automatically**. If set channel manually, just select the channel you want to specify. If "Auto" is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel. The default value is **11** in the USA/Canada market, **13** in the Europe market
Wireless Client	Allow user to set the function **Enabled** or **Disabled**.

Isolation	By the function, all wireless clients can't mutual link, but wireless client still link with LAN port adapter. The default value is **Disabled**.
Security	Press the setup button for detail configurations



Wireless Security Setup

Encryption: None

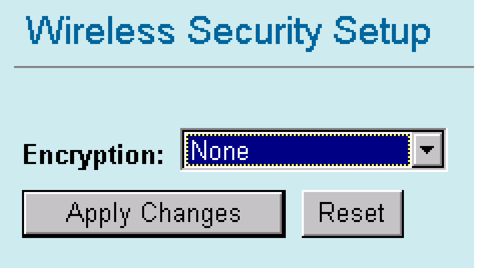
To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods: **Open System** or **Shared Key**. And WL-5470APv2 also support other wireless authentication and encryption methods for enhance your wireless network.

With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network and None data encryption. If you want secure your wireless network, you need to setup wireless security related function to enable security network.

None

Encryption: None (Encryption is set to **None** by default.**)**

If the Access Point is using **Encryption None**, then the wireless adapter will need to be set to the same authentication mode.



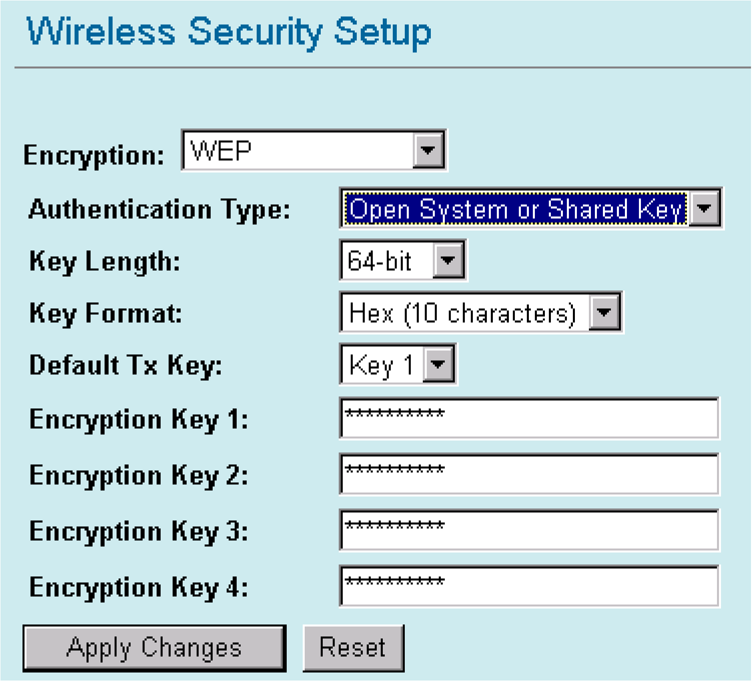
Wireless Security Setup

Encryption: None

WEP

Encryption: WEP

If selected WEP encryption, you must set WEP key value:



Wireless Security Setup

Encryption: WEP

Authentication Type: Open System or Shared Key

Key Length: 64-bit

Key Format: Hex (10 characters)

Default Tx Key: Key 1

Encryption Key 1: **********

Encryption Key 2: **********

Encryption Key 3: **********

Encryption Key 4: **********

Encryption	WEP
Authentication Type	You can select **Open System** or **Shared Key** type for authentication.
Key Length	You can set **64bit** or **128bit** Encryption.
Key Format	Select **ASCII** if you are using ASCII characters (**case-sensitive**). Select **HEX** if you are using hexadecimal numbers (**0-9, or A-F**).
Default TX Key	You can enter 4 different Encryption Key and select one key to use as default.

10 hexadecimal digits or **5 ASCII characters** are needed if **64-bit WEP** is used;

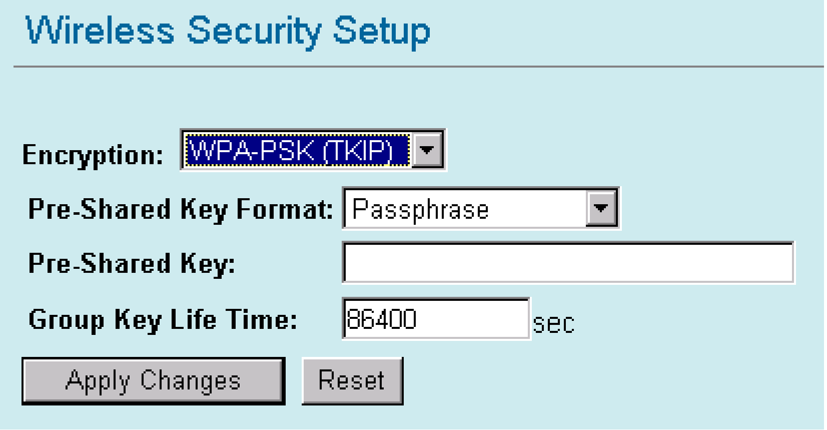
26 hexadecimal digits or **13 ASCII characters** are needed if **128-bit WEP** is used.

Shared Key is used when both the sender and the recipient share a secret key. So you can choose Open system, or one Shared Key authentication method.

WPA-PSK

Encryption: WPA-PSK (TKIP) or WPA-PSK (AES)

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.



