Air Live®

Powered by OvisLink Corp.

# G.DUO

Dual 11g Access Point

# User's Manual

## Copyright & Disclaimer

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

# Regulatory Information

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

# IMPORTANT NOTE

## FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

All Trademarks are properties of their respective holders.

# Table of Contents

# 1 Introduction

## 1.1 Overview

The G.DUO is a dual radio wireless multi-function device based on IEEE 802.11g/b 2.4GHz radio technologies. It features 2 WiFi radios for WISP and other applications that can not be achieved using single radio. In addition, it features passive PoE port for installations in places that have no nearby access to electricity (DC Injector is not included). Finally, it also comes with a WAN port and Gateway+AP mode that can turn G.DUO into a wireless router with 2 radios.

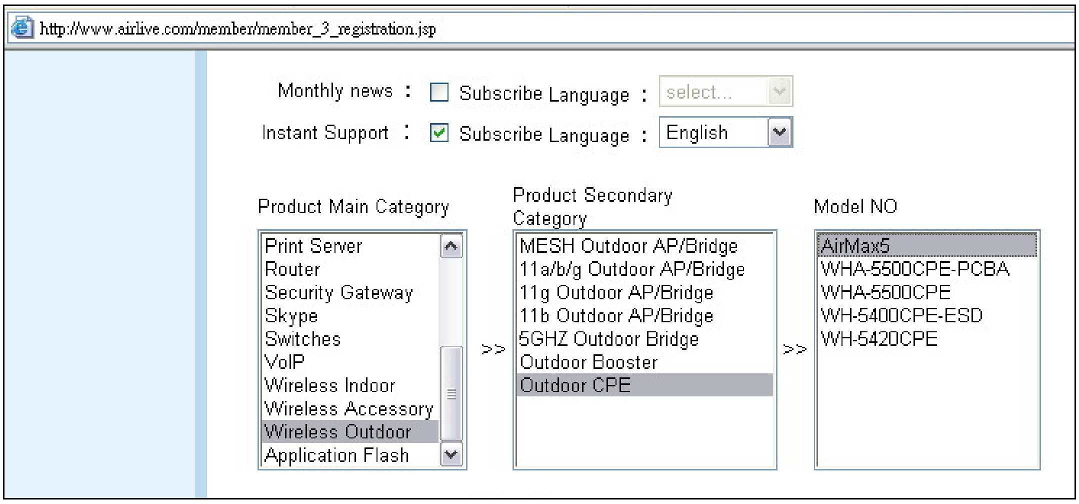
***If you encounter any technical issues, we strongly recommend you read through Chapter 12: Frequent Asked Questions. The answers you need are very likely to be there.***

## 1.2 Firmware Upgrade and Tech Support

If you encounter a technical issue that can not be resolved by information on this guide, we recommend that you visit our comprehensive website support at www.airlive.com. The tech support FAQ are frequently updated with latest information.

In addition, you might find new firmwares that either increase software functions or provide bug fixes for G.DUO. You can reach our on-line support center at the following link: http://www.airlive.com/support/support_2.jsp

Since 2009, AirLive has added the "Newsletter Instant Support System" on our website. AirLive Newsletter subscribers receives instant email notifications when there are new download or tech support FAQ updates for their subscribed airlive models. To become an AirLive newsletter member, please visit: http://www.airlive.com/member/member_3.jsp



http://www.airlive.com/member/member_3_registration.jsp

Monthly news : □ Subscribe Language : select...

Instant Support : ☑ Subscribe Language : English

Product Main Category: Wireless Outdoor

Product Secondary Category: Outdoor CPE

Model NO: AirMax5

## 1.3 Features

- Dual 11g CPU with 2 x 11g/b Radios
- 4MB Flash and 32MB SDRAM
- 5 wireless multi-function modes: WISP+AP, Dual AP, Client + AP, WDS+AP, Gateway+AP
- 2 x R-SMA connectors for external antenna.
- Passive PoE Port for 12V Passive POE System. Passive DC Injector not included
- 1 x WAN port for xDSL and Cable Modem.
- Wall Mount holes included
- Bandwidth Control
- Site Survey and Signal Strength indicator for antenna alignment
- Emergency firmware recovery mode
- Web, HTTPS, SSH/SSH2, Telnet, and SNMP managements

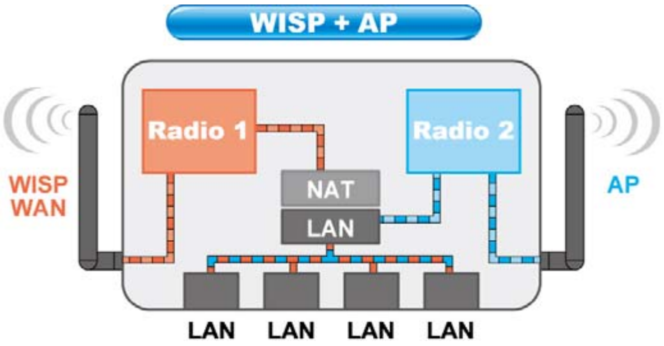
## 1.4 Wireless Operation Modes

The G.DUO can perform as a multi-function wireless device. Through the AirLogic web interface, users can easily select which wireless mode they wish the G.DUO to perform.

The G.DUO can be configured to operate in the following wireless operation modes:

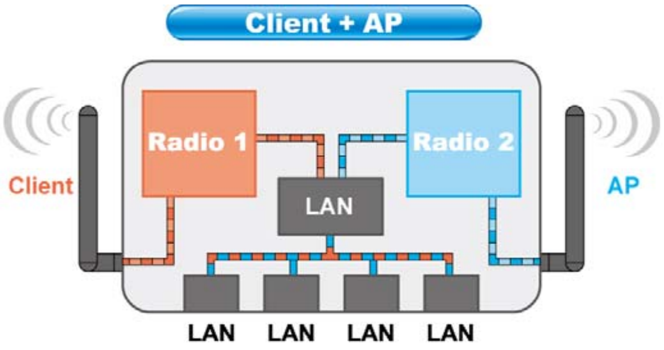
### 1.4.1 WISP + AP Mode

This mode is designed as 2-way wireless router for WISP subscriber. Radio1 acts as a client router to connect with outdoor AP; Radio1 works as a wireless AP for home. This combination allows WISP subscriber to share their Internet connection wirelessly.



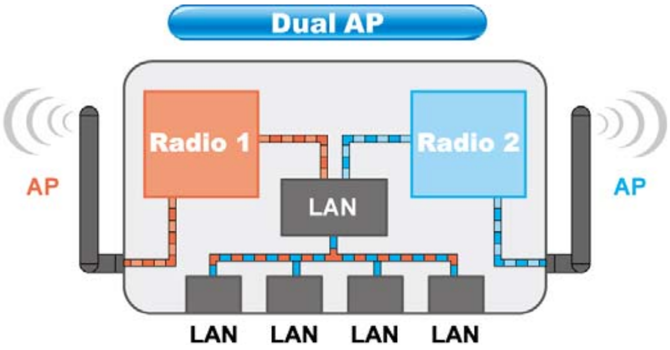
## 1.4.2 Client + AP mode

In this mode, Radio1 is working as a wireless client to connect with remote AP. Radio2 is working as an Access Point to redistribute the signal from Radio1. This combination creates a wireless repeater with 2 radios. It can be used to amplify the signal from remote AP.



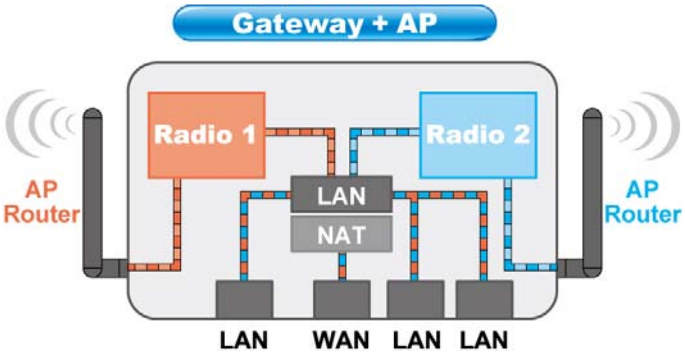
## 1.4.3 Dual AP Mode

In this mode, the G.DUO works as 2 Access Points. You can have both radios with directional antennas to create a larger coverage. *Please remember to set the channels of the radios as far apart as possible.*



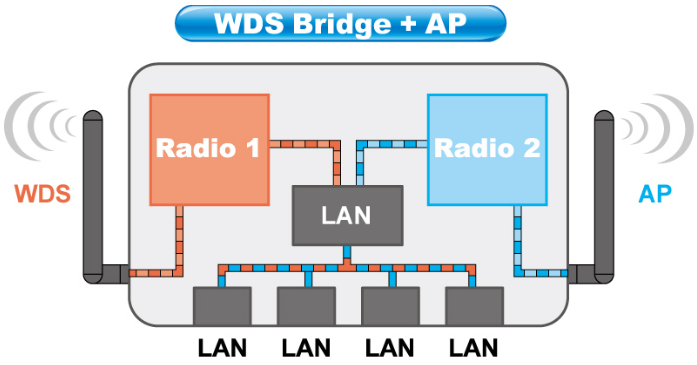
## 1.4.4 Gateway + AP

In this mode, both Radios are acting as wireless router. The WAN port is the LAN1 port. The application for this is to extend the wireless router's coverage. You can use 2 directional antennas to provide longer distance and wider coverage over large area, such as in the shopping center. When using this mode, it is recommended to use directional antennas for both radios to avoid mutual interference.



### 1.4.5 WDS + AP

In this mode, the Radio1 is working in WDS Bridge mode while Radio2 works as an Access Point. This mode is design to build a wireless backbone network while providing hotspot access through Radio2's AP network. It is ideal for Hotel Installation. When using this mode, please make sure that the channels are set apart between Radio1 and Radio2. Radio1 should install with directional antenna.



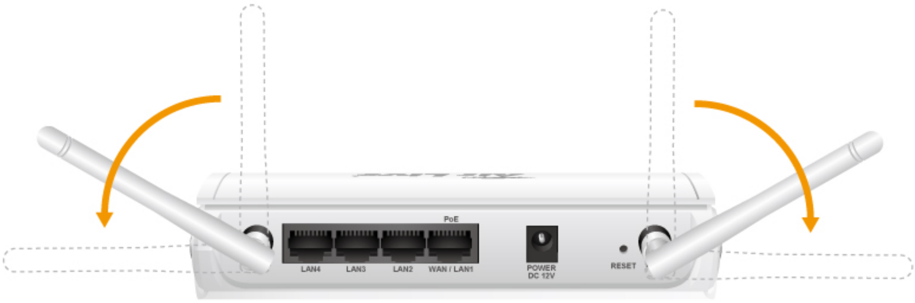
# 2 Installing the G.DUO

This section describes the hardware features and the hardware installation procedure for the G.DUO.   For software configuration, please go to chapter 3 for more details.

## 2.1 Before You Start

It is important to read through this section before you install the G.DUO

- It is recommended that you set the channels of the 2 radios as apart as possible to avoid mutual interference.   For example, Radio1 at channel 1 and Radio2 at Channel 11
- It is recommended that you adjust the antenna angles to get the best performance.   You can try to move the antenna outward as indicated on the diagram below if you encounter poor performance problem.



- The LAN1 port also work as the passive POE port and the WAN port(Gateway mode only)
- The passive PoE DC Injector is optional, it is not included with the package. Please use a 12V passive POE system with G.DUO's passive POE port.   Do not use 802.3af 48V system or PoE switch with the device.

## 2.2 Package Content

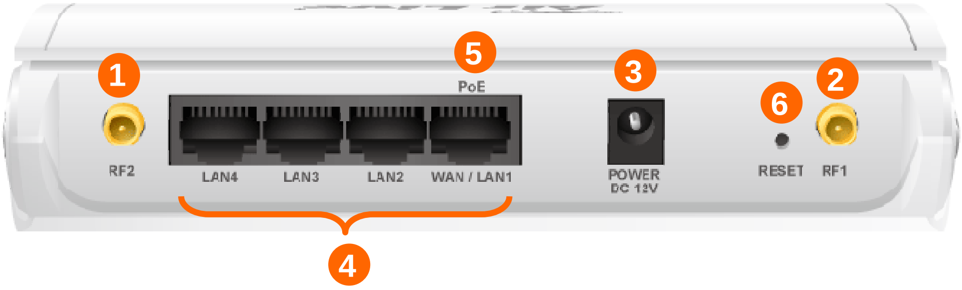
The G.DUO package contains the following items:

- One G.DUO main unit
- One 12V 1A DC power adapter
- 2 x Antennas (subject to change without notice)
- User's Guide CD

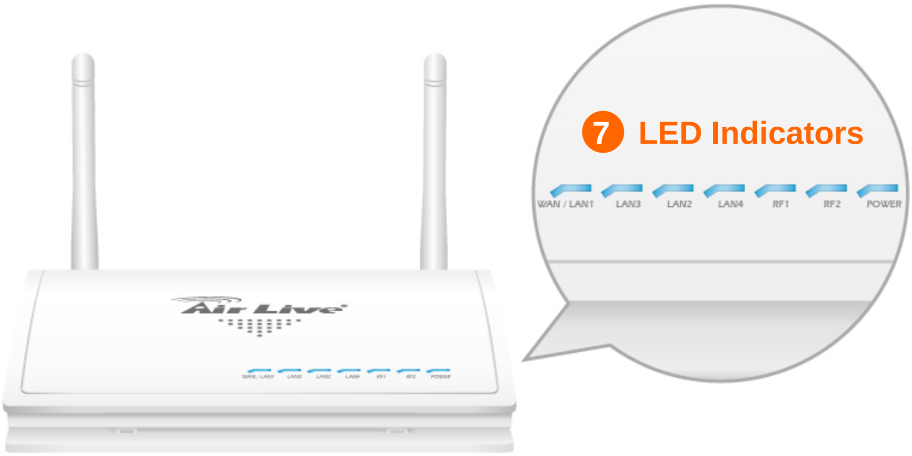
- Quick Start Guide

## 2.3 Knowing your G.DUO

Below are descriptions and diagrams of the product:

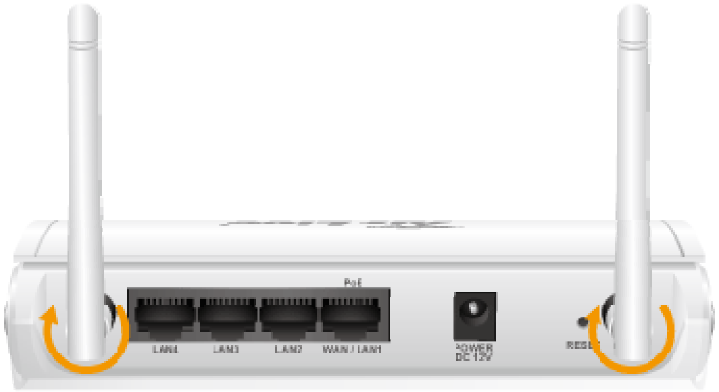


1 Radio 1 Antenna Connector
2 Radio 2 Antenna Connector
3 Power Adapter Connector
4 LAN Ports
5 WAN + Passive PoE Port
6 Reset Button

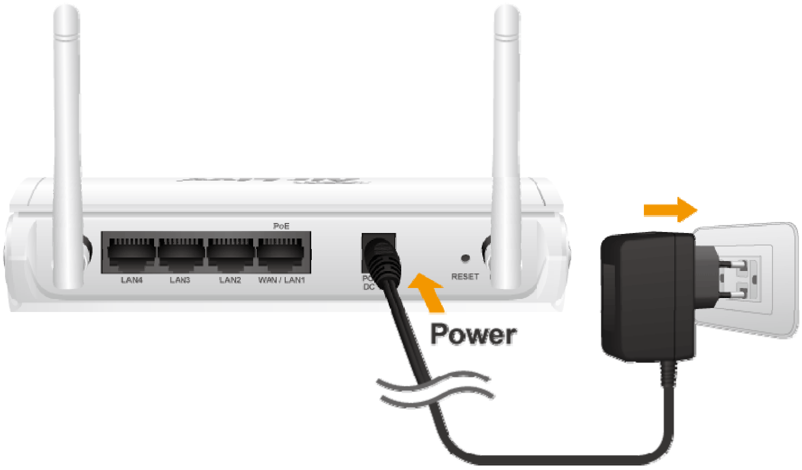


## 2.4 Hardware Installation

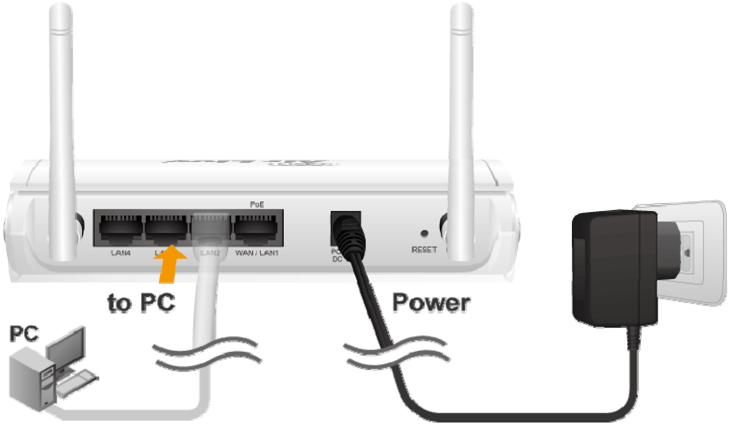
.1. Please install the antennas by turning clock wise into the RF1 and RF2 antenna connectors



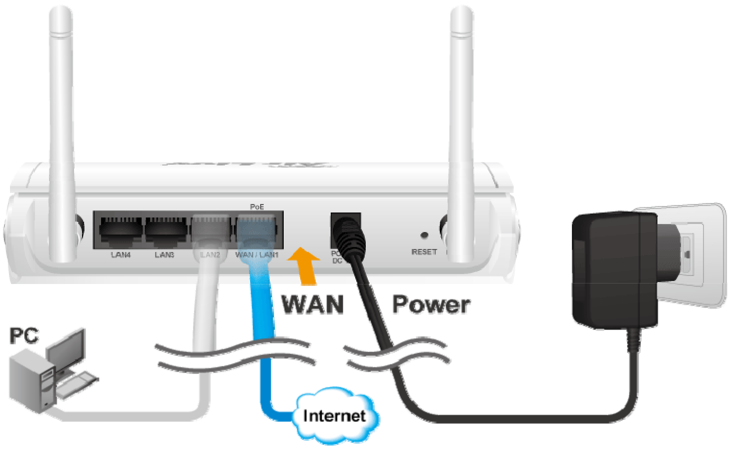
2. Now connect the power adapter to the G.DUO



3. Connect the Ethernet cable to one of the LAN port and the other end to your PC.

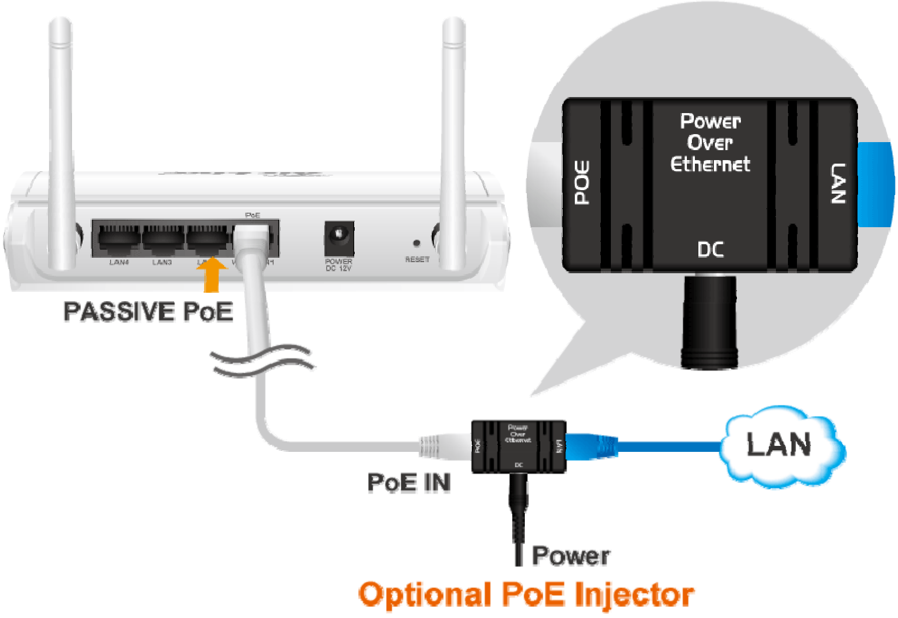


4. If you are using G.DUO in Gateway mode to share your xDSL or Cable modem connection, please connect the Internet cable to "WAN port".

