HAWKING TECHNOLOGY

HWL2

Hi-Gain WiFi Locator
Professional Edition

Users Manual

LIMITED WARRANTY

Hawking Technology guarantees that every HWL2 Hi-Gain WiFi Locator Professional Edition is free from physical defects in material and workmanship under normal use for two (2) years from the date of purchase. If the product proves defective during this two-year warranty period, call Hawking Customer Service in order to obtain a Return Authorization number. Warranty is for repair or replacement only. Hawking Technology does not issue any refunds. BE SURE TO HAVE YOUR PROOF OF PURCHASE. RETURN REQUESTS CAN NOT BE PROCESSED WITHOUT PROOF OF PURCHASE. When returning a product, mark the Return Authorization number clearly on the outside of the package and include your original proof of purchase.

IN NO EVEN SHALL HAWKING TECHNOLOGY'S LIABILTY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE OR ITS DOCUMENTATION.

Hawking Technology makes no warranty or representation, expressed, implied or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Hawking Technology reserves the right to revise or updates its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to:techsupport@hawkingtech.com

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 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 or more of the following measures:

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

FCC Caution

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

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 2.5cm (1 inch) during normal operation.

This EUT is compliance with SAR for general population /uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C.

Federal Communications Commission (FCC) RF Exposure Requirements

SAR compliance has been established in the laptop computer(s) configurations with PCMCIA slot on the side near the center, as tested in the application for Certification, and can be used in laptop computer(s) with substantially similar physical dimensions, construction, and electrical and RF characteristics. Use in other devices such a PDAs or lappads is not authorized. This transmitter is restricted for use with the specific antenna(s) tested in the application for Certification. The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

CONTENTS

1 INTRODUCTION 6

1.1 Features 7
1.2 Specifications 7
1.3 Package Contents 8

2 WIFI LOCATOR MODE – HOW TO USE 9

3 ADAPTER MODE – FIRST TIME INSTALLATION 12

4 CONFIGURATION UTILITY 18

1.1 Wireless Connection Status 18
1.2 Using the Utility 19
1.3 More Settings – Advanced Settings 20
1.4 Wireless Security Settings 21
1.5 Setting WPA and WPA2: 22
1.6 Using Profiles 23
1.7 Other Settings / Power Consumption Settings 24
1.8 Software Access Point Mode 26
1.9 Advanced / More Settings For AP Mode 28
1.10 Setting Wireless Security in AP Mode 28
1.11 Advanced Settings in AP Mode 29
1.12 MAC Address Filtering in AP Mode 29

5 TROUBLESHOOTING 30

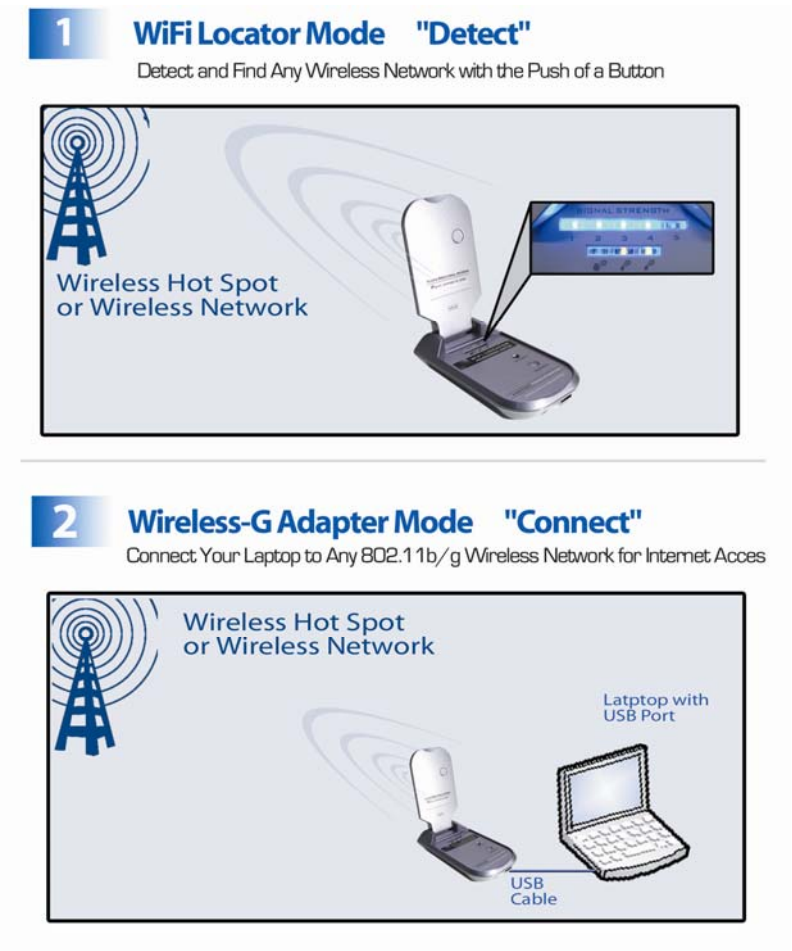
1 Introduction

-- Detect and Connect

Thank you for purchasing the Hawking Hi-Gain WiFi Locator Professional Edition. This Hi-Gain Wireless-G USB Adapter and Advanced Wireless Hot Spot Detector is designed to comply with the IEEE 802.11b/g Wireless LAN. The integration of Hawking's award winning Hi-Gain Advanced Antenna Technology and proven record in creating superior wireless products makes the HWL2 a very powerful wireless adapter/detector capable of obtaining wireless distances up to 3 times that of normal Wireless-G cards. The HWL2 detects any wireless network within a given vicinity, provides detailed information regarding the network and allows for fast easy connection to that same network.

This adapter supports the highest security standards to maintain a secure wireless connection within your wireless network. Along with the standard 64, 128, 256-bit WEP encryption, the HWL2 also supports WPA (Wi-Fi Protected Access) and WPA2 which combines IEEE 802.1x and TKIP (Temporal Key Integrity Protocol) technologies.

The Hawking HWL2 is a powerful, portable tool for the mobile user.



1.1 Features

- Detect and Connect to Any Wireless b/g Network (Bold)
- 2 Products in One: WiFi Locator + Wireless-G USB Adapter
- Finds Wireless Networks (Hot-Spots) w/o Taking Out Your Laptop
- Connects to your Laptop with USB 2.0 to access WiFi networks
- Detects and Indicates Wireless Networks with Security Enabled
- Hi-Gain Directional Flip-Open Antenna provides Optimal Wireless Range.
- Up to 300% performance increase when compared to standard wireless laptops
- Compact Pocket Sized Design

1.2 Specifications

- Standard: IEEE 802.11g/b
- Bus Type: USB 2.0 Type A
- Frequency Band: 2.4000~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g)
  BPSK, QPSK, CCK (11b)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128/256-bit WEP Data Encryption, WPA (IEEE 802.1x with TKIP), WPA2 and AES
- Antenna: Directional 5dBi Hi-Gain Antenna
- Drivers: Windows 98/SE/Me/2000/XP/2003 Server
- LED: (5x Signal Strength) (1x Power)(1x Wireless Security)(2x 802.11b/g)
- Transmit Power: 21~22 dBm (Typical w/ Antenna)

- Dimension: 92(L) x 56(W) x 25(H) mm
- Temperature: 32~131°F (0 ~55°C)
- Humidity: 0-95% (Non Condensing)
- Certification: FCC, CE

1.3 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

- One Hi-Gain WiFi Locator Professional Edition
- One USB 2.0 Extension Cable (100 cm)
- One Quick Installation Guide
- One CD (Driver/Install Wizard/Manual)
- One Hawking Wireless Hot Spot Finder Software (Inside the CD)

If any of the above items is missing, contact your supplier as soon as possible.