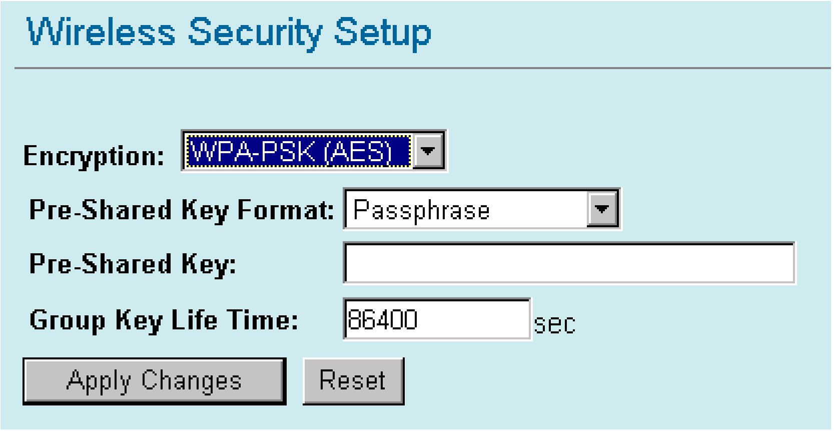
Wireless Security Setup

Encryption: WPA-PSK (TKIP)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Group Key Life Time: 86400 sec



Wireless Security Setup

Encryption: WPA-PSK (AES)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

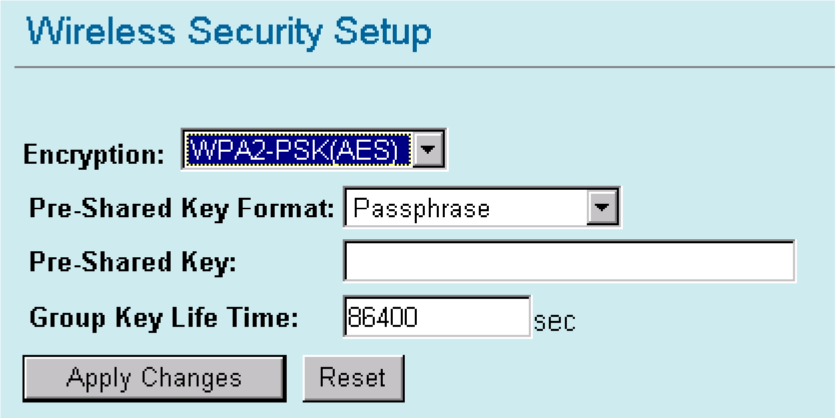
Group Key Life Time: 86400 sec

Encryption	You can select WPA-PSK (TKIP) or WPA-PSK (AES) method for data encryption.
Pre-shared Key	There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Group Key Life Time	Enter the number of seconds that will elapse before the group key change automatically. The default is 86400 seconds.

WPA2-PSK

Encryption: WPA2-PSK (AES) or WPA-PSK Mixed

WPA2-PSK authentication method is almost like WPA-PSK, You can choose the Pre-Shared Key format and enter the Pre-shared key,



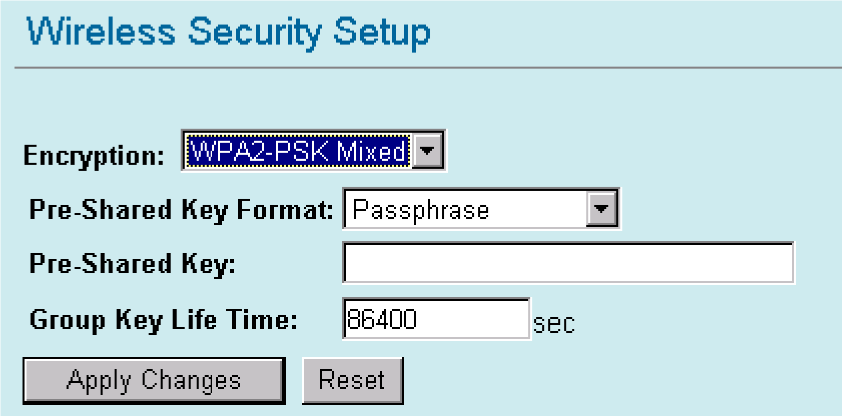
Wireless Security Setup

Encryption: WPA2-PSK(AES)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Group Key Life Time: 86400 sec



Wireless Security Setup

Encryption: WPA2-PSK Mixed

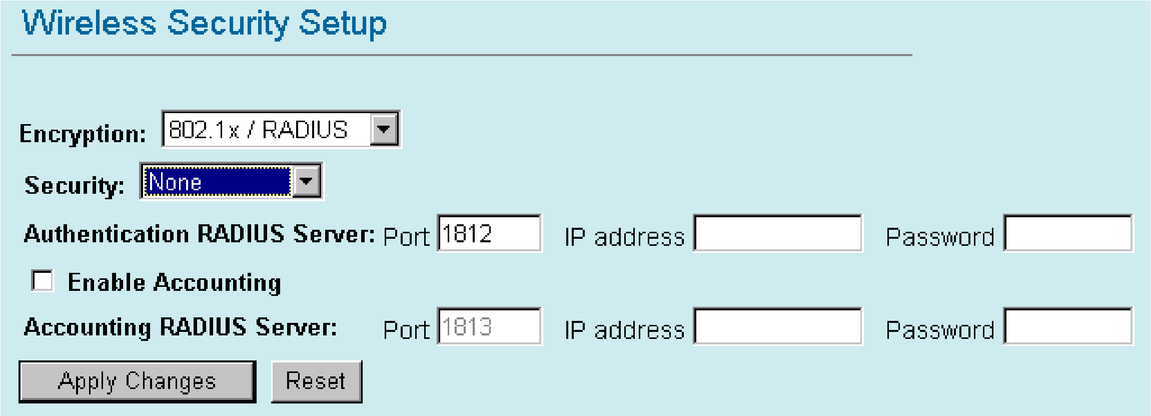
Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Group Key Life Time: 86400 sec

Encryption	You can select WPA2-PSK (AES) or WPA2-PSK Mixed method for data encryption
Pre-shared Key	There are two formats for choice to set the Pre-shared key, i.e. **Passphrase** and **Hex**. If **Hex** is selected, users will have to enter a 64 characters string. For easier configuration, the **Passphrase** (at least 8 characters) format is recommended.
Group Key Life Time	Enter the number of seconds that will elapse before the group key change automatically. The default is 86400 seconds.