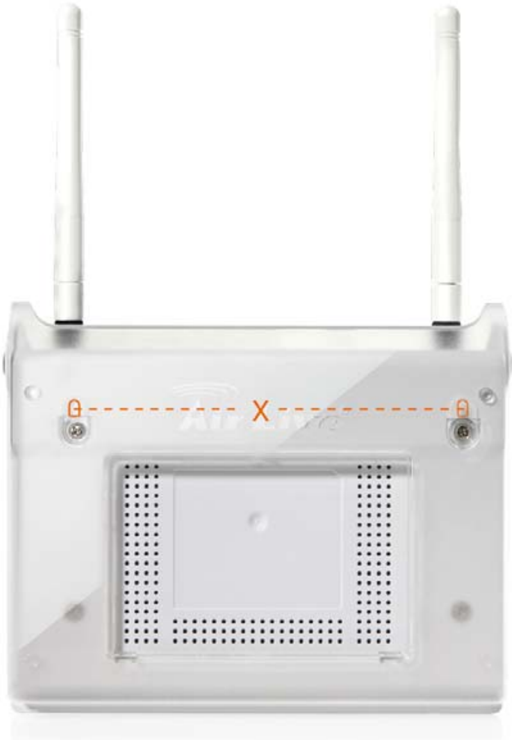
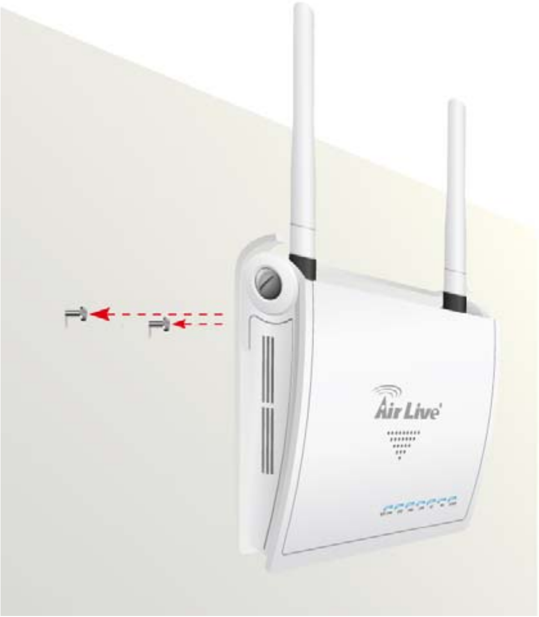


## 2.4.1 Passive PoE Installation

If you want to supply the power by using Passive PoE, please follow the installation diagram below. Please note that that the passive DC Injector is not included with G.DUO, it need to be purchased separately. G.DUO uses 12V passive PoE system.

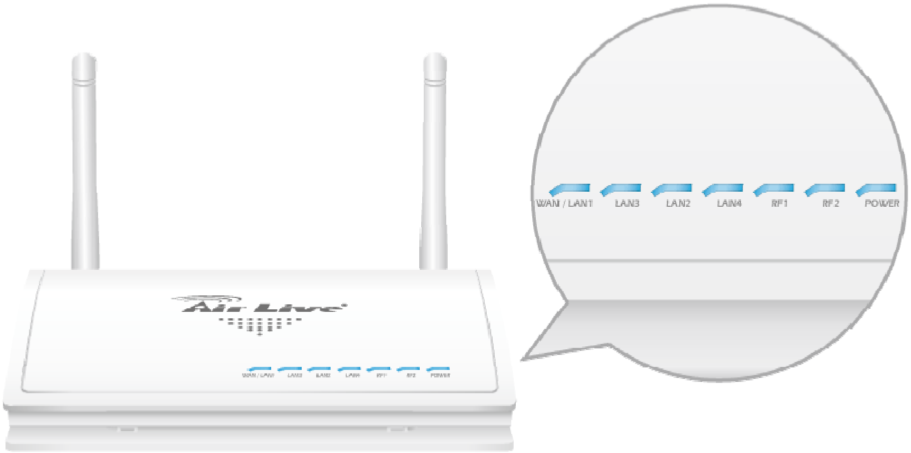


## 2.4.2 Wall Mount Installation

| |
|---|
| **1.** The holes for the wall mount screw are on the underside of the case. Please measure the distance between the holes. Then install 2 screws in the desire location with the measured distance apart from each other. Please do not screw all the way in, leave some space for mounting with the G.DUO |
|  |
| **2.** Now please hang the G.DUO on those 2 screws. |
|  |

## 2.5 LED Table

This section describes the LED behavior of G.DUO.  You can find the LED on the top side of the G.DUO.



**Power**

○ Steady Blue – Normal Operation<br>
● OFF – No Power

**RF1, RF2**

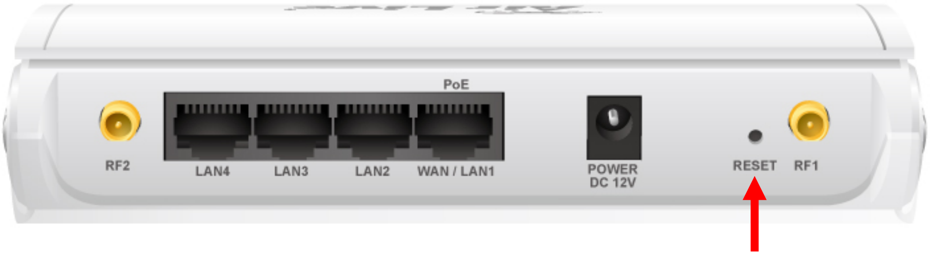
○ Slow Flashing :   Radio is active<br>
◐ Fast Flashing:   Transmitting Data<br>
● OFF:  Radio Disabled

**LAN1 ~4, WAN**

○ Steady Blue :   Link established<br>
◐ Fast Flashing:   Transmitting Data<br>
● OFF:  No Link

## 2.6 Restore Settings to Default

If you have forgotten your G.DUO's IP address or password, you can restore your G.DUO to the default settings by pressing on the "reset button" for more than 5 seconds.  You might need a pen or pencil for this operation.  The reset button is inside the bottom case. Please see diagram below for details.



# 3 Configuring the G.DUO

The G.DUO offers many different types of management interface. You can configure through standard web browser (http), secured web (https), command line (telnet), secured command shell (SSH), and SNMP management. In this chapter, we will explain G.DUO's available management interfaces and how to get into them.

## 3.1 Important Information

The following information will help you to get start quickly. However, we recommend you to read through the entire manual before you start. Please note the password and SSID are case sensitive.

- ❑ The default IP address is: 192.168.1.254 Subnet Mask: 255.255.255.0
- ❑ There is no password protection by default. To enable password protection, please go to "System Configuration -> Password Settings".
- ❑ The default SSID for Radio1 is "airlive1"
- ❑ The default SSID for Radio2 is "airlive2"
- ❑ The default wireless mode is : WISP + AP mode
- ❑ Please remember to "Apply Change" for settings to be saved and take effect.
- ❑ Please remember to "Reboot" the device after all settings are changed.
- ❑ Please keep the TX output power as low as possible for best performance.
- ❑ By default, the Telnet and SSH functions are turned off. To enable them, please go to "System Configuration" -> "System Management" menu.
- ❑ The Emergency Firmware Recovery only works when you connect to LAN2, LAN3, or LAN4 port. It will not work on LAN1
- ❑ By Default, the DHCP server is turned on in WISP+AP and Gateway+AP mode. The other modes' DHCP server are turned off.
- ❑ When you change the mode to WISP+AP or Gateway+AP mode, the GDUO's IP address might change to 192.168.1.254.

.

## 3.2 Prepare your PC

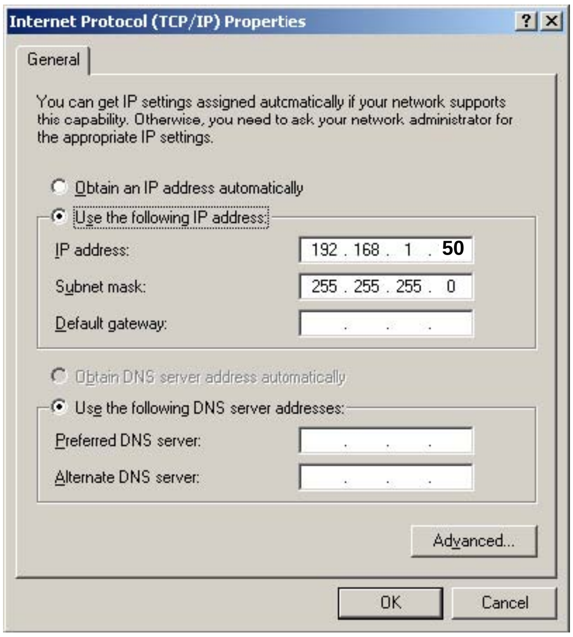
The G.DUO can be managed remotely by a PC through either the wired or wireless network. The default IP address of the G.DUO is **192.168.1.254** with a *subnet mask* of 255.255.255.0. This means the IP address of the PC should be in the range of 192.168.1.1` to 192.168.1.253.

To prepare your PC for management with the G.DUO, please do the following:

**1.** Connect your PC directly to the LAN port on the DC Injector of G.DUO

**2.** Set your PC's IP address to "Obtain an IP address Automatically". The G.DUO should provide your PC an valid IP address.

**3.** If you want to set your PC's IP address manually, please set to 192.168.1.50 (or other address in the same subnet)



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned autcmatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 50
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

You are ready now to configure the G.DUO using your PC.

## 3.3 Management Interface

The G.DUO can be configured using one the management interfaces below:

- **Web Management (HTTP):** You can manage G.DUO by simply typing its IP address in the web browser. Most functions of G.DUO can be accessed by web management interface. We recommend using this interface for initial configurations. To begin, simply enter G.DUO's IP address (default is 192.168.1.254) on the web browser..

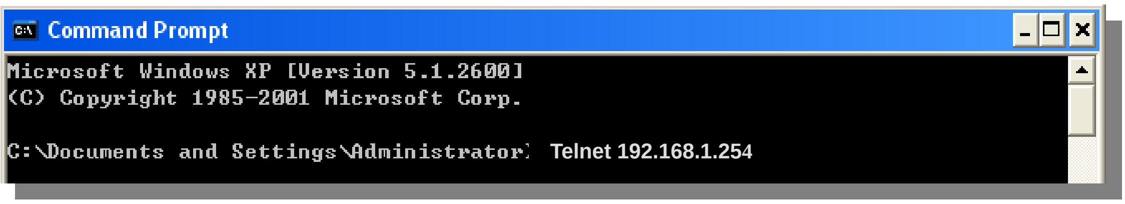
- **Secured Web Management (HTTPS):** HTTPS is also using web browser for configuration. But all the data transactions are securely encrypted using SSL encryption. Therefore, it is a safe and easy way to manage your G.DUO. We highly recommend WISP and service provider to use HTTPS for management.

  To begin, simply enter https://192.168.1.254 on your web browser. A security alert screen from your browser might pop up. Please grant all permission and get certificate to G.DUO.

- **Command Line Interface (Telnet):** G.DUO can be managed through the command line interface (CLI). Telnet does not encrypt its message. Therefore, it is not secure. The default Telnet management port is TCP port 23.

  ***By default, the G.DUO's Telnet interface is turned off.*** To enable it, please go to "System Configuration -> System Management" menu and enable "Telnet".