2 WiFi Locator Mode – How to Use

WiFi Locator Mode Basic Operation

Product Overview

Directional Hi-Gain Antenna
Helps to pinpoint the exact source of your wireless signal by detecting only the area in front of the antenna. Enhanced antenna technology allows the Locator to detect signals up to 1000ft away.

LED Description
(See Below)

Locate Button
Activiates the Locator. To do a quick scan for a WiFi network press and hold the button down.

USB 2.0 Port
Connects the HWL2 to a PC USB Port for charging the internal battery and connecting to the laptop to the internet

LED Description

Signal Strength LEDs
Displays the Signal Strength information of the associated or detected network.

Security LED
"On" when security (WEP/WPA) is enabled in the network.

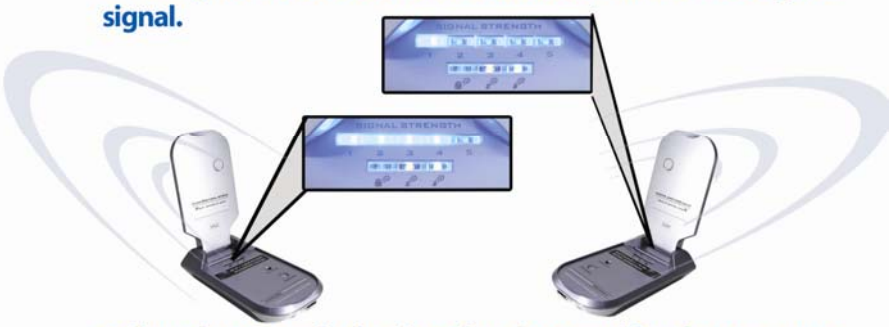
B/G LEDs
B: "On" when the network detected is an 802.11b network.
G: "On" when the network detected is an 802.11g network.
Note: When an 802.11a network is detected all lights are "off"

Power LED
"On" when the "LOCATE" button is pressed and the unit is detecting a network.
- When the HWL2 is connected to a PC via the USB cable the Power LED will blink as the unit is charging. When the unit is completely done charging the light will stay steady.

WiFi Locator Mode Basic Operation

1 **Remove** the WiFi Locator Professional Edition from the packaging and open the lid to reveal the LED readout and Locate button.

2 **To Find** the location of a wireless signal, hold down the LOCATE button in a desired direction. The LED lights will blink 3 times before displaying the results. To pinpoint the location of a wireless network or hot spot, repeat the step above in mulitple directions to find the direction with the strongest signal.



Follow the source in the direction that provides the strongest signal detection.

3 **Security** on Wireless Networks

Networks that have security enabled prohibit public access. You will not be able to connect to these networks unless you have the correct security key.

Security Enabled Security Off

The HWL2 security LED will light up when it detects a network with WEP, WPA or WPA2. It is also capable of detecting networks that do not broadcast their SSIDs.

WiFi Locator Mode

Basic Operation

4 **When** using the WiFi Locator, the HWL2 will detect the signal that is directly in front of the antenna. To operate the unit correctly please follow the illustrations below.

INCORRECT METHOD

CORRECT METHOD

Note: Pictures are of the HWL1. The instructions apply the same for the HWL2A.

5 **Recharging** the internal batteries on the HWL2A is done by connecting the Locator to the USB port of any Laptop while the Laptop is powered. When charging the Power LED will blink. When the unit is completely charged the Power LED will remain solid.

3 Adapter Mode – First Time Installation

Before you proceed with the installation, please notice following descriptions.

Note1: ***Please do not install the USB adapter into your computer before installing the software program from the CD.***

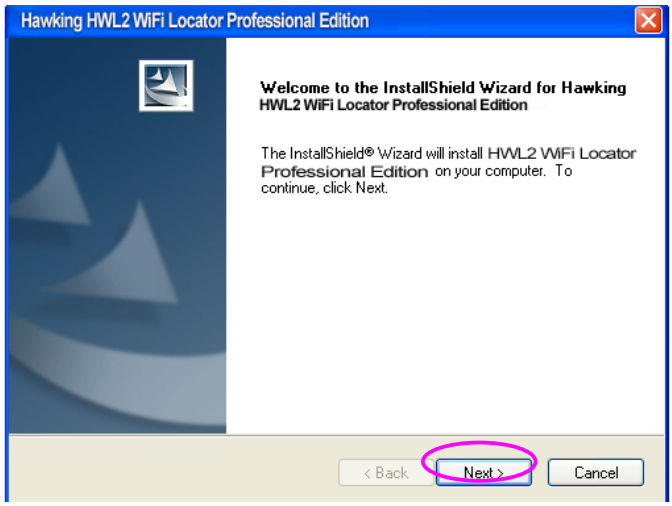
Note2: ***The following installation was operated in Windows XP. (Procedures are similar for Windows 98SE/Me/2000/2003 Server.)***

Note3: ***If you have previously installed a wireless adapter card or adapter, please uninstall the driver and utility.***

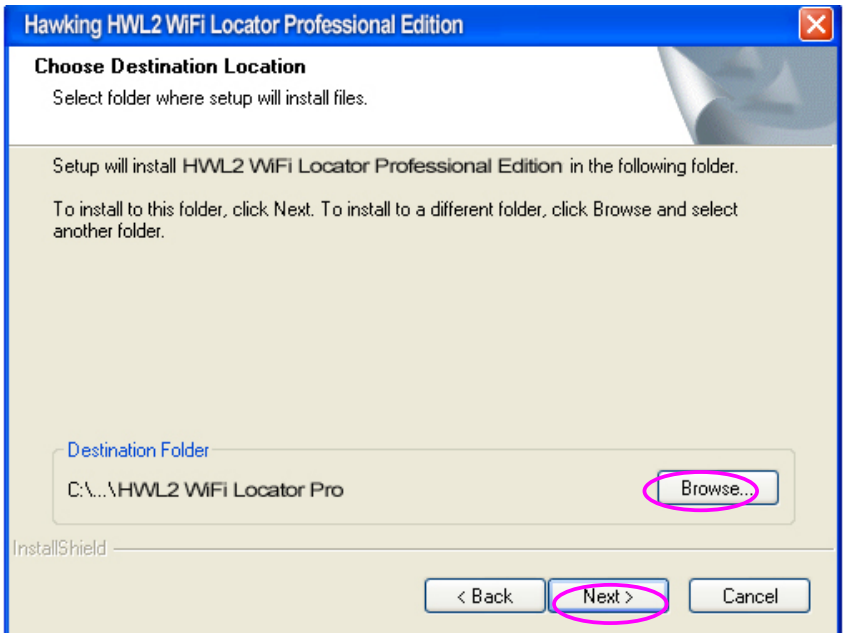
Please follow the instructions below to install the WiFi Locator Professional Edition as a Wireless USB Adapter.