802.1x / RADIUS



Wireless Security Setup

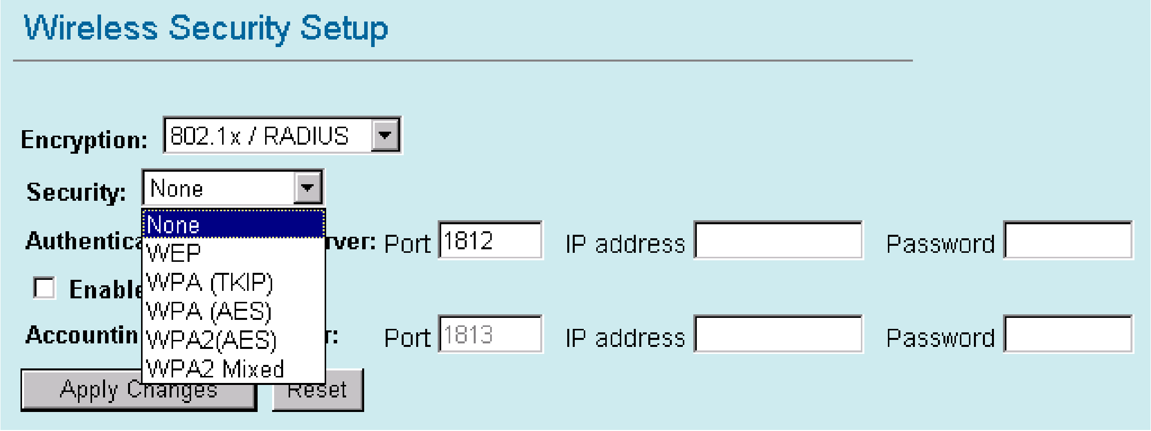
Encryption: 802.1x / RADIUS

Security: None

Authentication RADIUS Server: Port 1812 IP address Password

☐ Enable Accounting

Accounting RADIUS Server: Port 1813 IP address Password



Wireless Security Setup

Encryption: 802.1x / RADIUS

Security: None

Encryption: 802.1x / RADIUS

security	You can select None, WEP, WPA (TKIP), WPA (AES), WPA2 (AES), WPA2 Mixed method for data encryption.

Encryption: **None**

No data encryption and Use 802.1x Authentication is disable.

Encryption: **WEP**

802.1x Authentication is enabled and the RADIUS Server will proceed to check the 802.1x Authentication, and make the RADIUS server to issue the WEP key dynamically.

You can select WEP 64bits or WEP 128bits for data encryption.

Encryption: **WPA (TKIP) / WPA (AES)**

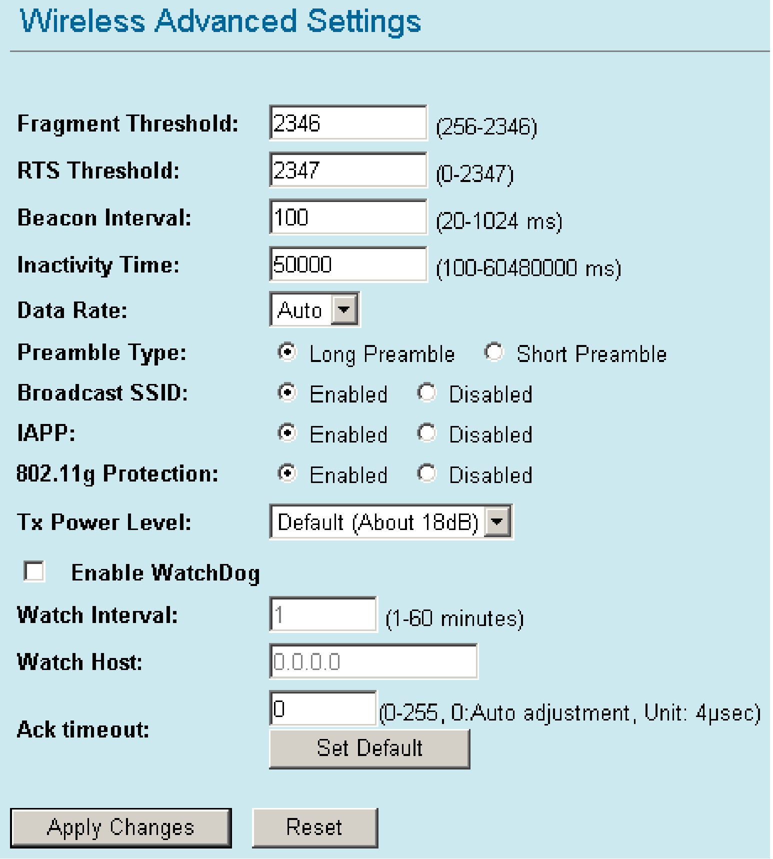
WPA-RADIUS authentication use WPA (Wi-Fi Protect Access) data encryption for 802.1x authentication.

WPA is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption.

Encryption: **WPA2-AES / WPA2-Mixed**

The two most important features beyond WPA to become standardized through 802.11i/WPA2 are: pre-authentication, which enables secure fast roaming without noticeable signal latency. Pre-authentication provides a way to establish a PMK security association before a client associates. The advantage is that the client reduces the time that it's disconnected to the network.

Authentication RADIUS Server	Enter the RADIUS Server IP address and Password provided by your ISP. **Port**: Enter the RADIUS Server's port number provided by your ISP. The default is 1812. **IP Address**: Enter the RADIUS Server's IP Address provided by your ISP. **Password**: Enter the password that the AP shares with the RADIUS Server.
Accounting RADIUS Server	Enter the Accounting RADIUS Server IP address and Password provided by your ISP
Advanced Settings	Press the setup button for detail configurations



Wireless Advanced Settings

Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 (20-1024 ms)

Inactivity Time: 50000 (100-60480000 ms)

Data Rate: Auto

Preamble Type: ● Long Preamble ○ Short Preamble

Broadcast SSID: ● Enabled ○ Disabled

IAPP: ● Enabled ○ Disabled

802.11g Protection: ● Enabled ○ Disabled

Tx Power Level: Default (About 18dB)

□ Enable WatchDog

Watch Interval: 1 (1-60 minutes)