  To use the CLI, please open the command line window. Then type "telnet 192.168.1.254" to start.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator] Telnet 192.168.1.254
```

To get a list of available command and their usage, please type "help" on the command prompt.

- **Secure Shell (SSH, SSH2)**: SSH is an encrypted Command Line Interface that allow user to send text commands through SSL encryption. Therefore, it provides the added advantage of security comparing to Telnet. The default management port for SSH/SSH2 is TCP/UDP port 22.

  ***By default, the G.DUO's SSH/SSH2 interface is turned off.*** To enable it, please go to "System Configuration -> System Management" menu and enable "SSH".

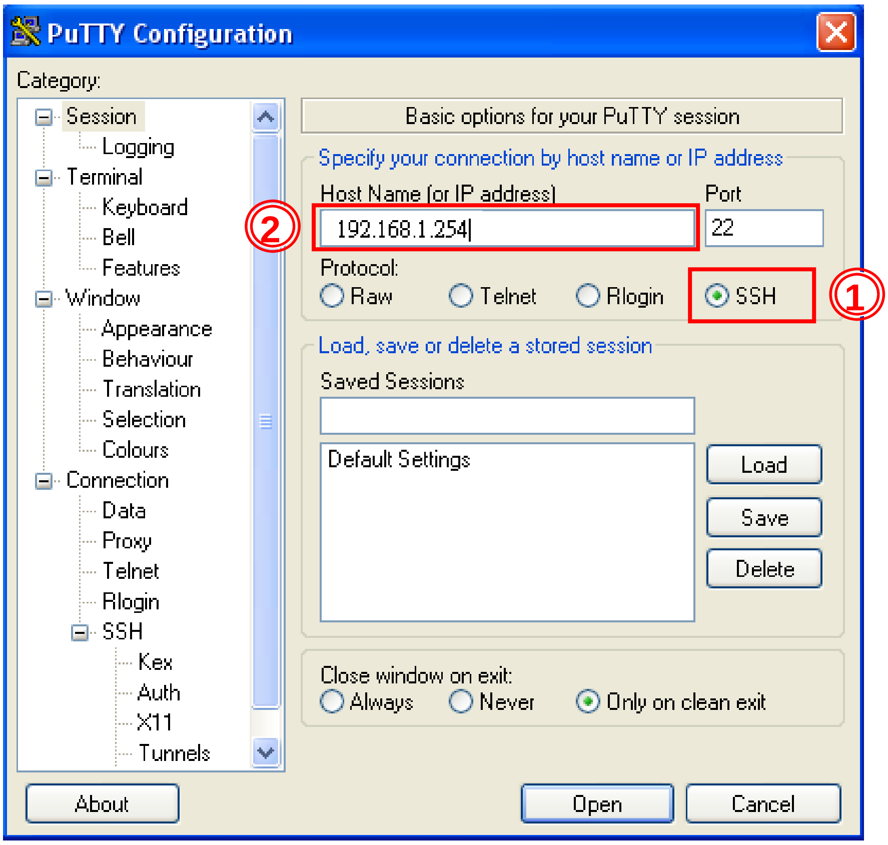
  To manage via the SSH/SSH2 protocol, you would need a SSH client. Free SSH clients are widely available on the Internet. You can find where to download them by using Internet search engine such as Google. In this guide, we will use a popular SSH/Telnet utility call Putty.

  Once you have download and install Putty. Please follow the figure below to make a connection with G.DUO:

  **1.** Choose "SSH" as indicated in the diagram

**2.** Enter the IP address of G.DUO

**3.** Click on "Open" to start the SSH session.



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.1.254

Port: 22

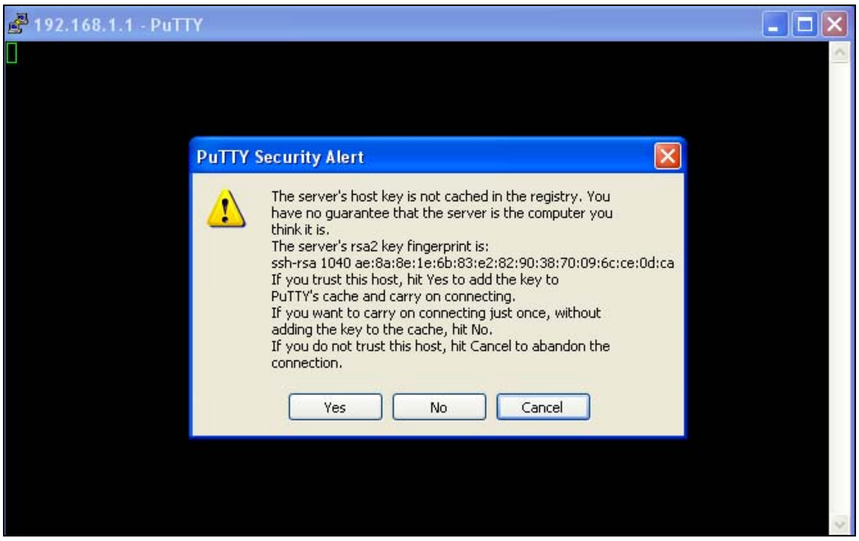
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

When the following screen appear, click on "Yes" to continue



192.168.1.1 - PuTTY

PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1040 ae:8a:8e:1e:6b:83:e2:82:90:38:70:09:6c:ce:0d:ca
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

If you have set up password, please enter your login and password. If not, you will enter the command prompt directly. Now you are ready to enter commands

To get a list of available command and their usage, please type "help" on the command prompt.

## 3.4 Introduction to Web Management

The G.DUO offers both normal (http) and secured (https) Web Management interfaces. Their share the same interface and functions, and they can both be accessed through web browsers. The only difference is HTTPS data are encrypted for extra security. Therefore, we will discuss them together as “Web Management” on this guide.

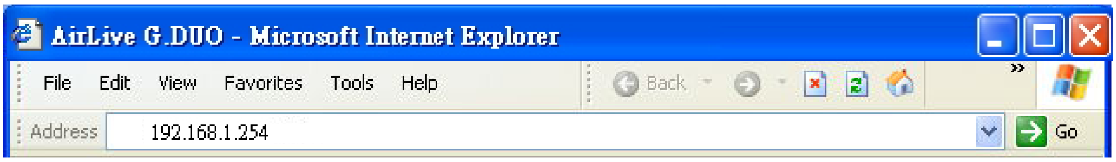
If you are placing the G.DUO behind router or firewall, you might need to open virtual server ports to G.DUO on your firewall/router

- HTTP: TCP Port 80
- HTTPS: TCP/UDP Port 443

This procedure is not necessary in most cases unless there is a router/firewall between your PC and G.DUO.

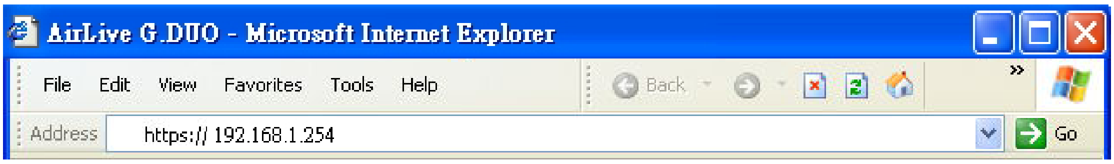
### 3.4.1 Getting into Web Management

**Normal Web Management (HTTP)**
To get into the Normal Web Management, simply type in the G.DUO’s IP address (default IP is 192.168.1.254) into the web browser’s address field.



Address 192.168.1.254

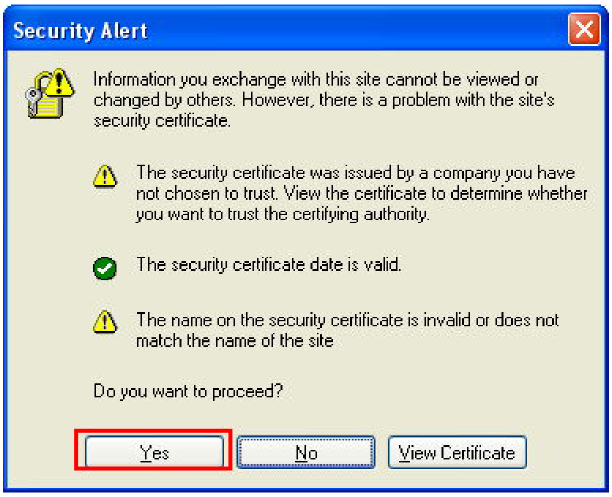
**Secured Web Management (HTTPS)**
To get into the Secured Web Management, just type “https://192.168.1.254 ” into the web browser’s address field. The “192.168.1.254” is G.DUO’s default IP address. If the IP address is changed, the address entered in the browser should change also.



Address https:// 192.168.1.254

A security warning screen from your browser will then pop-up depending on the browser you use. Please follow step below to clear the security screen.

- ❑ Internet Explorer: Select “Yes” to proceed



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

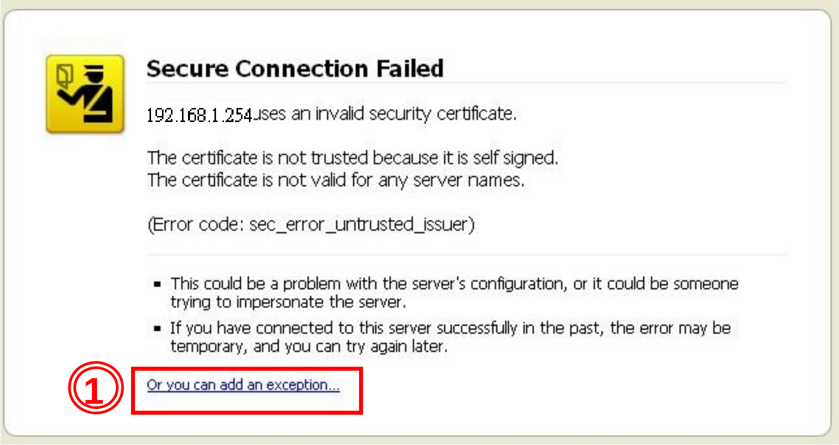
The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

- ❑ Firefox:

1. Select "or you can add an exception"



Secure Connection Failed

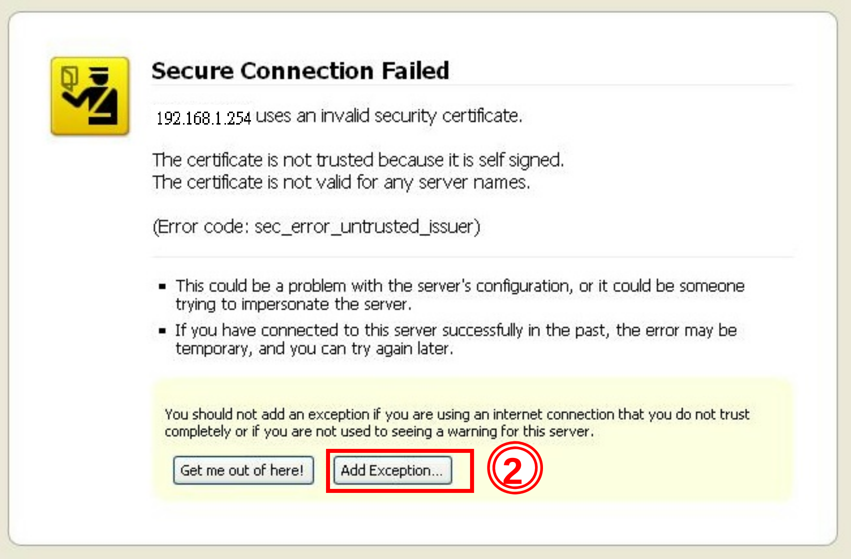
192.168.1.254 uses an invalid security certificate.

The certificate is not trusted because it is self signed.
The certificate is not valid for any server names.

(Error code: sec_error_untrusted_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

2. Click on "Add Exception"



Secure Connection Failed

192.168.1.254 uses an invalid security certificate.

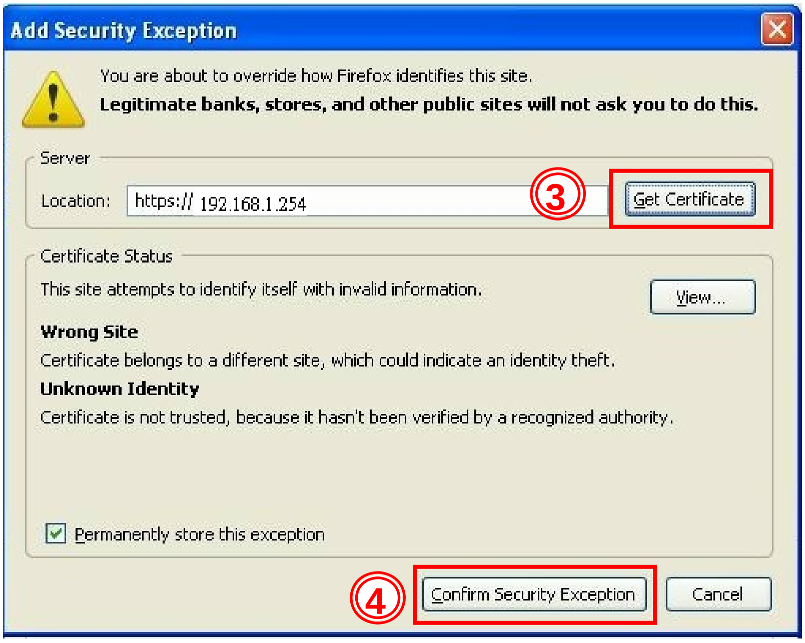
The certificate is not trusted because it is self signed.
The certificate is not valid for any server names.

(Error code: sec_error_untrusted_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

3. Click on “Get Certificate”. Then, please enter G.DUO’s IP address. Finally, please click on “Confirm Security Exception.”



Add Security Exception

You are about to override how Firefox identifies this site.

**Legitimate banks, stores, and other public sites will not ask you to do this.**

Server

Location: https:// 192.168.1.254

Certificate Status

This site attempts to identify itself with invalid information.

**Wrong Site**

Certificate belongs to a different site, which could indicate an identity theft.

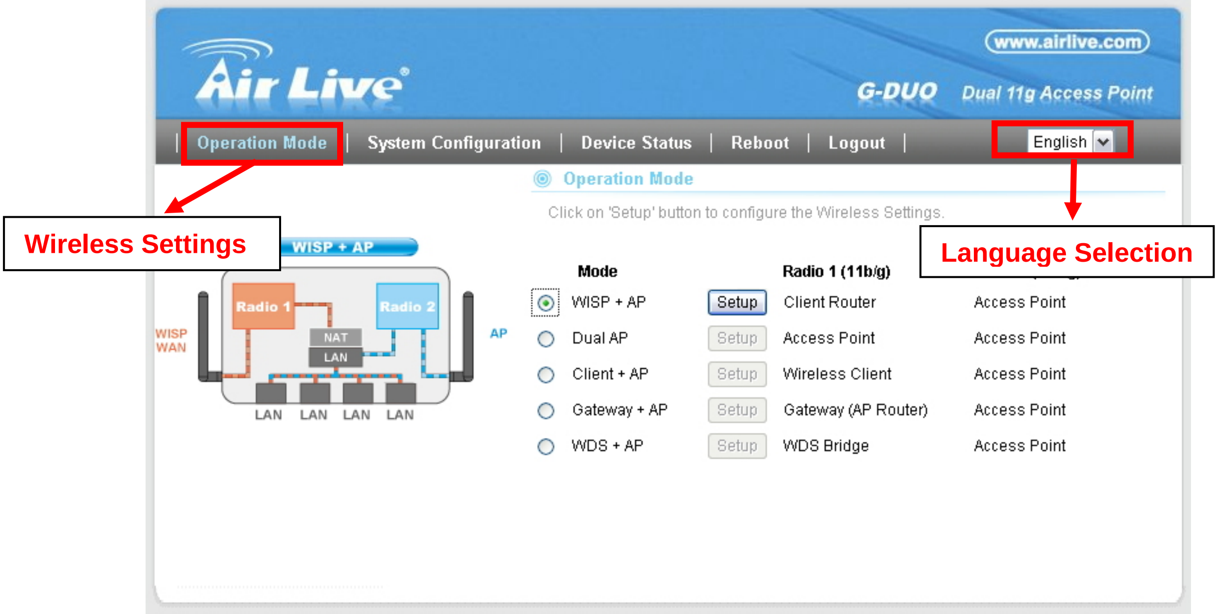
**Unknown Identity**

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

### 3.4.2 Web Menu Structure

After you enter the Web configuration, the following screen will appear:



Operation Mode

Click on 'Setup' button to configure the Wireless Settings.

| | Mode | | Radio 1 (11b/g) | |
|---|---|---|---|---|
| ● | WISP + AP | Setup | Client Router | Access Point |
| ○ | Dual AP | Setup | Access Point | Access Point |
| ○ | Client + AP | Setup | Wireless Client | Access Point |
| ○ | Gateway + AP | Setup | Gateway (AP Router) | Access Point |
| ○ | WDS + AP | Setup | WDS Bridge | Access Point |

- **Wireless Settings**: The G.DUO’s wireless settings are different between wireless modes. Only functions that are applicable to the wireless mode will show to simplify configuration. For this reason, the first step to configure the G.DUO is to select the wireless mode. The router mode specific functions are also in this menu category. For explanation of different wireless modes, please refer to Chapter 1.

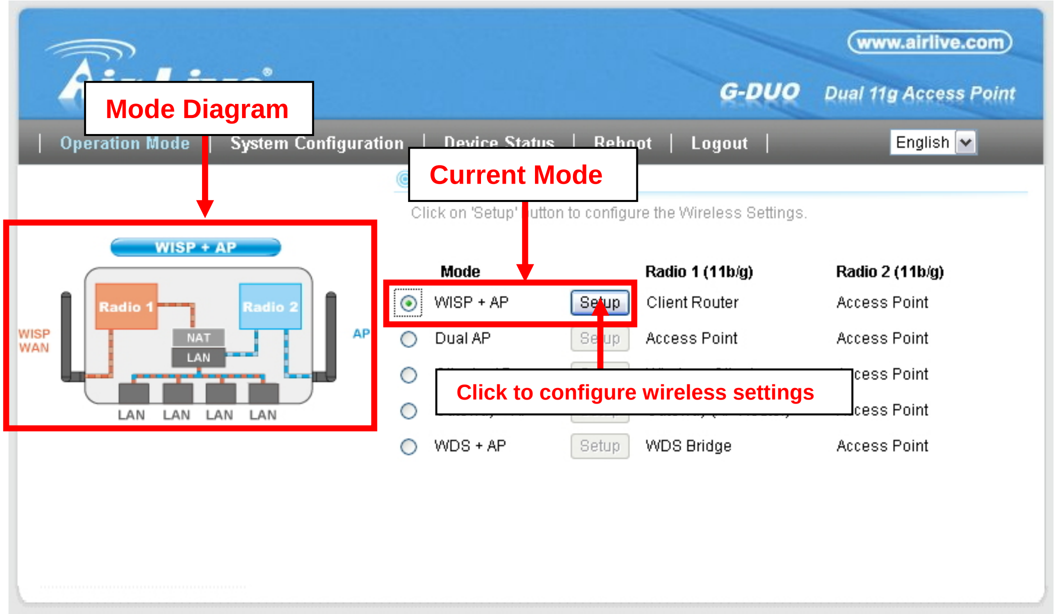
- **System Configuration:** All non-wireless and router mode settings are in this category. The system configurations including changing password, upload firmware, backup configuration, settings PING watchdog, and setting management interface. We recommend you should enable password protection during the first time login.
- **Device Status**: This section for monitoring the status of G.DUO. It provides information on device status, Ethernet status, wireless status, wireless client table, and system log.
- **Language Selection:** You can change the language for the Web interface from here.

## 3.5 Initial Configurations

We recommend users to browse through G.DUO's web management interface to get an overall picture of the functions and interface. Below are the recommended initial configurations for first time login:

### 3.5.1 Choose the wireless Operation Modes

The wireless settings of G.DUO are dependant on the wireless operation mode you choose. Therefore, the first step is to choose the operation mode. For explanation on when to use what operation mode, please refer to Chapter 1



Mode Diagram

Current Mode

Click on 'Setup' utton to configure the Wireless Settings.

| Mode | | Radio 1 (11b/g) | Radio 2 (11b/g) |
|---|---|---|---|
| ● WISP + AP | Setup | Client Router | Access Point |
| ○ Dual AP | Setup | Access Point | Access Point |
| ○ | | | cess Point |
| ○ | | | cess Point |
| ○ WDS + AP | Setup | WDS Bridge | Access Point |

Click to configure wireless settings

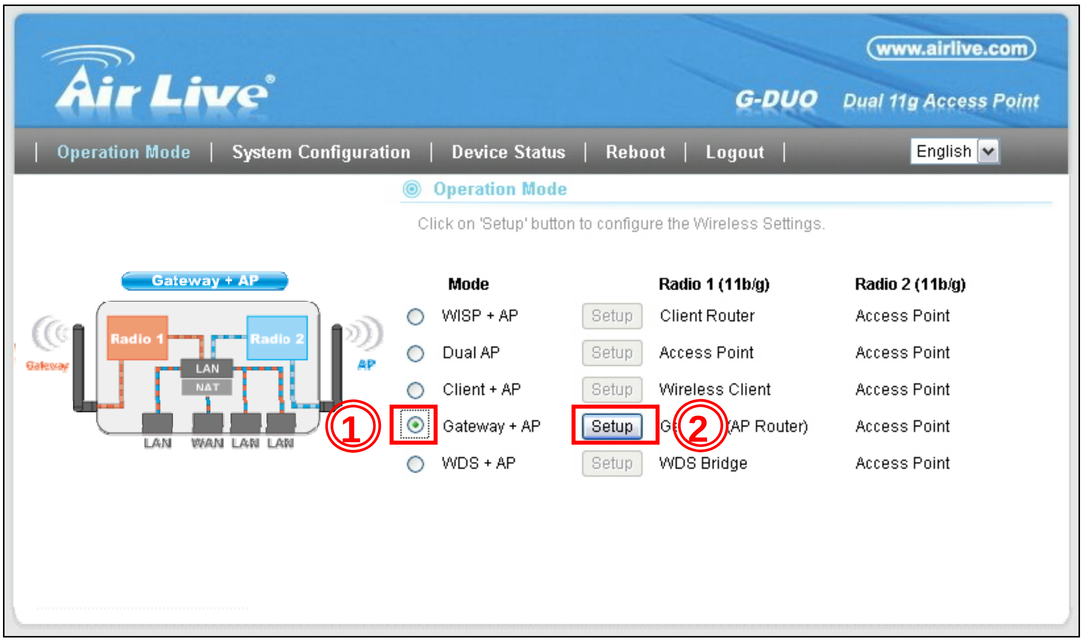
**Mode Diagram**: this shows you the operation flow between Radio1, Radio2, and the LAN/WAN ports. It helps you to understand how the mode works.

**Current Mode**: The active setup button indicates the current operation mode. When you press the “Setup Button”, it will bring you to the wireless setting page.

**Changing Mode**:

Follow the example below to change to “Gateway+AP” mode