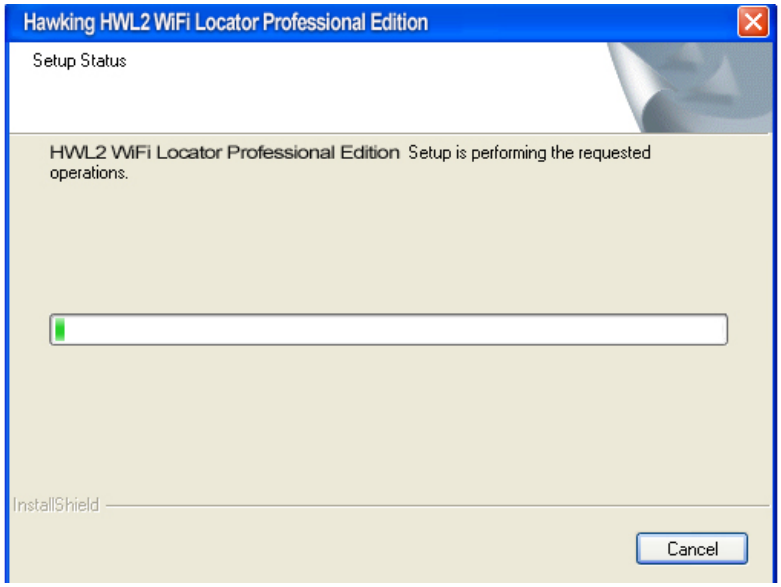
I. Install the Configuration Utility

A. Insert the Installation CD to your CD-ROM Drive. Execute the "Driver and Software Setup" program from the Autoload CD Menu. If your CD rom does not autoload, fine your CD-Rom drive and explore the contents. Double click the icon that says Autoload.exe.

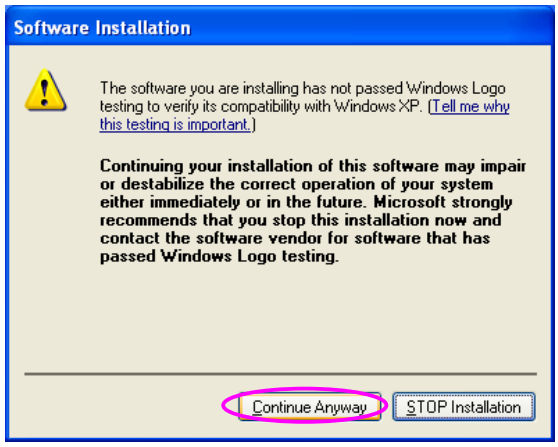


B. If you want to install the software program in another location, click “Browse” and select an alternative destination. Then, click “Next”.

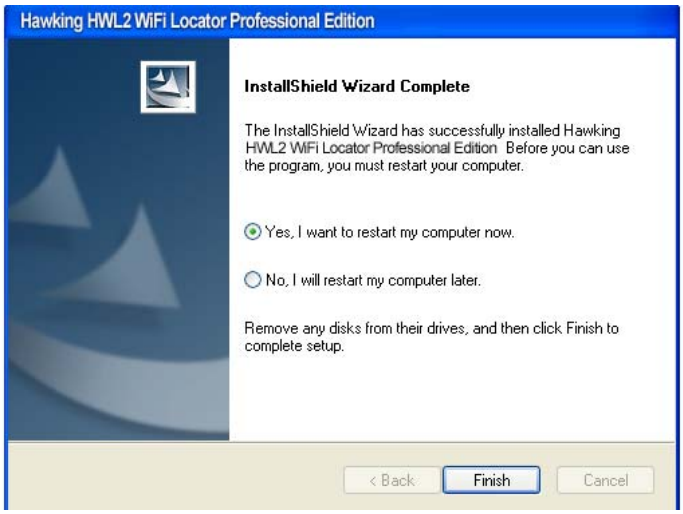




c. Click “Continue Anyway” to finish the installation.



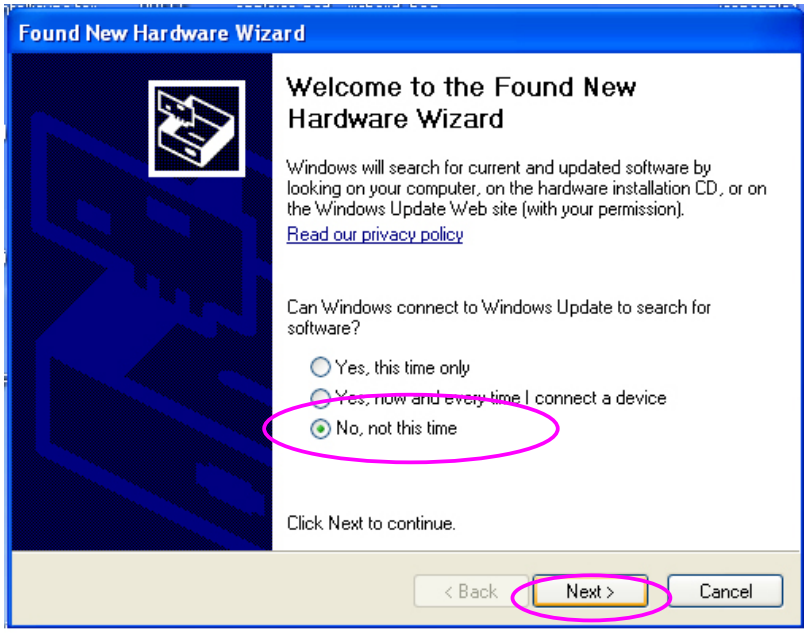
d) Click Finish to restart your computer after the installation.



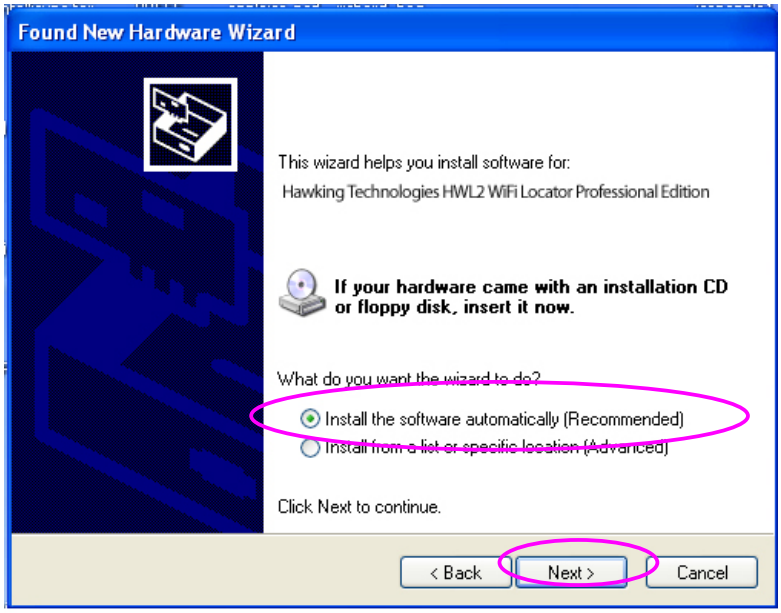
II. Install the USB Adapter

A. Plug the WiFi Locator Adapter into the USB port of your computer.

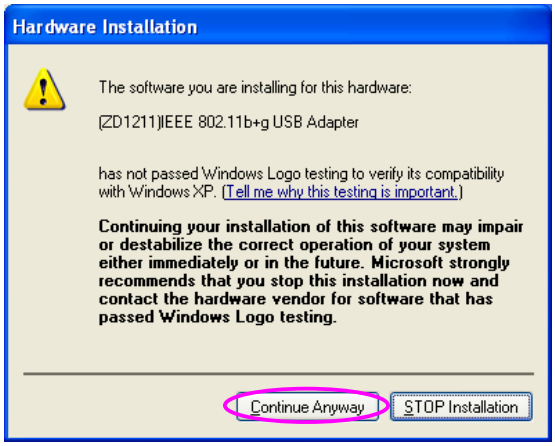
B. The “Found New Hardware Wizard” is displayed. Some computers will have the option of asking Windows Update to search automatically for software. If this happens on your computer select No not at this time.