Watch Host: 0.0.0.0

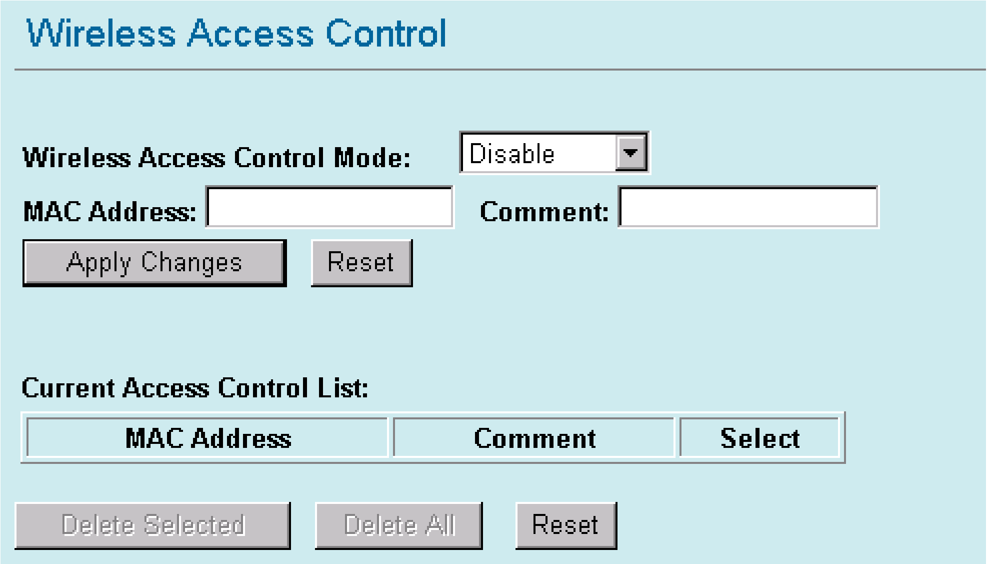
Ack timeout: 0 (0-255, 0:Auto adjustment, Unit: 4μsec)

It is not recommended that settings in this page to be changed unless advanced users want to change to meet their wireless environment for optimal performance.

Fragment Threshold	Fragmentation mechanism is used for improving the efficiency when high traffic flows along in the wireless network. If your 802.11g Wireless LAN PC Card often transmit large files in wireless

	network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346. The default value is **2346**.
RTS Threshold	RTS Threshold is a mechanism implemented to prevent the "**Hidden Node**" problem. "Hidden Node" is a situation in which two stations are within range of the same Access Point, but are not within range of each other. Therefore, they are hidden nodes for each other. When a station starts data transmission with the Access Point, it might not notice that the other station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS Threshold mechanism provides a solution to prevent data collisions. When you enable RTS Threshold on a suspect "hidden station", this station and its Access Point will use a Request to Send (RTS). The station will send an RTS to the Access Point, informing that it is going to transmit the data. Upon receipt, the Access Point will respond with a CTS message to all station within its range to notify all other stations to defer transmission. It will also confirm the requestor station that the Access Point has reserved it for the time-frame of the requested transmission. If the "Hidden Node" problem is an issue, please specify the packet size. *The RTS mechanism will be activated if the data size exceeds the value you set.*. The default value is **2347**. **Warning:** Enabling RTS Threshold will cause redundant network overhead that could negatively affect the throughput performance instead of providing a remedy. This value should remain at its default setting of **2347**. Should you encounter inconsistent data flow, only minor modifications of this value are recommended.
Beacon Interval	Beacon Interval is the amount of time between beacon transmissions. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point).
Data Rate	By default, the unit adaptively selects the highest possible rate for transmission. Select the basic rates to be used among the following options: Auto, 1, 2, 5.5, 11or 54 Mbps. For most networks the default setting is **Auto** which is the best choice. When **Auto** is enabled the transmission rate will

	select the optimal rate. If obstacles or interference are present, the system will automatically fall back to a lower rate.
Preamble Type	A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. In a "noisy" network environment, the Preamble Type should be set to **Long Preamble**. The **Short Preamble** is intended for applications where minimum overhead and maximum performance is desired. If in a "noisy" network environment, the performance will be decreased.
Broadcast SSID	Select **enabled** to allow all the wireless stations to detect the SSID of this Access Point.
IAPP	IAPP (Inter Access Point Protocol) is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and a secure exchange of station's security context between current access point (AP) and new AP during handoff period.
802.11g Protection	The 802.11g standard includes a protection mechanism to ensure mixed 802.11b and 802.11g operation. If there is no such kind of mechanism exists, the two kinds of standards may mutually interfere and decrease network's performance.
TX Power Level	For countries that impose limit on WLAN output power, it might be necessary to reduce TX (transmit) power. There are 7 TX Power Levels to choose from — select a level to make sure that the output power measured at the antenna end will not exceed the legal limit in your country.
Enable Watch dog	Check and enable this watch dog function
Watch Interval	Setup the interval time for watch dog function between 1 to 60 mins
Watch Host	Enter the watch dog host ip address .
ACK Timeout	When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the ACK Window to timeout on lost packets. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks You can set as default for auto adjustment.
Apply Change	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.
Access Control	Press the setup button for detail configurations



Wireless Access Control

Wireless Access Control Mode: Disable

MAC Address:

Comment:

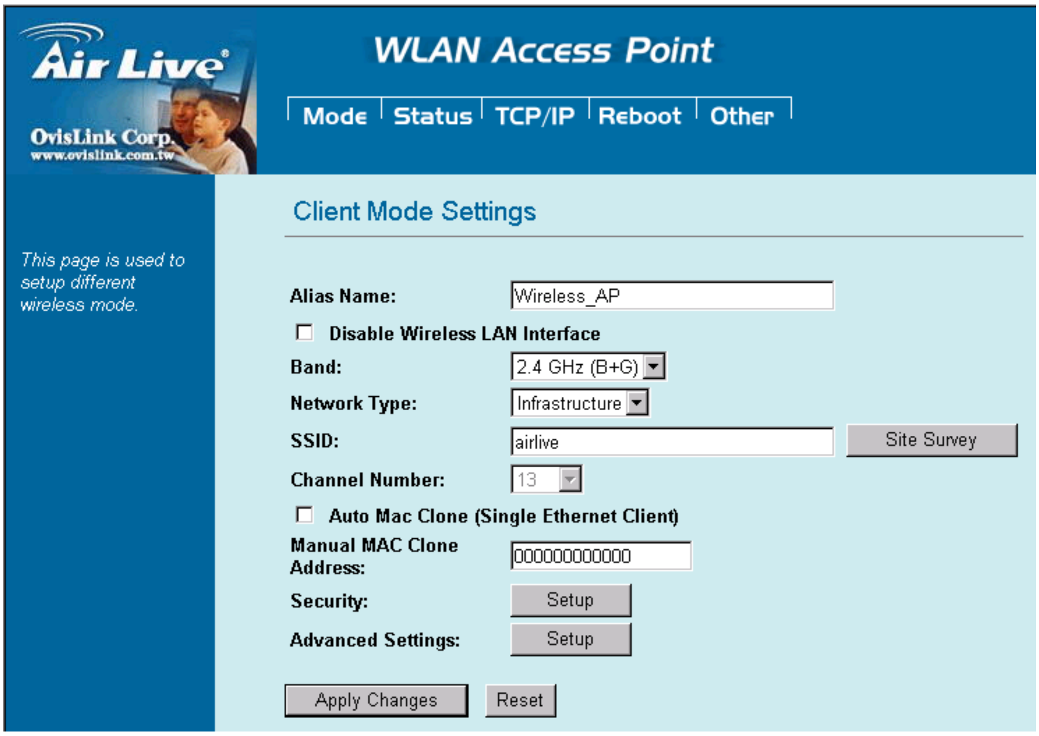
Current Access Control List:

MAC Address	Comment	Select

When **Enable Wireless Access Control** is checked, only those clients whose wireless MAC addresses listed in the access control list can access this Access Point. If the list contains no entries with this function being enabled, then no clients will be able to access this Access Point.

Wireless Access Control Mode	Select the Access Control Mode from the pull-down menu. **Disable**: Select to disable Wireless Access Control Mode. **Allow Listed**: Only the stations shown in the table can associate with the AP. **Deny Listed**: Stations shown in the table won't be able to associate with the AP.
MAC Address	Enter the MAC Address of a station that is allowed to access this Access Point.
Comment	You may enter up to 20 characters as a remark to the previous MAC Address.
Apply Changes	Press to save the new settings on the screen.
Reset	Press to discard the data you have entered since last time you press Apply Change.
Delete Selected	To delete clients from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**.
Delete All	To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox.
Reset	If you have made any selection, press **Reset** will clear all the select mark.

Client Mode Setting



Client Mode Settings

Alias Name: Wireless_AP

☐ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Network Type: Infrastructure

SSID: airlive [Site Survey]

Channel Number: 13

☐ Auto Mac Clone (Single Ethernet Client)

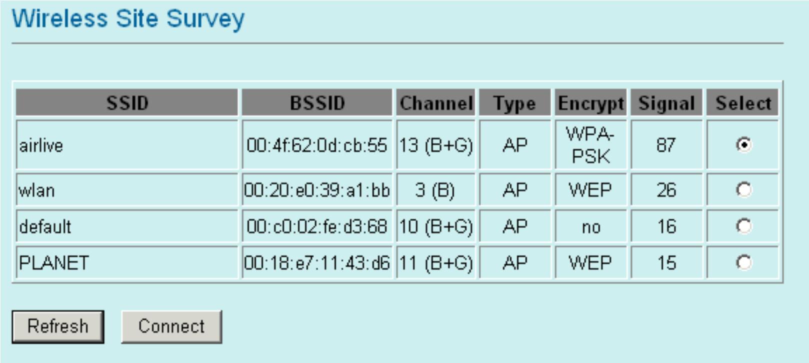
Manual MAC Clone Address: 000000000000

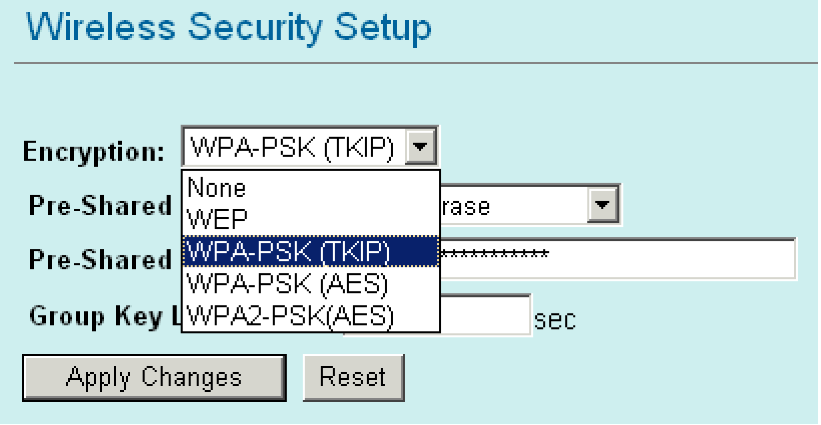
Security: [Setup]

Advanced Settings: [Setup]

[Apply Changes] [Reset]

Alias Name	You can set the alias name for this device. limited not exceed 32 characters.
☐ Disable Wireless LAN Interface	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⦿ 2.4GHz **(B):** 802.11b supported rate only. ⦿ 2.4GHz **(G):** 802.11g supported rate only. ⦿ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Network Type	Client mode have two Network type : **Infrastructure** A wireless network that is built around one or more access points, providing wireless clients access to wired LAN or Internet service. It is the most popular WLAN network structure today. **AdHoc** wireless network do not use wireless AP orrouter as the central hub of the network. Instead, wireless client are connected directly to each other.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless

<table>
<tr><td></td><td>network.</td></tr>
<tr><td><b>Site Survey</b></td><td>

Wireless Site Survey
<table>
<tr><th>SSID</th><th>BSSID</th><th>Channel</th><th>Type</th><th>Encrypt</th><th>Signal</th><th>Select</th></tr>
<tr><td>airlive</td><td>00:4f:62:0d:cb:55</td><td>13 (B+G)</td><td>AP</td><td>WPA-PSK</td><td>87</td><td>●</td></tr>
<tr><td>wlan</td><td>00:20:e0:39:a1:bb</td><td>3 (B)</td><td>AP</td><td>WEP</td><td>26</td><td>○</td></tr>
<tr><td>default</td><td>00:c0:02:fe:d3:68</td><td>10 (B+G)</td><td>AP</td><td>no</td><td>16</td><td>○</td></tr>
<tr><td>PLANET</td><td>00:18:e7:11:43:d6</td><td>11 (B+G)</td><td>AP</td><td>WEP</td><td>15</td><td>○</td></tr>
</table>