1. Select “Gateway + AP” mode.
2. Click on “Setup Button” button
3. The AP might ask you to confirm the mode change. Once confirm, the AP will reboot to its new mode.


www.airlive.com
G-DUO Dual 11g Access Point
| Operation Mode | System Configuration | Device Status | Reboot | Logout |
English
Gateway + AP
Radio 1
Radio 2
LAN
NAT
Gateway
AP
LAN WAN LAN LAN
1
2

Operation Mode

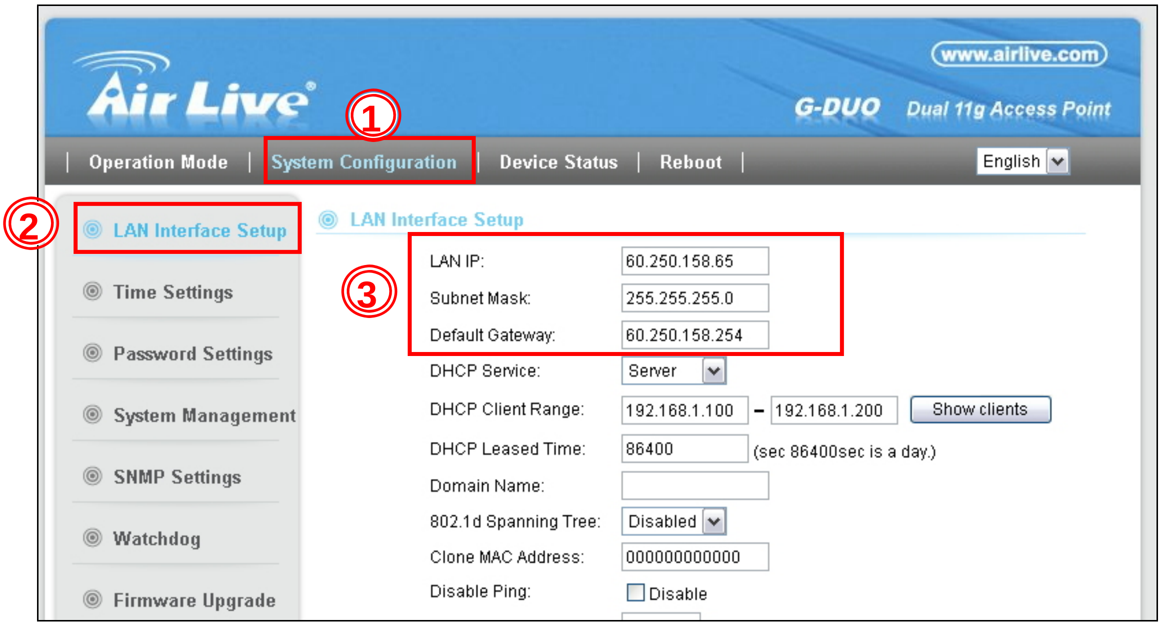
Click on 'Setup' button to configure the Wireless Settings.

| Mode | | Radio 1 (11b/g) | Radio 2 (11b/g) |
|---|---|---|---|
| ○ WISP + AP | Setup | Client Router | Access Point |
| ○ Dual AP | Setup | Access Point | Access Point |
| ○ Client + AP | Setup | Wireless Client | Access Point |
| ● Gateway + AP | Setup | G [illegible] (AP Router) | Access Point |
| ○ WDS + AP | Setup | WDS Bridge | Access Point |

## 3.5.2 Change the Device’s IP Address

The default IP address is at 192.168.1.254. You should change it to the same subnet as your network. Also, if you want to manage G.DUO remotely, you have to set the Gateway and DNS server information.

To setup the IP settings for G.DUO, please select “System Configuration” -> LAN Interface Setup”. After entering the IP information, click on “Apply” to finish.

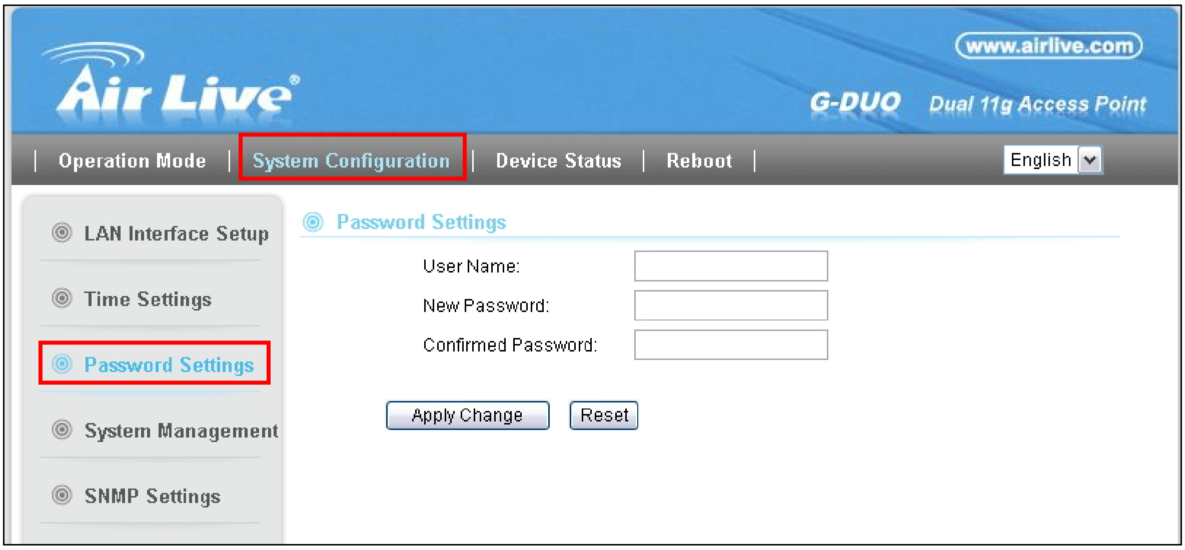


LAN Interface Setup

| | |
|---|---|
| LAN IP: | 60.250.158.65 |
| Subnet Mask: | 255.255.255.0 |
| Default Gateway: | 60.250.158.254 |
| DHCP Service: | Server |
| DHCP Client Range: | 192.168.1.100 – 192.168.1.200 |
| DHCP Leased Time: | 86400 (sec 86400sec is a day.) |
| Domain Name: | |
| 802.1d Spanning Tree: | Disabled |
| Clone MAC Address: | 000000000000 |
| Disable Ping: | □ Disable |

## 3.5.3 Enable Password Protection

The G.DUO's password protection is turned off by default. You should enable it and set your own password. To enable password protection, please go to *"System Configuration" -> "Password Settings"* menu. Then enter your username and password, and click on "Apply Change" button. You can also come to this menu to change your password in the future.

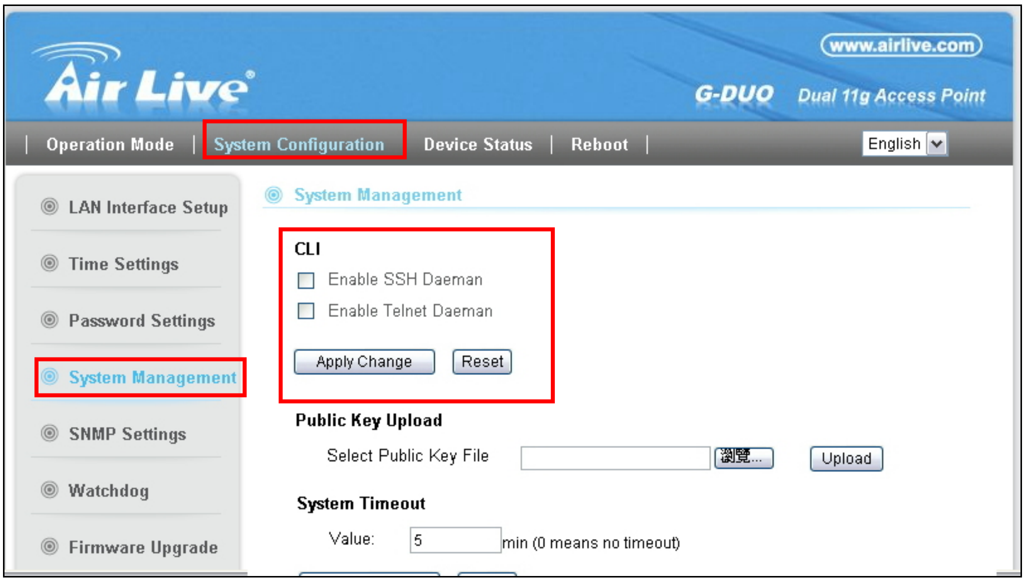


Password Settings

| | |
|---|---|
| User Name: | |
| New Password: | |
| Confirmed Password: | |

## 3.5.4 Enable Telnet or SSH

The Telnet and SSH management interface are turned off by default. If you wish to use them, please go to the "System Configuration -> System Management" menu. Check "Telnet" or "SSH", then click on "Apply Change" button.



System Management

CLI

□ Enable SSH Daeman

□ Enable Telnet Daeman

Apply Change | Reset

Public Key Upload

Select Public Key File [ ] 瀏覽... Upload

System Timeout

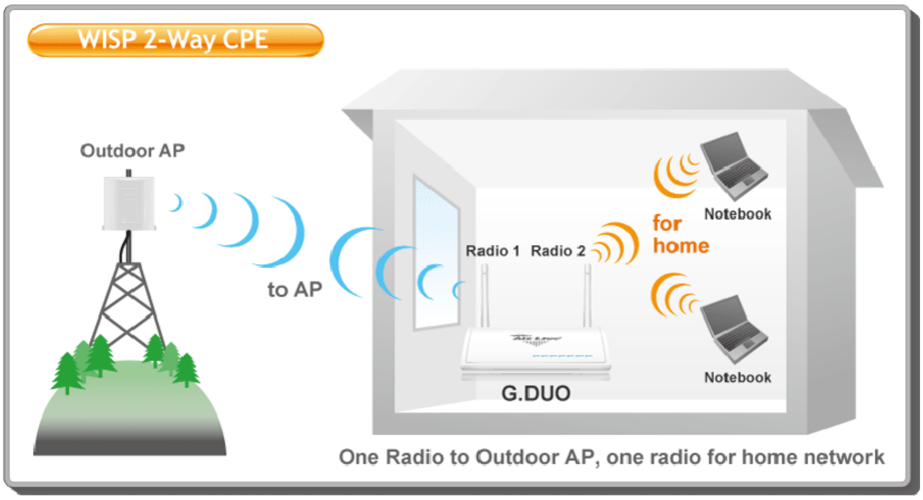
Value: 5 min (0 means no timeout)

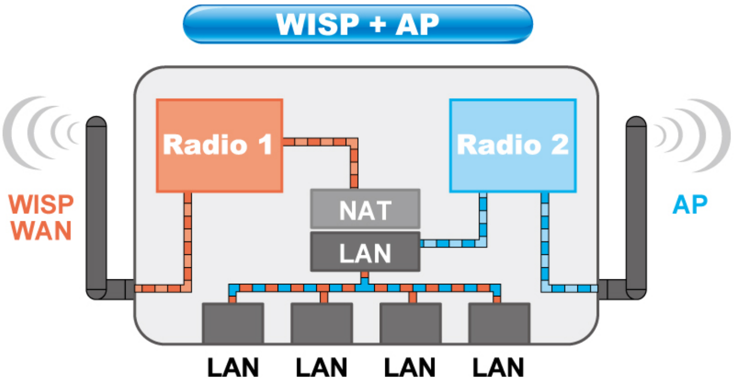
# 4 WISP + AP Mode

In this chapter, we will explain about the wireless settings for WISP+AP Mode. Please be sure to read through Chapter 1.4 and Chapter 3's "*Introduction to Web Management*" and *"Initial Configurations"* first.

## 4.1 Application for WISP+AP Mode

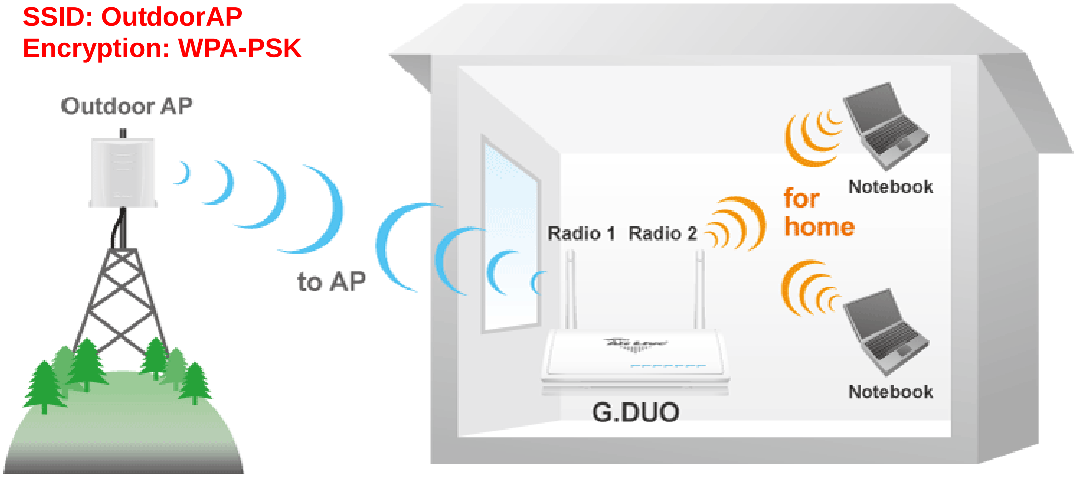
This mode is designed for WISP subscriber to have both Internet connection to WISP AP and wireless network for home. Radio1 acts as a client router to connect with outdoor AP; Radio1 works as a wireless AP for home. This combination allows WISP subscriber to share their Internet connection wirelessly. In this mode, the WAN on the Radio1 side.





## 4.2 Step-by-Step Example

In this example, we will use a G.DUO to establish a connection service to the WISP outdoor AP



### 4.2.1 Environment

In this example, the G.DUO will be connecting to the Outdoor AP using Radio1. Radio1 will be running in WISP mode which is also known as “Client Router”. Radio 2 will be running in AP mode to share the WISP connection wirelessly to the notebook PC.

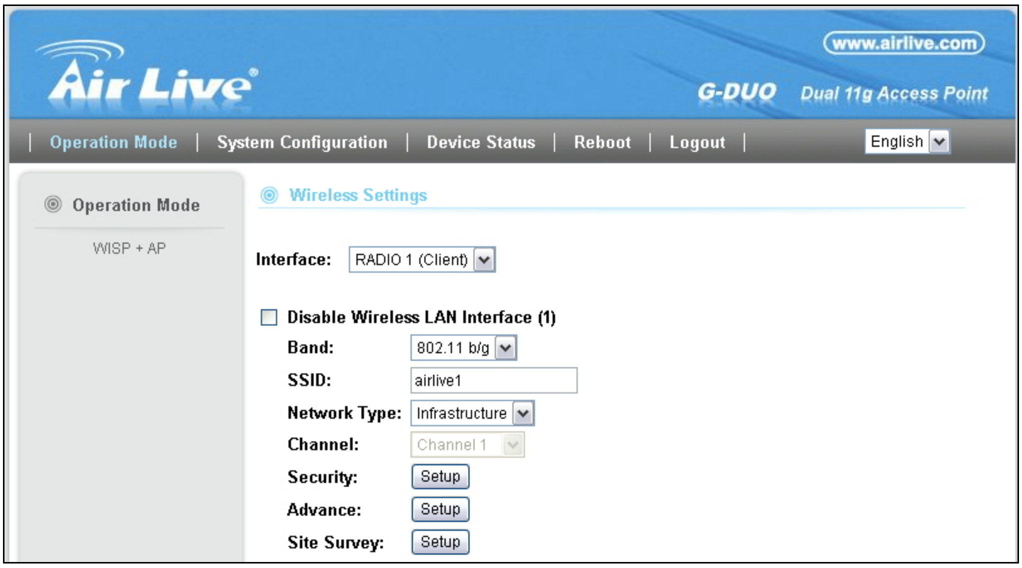
The configuration procedure should be as followed:

1. **Configure Radio1 first**.
2. Use “Site Survey” function to find the Outdoor AP and adjust antenna alignment using “Signal Survey” function
3. Use “Site Survey” to establish connection and enter encryption key with Outdoor AP
4. Configure the WAN type for the Radio1 to the Outdoor AP
5. Enable the “Remote Management” so WISP operator can manage the AP from remote
6. **Configure Radio2 now**
7. You should be able to keep default settings for most of the Radio2’s function
8. But you need to change the channel of Radio2 so it is as far apart from Radio1 as possible.
9. Set Encryption for Radio2.
10. You should be able to link the Notebook PC to “airlive2” SSID and enter the correct encryption key.

### 4.2.2 Configuration Steps

Radio1

**Step1:** Click on the wireless settings on WISP+AP mode. It should bring you to the "Wireless Setting" Page.



www.airlive.com
G-DUO Dual 11g Access Point
Operation Mode | System Configuration | Device Status | Reboot | Logout
English
Operation Mode
WISP + AP
Wireless Settings

Interface: RADIO 1 (Client)

□ Disable Wireless LAN Interface (1)

Band: 802.11 b/g

SSID: airlive1

Network Type: Infrastructure

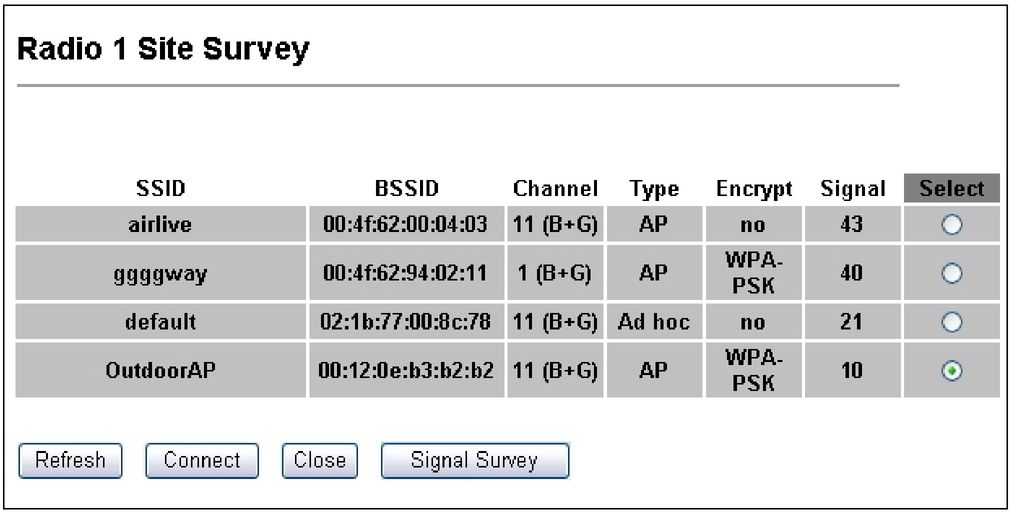
Channel: Channel 1

Security: Setup

Advance: Setup

Site Survey: Setup

**Step2:** Click on "Site Survey" Setup button. The following screen should appear with results of available APs in the area.



Radio 1 Site Survey

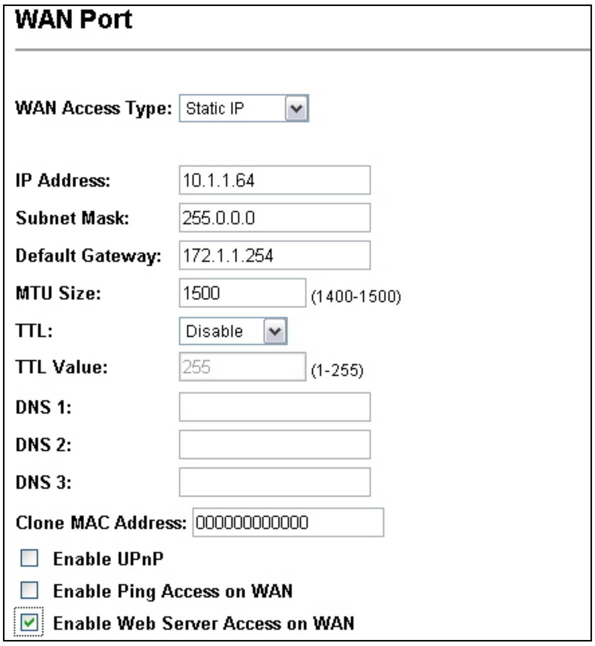
| SSID | BSSID | Channel | Type | Encrypt | Signal | Select |
|---|---|---|---|---|---|---|
| airlive | 00:4f:62:00:04:03 | 11 (B+G) | AP | no | 43 | ○ |
| ggggway | 00:4f:62:94:02:11 | 1 (B+G) | AP | WPA-PSK | 40 | ○ |
| default | 02:1b:77:00:8c:78 | 11 (B+G) | Ad hoc | no | 21 | ○ |
| OutdoorAP | 00:12:0e:b3:b2:b2 | 11 (B+G) | AP | WPA-PSK | 10 | ● |

**Step2:** Now select "Outdoor AP" on the list, then press "Signal Survey". Adjust your antenna until the signal level is at the highest.

**Step3**: Now close the window and go back to the "Site Survey" page. Select the "Outdoor AP" and press the "Connect" button. The G.DUO will inform you "encryption type mismatch!" and ask if you want to configure the encryption setting. Select "Yes" to proceed.

**Step4**: Choose “WPA”->”Personal(Pre Shared Key)” -> “TKIP”. Then enter the correct encryption key. The wireless connection should establish after this.

**Step5**: Go to the wireless setting page and select “WAN Port”. Enter the WAN information (in this example is “Static IP”) and check the “Enable Web Access on WAN” for remote management.



WAN Port

WAN Access Type: Static IP

IP Address: 10.1.1.64

Subnet Mask: 255.0.0.0

Default Gateway: 172.1.1.254

MTU Size: 1500 (1400-1500)

TTL: Disable

TTL Value: 255 (1-255)

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable UPnP

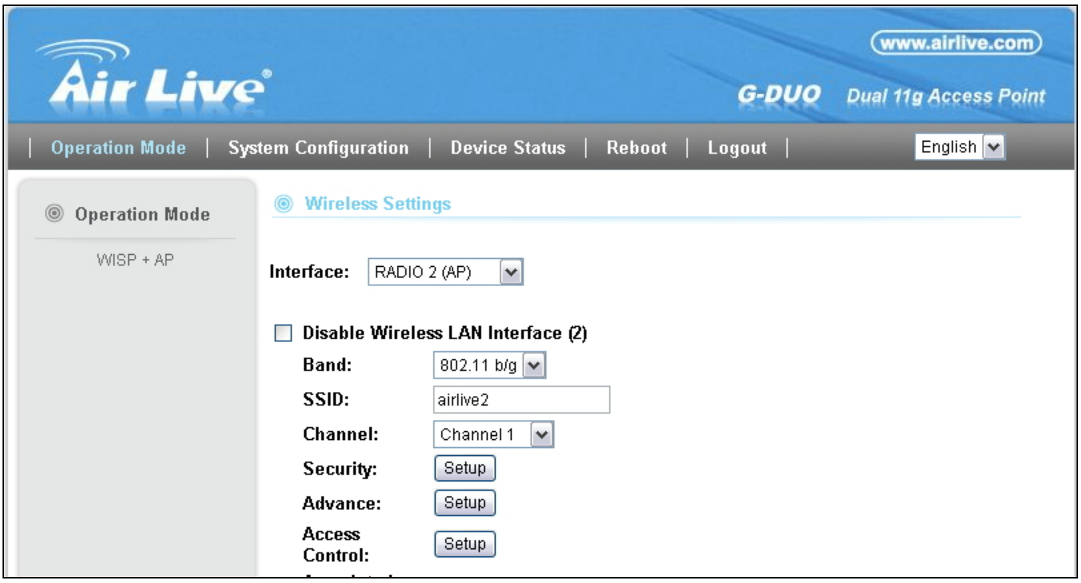
□ Enable Ping Access on WAN

☑ Enable Web Server Access on WAN

**Radio2**

**Step1:** Go to the wireless setting and change the interface to “Radio2”

**Step2:** Now we know the “Outdoor AP” is using Channel 11. Please set Radio2’s channel to as far as possible. In this case, it will be “Channel 1”.



www.airlive.com
G-DUO Dual 11g Access Point
| Operation Mode | System Configuration | Device Status | Reboot | Logout |
English
Operation Mode
WISP + AP

Wireless Settings

Interface: RADIO 2 (AP)

□ Disable Wireless LAN Interface (2)

Band: 802.11 b/g

SSID: airlive2

Channel: Channel 1

Security: Setup

Advance: Setup

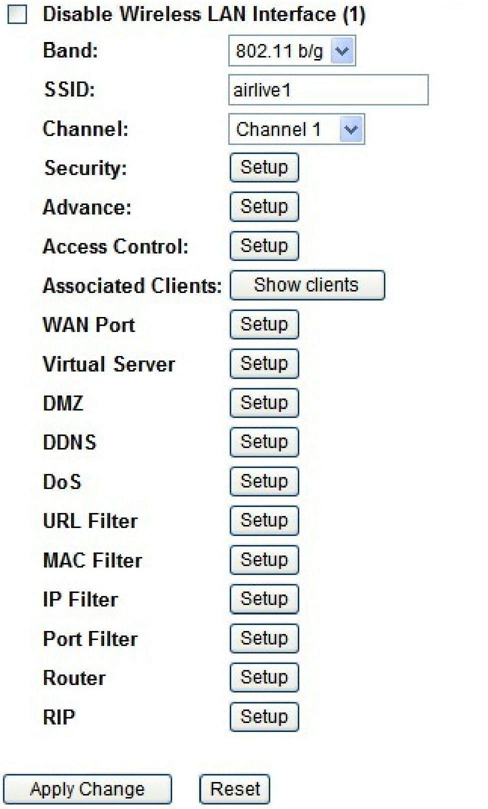
Access Control: Setup

**Step3:** Go to the “Security” setup and set your encryption as “WPA”->”Pre-Shared Key”->”TKIP”. Enter your encryption key. .

## 4.3 Radio1: WISP Router Mode Settings

The Radio1 is working in Client Mode with NAT routing function, it is also known as “Client Router”. The WAN is on the wireless side.