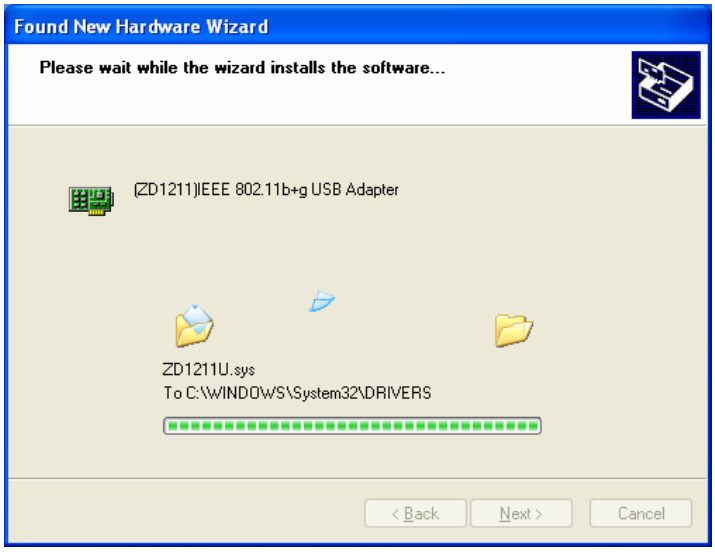


C. Select “Install the software automatically (Recommended)” and click “Next”.

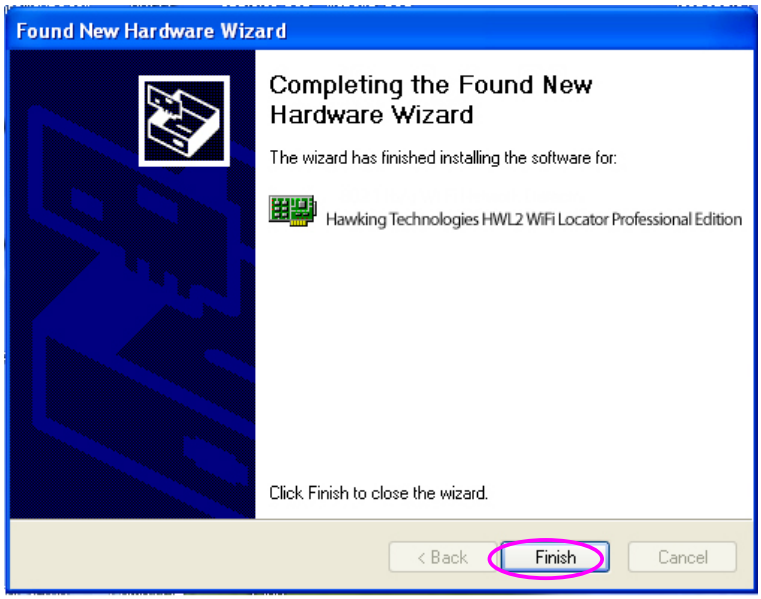


D. Click “Continue Anyway” and the system will start to install the USB adapter.





E. Click “Finish” to complete the installation.



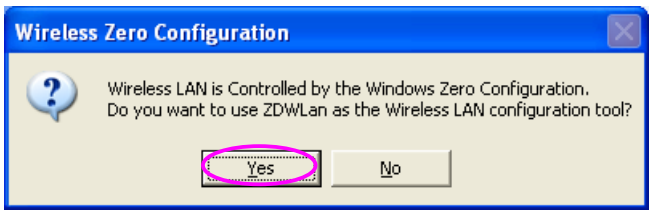
III. Using the Configuration Utility

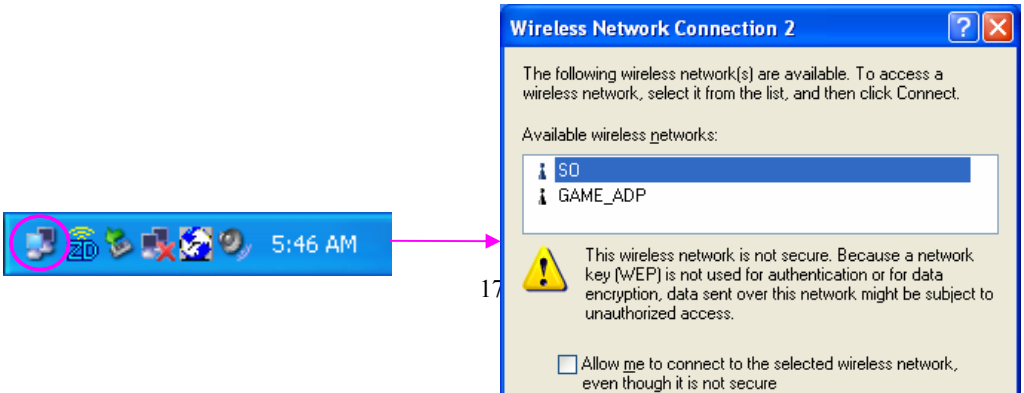
To setup the USB adapter, double-click the icon in the system tray.

For Windows XP, there is a “Windows Zero Configuration Tool” by default for you to setup wireless clients. If you want to use the Hawking Utility of the HWL2, please follow one of the ways as below. The Hawking Utility may provide more detailed features and options to adjust the adapter with.

First Method

A. Double-click the utility icon in the system tray.
B. Click “Yes” to use the utility of the USB





4 Configuration Utility

The Configuration Utility is a powerful application that helps you configure the Hawking Technologies WiFi Locator Professional Edition and monitor the link status during the communication process.

The Configuration Utility appears as an icon on the system tray of Windows while the card is running. You can open it by double-clicking the icon.

Right click the icon, there are some items for you to operate the configuration utility.

- Open Utility Window
  Select “Open Utility Window” to open the Configuration Utility tool.
- Exit Hawking Wireless Utility
  Select “Exit Hawking Wireless Utility” to close the Configuration Utility tool.

Before using the utility, you have to know some restrictions of the utility.

1. If you want to connect to an 11g (up to 54Mbps) network, please ensure to install the adapter to a PC or laptop with an available USB 2.0 interface. This adapter is backwards compatible with USB 1.1 or USB 1.0 interfaces, however due to the performance limitations of legacy interfaces the adapter cannot perform at its optimal level.
2. Under Ad-Hoc mode the adapter works in 802.11b mode only. This is a rule defined by the WiFi Organization. If you want to enable the data rate up to 54Mbps (11g), please follow the steps listed below.
   A. Go to “Network Connections”.
   B. Right Click the “Wireless Network Connection” and select “Properties”.
   C. From the pop-up screen, click “Configure”.
   D. Enter into “Advanced” page of the “Properties” screen.
   E. Enable the setting of “IBSS_G_Mode”.

1.1 Wireless Connection Status

When you open the Configuration Utility, the system will scan all channels to find the access points/stations within the accessible range of your card and automatically connect to the wireless device with the highest signal strength. From this screen, you can find details and information on the wireless networks in your environment.