Site survey displays all the active Access Points and IBSS in the neighborhood. You can select one AP to associate. Press Site Survey button to search the wireless device that this client want to connect.</td></tr>
<tr><td><b>Channel Number</b></td><td>Allow user to set the channel <b>manually</b> or <b>automatically</b>.
If set channel manually, just select the channel you want to specify.
If “Auto” is selected, user can set the channel range to have Wireless Access Point automatically survey and choose the channel with best situation for communication. All stations communicating with the Access Point must use the same channel.
when setup infrastructure of Client mode, the channel number can not
Be changed. You have to go to AP mode to change the channel number</td></tr>
<tr><td><b>Auto MAC Clone</b></td><td>Check the box to enable MAC Clone for Single Ethernet Client.</td></tr>
<tr><td><b>Manual MAC Clone Address</b></td><td>Enter the MAC Address of Single Ethernet Client.</td></tr>
<tr><td><b>Security</b></td><td>Please refer the AP mode settings→ Security for details.
In client mode are not supported with RADIUS 802.1x authentication.

Wireless Security Setup

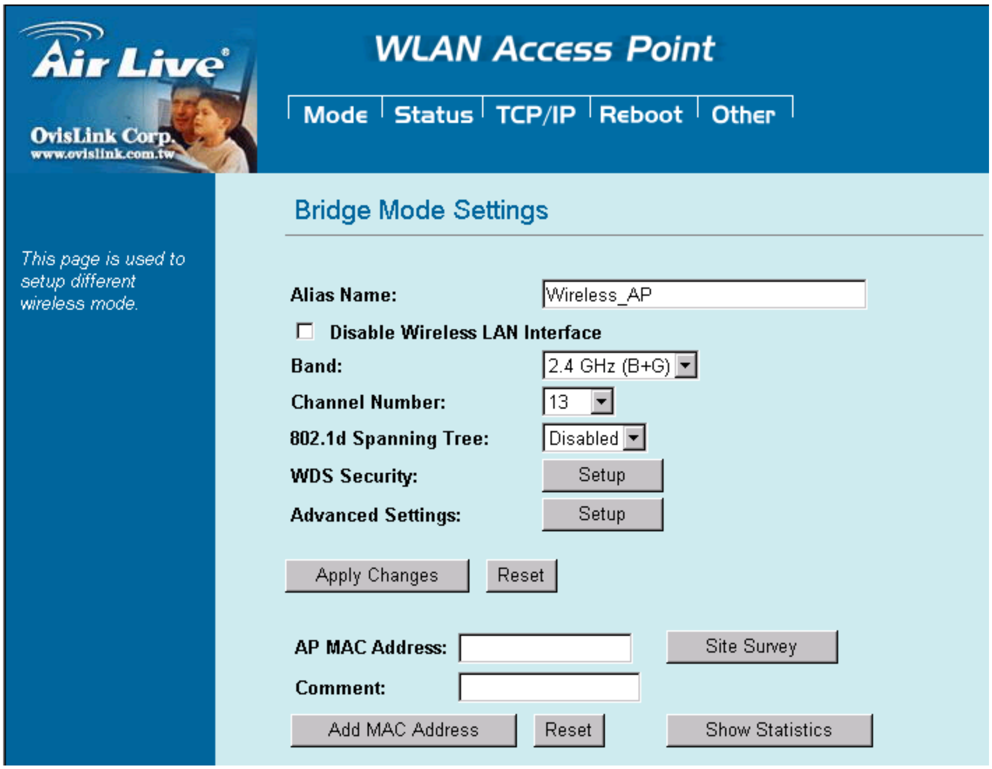
Encryption: WPA-PSK (TKIP)

Pre-Shared … rase

Pre-Shared … ***********

Group Key L… sec
</td></tr>
<tr><td><b>Advance Setting</b></td><td>Please refer the AP mode settings→ Advance Setting for details.</td></tr>
</table>

Bridge Mode Setting



This page is used to setup different wireless mode.

Bridge Mode Settings

Alias Name: Wireless_AP

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

Channel Number: 13

802.1d Spanning Tree: Disabled

WDS Security: Setup

Advanced Settings: Setup

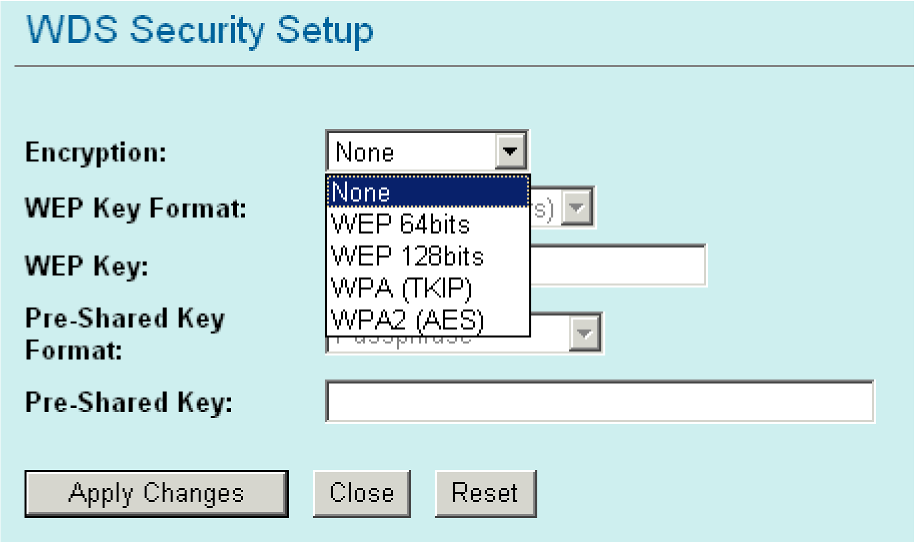
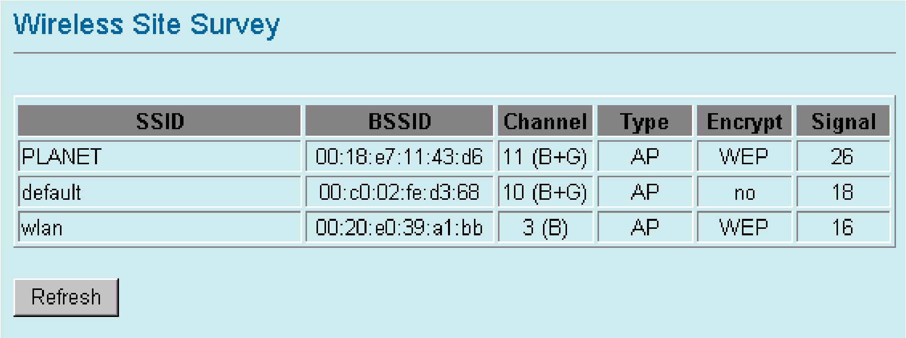
Apply Changes | Reset