When you select “Radio1” as the interface, the following screen will appear.



□ Disable Wireless LAN Interface (1)

| | |
|---|---|
| Band: | 802.11 b/g |
| SSID: | airlive1 |
| Channel: | Channel 1 |
| Security: | Setup |
| Advance: | Setup |
| Access Control: | Setup |
| Associated Clients: | Show clients |
| WAN Port | Setup |
| Virtual Server | Setup |
| DMZ | Setup |
| DDNS | Setup |
| DoS | Setup |
| URL Filter | Setup |
| MAC Filter | Setup |
| IP Filter | Setup |
| Port Filter | Setup |
| Router | Setup |
| RIP | Setup |

Apply Change    Reset

### 4.3.1 Basic Wireless Settings

- **Band:** You can choose between “802.11g/b”, “802.11g”, or “802.11b”. We recommend to leave the setting at “802.11g/b”.
- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on “Site Survey” button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11. For Client and WISP mode, this field is applicable only in Adhoc mode.

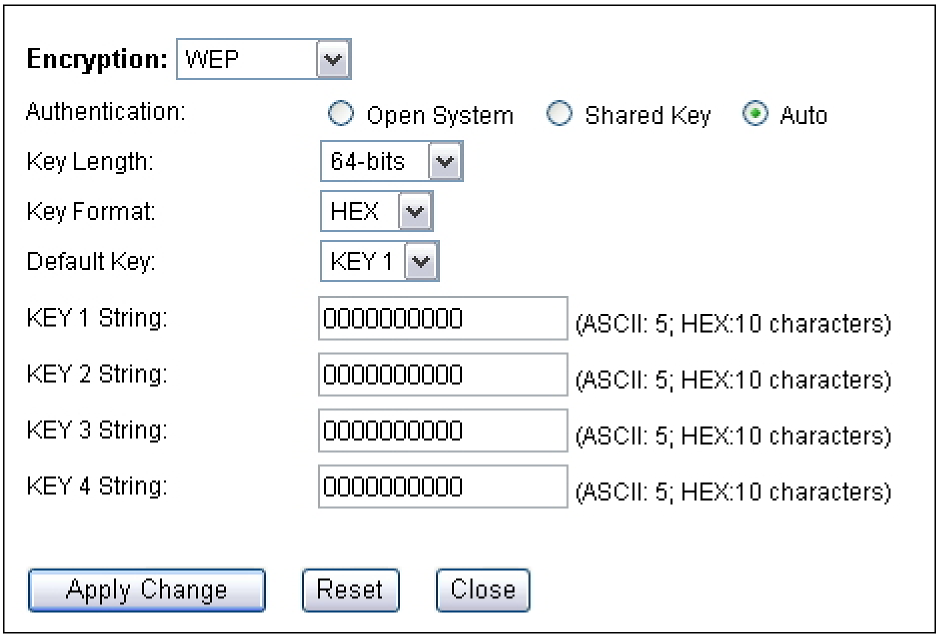
## 4.3.2 Security Settings

***Operation Mode -> Setup -> Security Settings***

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

### WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



**Encryption:** WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

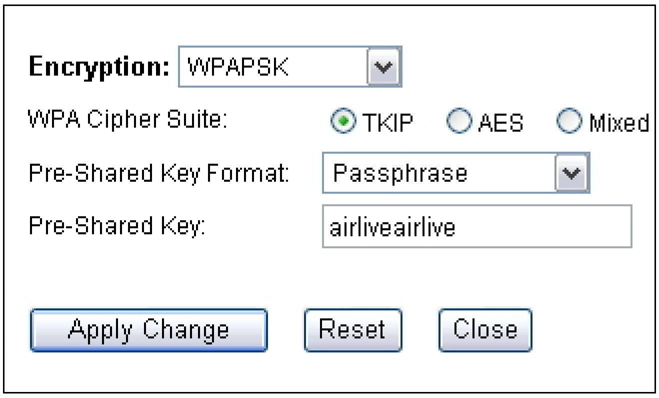
  - **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select "Auto".
  - **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5**

ASCII Characters if you choose this option. For example, “passw”

- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, “12345abcdef”
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, “airlivewepkey”
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, “1234567890abcdef1234567890”

### WPA-PSK, WPA2-PSK, WPA-AUTO

Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



**Encryption:** WPAPSK

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

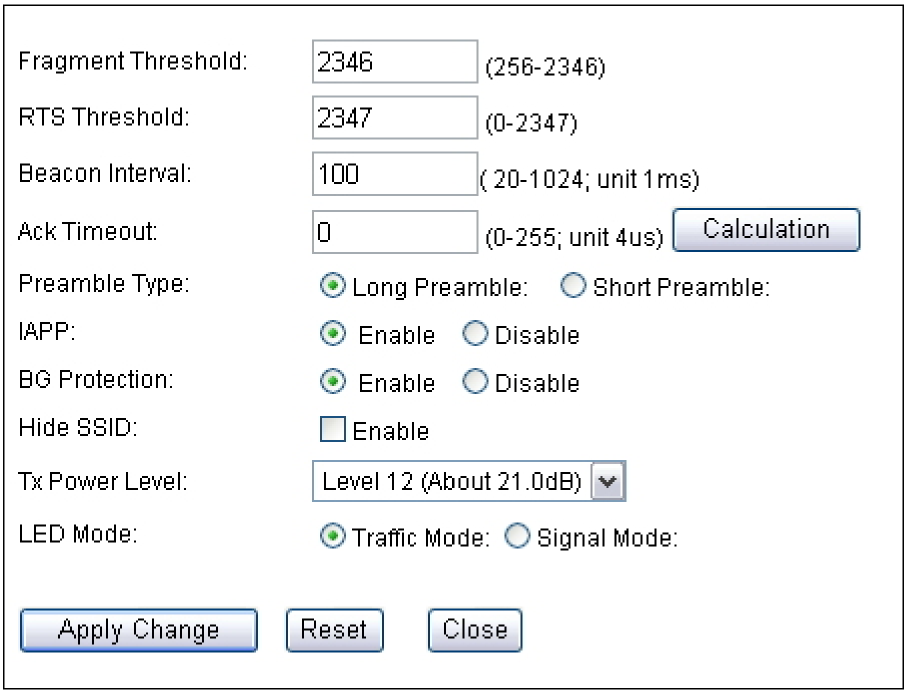
Pre-Shared Key Format: Passphrase

Pre-Shared Key: airliveairlive

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

## 4.3.3 Advance (Wireless Settings)

***Operation Mode -> Setup -> Advance***



|  |  |
|---|---|
| Fragment Threshold: | 2346 (256-2346) |
| RTS Threshold: | 2347 (0-2347) |
| Beacon Interval: | 100 ( 20-1024; unit 1ms) |
| Ack Timeout: | 0 (0-255; unit 4us) Calculation |
| Preamble Type: | ● Long Preamble: ○ Short Preamble: |
| IAPP: | ● Enable ○ Disable |
| BG Protection: | ● Enable ○ Disable |
| Hide SSID: | □ Enable |
| Tx Power Level: | Level 12 (About 21.0dB) |
| LED Mode: | ● Traffic Mode: ○ Signal Mode: |

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **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.

- **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.

- **BG 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..

- **Hide SSID:** Enable Hide SSID will make the AP network's SSID invisible. A device can link with the AP only if correct SSID name is entered.

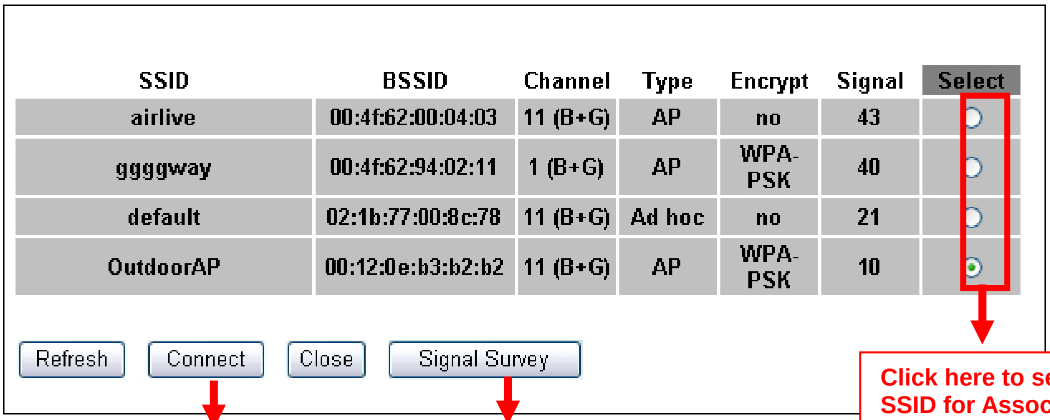
- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country's legal limit.

### 4.3.4 Site Survey

***Operation Mode -> Setup -> Site Survey***

You can scan for wireless networks around your location using the Site Survey function. From the site survey function, you can also perform antenna alignment and establish wireless connection

When you click on Site Survey, the following screen will appear. It might take awhile depending on number of available APs in the area.



| SSID | BSSID | Channel | Type | Encrypt | Signal | Select |
|---|---|---|---|---|---|---|
| airlive | 00:4f:62:00:04:03 | 11 (B+G) | AP | no | 43 | ○ |
| ggggway | 00:4f:62:94:02:11 | 1 (B+G) | AP | WPA-PSK | 40 | ○ |
| default | 02:1b:77:00:8c:78 | 11 (B+G) | Ad hoc | no | 21 | ○ |
| OutdoorAP | 00:12:0e:b3:b2:b2 | 11 (B+G) | AP | WPA-PSK | 10 | ● |

Click here to select SSID for Association or Signal Survey

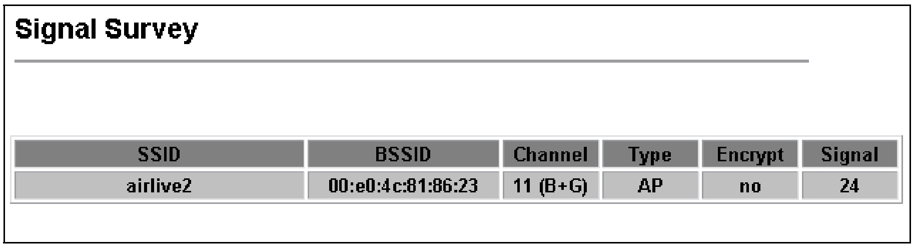
To connect with the selected SSID. This function is available only in Client Infrastructure or Bridge Infrastructure

For antenna alignment. It will display and update the Signal Strength conitnously

### 4.3.5 Signal Survey

***Operation Mode -> Setup -> Site Survey -> Signal Survey***

The Signal Survey will continuously display the SIGNAL STRENGTH value of the selected SSID for antenna alignment purpose. To use Signal Survey function, please enter the "Site Survey" function first; please refer to the instruction in the above section. Once you select the ESSID and click on the "Signal Survey" button, the following screen will appear.



Signal Survey

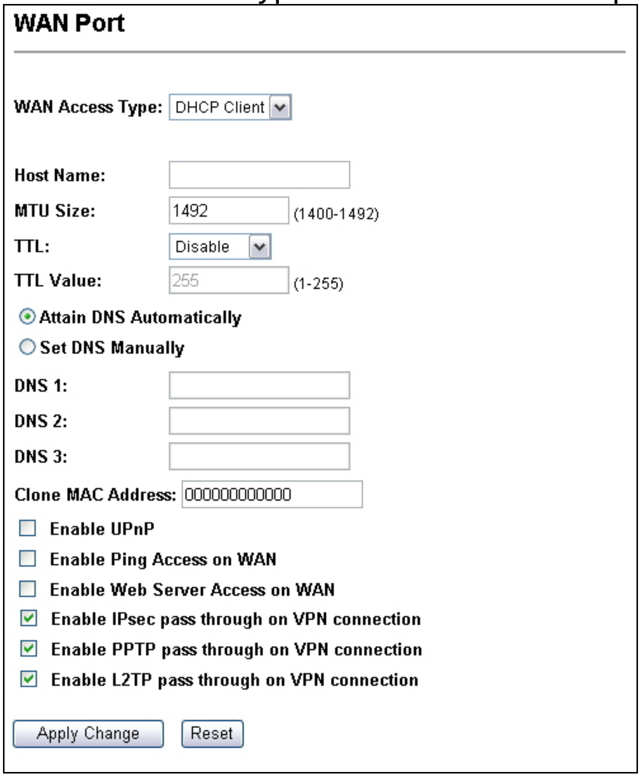
| SSID | BSSID | Channel | Type | Encrypt | Signal |
|---|---|---|---|---|---|
| airlive2 | 00:e0:4c:81:86:23 | 11 (B+G) | AP | no | 24 |

- **BSSID**: This is the remote AP's MAC address.
- **Channel**: The current scanned channel
- **Signal Strength**: This is signal strength number in percentage in 0 to 100 scale. The higher the number, the better signal.

### 4.3.6 WAN Port

***Operation Mode -> Setup -> WAN Port***

The G.DUO support different authentication and IP assignment standards for the WAN port. It includes fixed IP, DHCP, PPPoE, PPTP, L2TP, and Big Pond protocols. Please consult with your ISP about what authentication type is used for the WAN port connection.



WAN Port

WAN Access Type: DHCP Client

Host Name:

MTU Size: 1492 (1400-1492)

TTL: Disable

TTL Value: 255 (1-255)

● Attain DNS Automatically

○ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000

□ Enable UPnP

□ Enable Ping Access on WAN

□ Enable Web Server Access on WAN

☑ Enable IPsec pass through on VPN connection

☑ Enable PPTP pass through on VPN connection

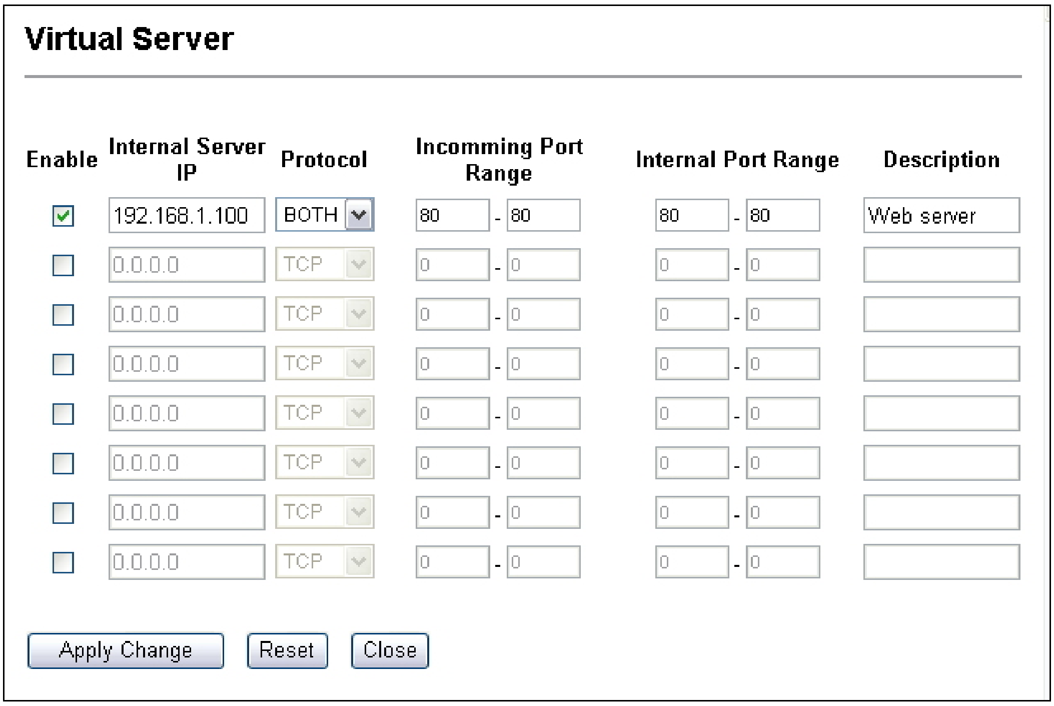
☑ Enable L2TP pass through on VPN connection

- **Clone MAC Address**: In this place, you can assign a MAC address for the WAN port. In case of WISP mode, it is Radio1's MAC address. For Gatway mode, it is the WAN/LAN1 MAC address.
- **Enable UPnP:** Check this field will enable Universal Plug n Play protocol
- **Enable Web Server Access on WAN:** Check this field will enable remote management from WAN side.

### 4.3.7 Virtual Server Settings

Virtual server allows you to specify one or more applications running on server computers on the LAN that may be accessed by any Internet user. Internet data destined for the specified public port will be directed to the specified private port number on the LAN client with the specified private IP address.

If you want to allow your web server, ftp server, or email server to be accessible from Internet, you would need to open specific port on the virtual server to your local IP address.



**Virtual Server**

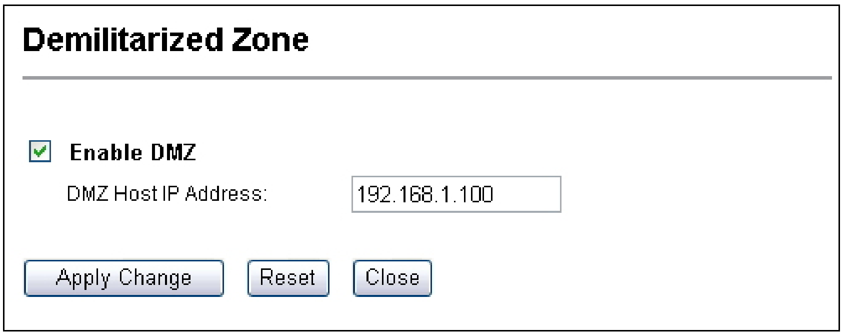
| Enable | Internal Server IP | Protocol | Incomming Port Range | Internal Port Range | Description |
|---|---|---|---|---|---|
| ☑ | 192.168.1.100 | BOTH | 80 - 80 | 80 - 80 | Web server |
| □ | 0.0.0.0 | TCP | 0 - 0 | 0 - 0 | |
| □ | 0.0.0.0 | TCP | 0 - 0 | 0 - 0 | |
| □ | 0.0.0.0 | TCP | 0 - 0 | 0 - 0 | |
| □ | 0.0.0.0 | TCP | 0 - 0 | 0 - 0 | |
| □ | 0.0.0.0 | TCP | 0 - 0 | 0 - 0 | |
| □ | 0.0.0.0 | TCP | 0 - 0 | 0 - 0 | |
| □ | 0.0.0.0 | TCP | 0 - 0 | 0 - 0 | |

For a list of most frequent used TCP and UDP ports. Please visit http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

### 4.3.8 DMZ

***Advanced Settings >> Multiple DMZ***

DMZ opens all TCP/UDP ports to particular IP address on the LAN side. It allows setting up servers behind the G.DUO.



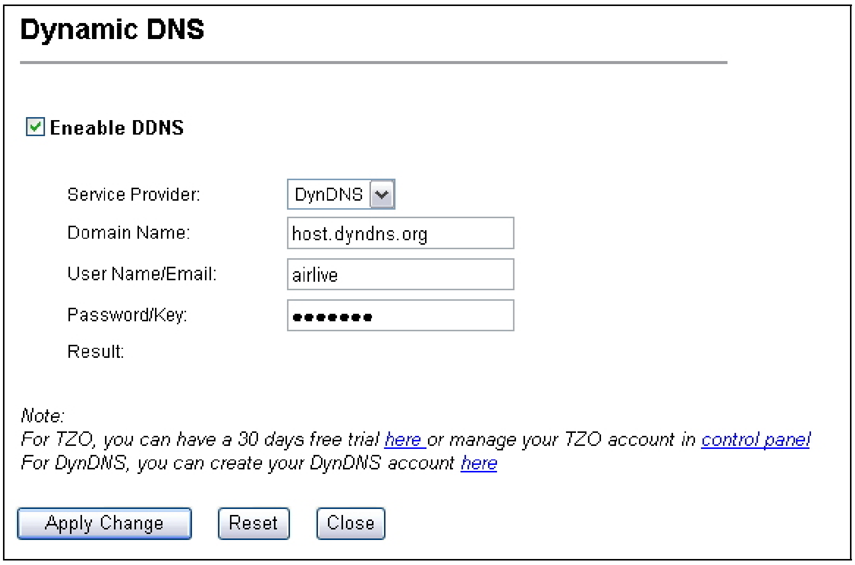
Demilitarized Zone

☑ Enable DMZ

DMZ Host IP Address: 192.168.1.100

### 4.3.9 DDNS

Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. The G.DUO support “Dyndns” and “TZO” service.



Dynamic DNS

☑ Eneable DDNS

Service Provider: DynDNS

Domain Name: host.dyndns.org