1.2 Using the Utility

If you are using Windows XP as your operating system , the “Zero Configuration” feature/tool of Windows XP must be disabled first , then the Hawking Wireless Utility can be used.

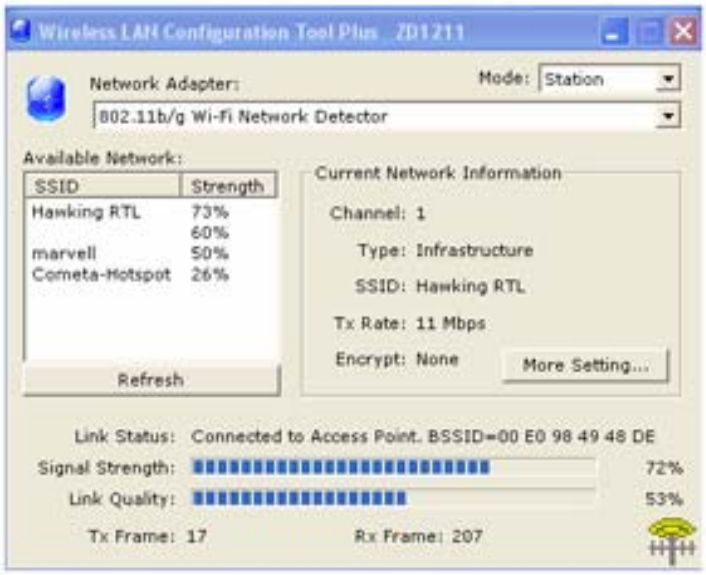


Figure 2-1

Open the Hawking Wireless Utility. The Utility Window is shown in “Figure 2-1”.
The adapter can be set in “**Station**” or “**Access Point**” Mode from the Mode drop down menu. This section will go over the “Station” Mode settings.

- You can site survey the neighboring SSID/wireless networks by pressing the “Refresh” key, the names of the wireless networks and their signal strength information will be shown in the “Available Networks” field.
- Double click the SSID site from the “Available Networks” field to connect directly to a specific SSID or wireless network.
- The information of the SSID is shown on the “Current Network Information”.
- Show the BSSID of the associated AP is diaplayed in the “Link Status” field.
- “Signal Strength” and “Link Quality” are shown below the BSSID and described with percentages.
- The number of TX Frames are displayed underneath the Signal Strength and Link Quality fields. The numbers here show the amount of data going out of your adapter to the network.
- The number of RX Frames are displayed underneath the Signal Strength and Link Quality fields. The numbers here show the amount of data coming into your adapter from the network.

1.3 More Settings – Advanced Settings

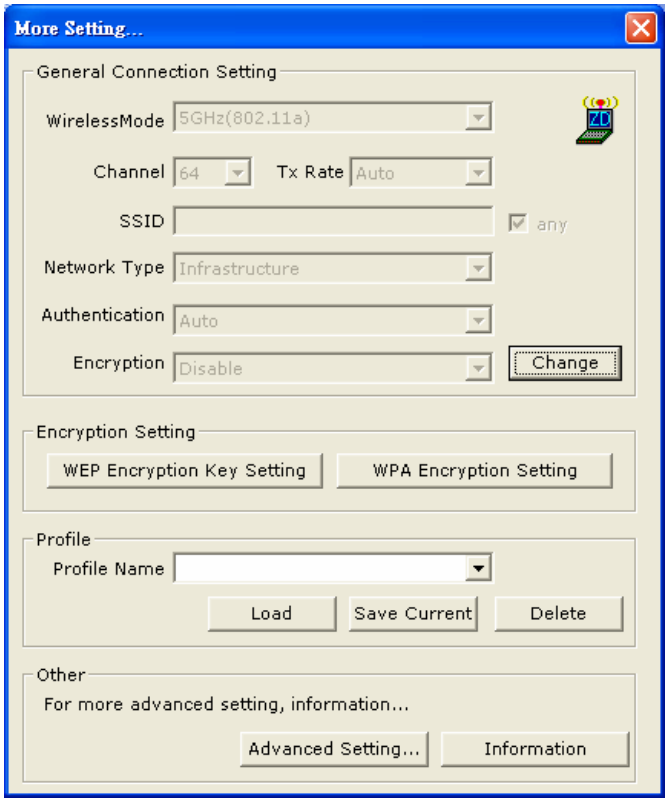


Figure 2-2

Click the " **More Settings** " icon of Figure 2-1 to enter "More settings " window. The window is shown in " Figure 2-2 ".

General Connection Settings:

- To adjust settings in the General Connection Settings page you will need to click the "Change" button.
- Press the "Change" button to modify the status, when the modification is finished, press "Apply" to save it. The button "Change" and "Apply" is alternately shown over the same position.
- Modify the SSID name from the "SSID" field. When use the item, the "any "will be unchecked previously.
- Change the channel using the drop down menu " Channel". When using this feature, Ad Hoc mode will automatically be set.
- Select the transmission rate using the " Tx Rate" drop down menu.
- Select the "Ad_Hoc" or "Infrastructure" Mode from the "Network Type" drop down menu.
- Select the Security settings: "Open System" , "Shared Key", "Auto", "WPA" , "WPA PSK", "WPA2", "WPA2 PSK" from the "**Authentication Mode**" drop down menu.
- Select the "Disable" ,"WEP", "TKIP" , "AES" by the "Encryption" drop down menu.

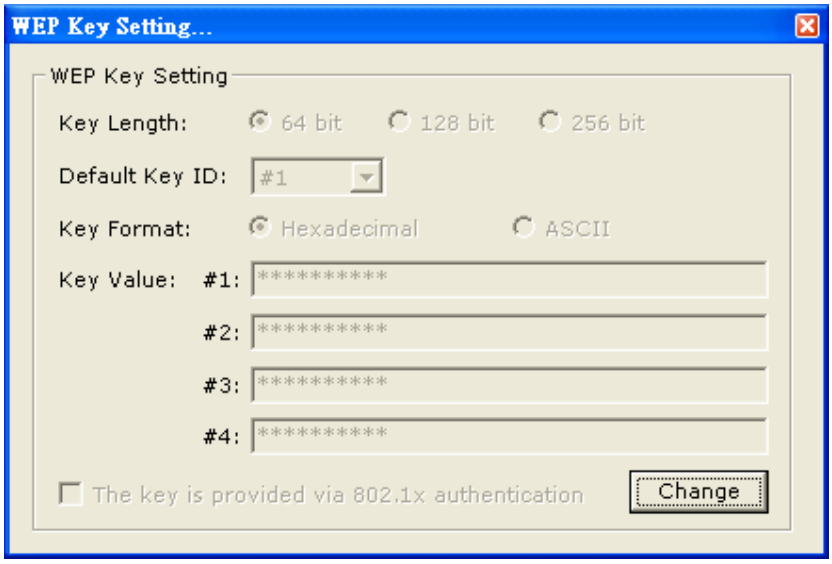


Figure 2-3

1.4 Wireless Security Settings

Setting WEP:

WEP Encryption is a standard wireless network security protocol used to protect wireless data from being hacked and intercepted.