AP MAC Address: | Site Survey

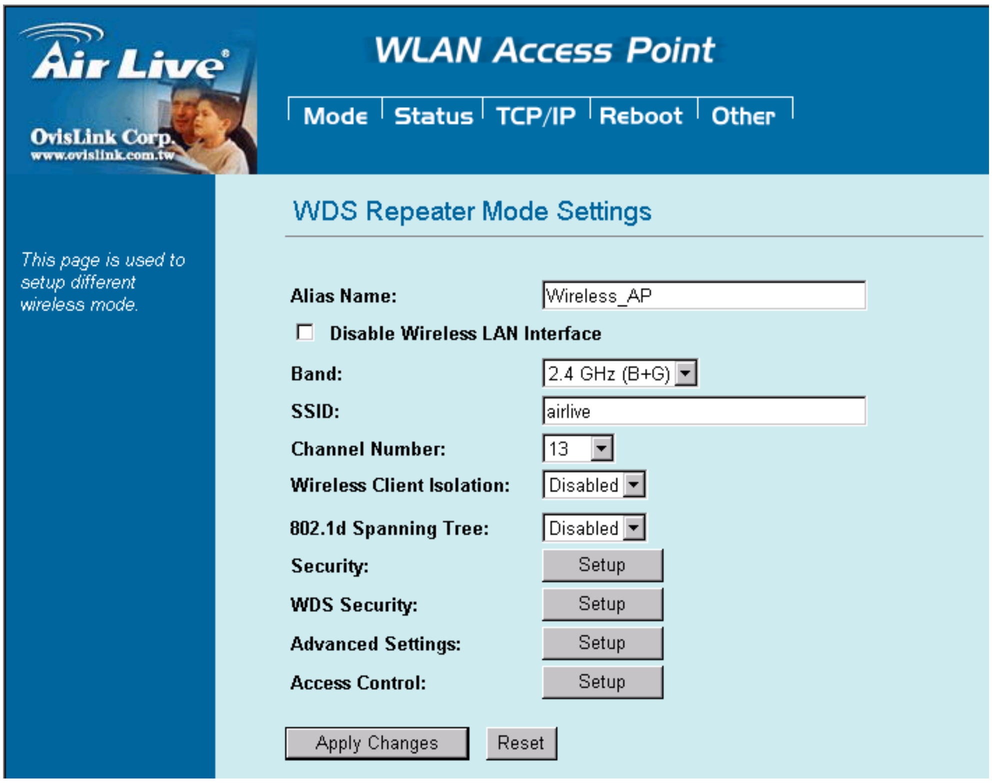
Comment:

Add MAC Address | Reset | Show Statistics

Alias Name	You can set the alias name for this device. limited not exceed 32 characters.
□ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
Channel Number	In Bridge mode, both wireless AP/Router devices need set to the same Channel number.
Security	Please refer the AP mode settings→ Security for details. But bridge mode is not supported with RADIUS 802.1x authentication.
WDS Security	To enable security between wireless AP/Router , you can select WEP 64bits, WEP 128bits, WPA (TKIP), WPA2(AES) for data encryption. For WEP encryption, Select **ASCII** if you are using ASCII characters. Select **HEX** if you are using hexadecimal numbers (**0-9, or A-F**). For WPA/WPA2 encryption, you need enter the Pre-Shared Key Information for the authentication purpose.

<table>
<tr><td></td><td>
WDS Security Setup
Encryption: None
WEP Key Format:
WEP Key:
Pre-Shared Key Format: Passphrase
Pre-Shared Key:
</td></tr>
<tr><td><b>Advance Setting</b></td><td>Please refer the AP mode settings→ Advance Setting for details.</td></tr>
<tr><td><b>AP MAC address</b></td><td>Enter 12 digits in hex numbers in the AP MAC address (<b>BSSID</b>) field and press the Add MAC Address Button to associate with other's Wireless access point.
Before you want to use bridge mode to connect each other to provide
A wireless bridge between 2 remote LANs, you need add the BSSID of other's wireless AP first.</td></tr>
<tr><td><b>Site Survey</b></td><td>Site survey displays all the active Access Points and IBSS in the neighborhood. Press Site Survey button to search the wireless device.

Wireless Site Survey
<table>
<tr><th>SSID</th><th>BSSID</th><th>Channel</th><th>Type</th><th>Encrypt</th><th>Signal</th></tr>
<tr><td>PLANET</td><td>00:18:e7:11:43:d6</td><td>11 (B+G)</td><td>AP</td><td>WEP</td><td>26</td></tr>
<tr><td>default</td><td>00:c0:02:fe:d3:68</td><td>10 (B+G)</td><td>AP</td><td>no</td><td>18</td></tr>
<tr><td>wlan</td><td>00:20:e0:39:a1:bb</td><td>3 (B)</td><td>AP</td><td>WEP</td><td>16</td></tr>
</table>
</td></tr>
<tr><td><b>Add MAC Address</b></td><td>Enter MAC address of remote access point.</td></tr>
<tr><td><b>Reset</b></td><td>Press to discard the data you have entered since last time you press Apply Change.</td></tr>
<tr><td><b>Show Statistics</b></td><td>List all packets information of traffic.</td></tr>
<tr><td><b>Delete Selected</b></td><td>To delete bridge from access to this Access Point, you may firstly check the <b>Select</b> checkbox next to the MAC address and Comments, and press <b>Delete Selected</b>.</td></tr>
<tr><td><b>Delete All</b></td><td>To delete all the clients from access to this Access Point, just press <b>Delete All</b> without selecting the checkbox.</td></tr>
</table>

WDS Mode Setting



This page is used to setup different wireless mode.