User Name/Email: airlive

Password/Key: ●●●●●●●

Result:

*Note:*
*For TZO, you can have a 30 days free trial here or manage your TZO account in control panel*
*For DynDNS, you can create your DynDNS account here*

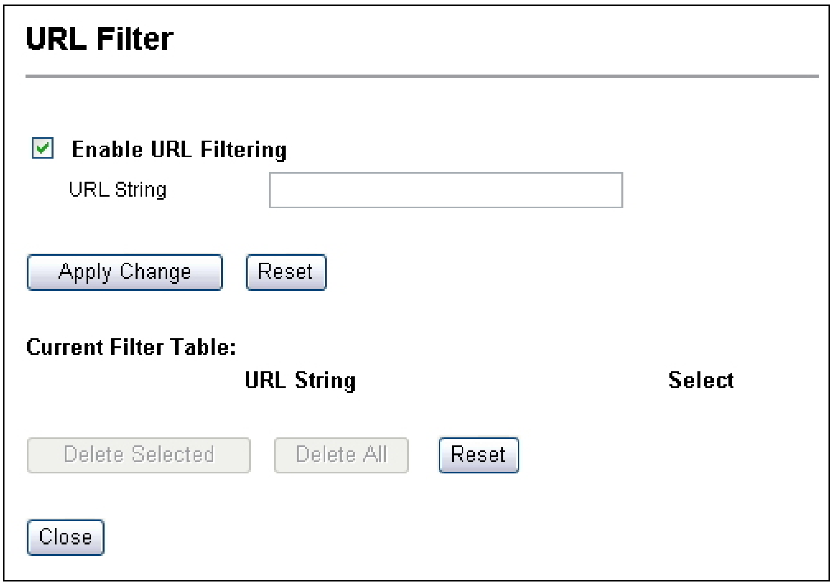
### 4.3.10 DoS (Denial of Service)

Denial of Service is a type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

The G.DUO provides a list of Firewall grade DoS control that protect your network from hacker attack.

### 4.3.11 URL Filter

The G.DUO provide URL filter function to stop access to certain website. It is especially useful for parents to stop children from accessing some websites.



URL Filter

☑ Enable URL Filtering

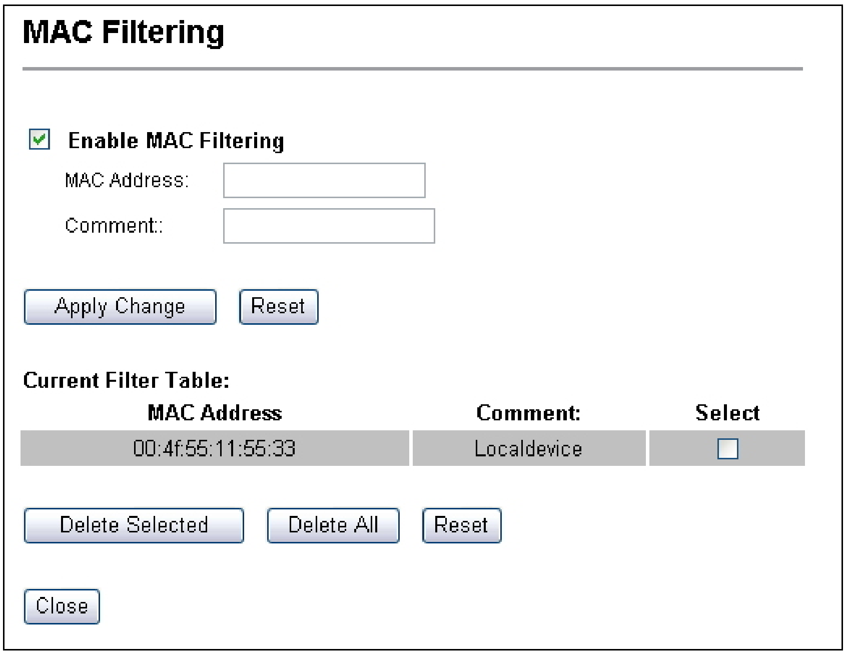
URL String

Current Filter Table:

| URL String | Select |
|---|---|

### 4.3.12 MAC Filter

MAC filter can filter out traffic from certain MAC addresses. It can prevent access to internet from certain station in the local LAN.



MAC Filtering

☑ Enable MAC Filtering

MAC Address:

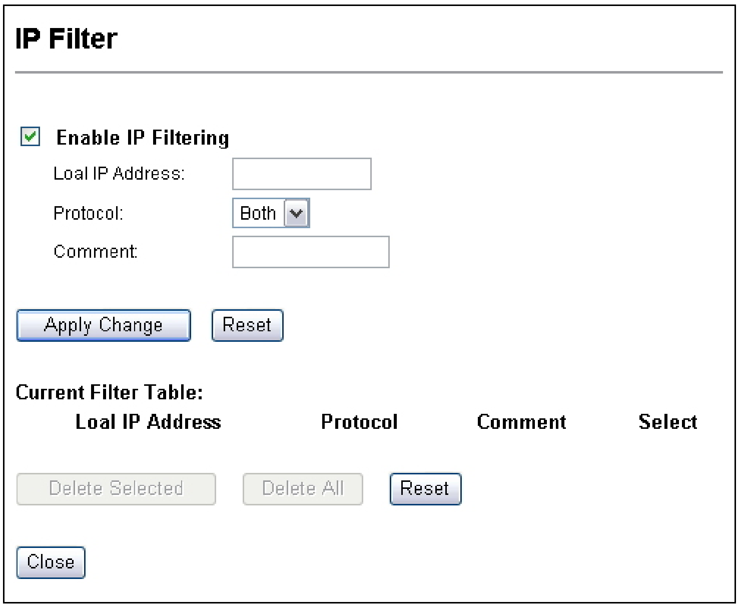
Comment::

Current Filter Table:

| MAC Address | Comment: | Select |
|---|---|---|
| 00:4f:55:11:55:33 | Localdevice | □ |

### 4.3.13 IP Filter

IP filtering allows you to block certain IP addresses from accessing the network.



**IP Filter**

☑ **Enable IP Filtering**

Loal IP Address:

Protocol: Both

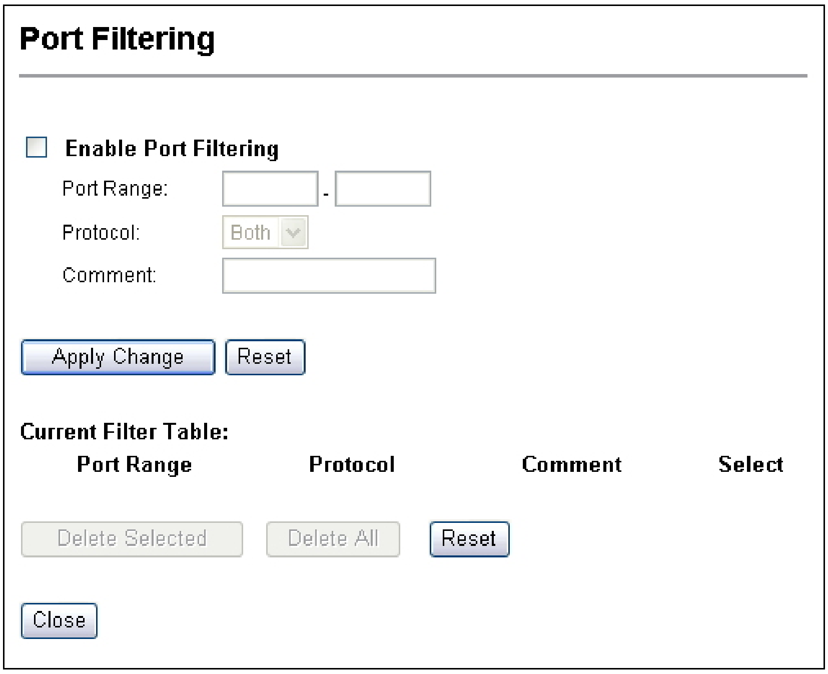
Comment:

**Current Filter Table:**

| Loal IP Address | Protocol | Comment | Select |
|---|---|---|---|

### 4.3.14 Port Filter

Port filtering allows you to block certain applications from accessing the network.



**Port Filtering**

☐ **Enable Port Filtering**

Port Range: -

Protocol: Both

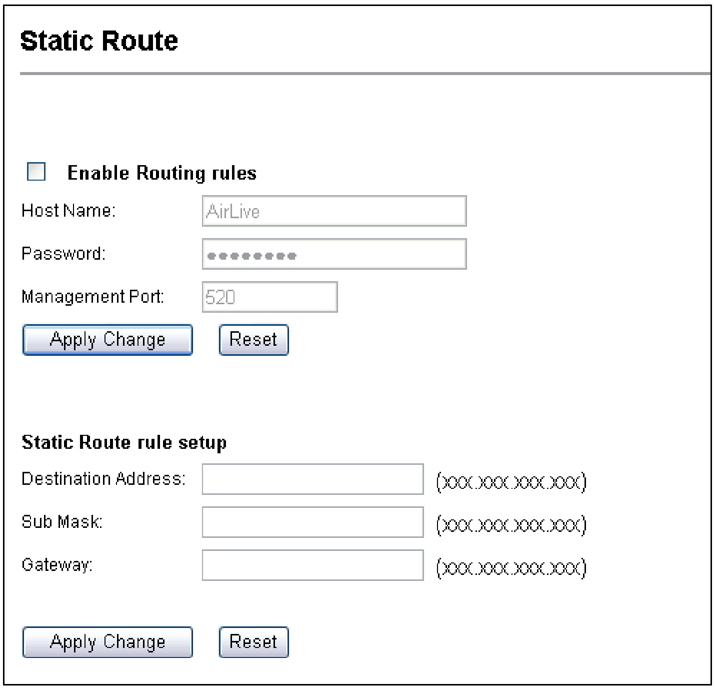
Comment:

**Current Filter Table:**

| Port Range | Protocol | Comment | Select |
|---|---|---|---|

### 4.3.15 Router (Static Route)

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.



Static Route

□ Enable Routing rules

Host Name: AirLive

Password: ●●●●●●●●

Management Port: 520

Static Route rule setup

Destination Address: (xxx.xxx.xxx.xxx)

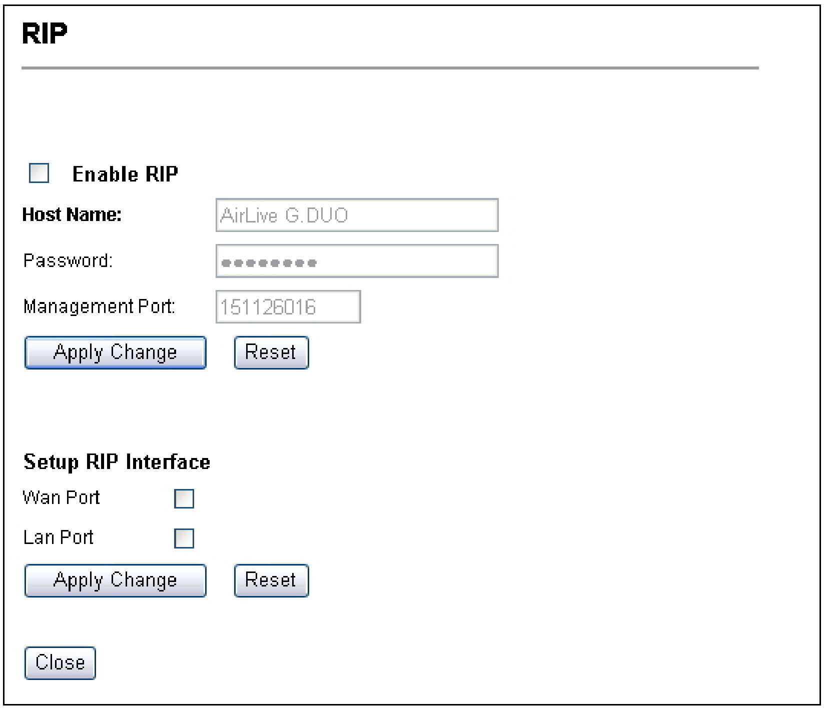
Sub Mask: (xxx.xxx.xxx.xxx)

Gateway: (xxx.xxx.xxx.xxx)

## 4.3.16 RIP (Routing Information Protocol

### *Operation Mode -> Setup -> Access Control*

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks



RIP

□ Enable RIP

Host Name: AirLive G.DUO

Password: ●●●●●●●●

Management Port: 151126016

Setup RIP Interface

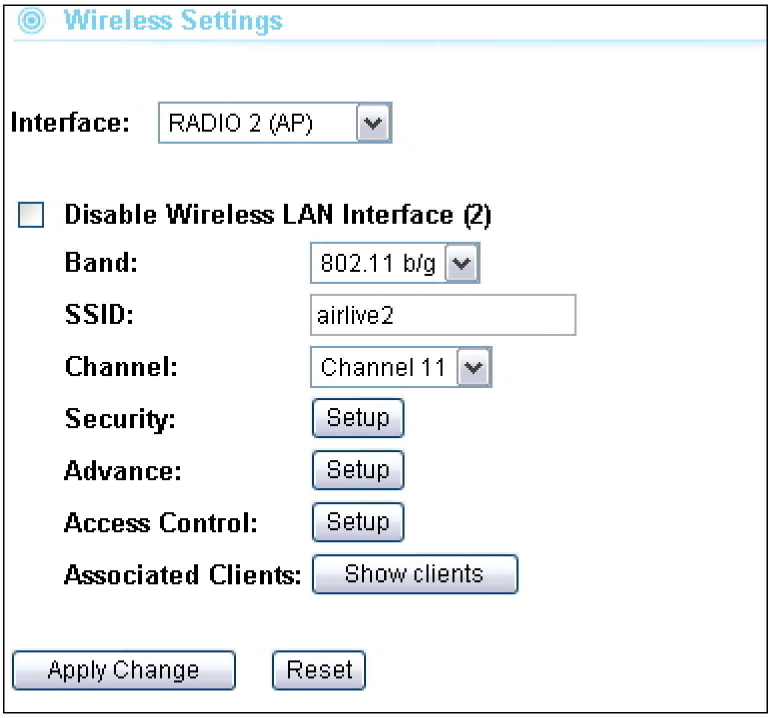
Wan Port □

Lan Port □

## 4.4 Radio2: AP Mode Settings

The Radio2 is working in Access Point Mode. The default SSID is “AirLive2”.

When you select “Radio2” as the interface, the following screen will appear:



Wireless Settings

Interface: RADIO 2 (AP)

☐ Disable Wireless LAN Interface (2)

Band: 802.11 b/g

SSID: airlive2

Channel: Channel 11

Security: Setup

Advance: Setup

Access Control: Setup

Associated Clients: Show clients

Apply Change   Reset

### 4.4.1 Basic Wireless Settings

- **Band:** You can choose between “802.11g/b”, “802.11g”, or “802.11b”. We recommend leaving the setting at “802.11g/b”.
- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on “Site Survey” button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11.

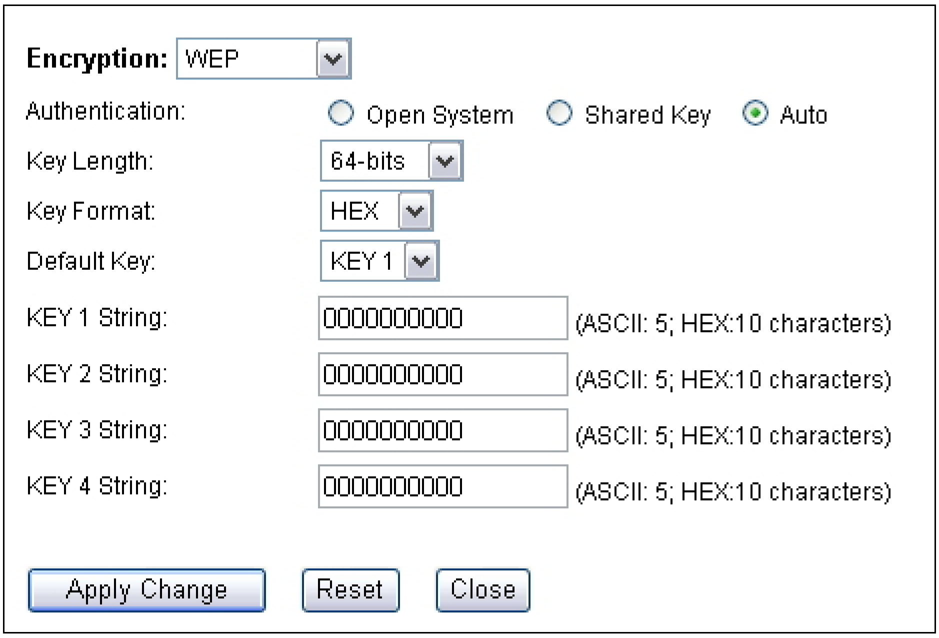
### 4.4.2 Security Settings

***Operation Mode -> Setup -> Security Settings***

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

## WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

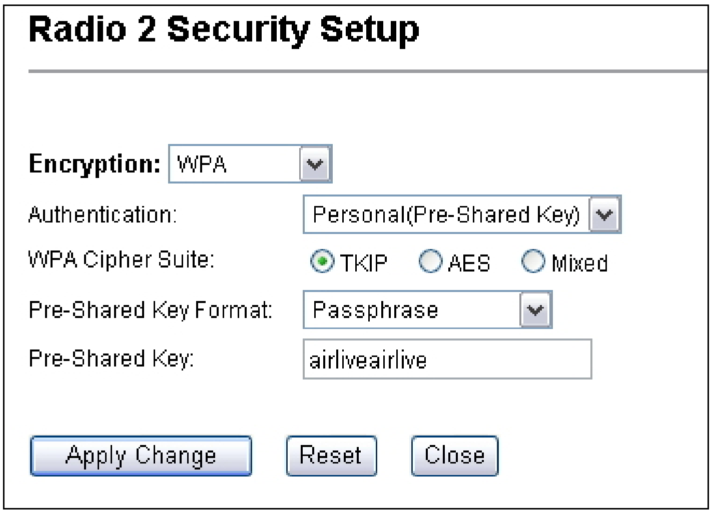
- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

  - **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select "Auto".
  - **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, "passw"
  - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, "12345abcdef"
  - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, "airlivewepkey"
  - **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example,

"1234567890abcdef1234567890"

## WPA-Personal, WPA2-Personal, WPA-Mixed (Pre-Shared Key)

The WPA Personal is also known as "WPA-PSK" encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



**Radio 2 Security Setup**

Encryption: WPA

Authentication: Personal(Pre-Shared Key)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

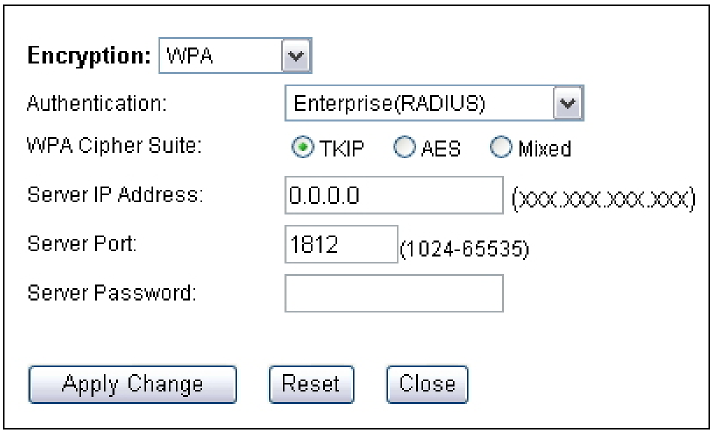
Pre-Shared Key Format: Passphrase

Pre-Shared Key: airliveairlive

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

## WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise (Radius)

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA or WPA2.



**Encryption:** WPA

Authentication: Enterprise(RADIUS)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

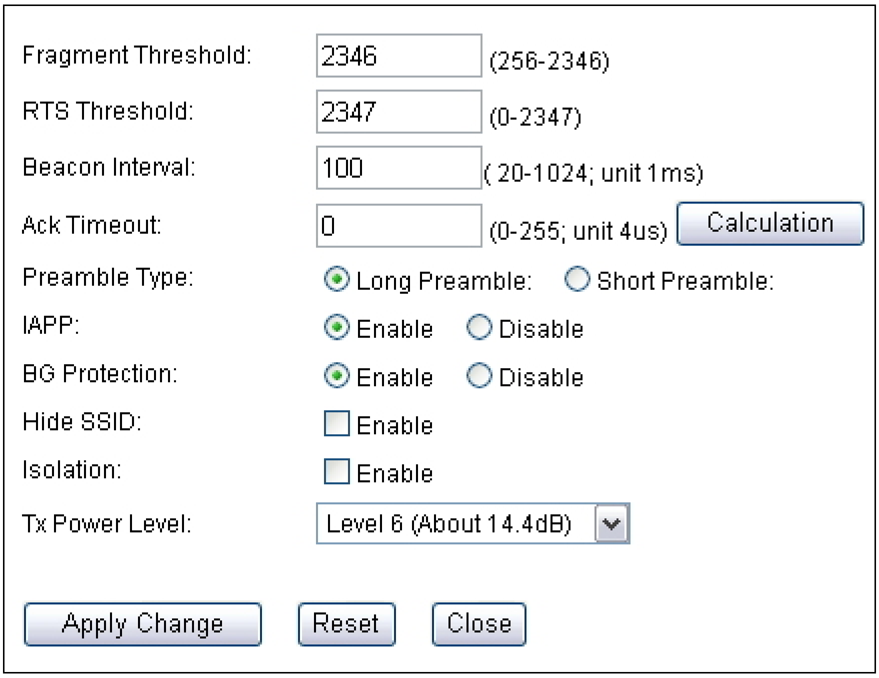
Server IP Address: 0.0.0.0 (xxx.xxx.xxx.xxx)

Server Port: 1812 (1024-65535)

Server Password:

## 4.4.3 Advance (Wireless Settings)

***Operation Mode -> Setup -> Advance***



Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 ( 20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us) Calculation

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Hide SSID: □ Enable

Isolation: □ Enable

Tx Power Level: Level 6 (About 14.4dB)

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **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.

- **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.

- **BG 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..

- **Hide SSID:** Enable Hide SSID will make the AP network's SSID invisible. A device can link with the AP only if correct SSID name is entered.

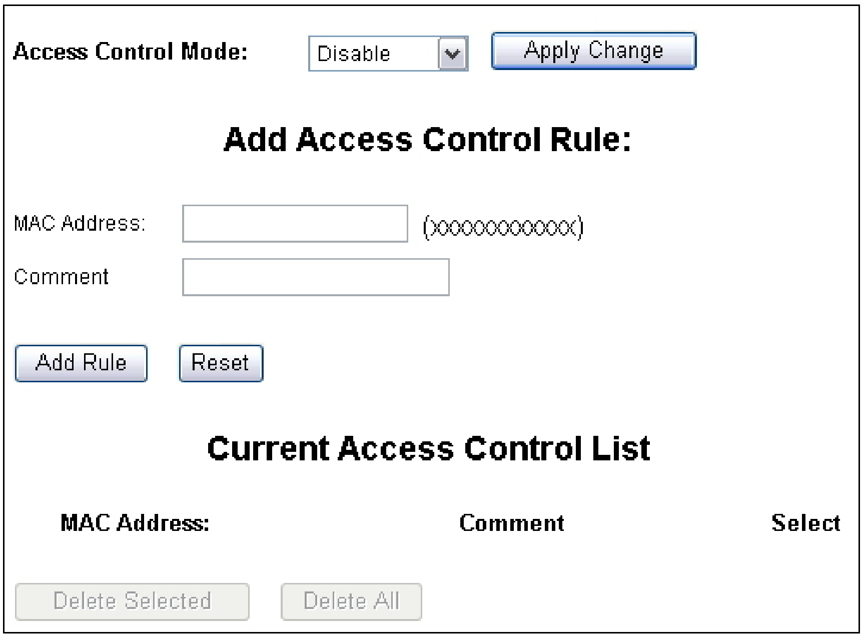
- **Isolation:** Enable Isolation will prevent wireless clients to see each other on the network.

- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country's legal limit.

### 4.4.4 Access Control

***Operation Mode -> Setup -> Access Control***

The G.DUO allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and Gateway modes.



Access Control Mode: Disable

Add Access Control Rule:

MAC Address: (xxxxxxxxxxxx)

Comment

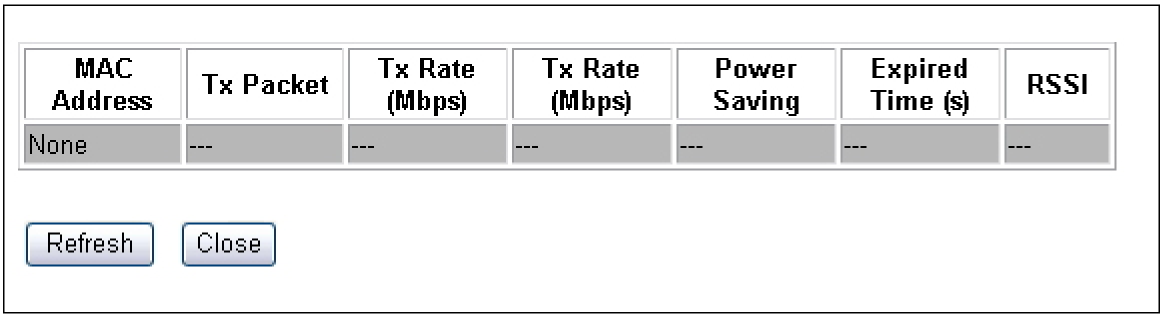
Current Access Control List

| MAC Address: | Comment | Select |
|---|---|---|

- **Access Control List**
  - **Disable:** When selected, no MAC address filtering will be performed.
  - **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
  - **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

### 4.4.5 Associated Clients

Click on this to show the current wireless clients associated to the AP. It will display MAC adderss, Trasmit packet, Tx rate, power saving, expire time, and signal strength.

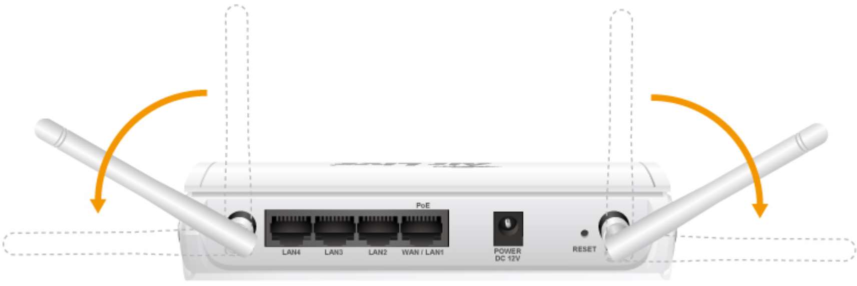


| MAC Address | Tx Packet | Tx Rate (Mbps) | Tx Rate (Mbps) | Power Saving | Expired Time (s) | RSSI |
|---|---|---|---|---|---|---|
| None | --- | --- | --- | --- | --- | --- |

# 5 Dual AP Mode

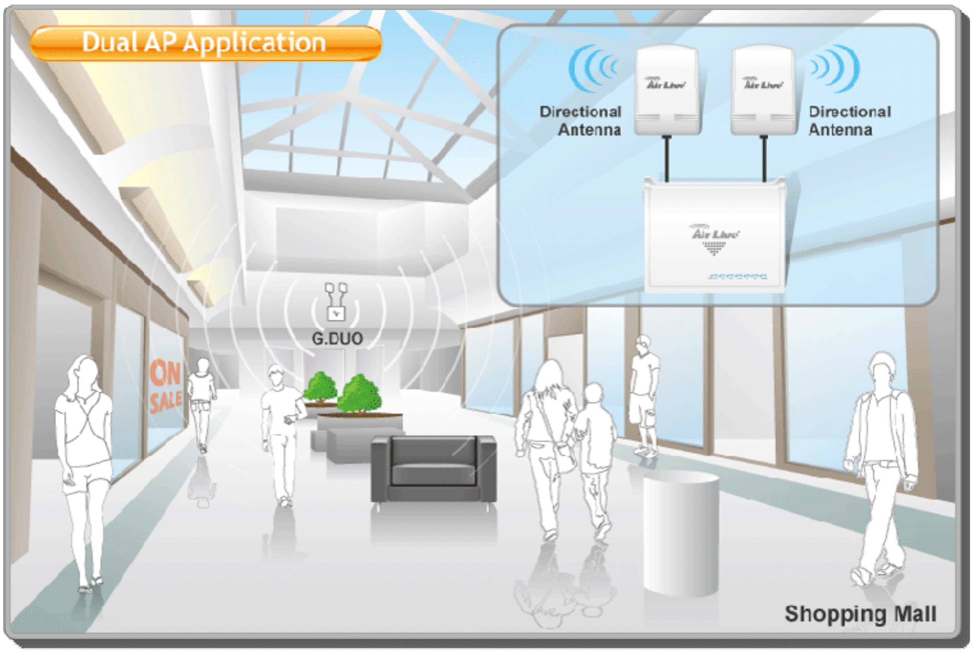
In this chapter, we will explain about the wireless settings for Dual Mode. Please be sure to read through Chapter 1.4 and Chapter 3's "*Introduction to Web Management*" and *"Initial Configurations"* first.

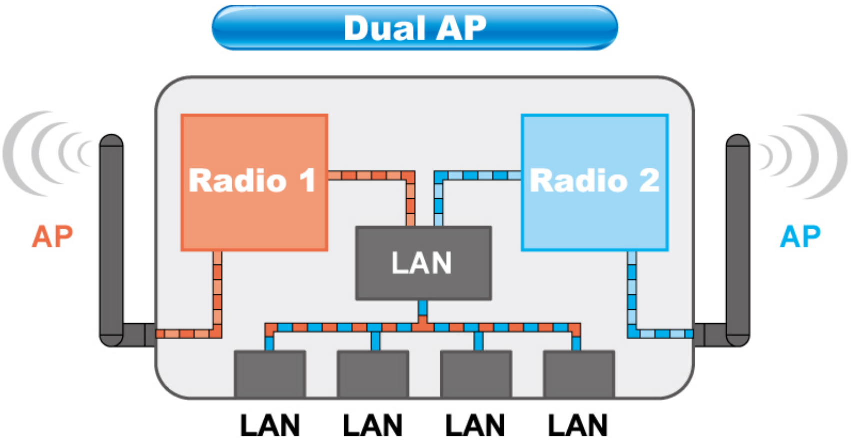
It is highly recommended that you use 2 directional antennas in this mode to achieve larger coverage and avoid mutual interference. If you need to use the supplied 2dBi omni antennas, please adjust them according to the diagram below:



## 5.1 Application for Dual AP Mode

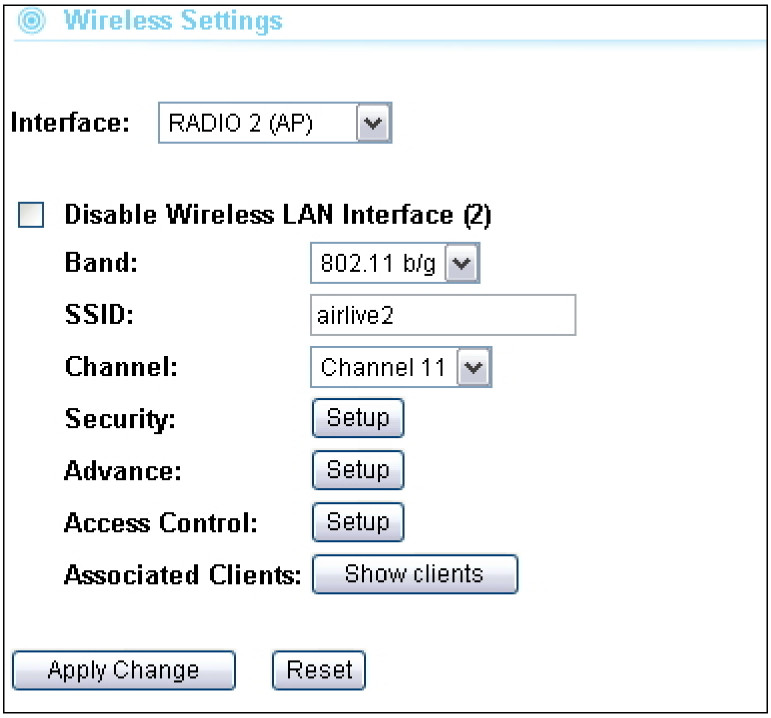
The Dual AP mode is designed to extend the wireless coverage of the Hotspot network. Therefore, you should use directional antennas (like a 10dBi panel antenna) to let each radio cover separate areas.





## 5.2 Radio1 and 2: AP Mode Settings

Since both Radio1 and Radio2 are Access Point mode. The configuration menu are the same. We will explain them together here. Radio1's default SSID is "airlive1", Radio2's default SSID is "airlive2".