- Select the "Open System" , "Shared Key" mode or "Auto" from the "authentication Mode" drop down menu.
- Select the "WEP" mode from the "Encryption" drop down menu.
- Press "WEP Encryption Setting" in Figure 2-2 to enter the "WEP Key Settings" page shown as Figure 2-3.
- Press the "Change" button to modify the contents of "WEP Key setting", when it is finished, press "Apply" to save it. The button "Change" and "Apply" is alternately shown in the same position.
- Select which "key length" 64,128 or 256 (bit) that you wish to use within your network. If you do not know this information check with your network administrator.
- Select which key set will be used by the field of "Default Key ID" Modify the 4 sets of keys depending on the selected key length in the field of "Key Value". The key value is used in hexadecimal format.
- Select which key format "hexadecimal" or "ASCII" will be used from the "Key Format" selection. .

Dynamic WEP:

If you checked the " The key is provided via 802.1x authentication" of Figure 2-3 , and press the button: "Apply" , the "Use previous 802.1x Setting" page should load as in Figure 2-4.
Press "Yes," if you wish to use previous settings. Select "No" , if you wish to have new settings. The setting method is the same as setting "TLS" and

"PAEP" items. (Refer to 2.3.2.3)

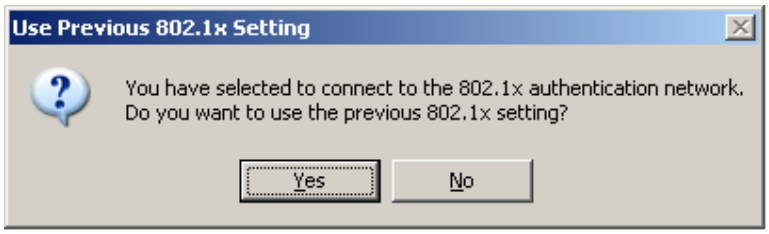


Figure 2-4

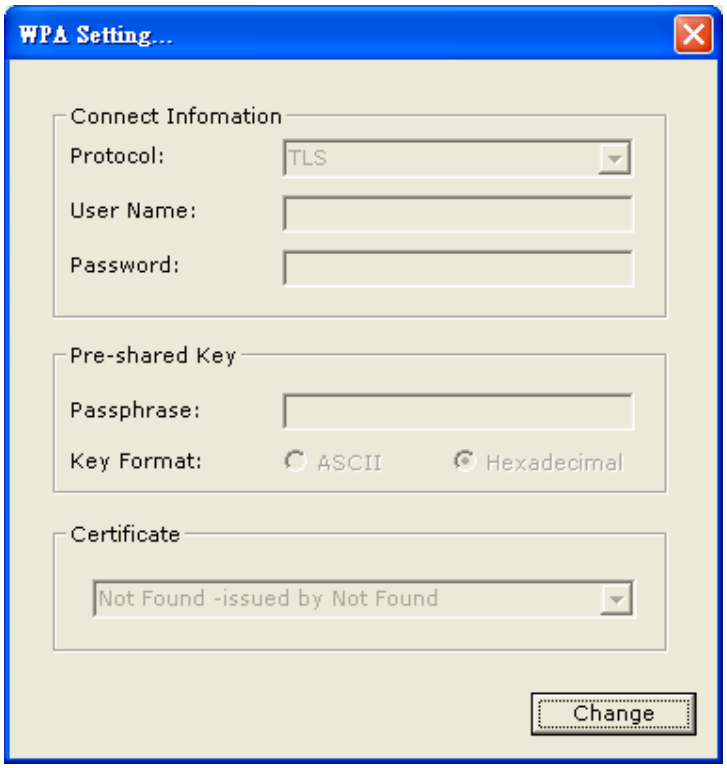


Figure 2-5

1.5 Setting WPA and WPA2:

WPA and WPA2 Security is an advanced wireless security standard. It is more complex than standard WEP encryption and offers more robust security features:

- Press the "Change" button to modify the contents of "WPA setting", when it is finished, select "Apply" to save your changes. The"Change" and "Apply" buttons are alternately shown in the same position.

- Select "WPA" , "WPA PSK", "WPA2" or "WPA2 PSK" from the "authentication Mode" drop down menu depending on what security

protocol your network is set on. Note: If you do not have this information please contact your system administrator for answers and assistance.

- Select "TKIP" or "AES" mode from the "Encryption" drop down menu depending on what is used in your specific network.. WPA , WPA PSK , WPA2 or WPA2 PSK encryption modes will use TKIP or AES.
- Select "WPA Encryption Settings" in Figure 2-2 to enter the "WPA Settings" page shown in Figure 2-5.
- After selecting the Authentication Protocol (i.e. WPA or WPA2) you must select "TLS" or "PEAP" from the "Protocol" drop down menu . If TLS is selected, the User name and Certificate of your network will be required to connect to a WPA/TLS enabled network. If PEAP is used, the User name, Password and Certificate need to be used for authentication to a specific network.
- If you selected the pre-share-key (WPA PSK or WPA2 PSK) protocol, you can enter your password in the "Passphrase" field for access to the specific network . If the ASCII format is checked, the password length can be selected from 8 bytes to 63 bytes depending on the user and network settings. If you check the Hexadecimal format, 64-bit characters must be keyed in.

1.6 Using Profiles

Profiles can be used to save the connection and authentication settings of previously connected networks. These profiles can be accessed at a later time when the network is present by simply loading a saved profile:

- Select the profile that has been saved previously from the "Profile name" drop down menu, then press the "Load " button to load the previously saved profile.
- Write the profile name in the "Profile name" field, and press the "Save Current" button to save the current status of the profile.
- Select the profile name that you wish to delete from the "Profile name" drop down menu, and press "Delete" button to delete it

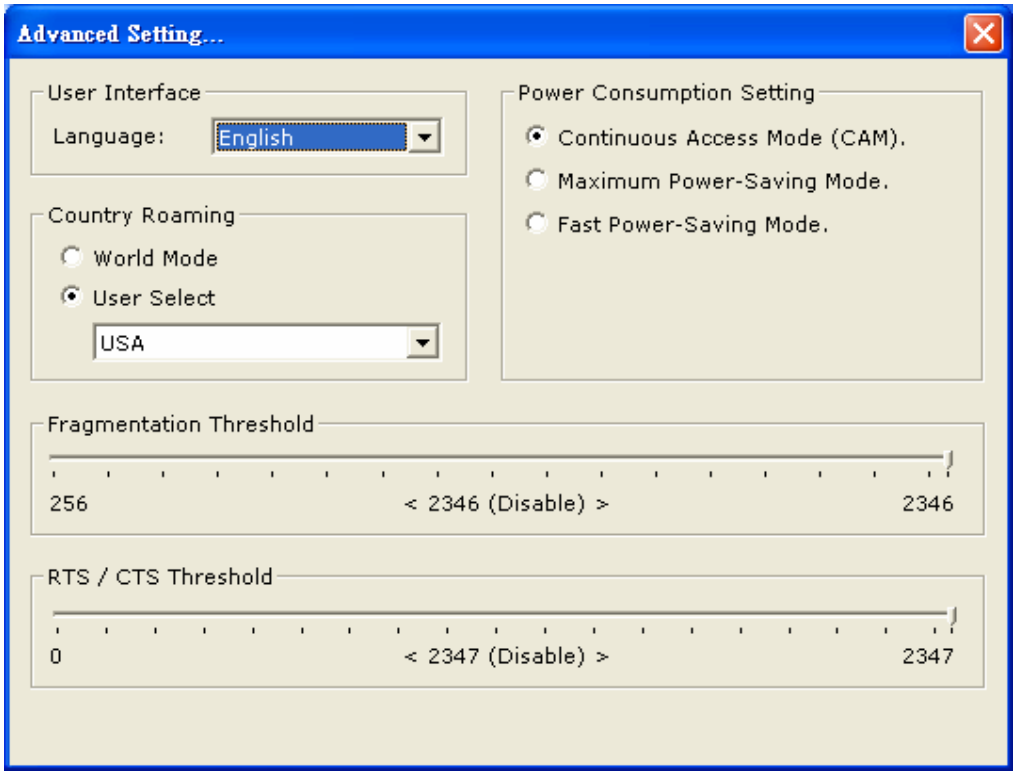


Figure 2-6

1.7 Other Settings / Power Consumption Settings

The "Other" settings page will allow you to adjust more advanced features of the Wireless adapter. It is recommended that these settings not be changed unless by an advanced wireless user.