WDS Repeater Mode Settings

Alias Name: Wireless_AP

□ Disable Wireless LAN Interface

Band: 2.4 GHz (B+G)

SSID: airlive

Channel Number: 13

Wireless Client Isolation: Disabled

802.1d Spanning Tree: Disabled

Security: Setup

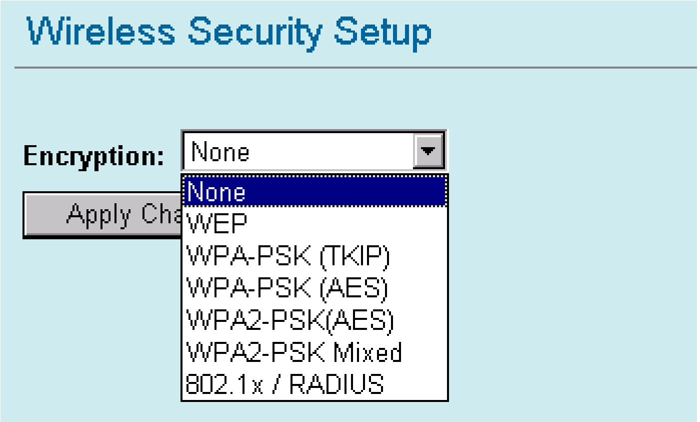
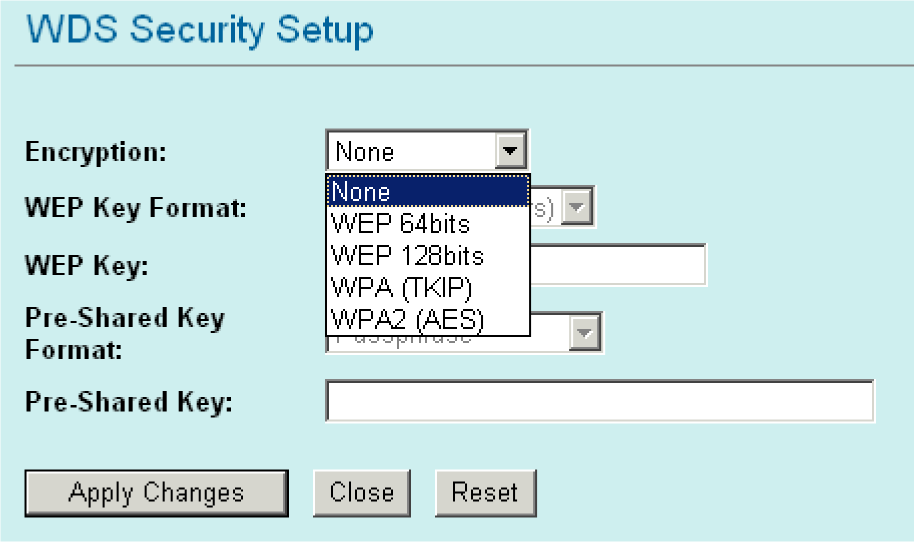
WDS Security: Setup

Advanced Settings: Setup

Access Control: Setup

Apply Changes | Reset

Alias Name	You can set the alias name for this device. limited not exceed 32 characters.
□ **Disable Wireless LAN Interface**	Check the box to disable the Wireless LAN Interface, by so doing, you won't be able to make wireless connection with this Access Point in the network you are located. In other words, this device will not be visible by any wireless station.
Band	You can choose one mode of the following you need. ⊙ 2.4GHz **(B):** 802.11b supported rate only. ⊙ 2.4GHz **(G):** 802.11g supported rate only. ⊙ 2.4GHz **(B+G):** 802.11b supported rate and 802.11g supported rate. The default is 2.4GHz **(B+G)** mode.
SSID	The SSID differentiates one WLAN from another; therefore, all access points and all devices attempting to connect to a specific WLAN must use the same SSID. It is case-sensitive and must not exceed 32 characters. A device will not be permitted to join the BSS unless it can provide the unique SSID. An SSID is also referred to as a network name because essentially it is a name that identifies a wireless network
Channel Number	The number of channels supported depends on the region of this Access Point. All stations communicating with the Access Point must use the same channel.
Wireless Client Isolation	When enabled, the wireless clients are separated from each other. Please refer the AP mode settings→ Wireless Client Isolation for details.

Security	Please refer the AP mode settings→ Security for details, This setting is use between Wireless client and this device.  Wireless Security Setup Encryption: None None WEP WPA-PSK (TKIP) WPA-PSK (AES) WPA2-PSK(AES) WPA2-PSK Mixed 802.1x / RADIUS Apply Cha
WDS Security	Please refer to the Bridge mode settings → WDS Security for details This setting is use between both wireless AP/Router devices.  WDS Security Setup Encryption: None WEP Key Format: WEP Key: Pre-Shared Key Format: Pre-Shared Key: None WEP 64bits WEP 128bits WPA (TKIP) WPA2 (AES) Apply Changes Close Reset
Advance Setting	Please refer the AP mode settings→ Advance Setting for details.
Access Control	Please refer the AP mode setting → Access Control for details.
AP MAC Address	Enter 12 digits in hex numbers in the AP MAC address (**BSSID**) field and press the Add MAC Address Button to associate with other's Wireless access point. Before you want to use bridge mode to connect each other to provide A wireless bridge between 2 remote LANs, you need add the BSSID of other's wireless AP first.
Delete Selected	To delete bridge from access to this Access Point, you may firstly check the **Select** checkbox next to the MAC address and Comments, and press **Delete Selected**.
Delete All	To delete all the clients from access to this Access Point, just press **Delete All** without selecting the checkbox.