Interface: RADIO 2 (AP)

□ Disable Wireless LAN Interface (2)

Band: 802.11 b/g

SSID: airlive2

Channel: Channel 11

### 5.2.1 Basic Wireless Settings

- **Band:** You can choose between "802.11g/b", "802.11g", or "802.11b". We recommend leaving the setting at "802.11g/b".

- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on “Site Survey” button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11.

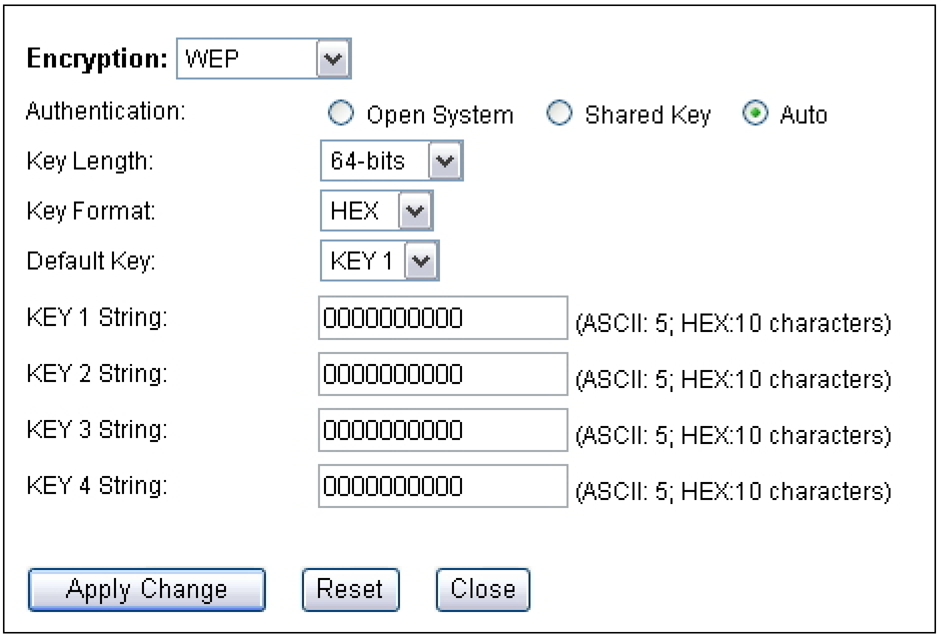
### 5.2.2 Security Settings

***Operation Mode -> Setup -> Security Settings***

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal, WPA Mixed.

#### WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



**Encryption:** WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

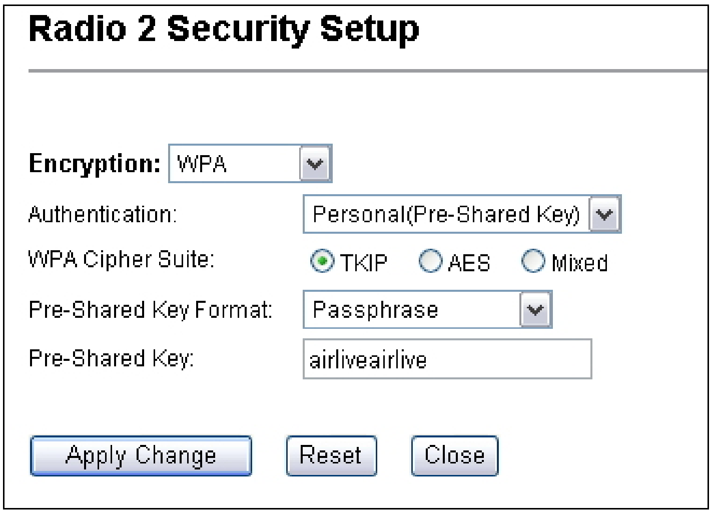
- **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select “Auto”.
- **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The

longer the Key Length, the more secure the encryption is.

- **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, "passw"
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, "12345abcdef"
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, "airlivewepkey"
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890"

## WPA-Personal, WPA2-Personal, WPA-Mixed (Pre-Shared Key)

The WPA Personal is also known as "WPA-PSK" encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



Radio 2 Security Setup

Encryption: WPA

Authentication: Personal(Pre-Shared Key)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

Pre-Shared Key Format: Passphrase

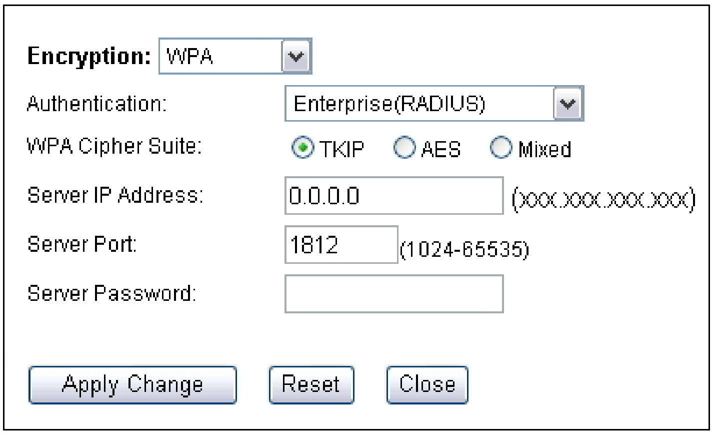
Pre-Shared Key: airliveairlive

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

### WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise (Radius)

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA or WPA2.



**Encryption:** WPA

Authentication: Enterprise(RADIUS)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

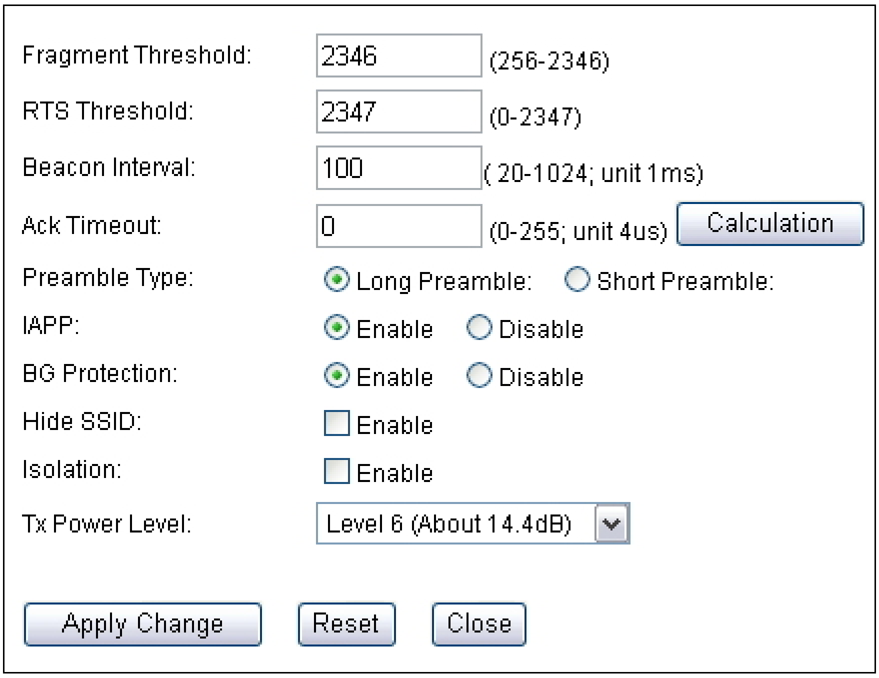
Server IP Address: 0.0.0.0 (xxx.xxx.xxx.xxx)

Server Port: 1812 (1024-65535)

Server Password:

## 5.2.3 Advance (Wireless Settings)

***Operation Mode -> Setup -> Advance***



Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 ( 20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us)

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Hide SSID: □ Enable

Isolation: □ Enable

Tx Power Level: Level 6 (About 14.4dB)

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **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.

- **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.

- **BG 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..

- **Hide SSID:** Enable Hide SSID will make the AP network's SSID invisible. A device can link with the AP only if correct SSID name is entered.

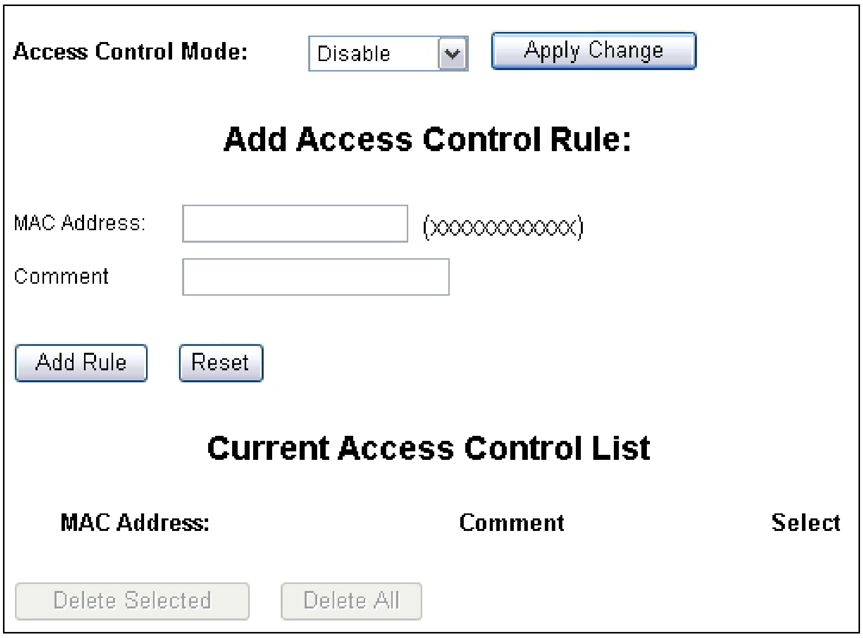
- **Isolation:** Enable Isolation will prevent wireless clients to see each other on the network.

- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country's legal limit.

### 5.2.4 Access Control

***Operation Mode -> Setup -> Access Control***

The G.DUO allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. This function is available only for Access Point and Gateway modes.

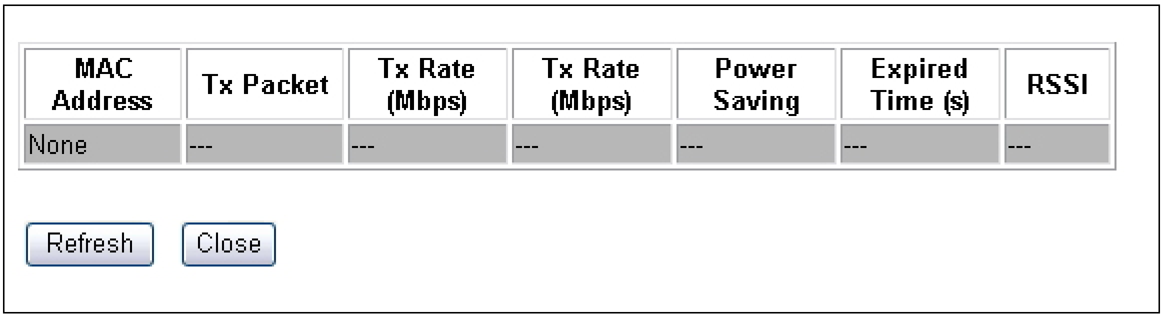


Access Control Mode: Disable

- **Access Control List**
  - **Disable:** When selected, no MAC address filtering will be performed.
  - **Allow list:** When selected, data traffic from only the specified devices in the table will be allowed in the network.
  - **Deny list:** When selected, data traffic from the devices specified in the table will be denied/discarded by the network.

### 5.2.5 Associated Clients

Click on this to show the current wireless clients associated to the AP. It will display MAC adderss, Trasmit packet, Tx rate, power saving, expire time, and signal strength.

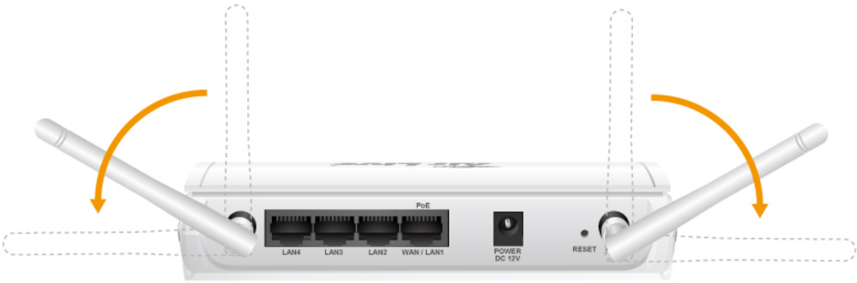


| MAC Address | Tx Packet | Tx Rate (Mbps) | Tx Rate (Mbps) | Power Saving | Expired Time (s) | RSSI |
|---|---|---|---|---|---|---|
| None | --- | --- | --- | --- | --- | --- |

# 6 Client + AP Mode

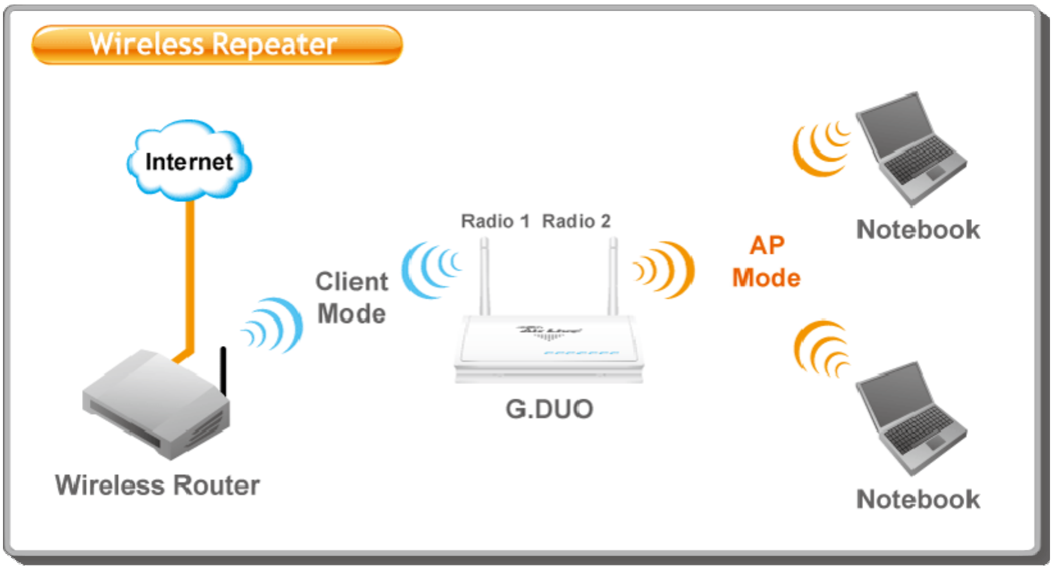
In this chapter, we will explain about the wireless settings for Client + AP Mode. Please be sure to read through Chapter 1.4 and Chapter 3's "*Introduction to Web Management*" and *"Initial Configurations"* first.

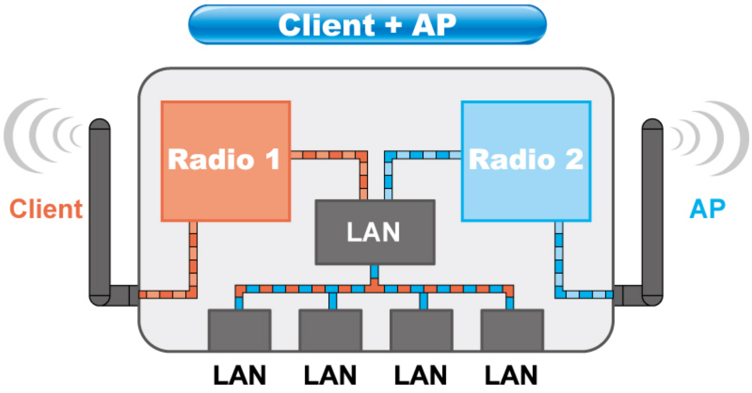
It is highly recommended that you use directional antenna for Radio1 in this mode to achieve larger coverage and avoid mutual interference. If you need to use the supplied 2dBi omni antennas, please adjust them according to the diagram below:



## 6.1 Application for Client + AP Mode

In this mode, the Radio1 is acting as wireless client to remote AP. Radio2 is performing as an Access Point. This mode is best used as a wireless repeater to extend the signal from remote Wireless Router.

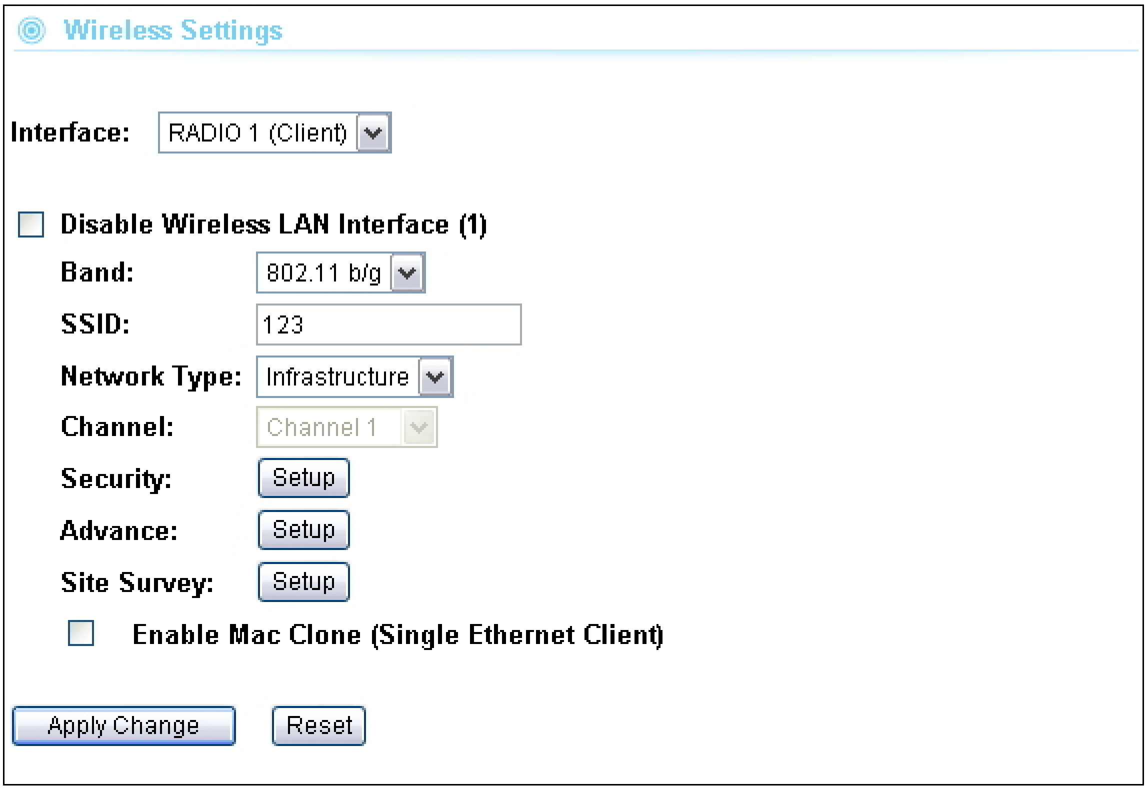




## 6.2 Radio1: Client Mode Settings

The Radio1 is working as wireless Client to Remote AP.

When you select "Radio1" as the interface, the following screen will appear.



Wireless Settings

Interface: RADIO 1 (Client)

□ Disable Wireless LAN Interface (1)

Band: 802.11 b/g

SSID: 123

Network Type: Infrastructure

Channel: Channel 1

Security: Setup

Advance: Setup

Site Survey: Setup

□ Enable Mac Clone (Single Ethernet Client)

### 6.2.1 Basic Wireless Settings

- **Band:** You can choose between "802.11g/b", "802.11g", or "802.11b". We recommend to leave the setting at "802.11g/b".
- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on "Site Survey" button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11. For Client and WISP mode, this field is applicable only in Adhoc

mode.

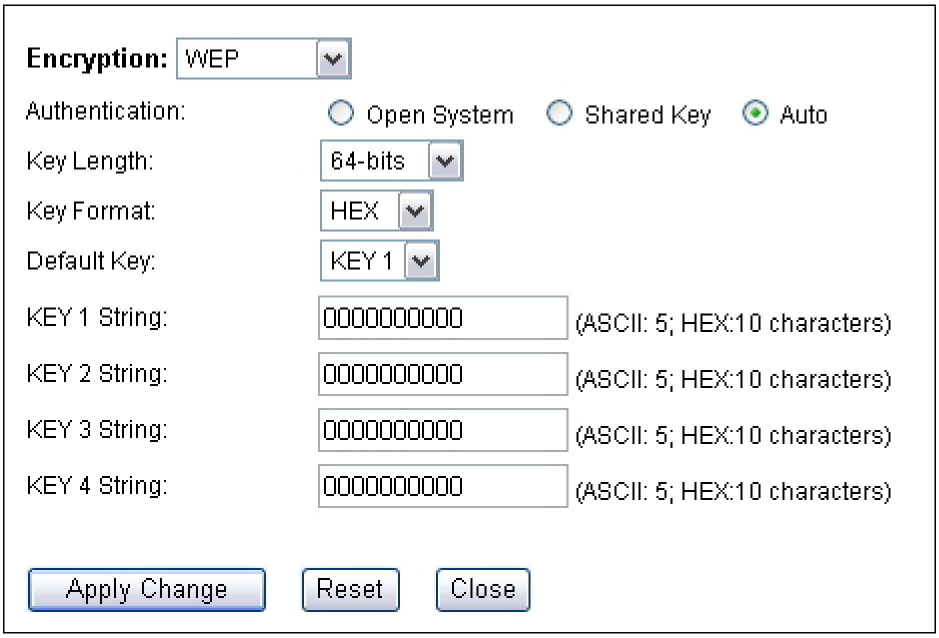
## 6.2.2 Security Settings

***Operation Mode -> Setup -> Security Settings***

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

### WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

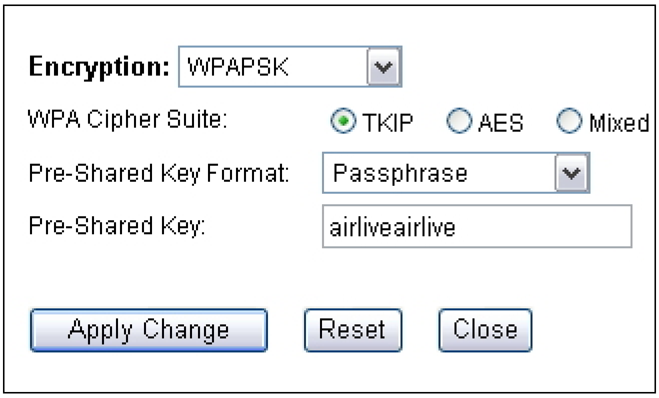
    - **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select "Auto".
    - **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
    - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f).

All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.

- **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, "passw"
- **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, "12345abcdef"
- **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, "airlivewepkey"
- **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890"

## WPA-PSK, WPA2-PSK, WPA-AUTO

Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.



**Encryption:** WPAPSK

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

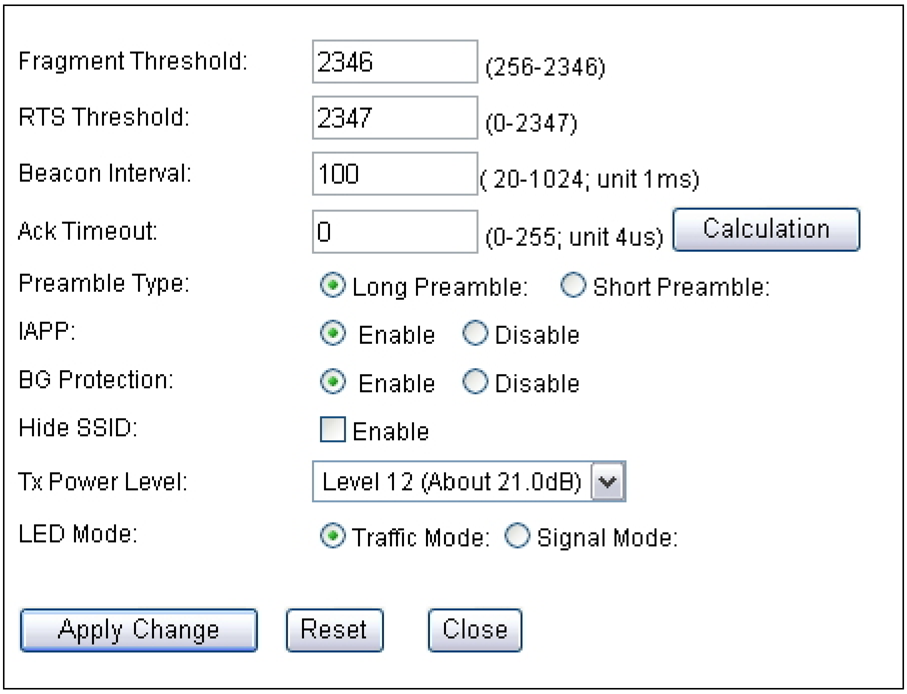
Pre-Shared Key Format: Passphrase

Pre-Shared Key: airliveairlive

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

### 6.2.3 Advance (Wireless Settings)

***Operation Mode -> Setup -> Advance***



Fragment Threshold: 2346 (256-2346)

RTS Threshold: 2347 (0-2347)

Beacon Interval: 100 ( 20-1024; unit 1ms)

Ack Timeout: 0 (0-255; unit 4us) Calculation

Preamble Type: ● Long Preamble: ○ Short Preamble:

IAPP: ● Enable ○ Disable

BG Protection: ● Enable ○ Disable

Hide SSID: □ Enable

Tx Power Level: Level 12 (About 21.0dB)

LED Mode: ● Traffic Mode: ○ Signal Mode:

- **Fragmentation:** When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

- **RTS Threshold:** RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of **2347**. It is recommended that this value does not deviate from the default too much.

- **Beacon Interval:** The device broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds. The default value is **100**, and a valid value should be between 1 and 65,535.