Press the "Advanced Settings" button to access the Advanced Settings page as seen in Figure 2-6.

- To change the Language of the Wireless Utility select the preferred language from the "Language" drop down menu.
- To adjust the Power Consumption of your wireless adapter, select which power save level you wish to use by checking off CAM Mode, Maximum Power-Saving mode or Fast Power-Saving mode. The default is CAM mode. For the lowest power consumption setting, select Maximum Power-Saving mode, throughput will be lower than it would be in CAM and Fast Power-Saving mode. The throughput of "Fast Power-Saving mode" is better than "Maximum Power-Saving mode", but saves less power when compared to "Maximum Power-Saving mode".
- The Country Roaming settings allow the user to predefine whether the adapter will be used internationally. Different countries have different settings for wireless adapters. Select other region from "User Select" drop down menu, or check "World Mode" to set the adapter in a world roaming mode. When the word mode is set, the adapter will adapt to the settings of the AP it is associated

to.

- The Fragmentation Threshold Settings bar allows for adjustment of fragmentation threshold point, the range is from 256 to 2346 bytes.
- The RTS / CTS Threshold bar, allows for adjustments of the RTS threshold point, the range is from 0 to 2347 bytes.

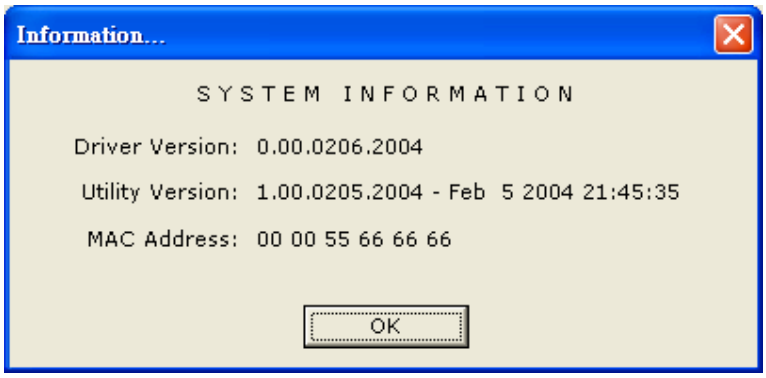


Figure 2-7

Press the "Information" button to view the Information page of the Utility as shown in Figure 2-7. It includes the Driver version, Utility Version and MAC Address of the associated adapter.

1.8 Software Access Point Mode

The Hawking Wireless Utility offers a special feature that allows the HWL2 to function as a 802.11b or 802.11g software access point.

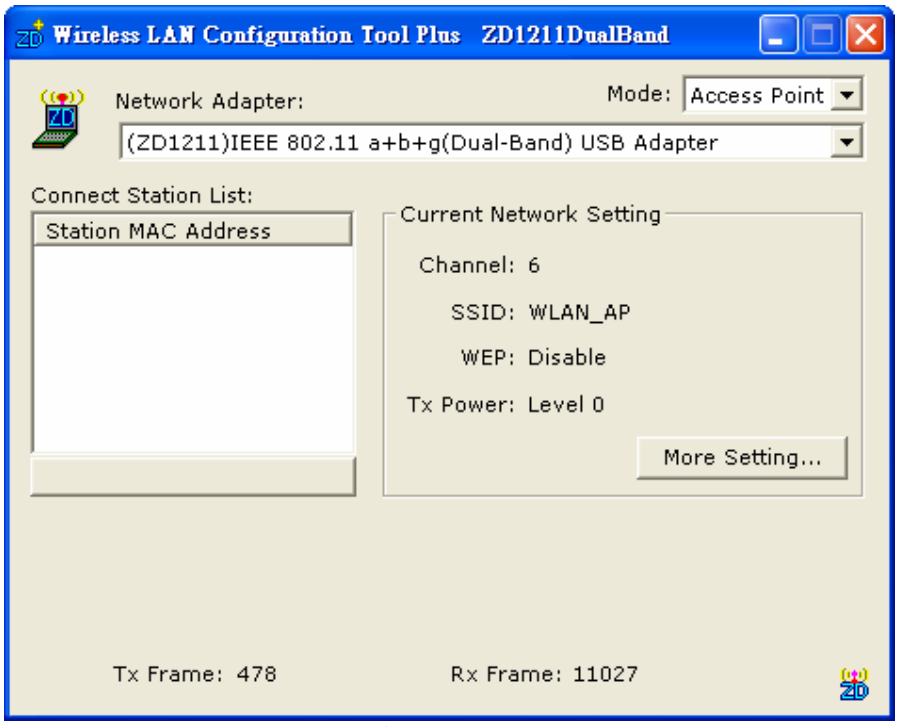


Figure 3-1

Open the Hawking Wireless Utility from the "Start Menu". The menu page should load. To change the mode to Soft AP, please select the option " Access Point" from the Mode drop down menu, as shown in Figure 3-1.

- "Network Adapter" shows the available network adapters that can be chosen for use in AP Mode.
- The clients that associate to the access points will have their MAC addresses shown in the field of the "Station MAC Address".
- The current status of the AP is shown in the "current Network Setting" field. This field displays the Current Channel information, as well as the Access Point's SSID. The status of WEP encryption is displayed as disabled or enabled. The Tx power level is shown too (The function not available).
- The Tx Frame shows how many frames have been transmitted by the soft AP.
- The Rx Frame shows how many frames have been received by the soft AP.

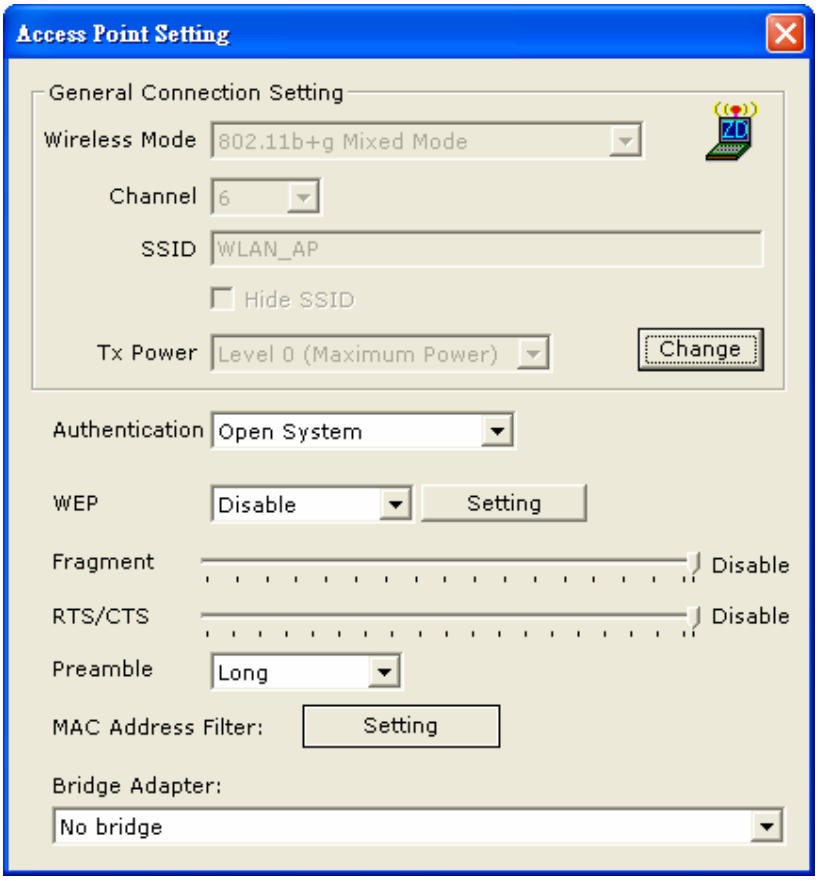


Figure 3-2

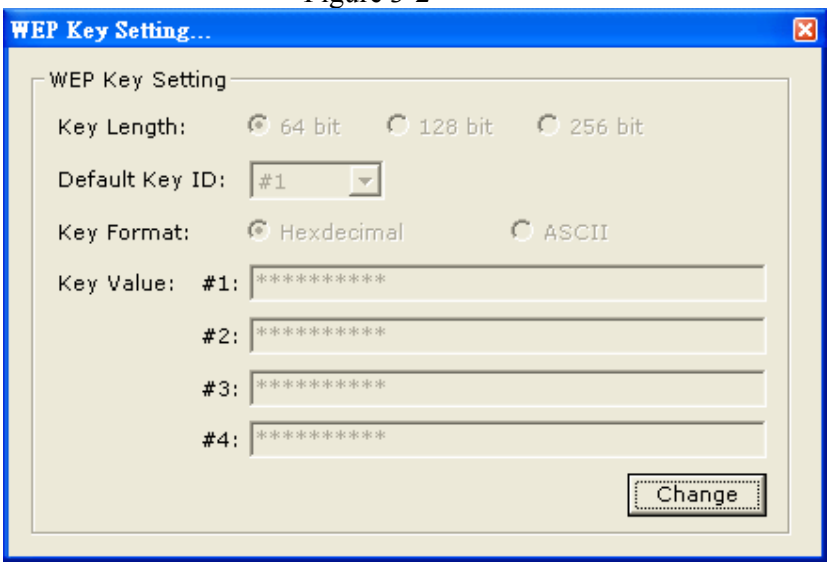


Figure 3-3

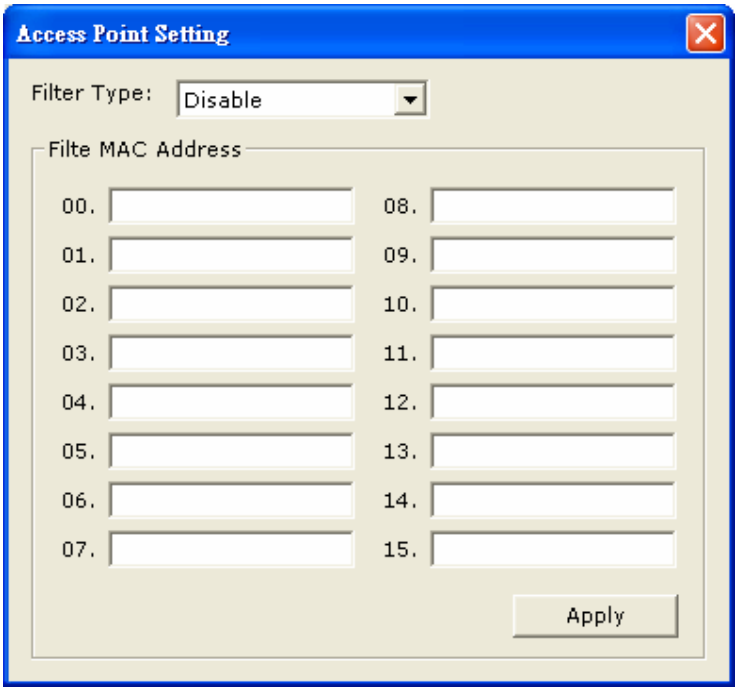


Figure 3-4

1.9 Advanced / More Settings For AP Mode

Click the **" More Setting "** icon of Figure 3-1 to enter the "More setting " menu. The "Access Point Setting" page is shown in " Figure 3-2 ".

- Press the "Change" button to modify the "General Connecting Settings" , and press the "Apply" button to save the changes. The "Change" and "Apply" buttons are alternately shown in the same position.
- Select the wireless mode of your soft AP by selecting " 802.11b+g Mixed Mode" , "802.11g only" , "802.11b only" or "802.11a only" mode from the "Wireless Mode"drop down menu.
- Select the channel from the drop down menu " Channel".
- Modify the SSID name from the "SSID" field.
- Check the "Hide SSID" box to hide the SSID from outside clients attempting to connect to your Soft AP. When outside computers attempt to search for local networks, your specific SSID will not be displayed.
- There are 4 sets transmit power level that can be selected in the "Tx power" field.(Level 0 is the only available selection for this model).

1.10 Setting Wireless Security in AP Mode

- Enable or Disable WEP encryption from the drop down menu "WEP".
- Press the "Settings" button to open the "WEP key settings" page shown in Figure 3-3. Press the "Change" button to modify the contents of the "WEP Key setting", when it is finished, press "Apply" to save it. The button "Change" and "Apply" are alternately shown in the same position. Select which key length

64,128 or 256 bits you wish to use for your network.
Select a "Default Key ID" for your network from the default Key field. Modify the 4 sets key depending on the selected key length on the field of "Key Value". Depending on which key mode you choose to enter, "hexadecimal" or "ASCII" the key value will change accordingly. For more information regarding hexadecimal or ASCII keys please contact our Techsupport..

- Select "Open System" or "Shared Key" mode from the "authentication Mode" drop down menu depending on what type of security you wish to setup in your network.

1.11 Advanced Settings in AP Mode

- Adjust the fragmentation threshold point by sliding the bar left and right. The range is from 256 to 2346 (Disable) bytes.
- Adjust the "RTS / CTS" settings by sliding the bar left and right. The threshold point range is from 0 to 2347(Disable) bytes.
- The advanced settings tab allows users to adjust their Preamble to long or short. If you are an advanced user you may set the value here. Otherwise it is recommended that you use the default setting.

1.12 MAC Address Filtering in AP Mode

- **MAC Address Filtering** - to use MAC address filtering, select the Mac Address Filter button. The menu page will load as shown in Figure 3-4. Select "Disable" or "Accept" or "Filter" from the field in the drop down menu "Filter Type". The MAC Address filtering option supports up to 16 sets of MAC. When you have finished setting your values, click apply to save your settings.

- **Bridge Adapter**
- To use the adapter as a Bridge Adapter you must first select the adapter from the drop down menu.

5 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the adapter.

1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks.

802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. What is the IEEE 802.11b standard ?

The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate successfully and efficiently.

3. What does IEEE 802.11 feature support ?

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

4. What is Ad-hoc ?

An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. What is Infrastructure ?

An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. What is BSS ID ?

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. What is WEP ?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. Can Wireless products support printer sharing ?

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air ?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS ? What is FHSS ? And what are their differences ?

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum ?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).