- **AckTimeOut:** When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. In most conditions, please put ACKtimeout value at zero(default value). The AP will calculate the ACKtimeout automatically when the value is zero. However, you can also enter the ACKtimeout manually.

- **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.

- **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.

- **BG 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..

- **Hide SSID:** Enable Hide SSID will make the AP network’s SSID invisible. A device can link with the AP only if correct SSID name is entered.

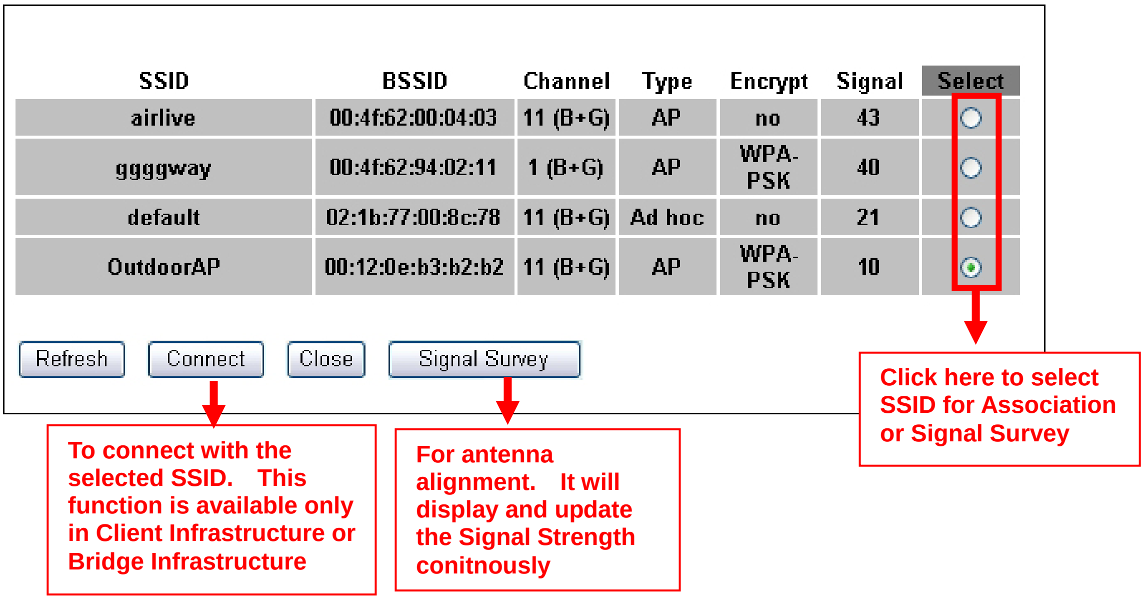
- **TX Power Level:** You can set your TX Output power level here. Please note the maximum allowable TX output power in EU is 20dBm. Please do not exceed your country’s legal limit.

## 6.2.4 Site Survey

***Operation Mode -> Setup -> Site Survey***

You can scan for wireless networks around your location using the Site Survey function. From the site survey function, you can also perform antenna alignment and establish wireless connection

When you click on Site Survey, the following screen will appear. It might take awhile depending on number of available APs in the area.



| SSID | BSSID | Channel | Type | Encrypt | Signal | Select |
|---|---|---|---|---|---|---|
| airlive | 00:4f:62:00:04:03 | 11 (B+G) | AP | no | 43 | ○ |
| ggggway | 00:4f:62:94:02:11 | 1 (B+G) | AP | WPA-PSK | 40 | ○ |
| default | 02:1b:77:00:8c:78 | 11 (B+G) | Ad hoc | no | 21 | ○ |
| OutdoorAP | 00:12:0e:b3:b2:b2 | 11 (B+G) | AP | WPA-PSK | 10 | ● |

Click here to select SSID for Association or Signal Survey

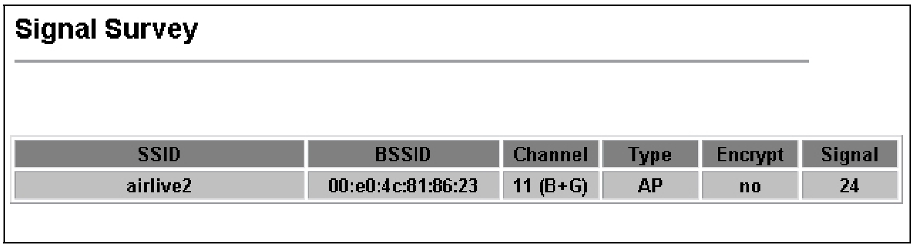
To connect with the selected SSID. This function is available only in Client Infrastructure or Bridge Infrastructure

For antenna alignment. It will display and update the Signal Strength conitnously

## 6.2.5 Signal Survey

***Operation Mode -> Setup -> Site Survey -> Signal Survey***

The Signal Survey will continuously display the SIGNAL STRENGTH value of the selected SSID for antenna alignment purpose. To use Signal Survey function, please enter the "Site Survey" function first; please refer to the instruction in the above section. Once you select the ESSID and click on the "Signal Survey" button, the following screen will appear.



Signal Survey

| SSID | BSSID | Channel | Type | Encrypt | Signal |
|---|---|---|---|---|---|
| airlive2 | 00:e0:4c:81:86:23 | 11 (B+G) | AP | no | 24 |

- **BSSID**: This is the remote AP's MAC address.
- **Channel**: The current scanned channel
- **Signal Strength**: This is signal strength number in percentage in 0 to 100 scale. The higher the number, the better signal.

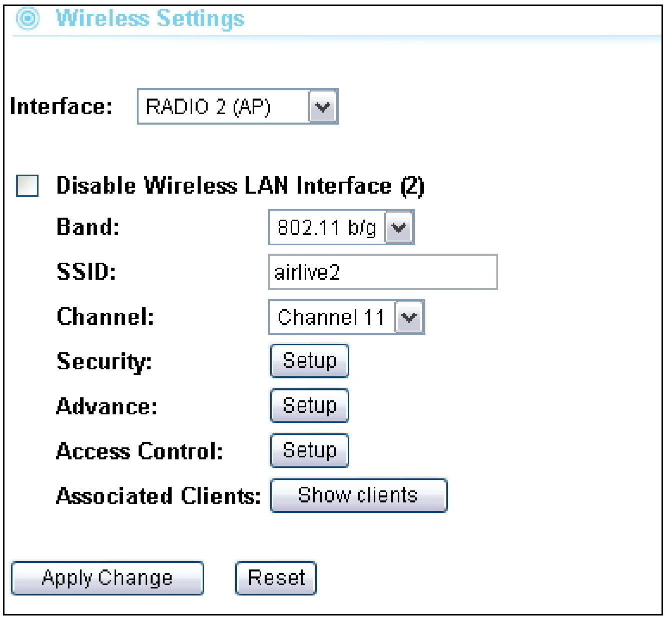
## 6.2.6 Enable MAC Clone (Single Ethernet Client)

When this function is enabled, G.DUO will replace the MAC address of Radio1 with the first PC's MAC address caught from the LAN port. It will allow one single Ethernet client only. Please use this function only if you want to limit the Ethernet client to only one.

## 6.3 Radio2: AP Mode Settings

The Radio2 is working in Access Point Mode. The default SSID is "AirLive2".

When you select "Radio2" as the interface, the following screen will appear:



Wireless Settings

Interface: RADIO 2 (AP)

☐ Disable Wireless LAN Interface (2)

Band: 802.11 b/g

SSID: airlive2

Channel: Channel 11

Security: Setup

Advance: Setup

Access Control: Setup

Associated Clients: Show clients

Apply Change Reset

### 6.3.1 Basic Wireless Settings

- **Band:** You can choose between "802.11g/b", "802.11g", or "802.11b". We recommend leaving the setting at "802.11g/b".
- **SSID:** The SSID setting of the remote AP. If you are not sure, you can click on "Site Survey" button to scan for AP.
- **Channel**: Wireless Channel used. For EU, it is channel 1~13. For U.S.A., it is channel 1~11.

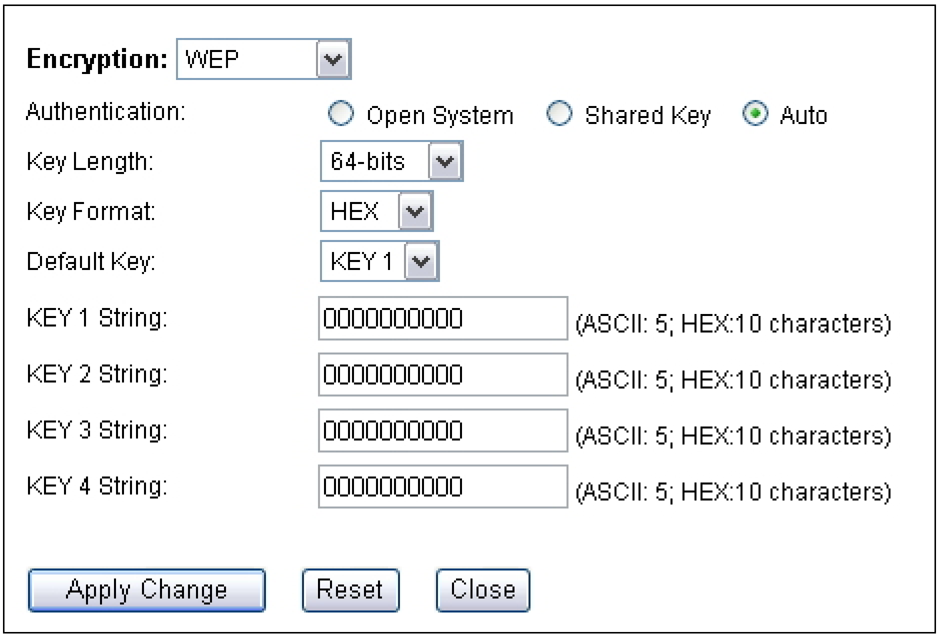
### 6.3.2 Security Settings

***Operation Mode -> Setup -> Security Settings***

Security settings allow you to use encryption to secure your data from eavesdropping. You can select different security policy to provide association authentication and/or data encryption. The G.DUO features various security policies including WEP, 802.1x, WPA, WPA Personal, WPA2, WPA2 Personal , WPA Mixed.

#### WEP

WEP Encryption is the oldest and most available encryption method. However, it is also the least secure.



Encryption: WEP

Authentication: ○ Open System ○ Shared Key ● Auto

Key Length: 64-bits

Key Format: HEX

Default Key: KEY 1

KEY 1 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 2 String: 0000000000 (ASCII: 5; HEX:10 characters)

KEY 3 String: 0000000000 (ASCII: 5; HEX:10 characters)

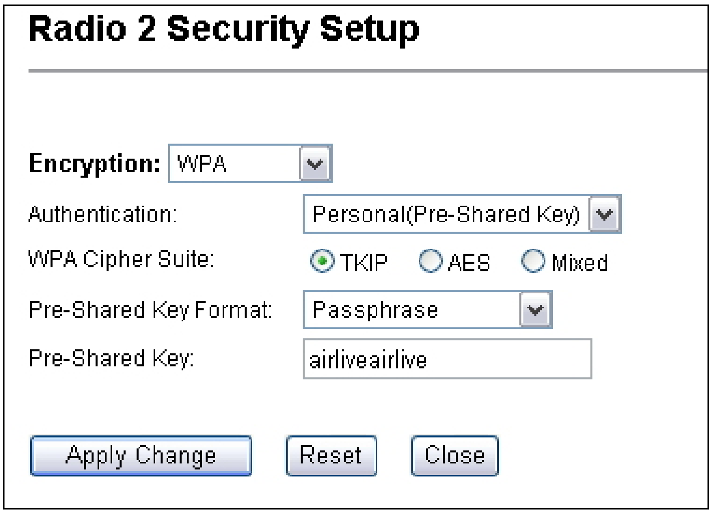
KEY 4 String: 0000000000 (ASCII: 5; HEX:10 characters)

- **Select one of the WEP key for wireless network:** There are total of 4 possible keys for WEP encryption. You need to choose which key will be used for encryption. All wireless devices on the same network have to use the same settings. We recommend using WEP Key 1 as in default setting.

  - **Authentication:** 2 types of Authentication are offered. Open system and Shared key. If you are not sure which one to use, please select "Auto".
  - **Key Length:** The G.DUO offers 64bit and 128 bit for WEP key length. The longer the Key Length, the more secure the encryption is.
  - **Key Type:** 2 types are available: ASCII and HEX. ASCII is a string of ASCII code including alphabetical characters, space, signs and numbers (i.e. "airlivepass12"). HEX is a string of 16-bit hexadecimal digits (0..9, a, b, c, d, e, f). All wireless devices on the network must match the exact key length and Key type. Some Wireless clients only allow HEX type for WEP.
  - **ASCII-64:** This is a key with 64-bit key length of ASCII type. Please enter **5** ASCII Characters if you choose this option. For example, "passw"
  - **HEX-64:** This is a key with 64-bit key length of HEX type. Please enter **10** Hexadecimal digits if you choose this option. For example, "12345abcdef"
  - **ASCII-128:** This is a key with 64-bit key length of ASCII type. Please enter **13** ASCII Characters if you choose this option. For example, "airlivewepkey"
  - **HEX-128:** This is a key with 128-bit key length of HEX type. Please enter **26** Hexadecimal digits if you choose this option. For example, "1234567890abcdef1234567890"

## WPA-Personal, WPA2-Personal, WPA-Mixed (Pre-Shared Key)

The WPA Personal is also known as "WPA-PSK" encryption. Wi-Fi Protected Access (WPA) introduces the Temporal Key Integrity Protocol (TKIP) that provides added security. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA-PSK or WPA2-PSK.


Radio 2 Security Setup

Encryption: WPA

Authentication: Personal(Pre-Shared Key)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

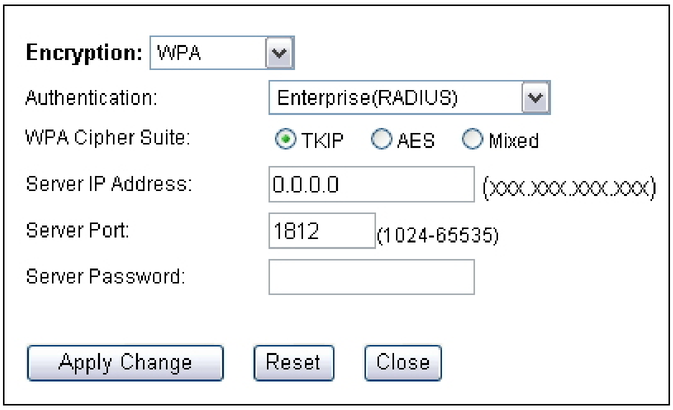
Pre-Shared Key Format: Passphrase

Pre-Shared Key: airliveairlive

- **Encryption Type**: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Mixed** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.
- **Pre-Shared Key Format**: You can select between Passphrase(ASCII) or HEX format. Please select Passphrase if you are not sure what to use.
- **Pre-Shared Key**: Enter the password key here..

## WPA-Enterprise, WPA2-Enterprise, WPA-Mixed Enterprise (Radius)

Wi-Fi Protected Access (WPA) Enterprise uses Radius Server as the authenticator. WPA2 adds full support for 802.11i standard and the CCMP (AES Encryption). The WPA-Mixed tries to authenticate wireless clients using both WPA or WPA2.


Encryption: WPA

Authentication: Enterprise(RADIUS)

WPA Cipher Suite: ● TKIP ○ AES ○ Mixed

Server IP Address: 0.0.0.0 (xxx.xxx.xxx.xxx)

Server Port: 1812 (1024-65535)

Server Password: