

ZyXEL

WM5204Z

Wireless LAN USB 2.0 Adapter

User's Manual

Release 2.0

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.

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.

FCC Caution:

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

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.



This device is intended only for OEM integrators under the following conditions:

- 1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and
- 2) The transmitter module may not be co-located with any other transmitter or antenna,
- 3) For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as 3 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in devices where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example access points, routers, wireless ASDL modems, and similar equipment). The final end product must be labeled in a visible area with the following: "Contains TX FCC ID:

I88WM5204Z

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how

to install or remove this RF module in the user's manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.

注意！

依據 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本模組於取得認證後將依規定於模組本體標示審合格籤，並要求平台上標示「本產品內含射頻模組：ID 編號」

About this manual

This User's Manual describes how to install and operate your 802.11b/g Wireless LAN Module. Please read this manual before you install the product. This manual includes the following topics:

- I Product description and features.
- I Software installation procedure for certification use

Company Confidential

Table of Contents

CHAPTER 1: INTRODUCTION	1
FEATURES	1
CHAPTER 2: INSTALLATION	2
FOR WINDOWS 2000/XP.....	2
Install the Software.....	2
Install the Hardware.....	4
Verification.....	5
FOR WINDOWS VISTA.....	6
Install the Software.....	6
Install the Hardware.....	8
Verification.....	8
NETWORK CONNECTION.....	9
IP Address.....	9
FOR LINUX KERNEL 2.4/2.6 INSTALLATION	10
Install the Hardware.....	10
Install the Software.....	10
FOR MAC OS 10.5 INSTALLATION.....	12
Install the Software.....	12
Install the Hardware.....	13
CHAPTER 3: UTILITY CONFIGURATION.....	14
FOR WINDOWS 2000/XP.....	14
Station Mode.....	15
Utility Menu List.....	32
Soft AP mode.....	33
FOR WINDOWS VISTA.....	40
Station Mode.....	41
Utility Menu List.....	57
Soft AP mode.....	58
CHAPTER 4: UNINSTALLATION.....	65
FOR WINDOWS 2000/XP.....	65
FOR WINDOWS VISTA.....	67
FOR MAC OS 10.5.....	69
FOR LINUX KERNEL 2.4/2.6	71

Chapter 1:

Introduction

The Wireless LAN Module is an IEEE802.11b/g Module that connects your notebook to a wireless local area network. The Wireless LAN Module fully complies with IEEE 802.11 b/g standards, delivers reliable, cost-effective, feature rich wireless connectivity at high throughput from an extended distance.

It allows you to take full advantage of your notebook's mobility with access to real-time information and online services anytime and anywhere.

Features

- Ø 1T1R Mode with 54Mbps PHY Rate for both.
- Ø Complies with IEEE 802.11 b/g standards.
- Ø Supports WEP 64/128 bits, WPA, WPA2.
- Ø Supports WMM and WMM-PS.
- Ø Supports WPS configuration.
- Ø Portable and mini-size design.
- Ø Compatible with Microsoft Windows 2000/XP/Vista, Mac OS 10.3/10.4/10.5, and Linux Kernel 2.4/2.6 operating systems.

Chapter 2: Installation

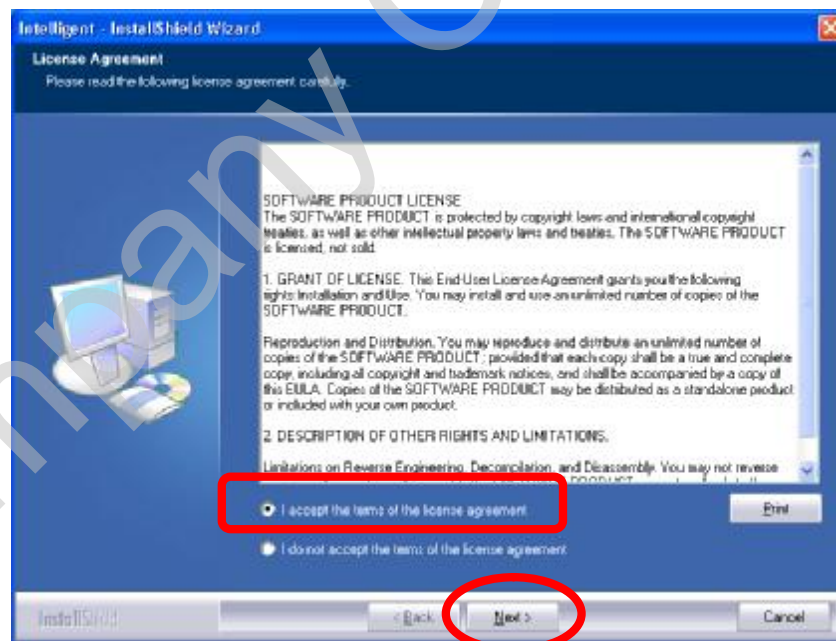
For Windows 2000/XP

Install the Software

Note:

Do not insert the Wireless LAN Module into the computer until the Install Shield Wizard has finished installing.

1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically.
2. When the License Agreement screen appears, please read the contents and select “**I accept the terms of the license agreement**” then click **Next** to continue.

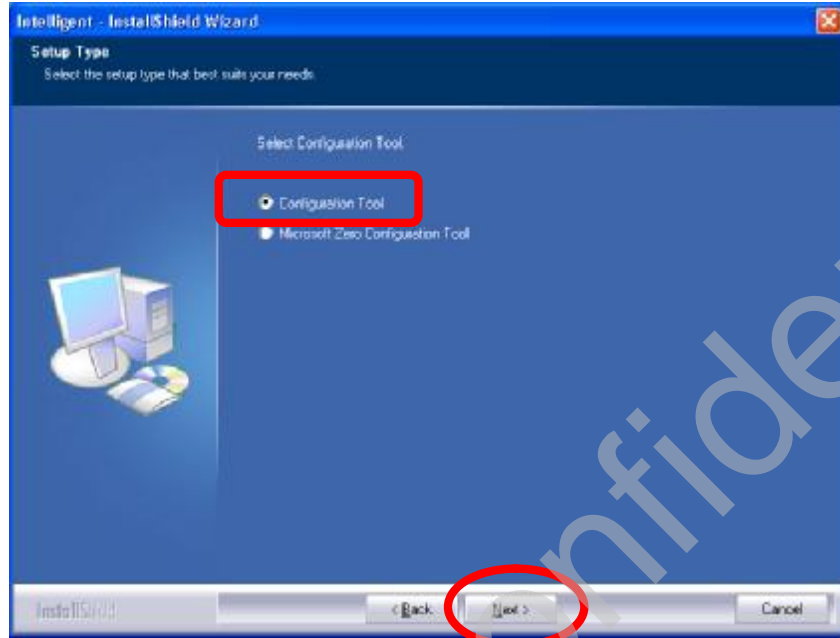


3. Select the check box to choose a **Configuration Tool** from the listed two choices.

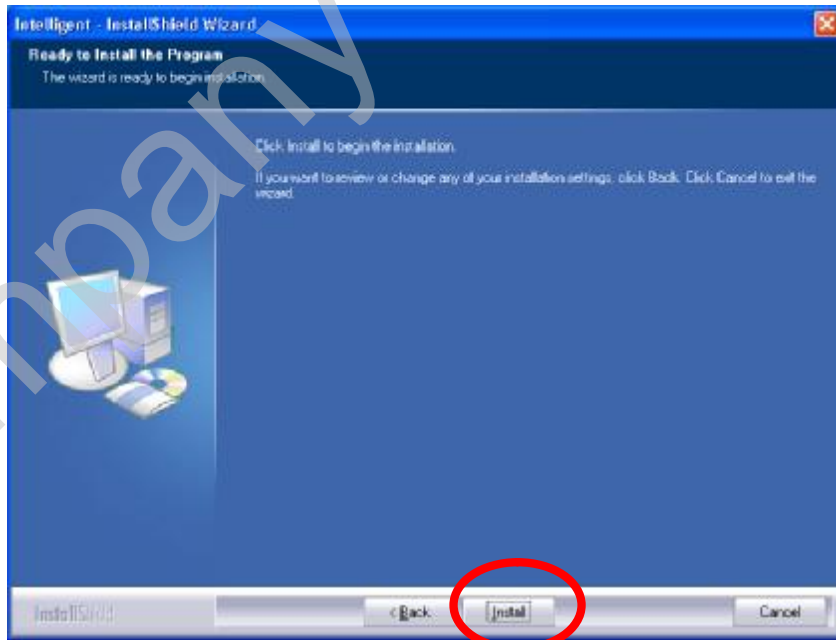
I Configuration Tool: Choose to use the configuration utility.

- I **Microsoft Zero Configuration Tool**: Choose to use Windows XP's built-in Zero Configuration Utility (ZCU).

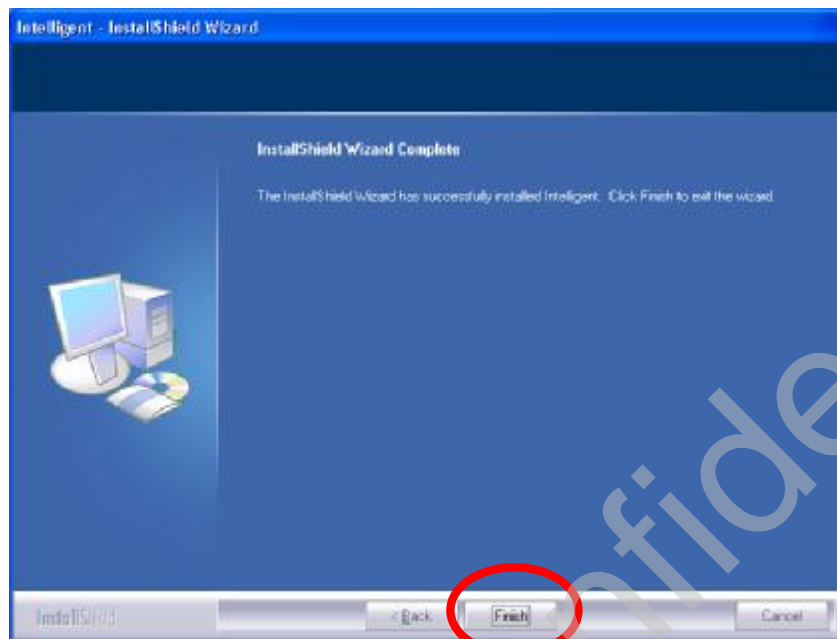
Click **Next** to continue.



5. When prompt to the following message, please click **Install** to begin the installation.



- When the following screen appears, click **Finish** to complete the software installation.



Install the Hardware

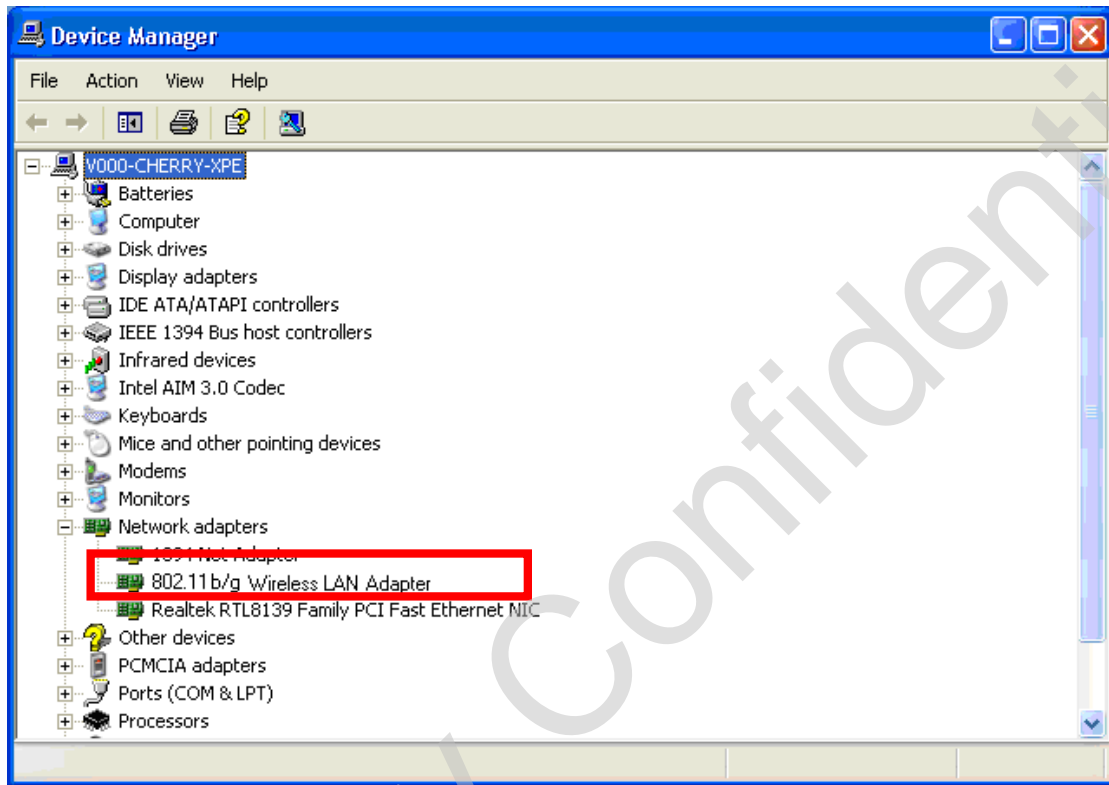
Note:

Insert the Wireless LAN Module after software installation.

Insert the Wireless LAN Module into the computer. The system will automatically detect the new hardware.

Verification

To verify if the device is active in the computer. Go to **Start > Setting > Control Panel > System > Hardware > Device Manager**. Expand the **Network Adapters** category. If the **802.11b/g Wireless LAN Module** is listed here, it means that the device is properly installed and enabled.



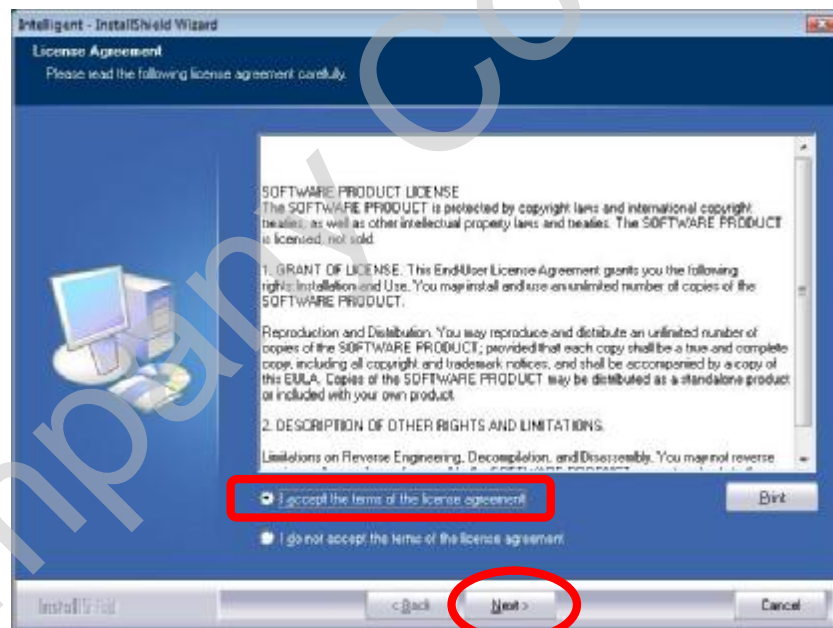
For Windows Vista

Install the Software

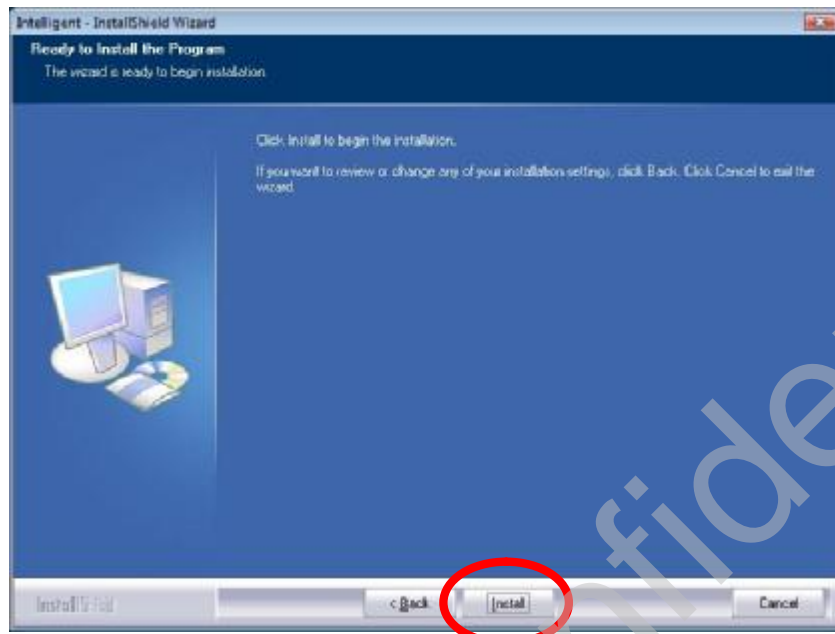
Note:

Do not insert the Wireless LAN Module into the computer until the Install Shield Wizard has finished installing.

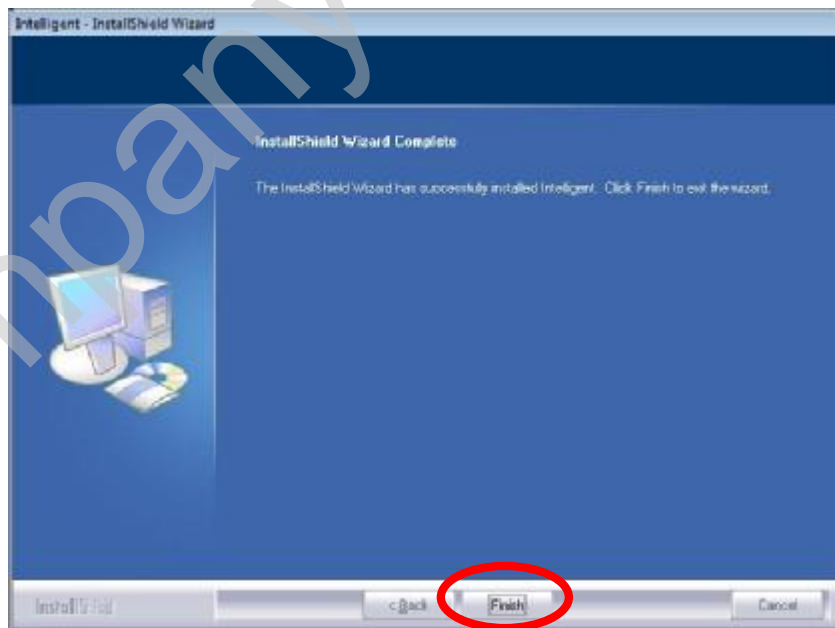
1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically.
2. When the **License Agreement** screen appears, please read the contents and select “**I accept the terms of the license agreement**” then click **Next** to continue.



3. When prompt to the following message, please click **Install** to begin the installation.



4. When the following screen appears, click **Finish** to complete the software installation.



Install the Hardware

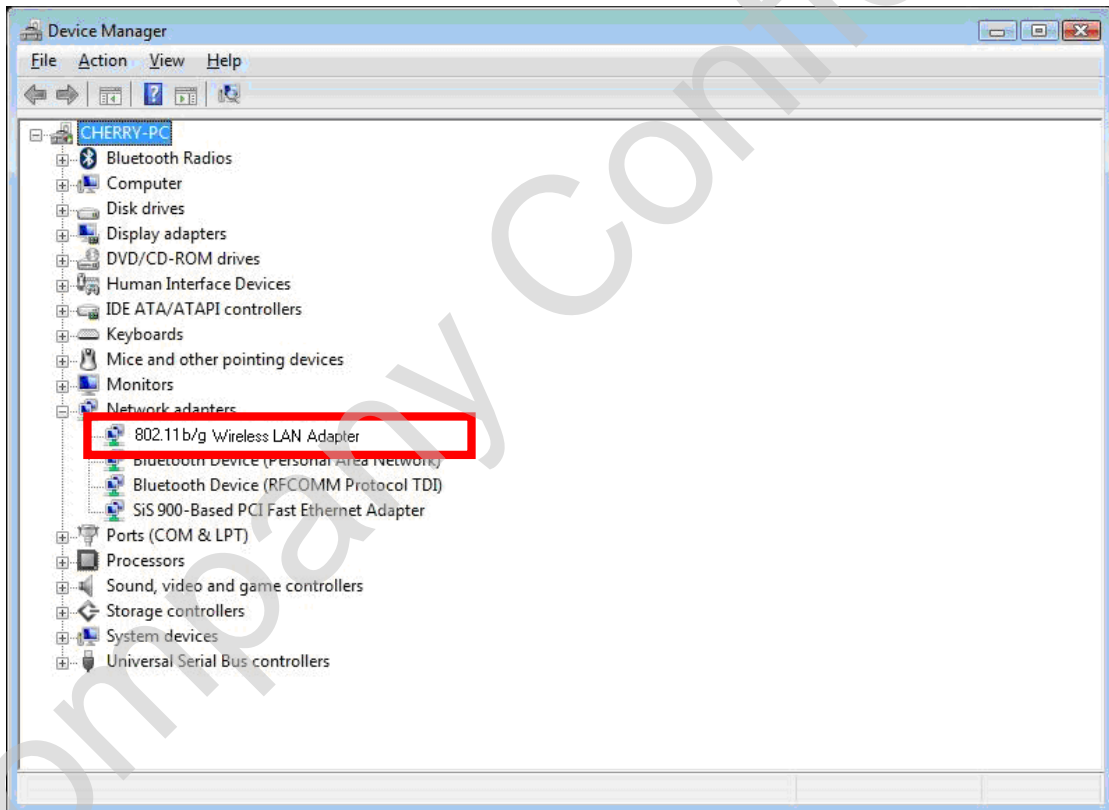
Note:

Insert the Wireless LAN Module when finished software installation.

Insert the Wireless LAN Module into the computer. The system will automatically detect the new hardware.

Verification

To verify if the device is active in the computer. Go to **Start > Setting > Control Panel > System > Hardware > Device Manager**. Expand the **Network Adapters** category. If the **802.11b/g Mini Wireless LAN Adapter** is listed here, it means that the device is properly installed and enabled.



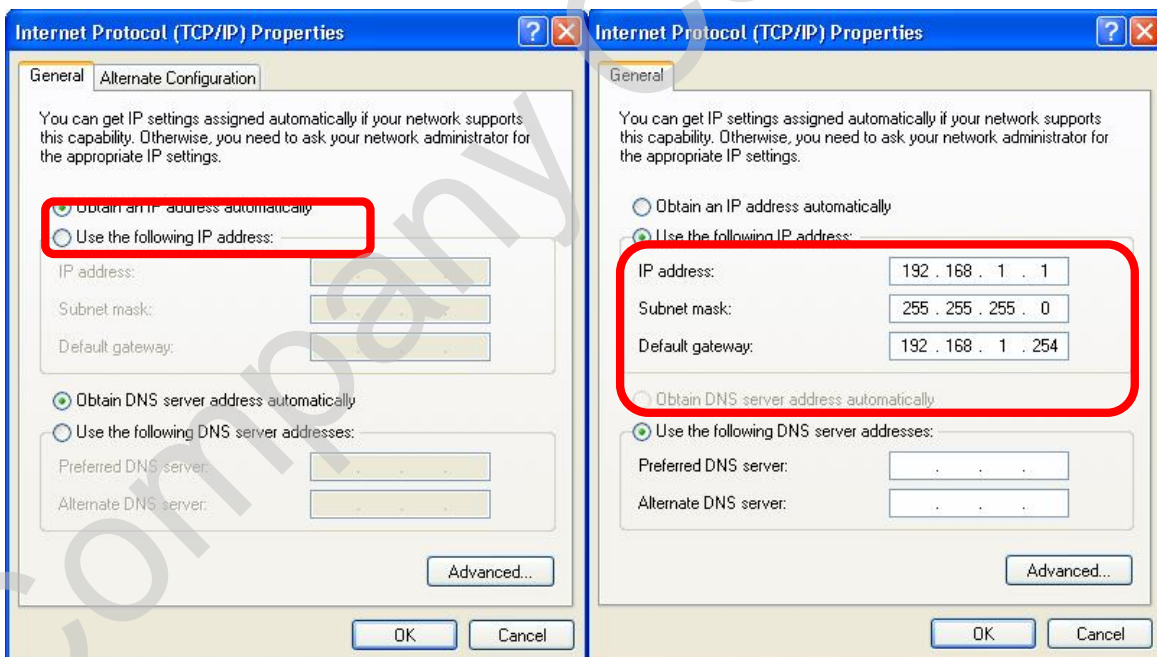
Network Connection

IP Address

Note:

When assigning IP address(es) to computers on the network, remember to have IP address for each computer set on the same subnet mask. If the Broadband Router has enabled its DHCP server function, it won't be necessary to assign static IP address for PC.

1. To configure a dynamic IP address (i.e. if the broadband Router has enabled the DHCP server function), check the **Obtain an IP address automatically** option.
2. To configure a fixed IP address (if DHCP server function is not enabled in Broadband Router, or when PC needs to be assigned a static IP address), check the **Use the following IP address** option. Then, enter an IP address into the empty field; for example, enter **192.168.1.1** in the IP address field, **255.255.255.0** for the Subnet Mask, and **192.168.1.254** for the default gateway.



For Linux Kernel 2.4/2.6 Installation

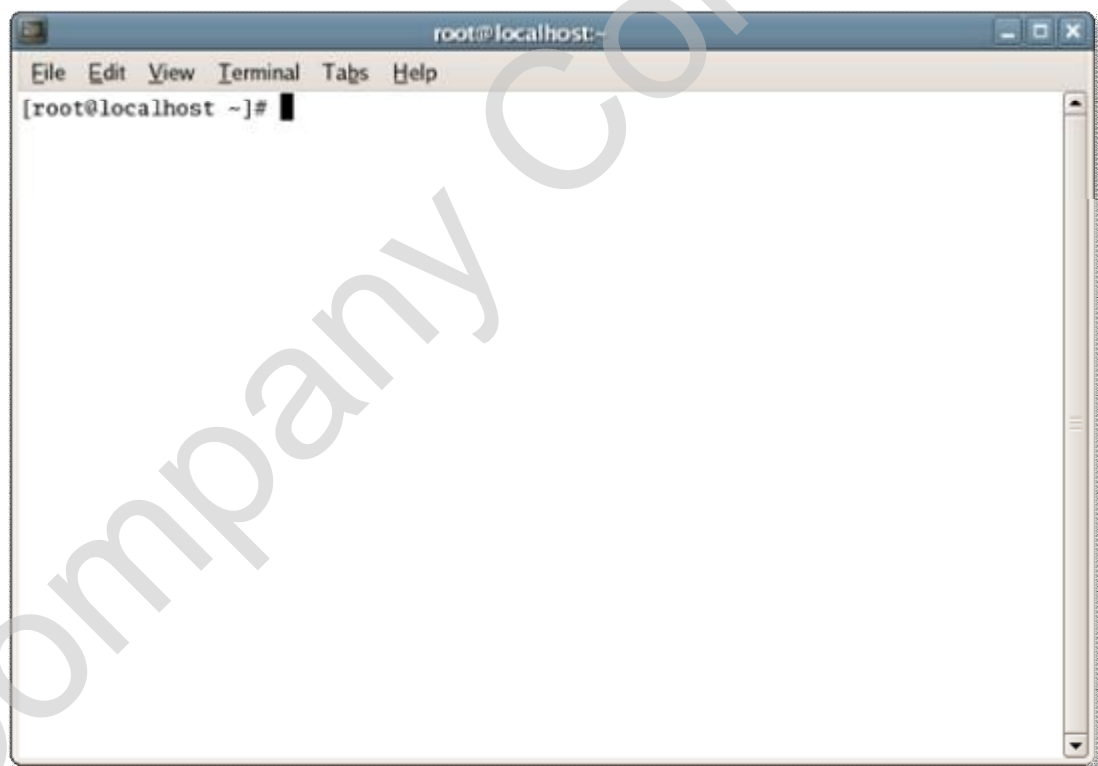
Install the Hardware

Note:

Please insert the Wireless LAN Module into the PC USB port BEFORE the driver installation.

Install the Software

Please execute the Terminal program and follow the steps below to install the driver of Wireless LAN Module.



1. Go to root

```
# cd /home
```

```
# mkdir DRIVER(example)
```

```
# cd DRIVER
```

```
# cp xxx_RT3070_Linux_STA_x.x.x.x.tar.bz2 /home/DRIVER
```



```
2. # tar -jxvf xxx_RT3070_Linux_STA_x.x.x.x.tar.bz2
    go to "/xxx_RT3070_Linux_STA_x.x.x.x" directory.
3. # make clean
4. # make
PS: If there is ERROR Message after compile, then user may need to recheck the Makefile or .c and .h
5. # cd /etc/Wireless/
6. # mkdir RT2870STA
7. go to "./home/DRIVER/xxx_RT3070_Linux_STA_x.x.x.x" directory
8. # cp RT2870STA.dat /etc/Wireless/RT2870STA/RT2870STA.dat
9. go to "./home/DRIVER/xxx_RT3070_Linux_STA_x.x.x.x/os/linux/" directory.
Load driver
[kernel 2.4]
# /sbin/insmod rt3070sta.o
# /sbin/ifconfig ra0 inet YOUR_IP up
[kernel 2.6]
# /sbin/insmod rt3070sta.ko
# /sbin/ifconfig ra0 inet YOUR_IP up
Unload driver
# /sbin/ifconfig ra0 down
# /sbin/rmmod rt3070sta
10. Scan AP
    # iwlist ra0 scanning
11. Connect to AP
    # iwpriv ra0 set SSID="AP's SSID"
12. Check status
    # iwconfig ra0 or # ifconfig ra0
```

Note:

- 1. Supporting Kernel: Linux kernel 2.4 and 2.6 series. Tested in Redhat 7.3 or later.**
- 2. Clear DHCP on ra0**
killall dhclient
- 3. Get DHCP from AP**
dhclient ra0

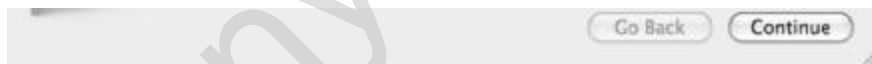
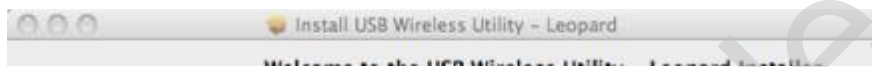
For Mac OS 10.5 Installation

Install the Software

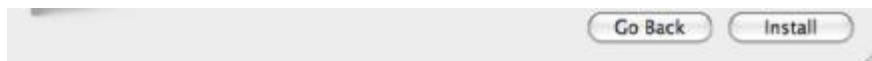
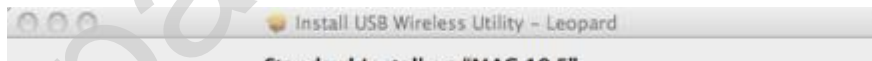
Note:

Do not insert the Wireless LAN Module into the computer until the installation finished.

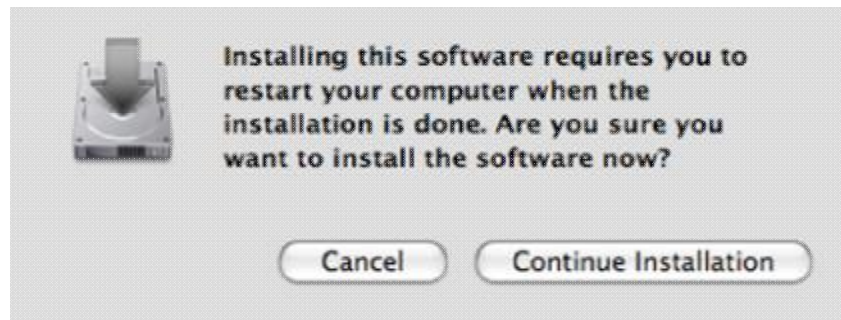
1. Insert the included CD-ROM into the CD-ROM drive of your computer. Please find and execute the xxx.dmg file, then select the install Mac version of your PC, and click the USBWireless-Leopard.pkg file to install.
2. When the Welcome screen appears, click **Continue** to start.



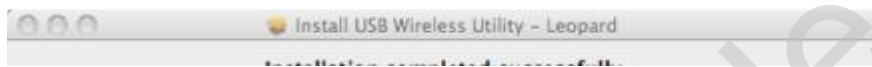
3. Please click **Install** to process the installation.



4. The computer restart message will show up, please click **Continue Installation** to install.



5. After finished the installation, please click **Restart** to complete the installation.



Note: Mac OS support version 10.3, 10.4, 10.5.

Install the Hardware

Note:

Insert the Wireless LAN Module when finished software installation.

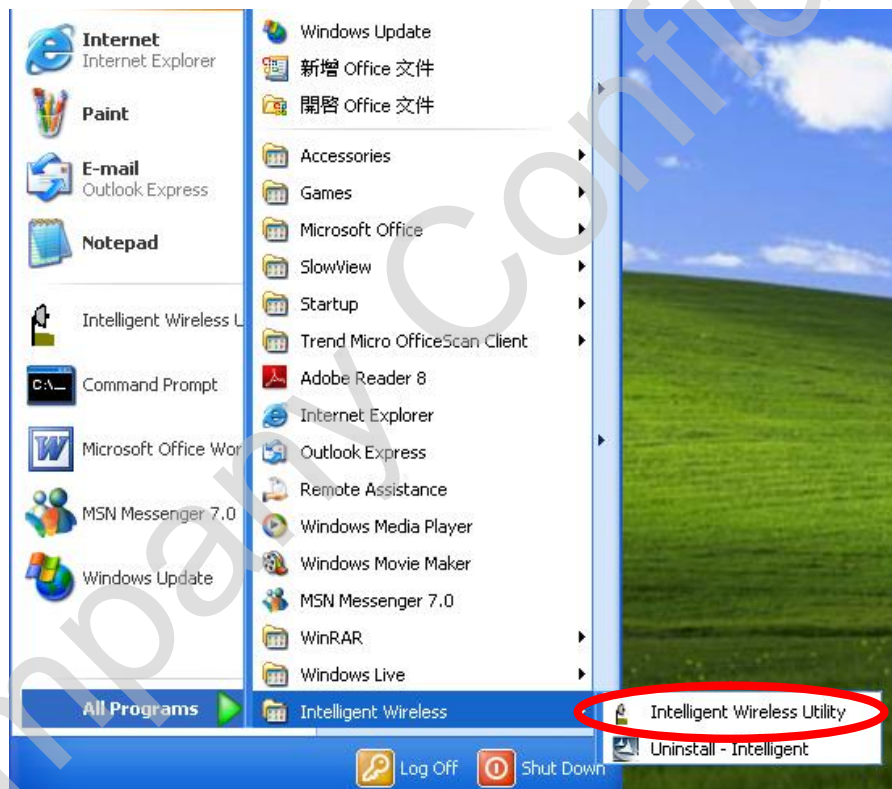
Insert the Wireless LAN Module into the USB Port of the computer. The system will automatically detect the new hardware.

Chapter 3: Utility Configuration

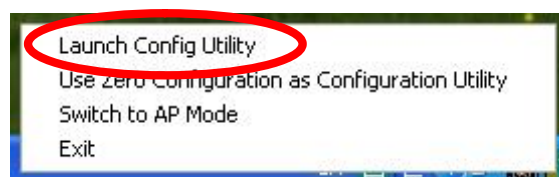
For Windows 2000/XP

After the Wireless LAN Module has been successfully installed, users can use the included Configuration Utility to set the preference.

Go to **Startg (All) Programg Intelligent Wirelessg Intelligent Wireless Utility.**



Users can also open the Configuration Utility by double clicking or right clicking the icon in the task tray to select **Launch Config Utility.**



Station Mode

IMPORTANT NOTICE:

Under screen resolution 800 x 600 pixels, if users click the triangle button, at the lower right corner of the utility window, to expand the station linking information, it will NOT be displayed completely.

Profile

Profile can let users book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add**, **Edit**, **Delete**, and **Activate** profiles.

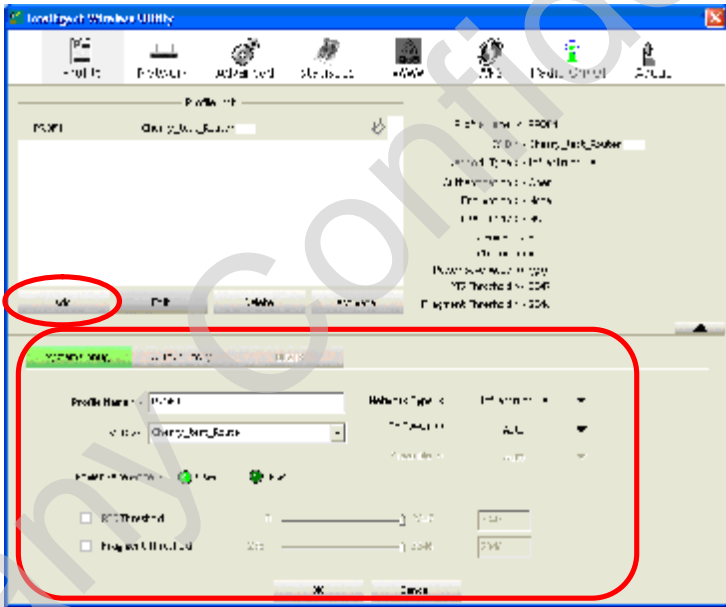
▼ Click this button to show the information of Status Section.

▲ Click this button to hide the information of Status Section.



Profile Tab

Profile Name	Here shows a distinctive name of profile in this column. The default is PROF# (#1, #2, #3...)
SSID	The SSID is the unique name shared among all wireless access points in the wireless network.
Network Type	Shows the network type of the device, including Infrastructure.
Authentication	Shows the authentication mode.
Encryption	Shows the encryption type.

Use 802.1x	Whether or not use 802.1x feature.
Tx Power	Transmit power, the amount of power used by a radio transceiver to send the signal out.
Channel	Shows the selected channel that is currently in use.
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode.)
RTS Threshold	Shows the RTS Threshold of the device.
Fragment Threshold	Shows the Fragment Threshold of the device.
Add	<p>Click to add a profile from the drop-down screen.</p> <p>System Configuration tab:</p>  <p>Profile Name: Users can enter profile name, or use default name defined by system. The default is PROF# (#1, #2, #3....).</p> <p>SSID: The SSID is the unique name shared among all wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network. Users can use pull-down menu to select from available access points.</p> <p>Network Type:</p> <p>The Infrastructure is intended for the connection between wireless network cards and an access point. With the Wireless LAN Module, users can connect wireless LAN to a wired global network via an access point.</p> <p>Tx Power: Transmit power, the amount of power used by a radio transceiver to send the signal out. Select the Tx power percentage from the pull-down list including Auto, 100%, 75%, 50%, 25%, 10% and Lowest.</p>

Power Save Mode:

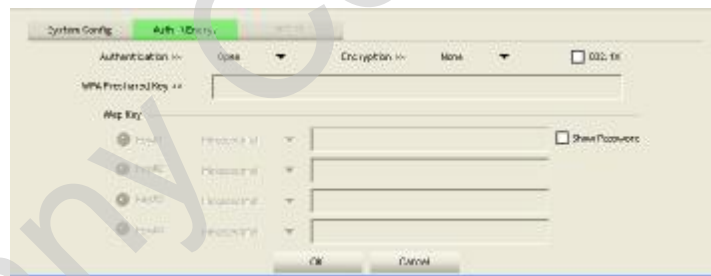
- **CAM (Constantly Awake Mode):** When this mode is selected, the power supply will be normally provided even when there is no throughput. (Default power save mode is CAM.)
- **PSM (Power Saving Mode):** When this mode is selected, this device will stay in power saving mode even when there is high volume of throughput.

RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or key in the value directly. (The default value is 2347.) RTS/CTS Threshold is a mechanism implemented to prevent the “**Hidden Node**” problem. If the “Hidden Node” problem is an issue, users have to specify the packet size. The RTS/CTS mechanism will be activated if the data size exceeds the values that have been set.

This value should remain at its default setting of 2347. Should users encounter inconsistent data flow, only minor modifications of this value are recommended.

Fragment Threshold: Users can adjust the Fragment threshold number by sliding the bar or key in the value directly. (The default value is 2346.) The mechanism of Fragmentation Threshold is used to improve the efficiency when high traffic flows along in the wireless network. If the Wireless LAN Module often transmits large files in wireless network, users can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346.

Authentication and Security tab:



Authentication Type: There are several types of authentication modes including **Open, Shared, Leap, WPA, WPA-PSK, WPA2 and WPA2-PSK.**

- **Open:** If the access point or wireless router is using “**Open**” authentication, then the Wireless LAN Module will need to be set to the same authentication type.
- **Shared:** Shared key is when both the sender and the recipient share a secret key.
- **LEAP:** Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication (only with CCX mode enabled.)
- **WPA/ WPA-PSK/ WPA2/ WPA2-PSK:** WPA or WPA-PSK authentications offer two encryption methods, TKIP and AES. For WPA-PSK, select the type of algorithm TKIP or AES and then enter a WPA Shared Key of 8-64 characters in the WPA Pre-shared Key field.

Encryption Type: For **Open** and **Shared** authentication mode, the selection of encryption type are **None** and **WEP**. For **WPA, WPA2,**

WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both **TKIP** and **AES**.

WPA Pre-shared Key: This is the shared secret key between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

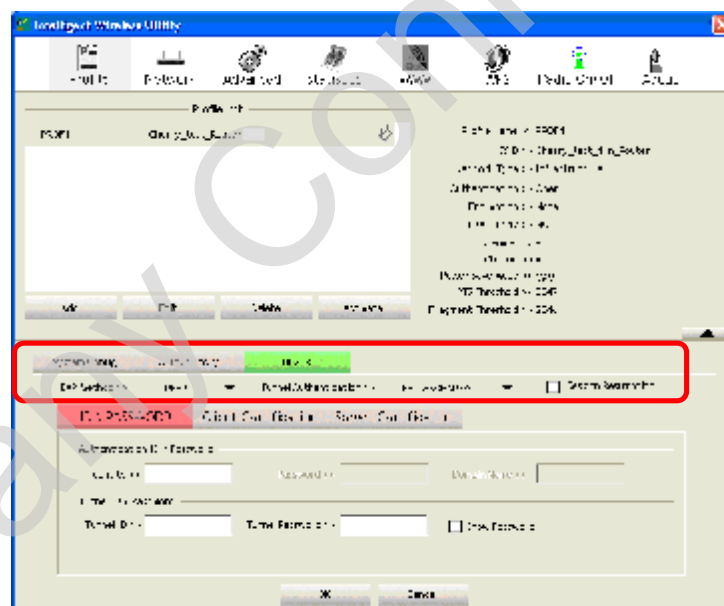
WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys.

- [ASCII \(64 bits\): 5 ASCII characters](#) (case sensitivity).
- [ASCII \(128 bits\): 13 ASCII characters](#) (case sensitivity).
- [Hexadecimal \(64 bits\): 10 Hex characters](#) (0~9, a~f).
- [Hexadecimal \(128 bits\): 26 Hex characters](#) (0~9, a~f).

Show Password: Check this box to show the passwords that have been entered.

802.1x Setting: When users use radius server to authenticate client certificate for WPA authentication mode (WPA authentication do not support EAP Method- MD5-Challenge).

802.1x tab:



EAP Method:

- **PEAP:** Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- **TLS / Smart Card:** Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications

between the WLAN client and the access point.

- **TTLS:** Tunnelled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- **EAP-FAST:** Flexible Authentication via Secure Tunnelling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication now.
- **MD5-Challenge:** Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network. (Only Open and Shared authentication mode can use this function.)

Tunnel Authentication:

- **Protocol:** Tunnel protocol, List information including **EAP-MSCHAP v2, EAP-TLS/ Smart Card, and Generic Token Card.**
- **Tunnel Identity:** Identity for tunnel.
- **Tunnel Password:** Password for tunnel.

Session Resumption: Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. Users can click the box to enable or disable this function.

ID/PASSWORD tab:



ID/ PASSWORD: Identity and password for server.

- **Authentication ID / Password:** Identity, password and domain name for server. Only "EAP-FAST" EAP method and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.
- **Tunnel ID / Password:** Identity and Password for server.

Show Password: Check this box to show the passwords that have been entered.

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

Client Certification tab:

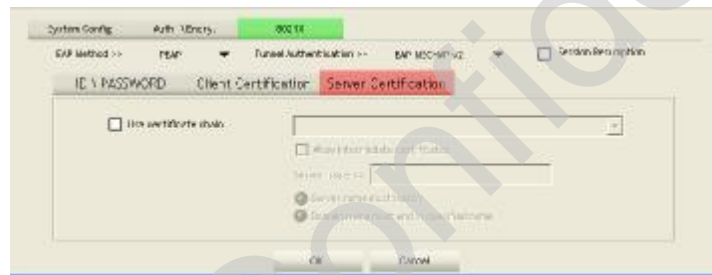


Use Client certificate: Choose to enable server authentication.

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

Server Certification tab:



Use certificate chain: Choose use server that issuer of certificates.

Allow intimidate certificates: It must be in the server certificate chain between the server certificate and the server specified in the certificate issuer must be field.

Server name: Enter an authentication sever.

Server name must match: Click to enable or disable this function.

Domain name must end in specified name: Click to enable or disable this function.

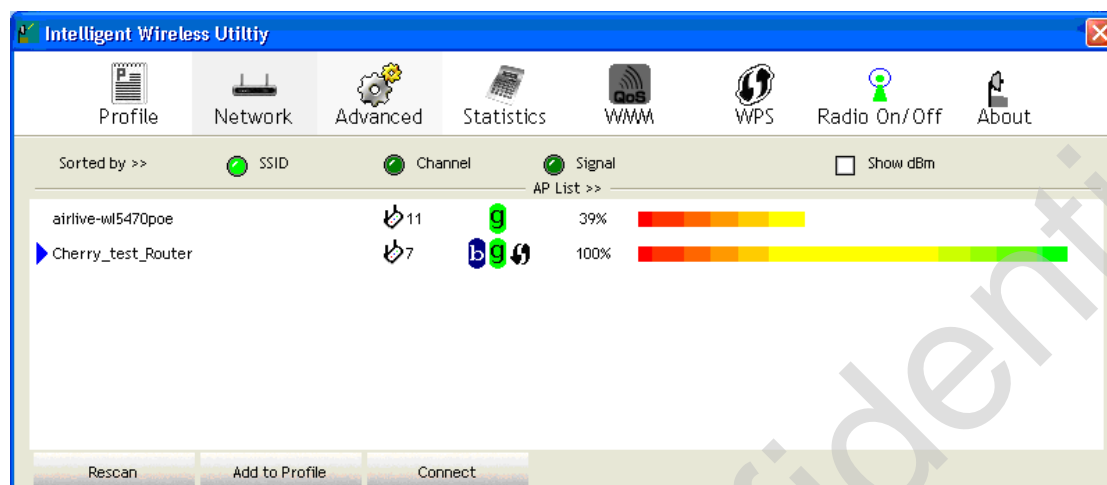
OK: Click to save settings and exit this page.

Cancel: Click call off the settings and exit.

Delete	Click to delete an existing profile.
Edit	Click to edit a profile.
Activate	Click to make a connection between devices.

Network

The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.

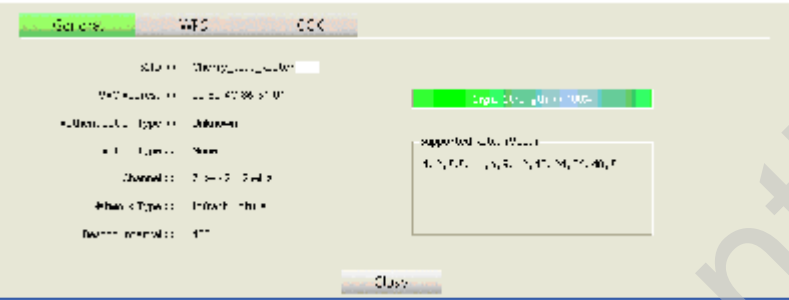



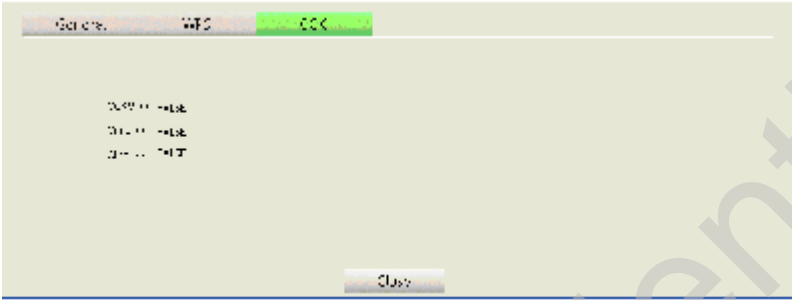
Network Tab

Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.
Show dBm	Check the box to show the dBm of the AP list.
SSID	Shows the name of BSS network.
Network Type	Network type in use, Infrastructure for BSS.
Channel	Shows the currently used channel.
Wireless mode	AP support wireless mode. It may support 802.11b, 802.11g wireless mode.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, Not Use and WPS.
Signal	Shows the receiving signal strength of specified network.
Rescan	Click to search and refresh the access point list.
Add to Profile	Select an item (SSID) on the list and then click to add it into the profile list.
Connect	Select an item (SSID) on the list and then click to make a connection.

Access Point (AP) Information

Double click on the intended AP to see AP's detail information that divides into four parts. They are General, WPS, CCX information. The introduction is as following:

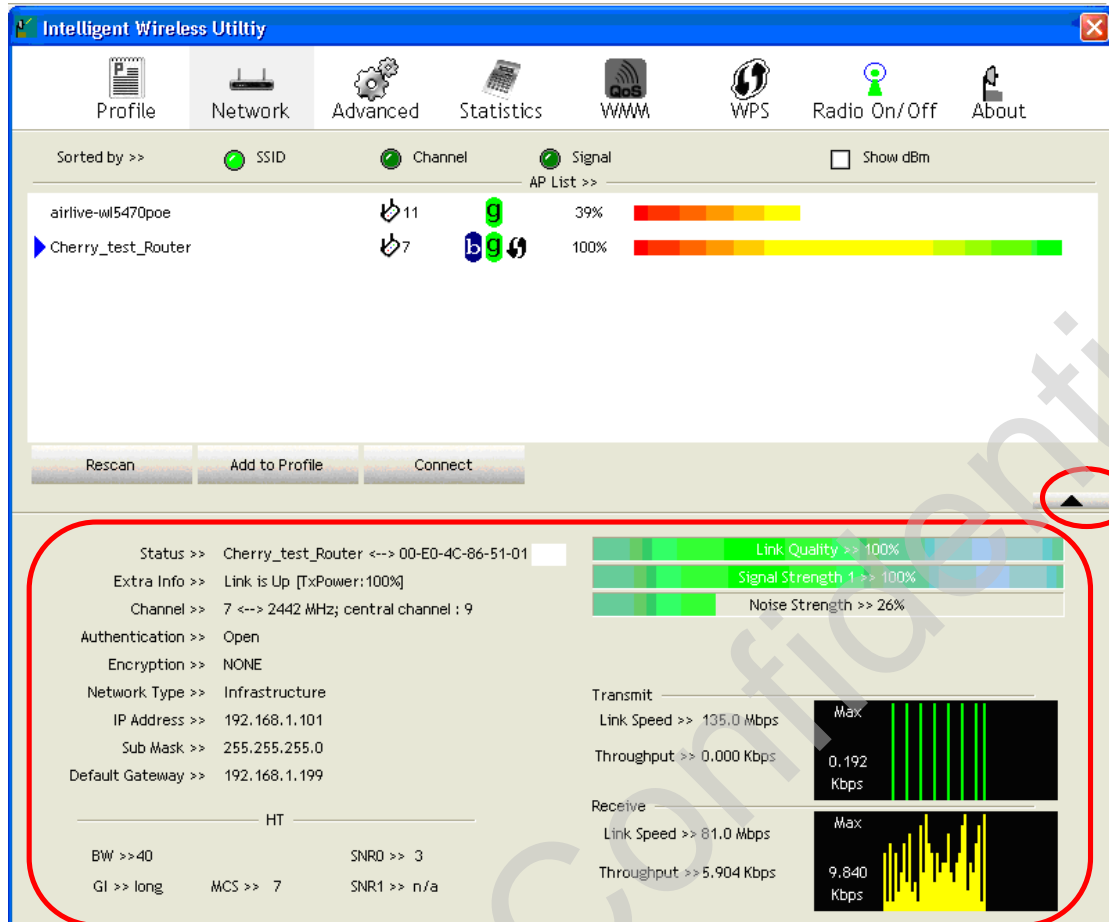
<p>General</p>	 <p>General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates.</p> <p>Close: Click this button to exit the information screen.</p>
<p>WPS</p>	 <p>WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.</p> <p>Authentication Type: There are four types of authentication modes supported by RaConfig. They are Open, Shared, WPA-PSK, WPA securities, WPA2-PSK and WPA2.</p> <p>Encryption Type: For Open and Shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.</p> <p>Config Methods: Correspond to the methods the AP supports as an Enrollee for adding external Registrars.</p> <p>Device Password ID: Indicate the method or identifies the specific password that the selected Registrar intends to use.</p> <p>Selected Registrar: Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE"</p> <p>State: The current configuration state on AP. The values are "Unconfigured" and "Configured."</p> <p>Version: WPS specified version.</p> <p>AP Setup Locked: Indicate if AP has entered a setup locked state.</p>

	<p>UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes.</p> <p>RF Bands: Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz."</p> <p>Close: Click this button to exit the information screen.</p>
<p>CCX</p>	 <p>CCX information contains CCKM, Cmic and Ckip information.</p> <p>Close: Click this button to exit the information screen.</p>

Link Status

Click the triangle button at the lower right corner of the window to expand the link status. The link status page displays the detail information of current connection.

- Click this button to show the information.
- Click this button to hide the information.

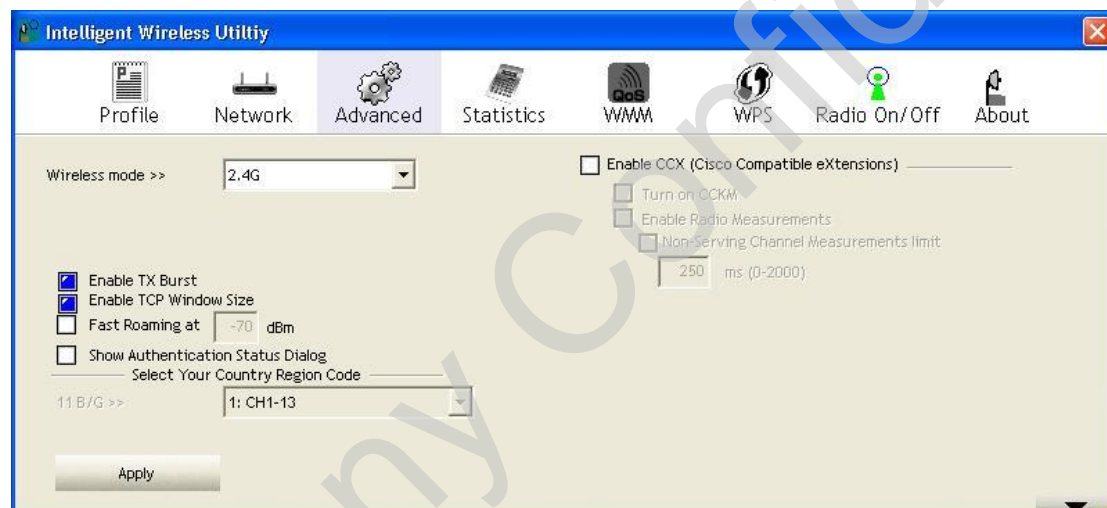


Link Status Tab	
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.
Extra Info	Shows the link status and TX power percentage.
Channel	Shows the current channel in use.
Authentication	Authentication mode used within the network, including Unknown, Open, Shared, Leap, WPA-PSK, WPA2-PSK, WPA and WPA2.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
Network Type	Network type in use, Infrastructure for BSS.
IP Address	Shows the IP address information.
Sub Mask	Shows the Subnet Mask information.
Default Gateway	Shows the default gateway information.
Link Quality	Shows the connection quality based on signal strength and TX/RX packet error rate.

Signal Strength 1	Shows the receiving signal strength, users can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength in the wireless environment.
Transmit	Shows the current Link Speed and Throughput of the transmit rate.
Receive	Shows the current Link Speed and Throughput of receive rate.
Link Speed	Shows the current transmitting rate and receiving rate.
Throughput	Shows the transmitting and receiving speed of data.

Advanced

This Advanced page provides advanced and detailed settings for the wireless network.



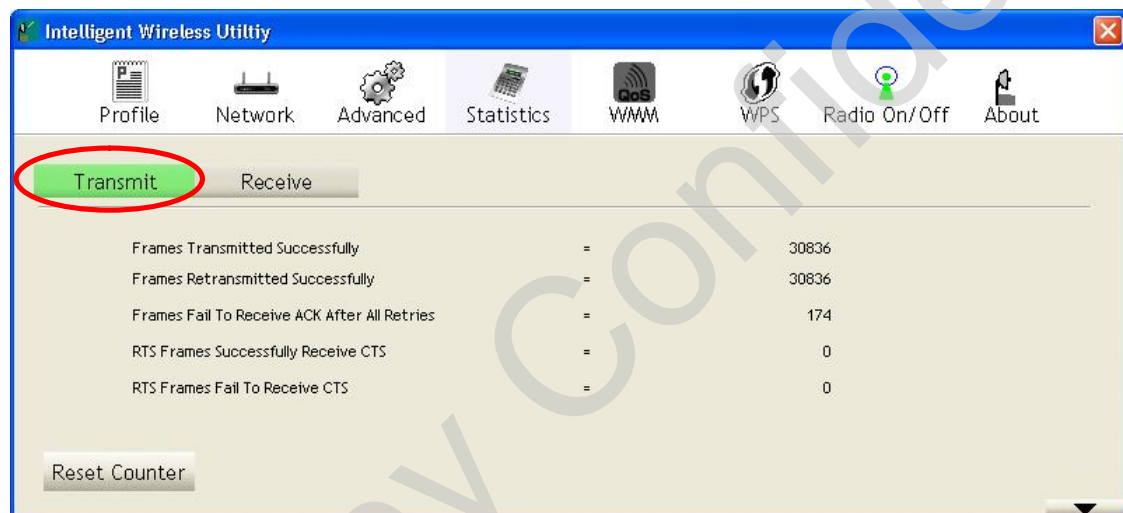
Advanced Tab

Wireless mode	Here supports 2.4G (included 802.11b/g) wireless mode.
Enable TX Burst	Check to enable this function. This function enables the Wireless LAN Module to deliver better throughput during a period of time, it only takes effect when connecting with the AP that supports this function.
Enable TCP Window Size	Check to increase the transmission quality. The large TCP window size the better performance.
Fast Roaming at dBm	Check to set the roaming interval, fast to roaming, setup by transmits power. (Default setting is -70dBm.)
Show Authentication Status Dialog	When connected AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog displays the process about 802.1x authentications.

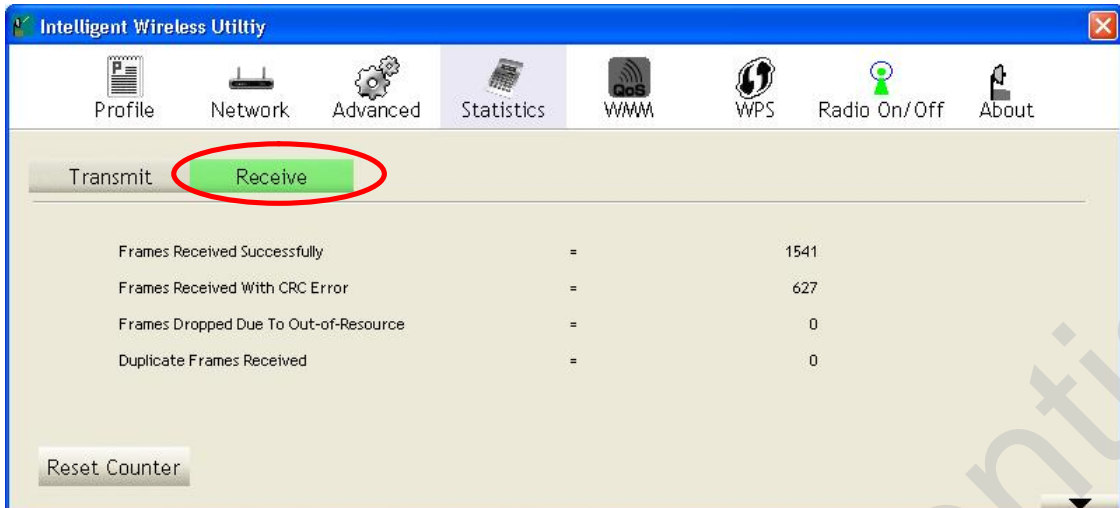
<p>Enable CCX</p> <p>(Cisco Compatible extensions)</p>	<p>Check to enable the CCX function.</p> <ul style="list-style-type: none"> • Turn on CCKM. • Enable Radio Measurements: Check to enable the Radio measurement function. • Non-Serving Measurements limit: Users can set channel measurement every 0~2000 milliseconds. (Default is set to 250 milliseconds.)
<p>Apply</p>	<p>Click to apply above settings.</p>

Statistics

The Statistics screen displays the statistics on the current network settings.



Transmit	
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Retransmitted Successfully	Shows information of packets successfully sent with one or more retries.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS.
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.
Reset Counter	Click this button to reset counters to zero.

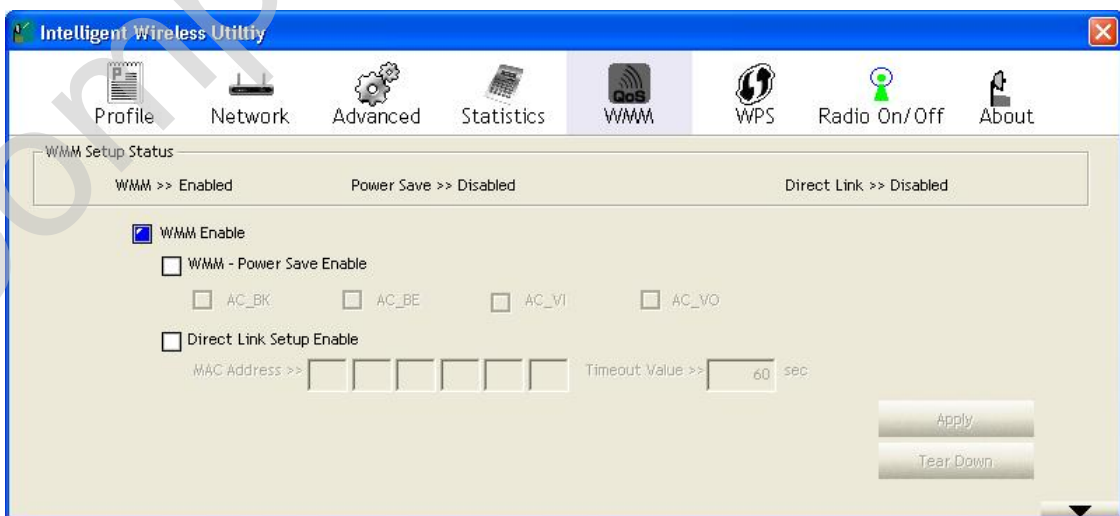


Receive Statistics

Frames Received Successfully	Shows information of packets received successfully.
Frames Received With CRC Error	Shows information of packets received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.
Duplicate Frames Received	Shows information of packets received more than twice.
Reset Counter	Click this button to reset counters to zero.

WMM/ QoS

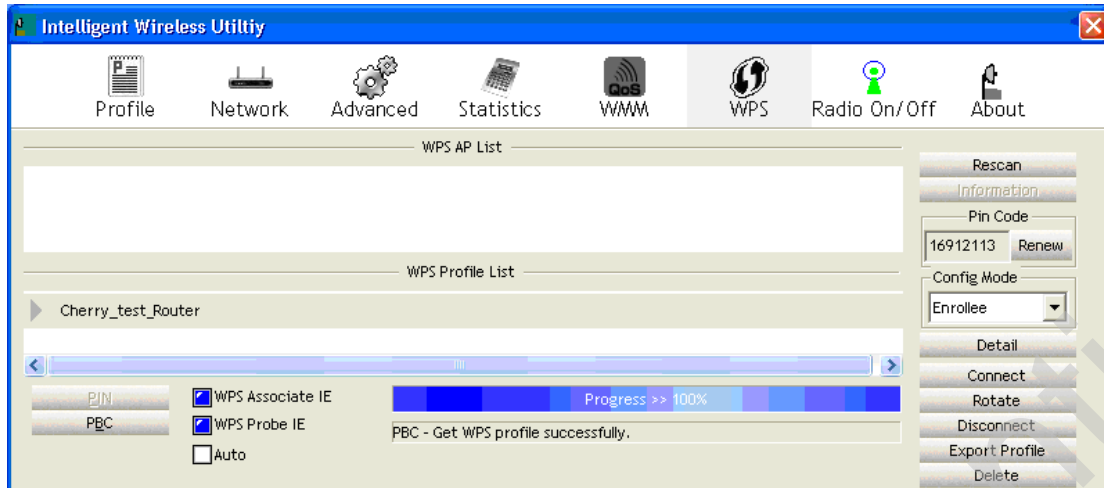
The WMM page shows the Wi-Fi Multi-Media power save function and Direct Link Setup (DLS) that ensure the wireless network linking quality.




WMM/QoS Tab	
WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	Select a power save mode that preferred. <input type="checkbox"/> AC_BK (Access Category Background) <input type="checkbox"/> AC_BE (Access Category Best Effort) <input type="checkbox"/> AC_VI (Access Category Video) <input type="checkbox"/> AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup (DLS). This function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.
MAC Address	The setting of DLS(Direct Link Setup) indicates as follow : Fill in the blanks of Direct Link with MAC Address of target STA, and the STA must conform to two conditions: <input type="checkbox"/> Connecting with the same AP that supports DLS feature. <input type="checkbox"/> DLS enabled.
Timeout Value	Timeout Value represents that it disconnect automatically after few seconds. The value is integer that must be between 0~65535. It represents that it always connects if the value is zero. (Default setting of Timeout Value is 60 seconds.)
Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA MAC address, then click "Tear Down" button to disconnect the STA.

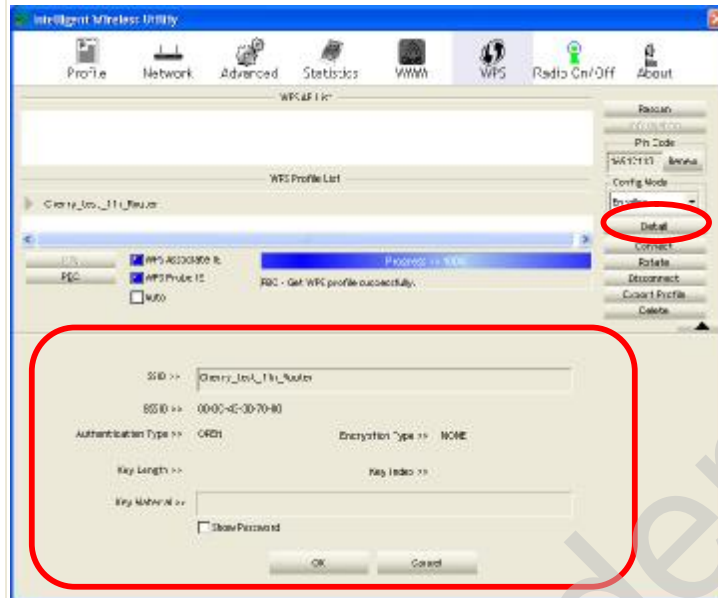
WPS

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.



WPS Tab

WPS AP List	Display the information of surrounding APs with WPS IE from last scan result. List information included SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.
Rescan	Issue a rescan command to wireless NIC to update information on surrounding wireless network.
Information	<p>Display the information about WPS IE on the selected network. List information included Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.</p> 
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use " Renew " button to re-generate new PIN Code.
Config Mode	Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.
Detail	Click the Detail button to show the information about Security and Key in the credential.



If selected the AP that listed in the WPS Profile List field, users can click the **Detail** button to see more AP information.

SSID: Shows the connected AP network name.

BSSID: The MAC address of the connected AP. Fixed and cannot be changed.

Authentication Type: The authentication type support Open, WPA-PSK and WPA2-PSK.

Encryption Type: For **Open** authentication mode, the selection of encryption type are **NONE** and **WEP**. For **WPA-PSK** and **WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.

Key Length: Only valid when using **Open** authentication mode and **WEP** encryption. There are key lengths 5, 10, 13 and 26.

Key Index: Only valid when using **Open** authentication mode and **WEP** encryption. There are 1~4 key index.

Key Material: The key material can be used to ensure the security of the wireless network. Fill in the appropriate value or phrase in **Key Material** field.

Show Password: Check this box to show the passwords that have been entered.

OK: Click to save and apply the new settings.

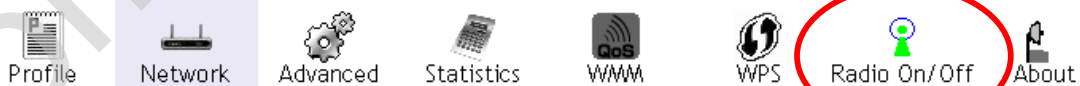
Cancel: Click to leave and discard the settings.

Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to rotate to connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.

Export Profile	Export all credentials to Profile.
Delete	Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.
PIN	<p>Registrar: Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in two minutes and get IP address.</p> <p>Enrollee: Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address.</p>
PBC	Start to add to AP using PBC (Push Button Configuration) method. Click this button to connect the AP which supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.
<p>Note:</p> <p>After the users click PIN or PBC, please do not rescan within two minutes of the connection. If users want to stop this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.</p>	
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Auto	Check this box the device will connect the AP automatically.
Progress Bar	Display rate of progress from Start to Connected status.
Status Bar	Display currently WPS Status.

Radio On/Off

Click this Radio On/Off button to turn ON or OFF radio function.



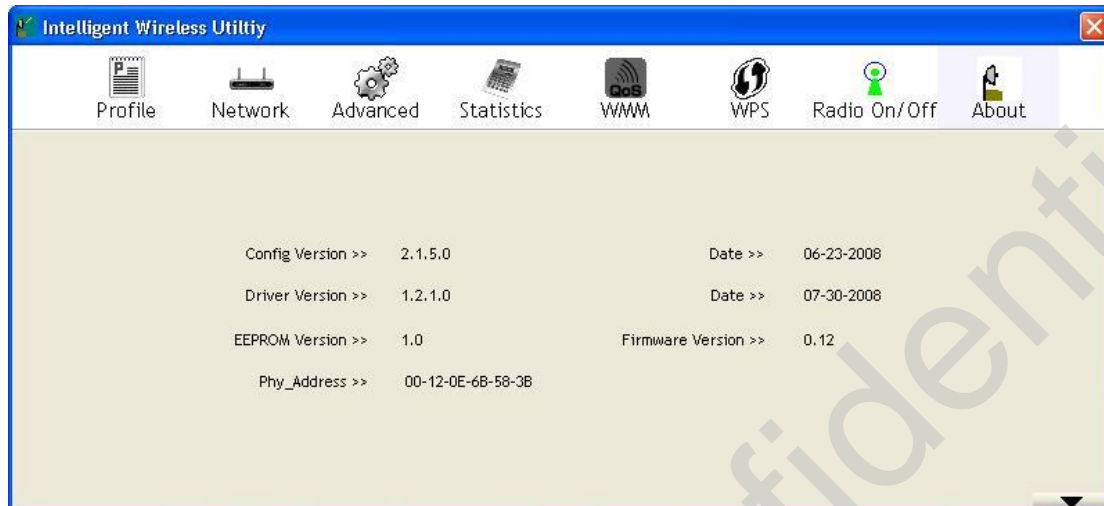
This icon shows radio is On.



This icon shows radio is Off.

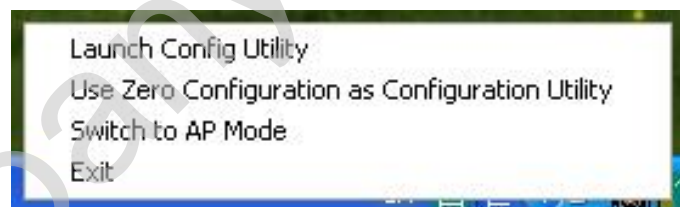
About

This page displays the information of the Wireless LAN Module including, Config Version/ Date, Driver Version/ Date, EEPROM Version, Firmware Version and Phy_Address.



Utility Menu List

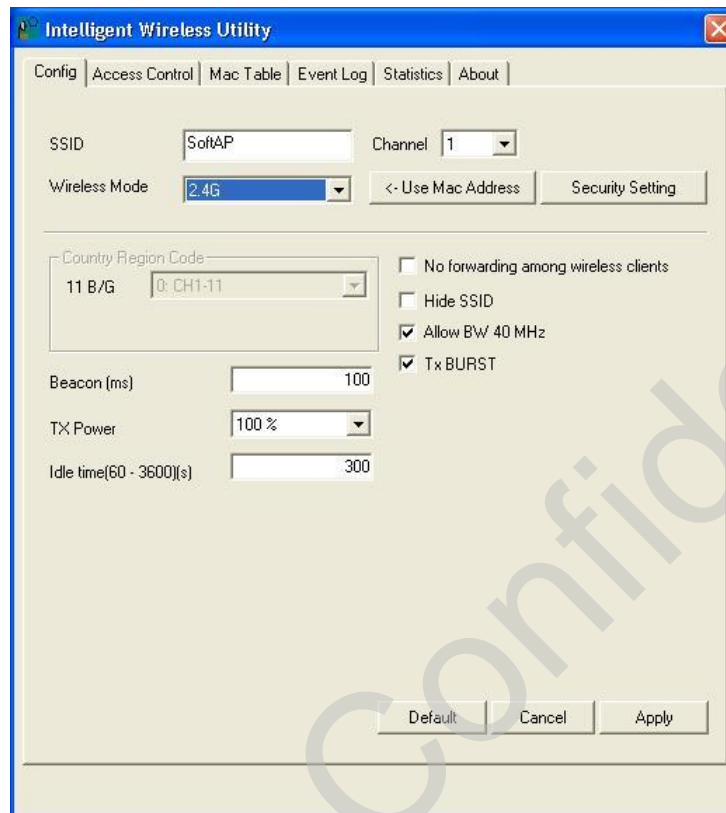
To access the utility menu list, please right click the utility icon in the task tray.



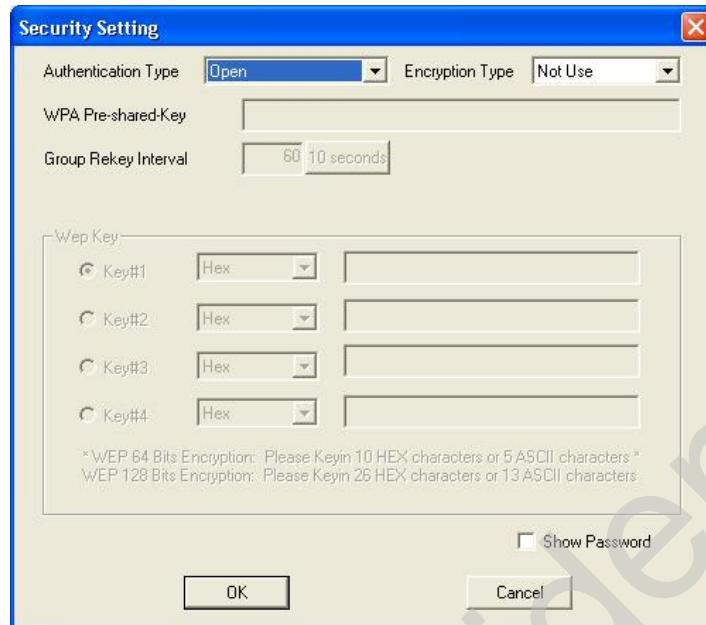
- I **Launch Config Utility:** Select to open the utility screen.
- I **Use Zero Configuration as Configuration Utility:** Select to use the Windows XP built-in utility (Zero configuration utility).
- I **Switch to AP Mode:** Select to make the Wireless LAN Module act as a wireless AP.
- I **Exit:** Select to close the utility program.

Soft AP mode

Config



Config	
SSID	AP name of user type. Users also can click Use Mac Address button to display it.
Channel	Manually force the AP using the channel. (The system default is CH 1.)
Wireless Mode	Here supports 2.4G (included 802.11b/g) wireless mode. (The system default is 2.4G.)
Use Mac Address	Click this button to replace SSID by MAC address.
Security Setting	Authentication mode and encryption algorithm used within the AP. (The system default is no authentication and encryption.)



Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. (System authentication type default is Open.)

Encryption Type: For **Open** and **Shared** authentication mode, the selections of encryption type are **Not Use** and **WEP**. For **WPA-PSK**, **WPA2-PSK**, and **WPA-PSK/ WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**. (System authentication type default is Not Use.)

WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK and WPA-PSK/ WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

Group Re-key Interval: Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode to renew key. Users can set to change by seconds or packets. (Default is 600 seconds.)

WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys.

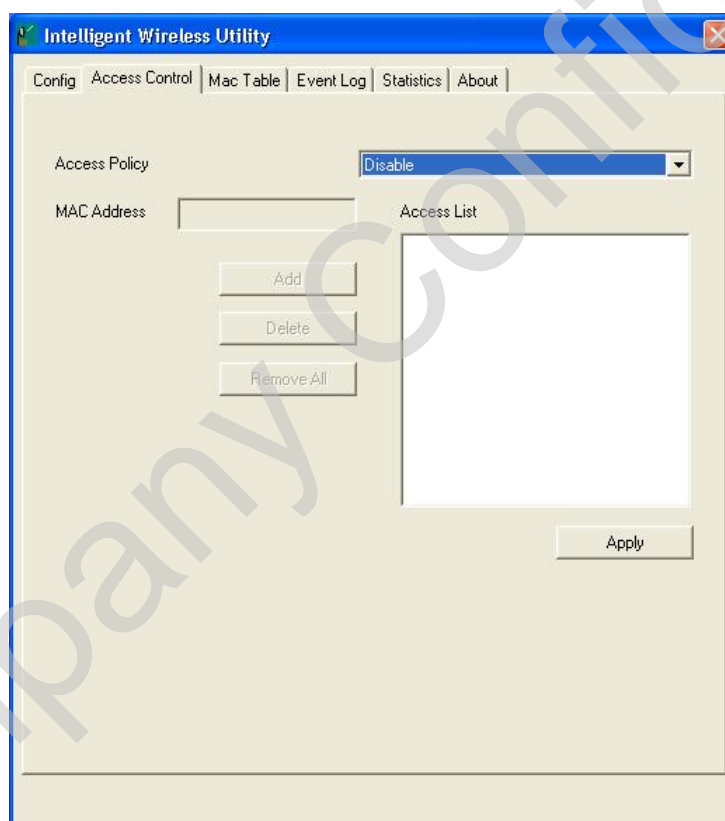
- [ASCII \(64 bits\): 5 ASCII characters](#) (case sensitivity).
- [ASCII \(128 bits\): 13 ASCII characters](#) (case sensitivity).
- [Hexadecimal \(64 bits\): 10 Hex characters](#) (0~9, a~f).
- [Hexadecimal \(128 bits\): 26 Hex characters](#) (0~9, a~f).

Show Password: Check this box to show the passwords that have been entered.

Beacon (ms)	The time between two beacons. (The system default is 100 ms.)
TX Power	Manually force the AP transmits power from the pull-down list 100%, 75%, 50%, 25% and lowest. (The system default is 100%)
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. (Default value of idle time is 300 seconds.)

No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. (The system default is no forwarding.)
Hide SSID	Do not display AP name. (System default is disabled.)
Tx BURST	This function enables the adapter to deliver better throughput during a period, it only takes effect when connecting with the AP that supports this function. (Default setting is enabled.)
Default	Use the system default value.
Apply	Click to apply the above settings.

Access Control



Access Control

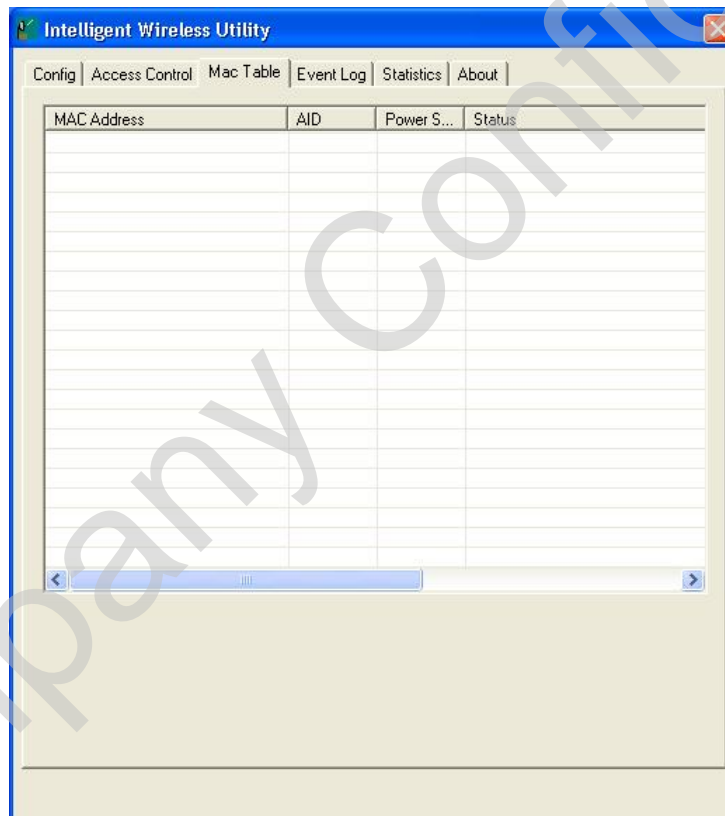
Access Policy

User chooses whether AP start the function or not. (System default is Disable.)

- I Disable:** Do not use this access control function.
- I Allow All:** Only the MAC address listed in the Access List can connect with this soft AP.

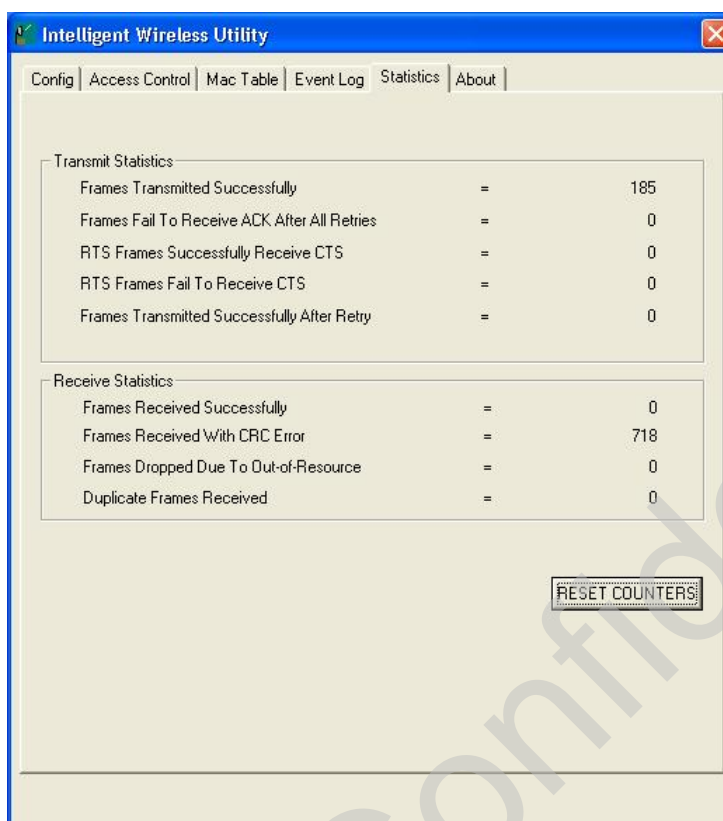
	I Reject All: Only the MAC address listed in the Access List can NOT connect with this soft AP.
MAC Address	Manually force the MAC address using the function. Enter the MAC address in the column and click Add button, then the MAC address will be listed in the Access List pool.
Access List	Display all MAC Address that have been set.
Add	Add the MAC address that users would like to set.
Delete	Delete the Mac address that has been set.
Remove All	Remove all Mac address in the Access List.
Apply	Apply the above changes.

MAC Table



MAC Table	
MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	The station of current connect whether it have to support.
Status	The status of current connection.

Statistics



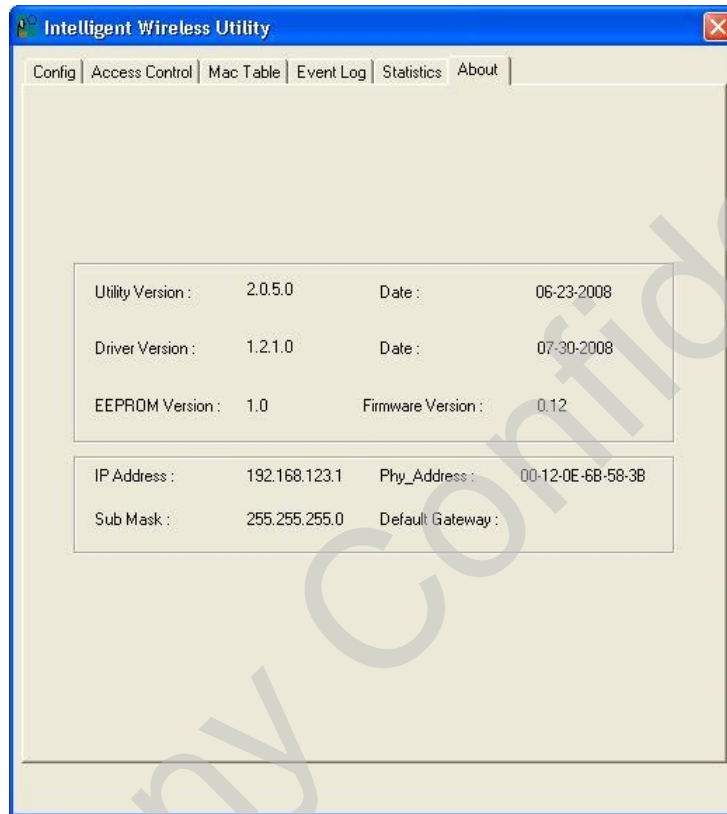
Transmit Statistics	
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS.
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Shows information of packets successfully sent with one or more retries.
Receive Statistics	
Frames Received Successfully	Shows information of packets received successfully.
Frames Received With CRC Error	Shows information of packets received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.
Duplicate Frames Received	The number of duplicate packets received.

Reset Counter

Reset counters to zero.

About

This page displays the Wireless LAN Module and driver version information.



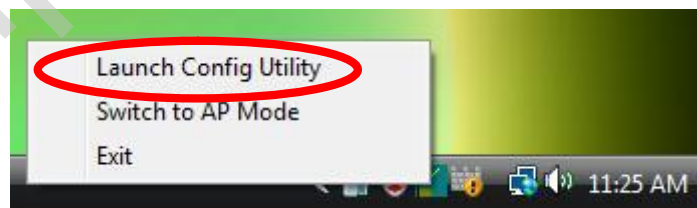
For Windows Vista

After the Wireless LAN Module has been successfully installed, users can use the included Configuration Utility to set the preference.

Go to Startg (All) Programg Intelligent Wirelessg Intelligent Wireless Utility.



Open the Configuration Utility by double clicking or right clicking the icon in the tray to select **Launch Config Utility**.



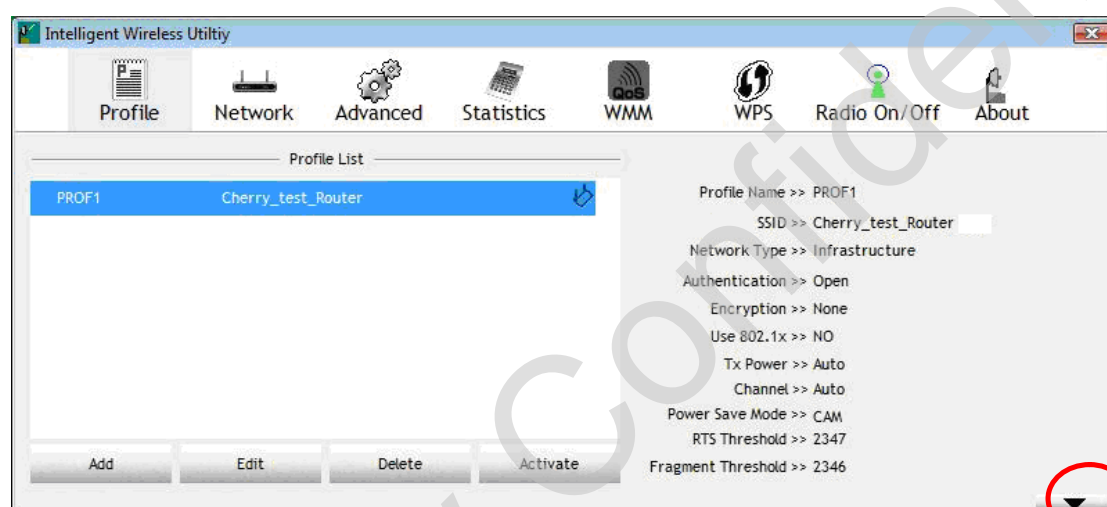
Station Mode

Profile

Profile can book keeping the favorite wireless setting among home, office, and other public hot-spot. Users may save multiple profiles, and activate the correct one at preference. The Profile manager enables users to **Add**, **Edit**, **Delete**, and **Activate** profiles.

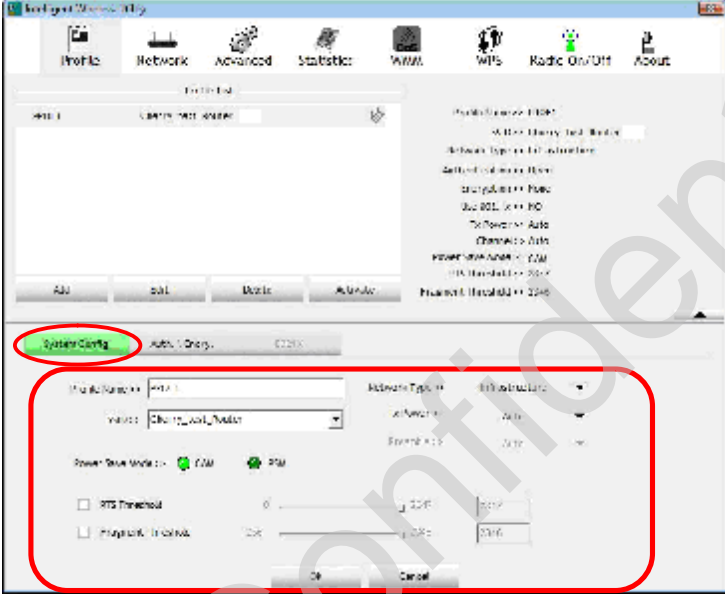
▼ Click this button to show the information.

▲ Click this button to hide the information.



Profile Tab

Profile Name	Users may enter a distinctive name of profile in this column. The default is PROF# (#1, #2, #3....)
SSID	The SSID is the unique name shared among all wireless access points in the wireless network.
Network Type	Shows the network type of the device, including Infrastructure.
Authentication	Shows the authentication mode.
Encryption	Shows the encryption type.
Use 802.1x	Whether use 802.1x feature or not.
Tx Power	Transmit power, the amount of power used by a radio transceiver to send the signal out.
Channel	Shows the selected channel that is currently in use.
Power Save Mode	Choose from CAM (Constantly Awake Mode) or PSM (Power Saving Mode.)

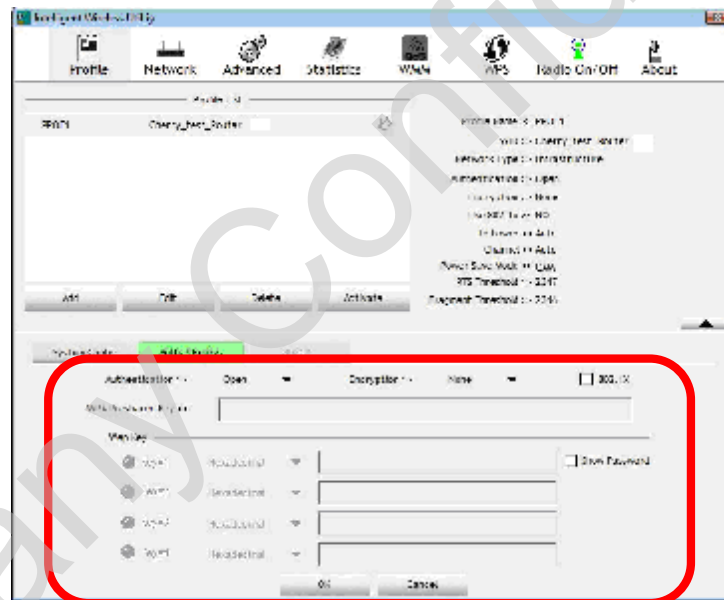
RTS Threshold	Shows the RTS Threshold of the device.
Fragment Threshold	Shows the Fragment Threshold of the device.
Add	<p>Click to add a profile from the drop-down screen.</p> <p>System Configuration tab:</p>  <p>Profile Name: Users can enter profile name, or use default name defined by system. The default is PROF# (#1, #2, #3....).</p> <p>SSID: The SSID is the unique name shared among all wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network. Users can use pull-down menu to select from available access points.</p> <p>Network Type: There are two types, Infrastructure and Ad hoc modes.</p> <ul style="list-style-type: none"> • The Infrastructure is intended for the connection between wireless network cards and an access point. With the Wireless LAN Module, users can connect wireless LAN to a wired global network via an access point. • The Ad hoc lets users set a small wireless workgroup easily and quickly. Equipped with the Wireless LAN Module, users can share files and printers between each PC and laptop. <p>Tx Power: Transmit power, the amount of power used by a radio transceiver to send the signal out. Select the Tx power percentage from the pull-down list including Auto, 100%, 75%, 50%, 25%, 10% and Lowest.</p> <p>Power Save Mode:</p> <ul style="list-style-type: none"> • CAM (Constantly Awake Mode): When this mode is selected, the power supply will be normally provided even when there is no throughput. (Default power save mode is CAM.) • PSM (Power Saving Mode): When this mode is selected, this device will stay in power saving mode even when there is high volume of

throughput.

RTS Threshold: Users can adjust the RTS threshold number by sliding the bar or key in the value directly. (The default value is 2347.) RTS/CTS Threshold is a mechanism implemented to prevent the “**Hidden Node**” problem. If the “Hidden Node” problem is an issue, users have to specify the packet size. *The RTS/CTS mechanism will be activated if the data size exceeds the value that have been set.* This value should remain at its default setting of 2347. Should users encounter inconsistent data flow, only minor modifications of this value are recommended.

Fragment Threshold: Users can adjust the Fragment threshold number by sliding the bar or key in the value directly. (The default value is 2346.) The mechanism of Fragmentation Threshold is used to improve the efficiency when high traffic flows along in the wireless network. If the Wireless LAN Module often transmits large files in wireless network, users can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346.

Authentication and Encryption tab:



Authentication Type: There are six type of authentication modes including Open, Shared, WPA, WPA-PSK, WPA2 and WPA2-PSK.

- **Open:** If the access point or wireless router is using “**Open**” authentication, then the Wireless LAN Module will need to be set to the same authentication type.
- **Shared:** Shared key is when both the sender and the recipient share a secret key.
- **WPA/ WPA-PSK/ WPA2/ WPA2-PSK:** WPA-PSK offers two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES and then enter a WPA Shared Key of 8-63 characters in the WPA Pre-shared Key field.

Encryption Type: For **Open** and **Shared** authentication mode, the selection of encryption type are **None** and **WEP**. For **WPA**, **WPA2**, **WPA-PSK** and **WPA2-PSK** authentication mode, the encryption type

supports both **TKIP** and **AES**.

WPA Pre-shared Key: This blank is the shared secret key between AP and STA. For **WPA-PSK** and **WPA2-PSK** authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

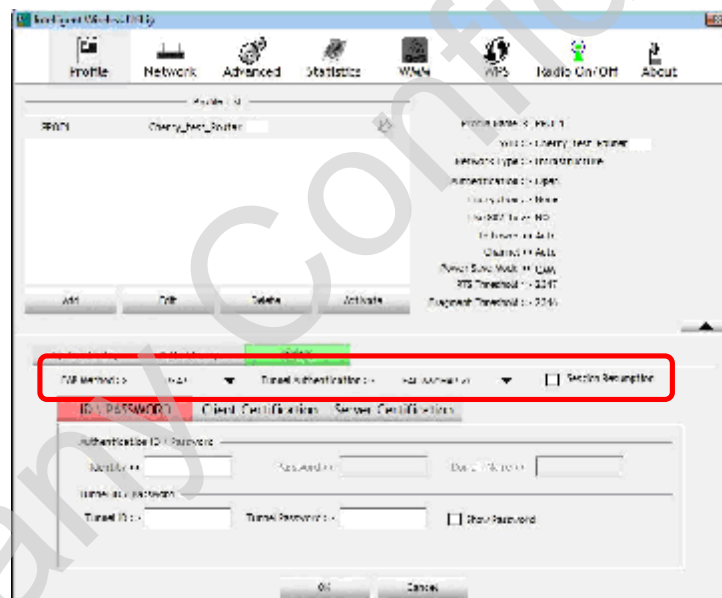
WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys.

- [ASCII \(64 bits\): 5 ASCII characters](#) (case sensitivity).
- [ASCII \(128 bits\): 13 ASCII characters](#) (case sensitivity).
- [Hexadecimal \(64 bits\): 10 Hex characters](#) (0~9, a~f).
- [Hexadecimal \(128 bits\): 26 Hex characters](#) (0~9, a~f).

Show Password: Check this box to show the passwords that have been entered.

802.1x Setting: When users use radius server to authenticate client certificate for WPA authentication mode.

802.1x tab:



EAP Method:

- **PEAP:** Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- **TLS / Smart Card:** Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

Tunnel Authentication:

- **Protocol:** Tunnel protocol, List information including

EAP-MSCHAP v2 and EAP-TLS/ Smart Card.

- **Tunnel Identity:** Identity for tunnel.
- **Tunnel Password:** Password for tunnel.

Session Resumption: Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. Users can click the box to enable or disable this function.

ID\PASSWORD tab:



ID/ PASSWORD: Identity and password for server.

- **Authentication ID / Password:** Identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.
- **Tunnel ID / Password:** Identity and Password for server.

Show Password: Check this box to show the passwords that have been entered.

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

Client Certification tab:




Users can select **Use a certificate on this computer**, a client certificate for server authentication. Or users can select **Use my smart card** to enable the Client Certification function.

OK: Click to save settings and exit this page.

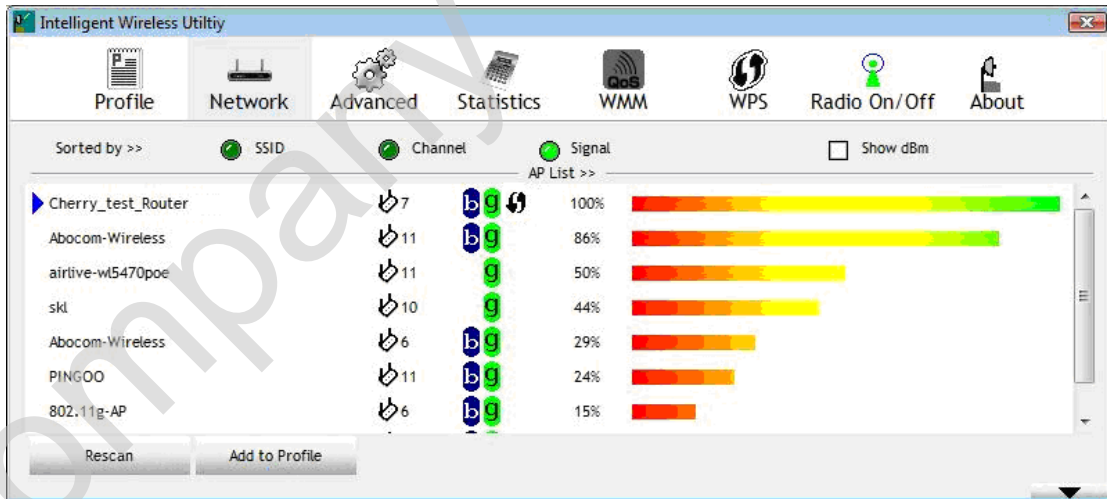
Cancel: Click to call off the settings and exit.

Server Certification tab:

	 <p>Use certificate chain: Choose use server that issuer of certificates.</p> <p>Server name: Enter an authentication sever name.</p> <p>OK: Click to save settings and exit this page.</p> <p>Cancel: Click call off the settings and exit.</p>
Delete	Click to delete an existing profile.
Edit	Click to edit a profile.
Activate	Click to make a connection between devices.

Network

The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.

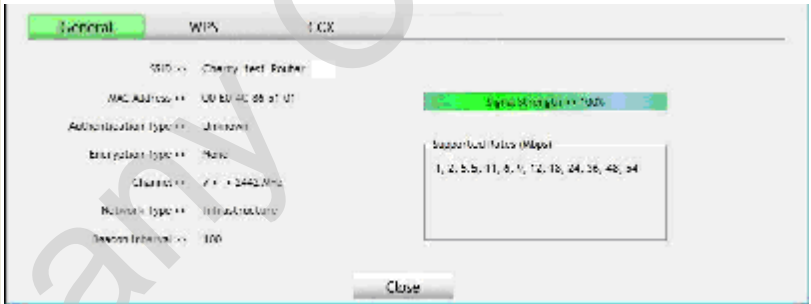




Network Tab	
Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.
Show dBm	Check the box to show the dBm of the AP list.
SSID	Shows the name of BSS network.

Network Type	Network type in use, Infrastructure for BSS.
Channel	Shows the currently used channel.
Wireless mode	AP support wireless mode. It may support 802.11b or 802.11g wireless mode.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
Signal	Shows the receiving signal strength of specified network.
Rescan	Click to refresh the AP list.
Add to Profile	Select an item on the list and then click to add it into the profile list.

Access Point (AP) Information

Double click on the intended AP to see AP's detail information that divides into four parts. They are General, WPS, CCX information. The introduction is as following:

General	 <p>General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates.</p> <p>Close: Click this button to exit the information screen.</p>
WPS	 <p>WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup</p>

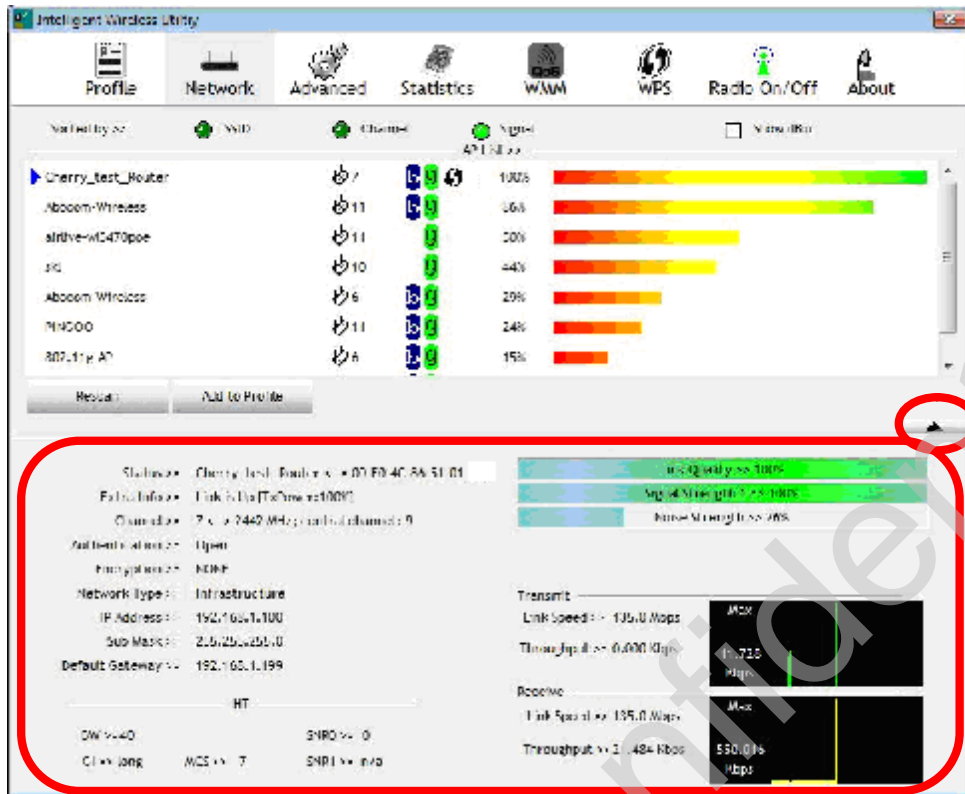
	<p>Locked, UUID-E and RF Bands.</p> <p>Authentication Type: There are four types of authentication modes supported by RaConfig. They are Open, Shared, WPA-PSK, WPA securities, WPA2-PSK and WPA2.</p> <p>Encryption Type: For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.</p> <p>Config Methods: Correspond to the methods the AP supports as an Enrollee for adding external Registrars.</p> <p>Device Password ID: Indicate the method or identifies the specific password that the selected Registrar intends to use.</p> <p>Selected Registrar: Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE".</p> <p>State: The current configuration state on AP. The values are "Unconfigured" and "Configured".</p> <p>Version: WPS specified version.</p> <p>AP Setup Locked: Indicate if AP has entered a setup locked state.</p> <p>UUID-E: The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes.</p> <p>RF Bands: Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz".</p> <p>Close: Click this button to exit the information screen.</p>
<p>CCX</p>	 <p>CCX information contains CCKM, Cmic and Ckip information.</p> <p>Close: Click this button to exit the information screen.</p>

Link Status

Click the triangle button at the right down corner of the windows to expand the link status. The link status page displays the detail information of current connection.

▼ Click this button to show the information.

▲ Click this button to hide the information.

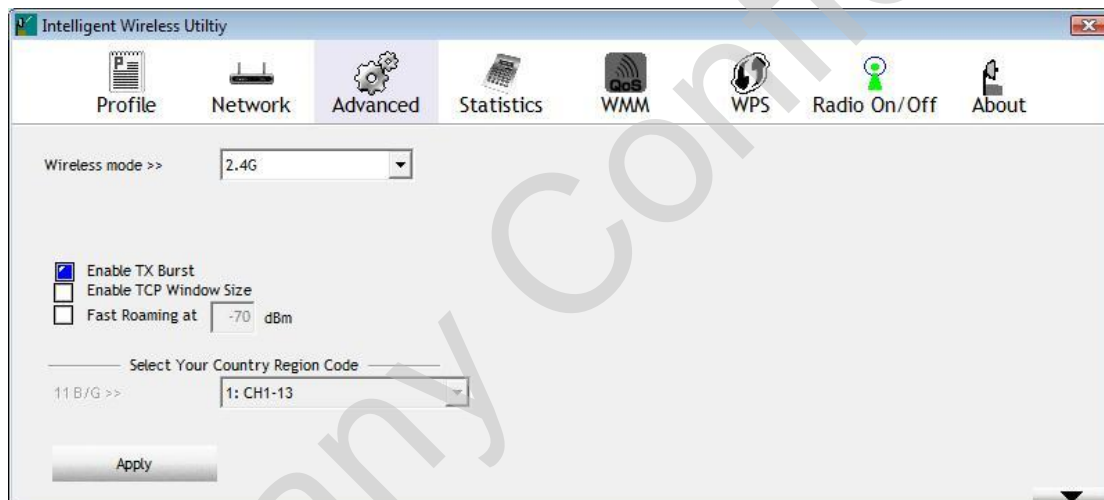


Link Status	
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.
Extra Info	Shows the link status and Tx power percentage.
Channel	Shows the current channel in use.
Authentication	Authentication mode used within the network, including Unknown, Open, Shared, WPA-PSK, WPA2-PSK, WPA and WPA2.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
Network Type	Network type in use, Infrastructure for BSS.
IP Address	Shows the IP address information.
Sub Mask	Shows the Subnet Mask information.
Default Gateway	Shows the default gateway information.
Link Quality	Shows the connection quality based on signal strength and TX/RX packet error rate.

Signal Strength 1	Shows the Receiving signal strength, users can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength in the wireless environment.
Transmit	Shows the current Link Speed and Throughput of the transmit rate.
Receive	Shows the current Link Speed and Throughput of receive rate.
Link Speed	Shows the current transmitting rate and receiving rate.
Throughput	Shows the transmitting and receiving speed of data.

Advanced

This Advanced page provides advanced and detailed settings for the wireless network.

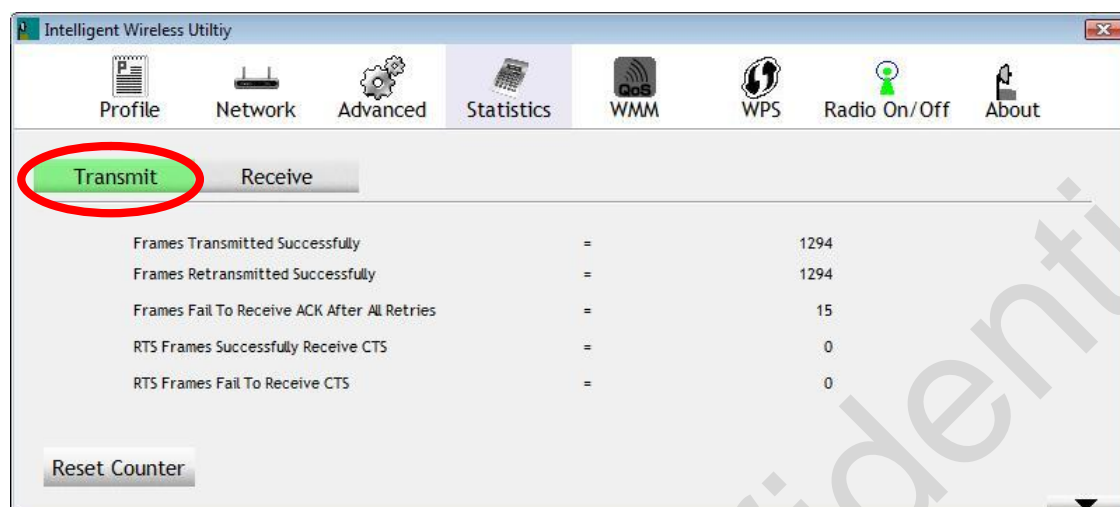


Advanced Tab

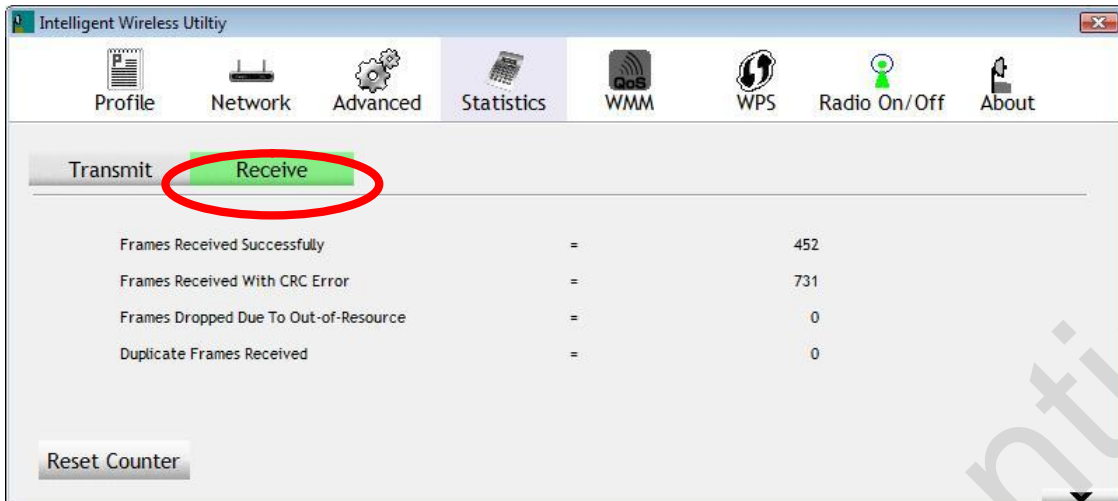
Wireless mode	Here supports 2.4G (included 802.11b/g) wireless mode.
Enable TX Burst	Check to enable this function. This function enables the Wireless LAN Module to deliver better throughput during a period of time, it only takes effect when connecting with the AP that supports this function.
Enable TCP Window Size	Check to increase the transmission quality. The large TCP window size the better performance.
Fast Roaming at	Check to set the roaming interval, fast to roaming, setup by transmits power.
Apply	Click to apply above settings.

Statistics

The Statistics screen displays the statistics on the current network settings.



Transmit Statistics Tab	
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Retransmitted Successfully	Shows information of packets successfully sent with one or more retries.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS frame.
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.
Reset Counter	Click this button to reset counters to zero.

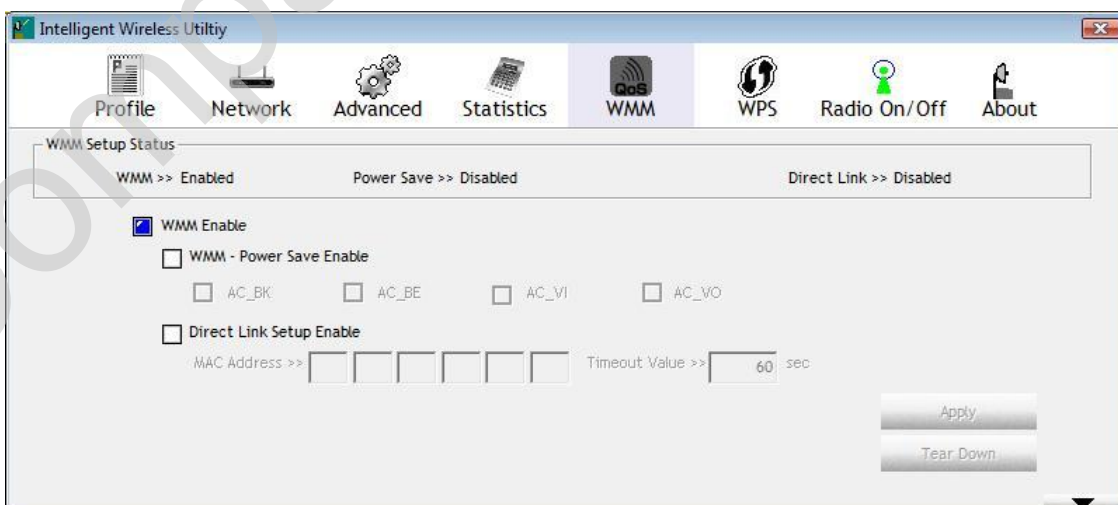


Receive Statistics Tab

Frames Received Successfully	Shows information of packets received successfully.
Frames Received With CRC Error	Shows information of packets received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.
Duplicate Frames Received	Shows information of packets received more than twice.
Reset Counter	Click this button to reset counters to zero.

WMM/ QoS

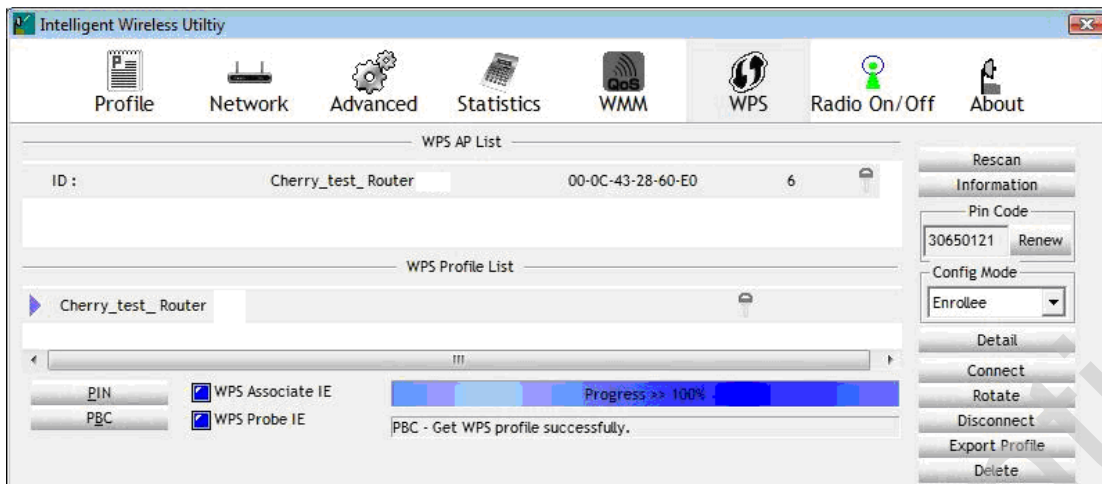
The WMM page shows the Wi-Fi Multi-Media power save function and Direct Link Setup that ensure the wireless network linking quality.



WMM/QoS Tab	
WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	Select a power save mode that preferred. <input type="checkbox"/> AC_BK (Access Category Background) <input type="checkbox"/> AC_BE (Access Category Best Effort) <input type="checkbox"/> AC_VI (Access Category Video) <input type="checkbox"/> AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup (DLS). This function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.
MAC Address	The setting of DLS(Direct Link Setup) indicates as follow : Fill in the blanks of Direct Link with MAC Address of target STA, and the STA must conform to two conditions: <input type="checkbox"/> Connecting with the same AP that supports DLS feature. <input type="checkbox"/> DLS enabled.
Timeout Value	Timeout Value represents that it disconnect automatically after few seconds. The value is integer that must be between 0~65535. It represents that it always connects if the value is zero. (Default value of Timeout Value is 60 seconds.)
Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA, then click "Tear Down" button to disconnect the STA.

WPS

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. The STA as an Enrollee or external Registrar supports the configuration setup using PIN (Personal Identification Number) configuration method or PBC (Push Button Configuration) method through an internal or external Registrar.



WPS Tab

WPS AP List

Display the information of surrounding APs with WPS IE from last scan result. List information included SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.

Rescan

Issue a rescan command to wireless NIC to update information on surrounding wireless network.

Information

Display the information about WPS IE on the selected network. List information included Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.



PIN Code

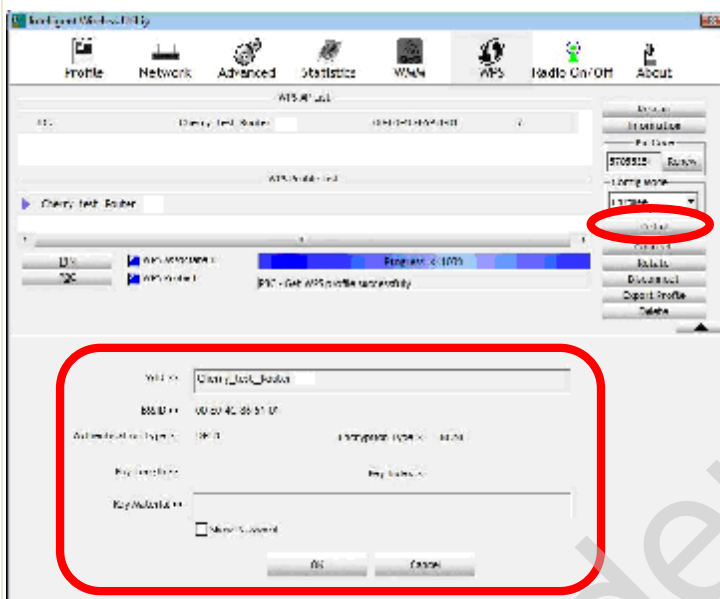
8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use "**Renew**" button to re-generate new PIN Code.

Config Mode

Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.

Detail

Click the **Detail** button to show the information about Security and Key in the credential.



If selected the AP that listed in the WPS Profile List field, click the **Detail** button to see more AP information.

SSID: Shows the connected AP network name.

BSSID: The MAC address of the connected AP. Fixed and cannot be changed.

Authentication Type: The authentication type support Open, WPA-PSK and WPA2-PSK.

Encryption Type: For **Open** authentication mode, the selection of encryption type are **NONE** and **WEP**. For **WPA-PSK** and **WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**.

Key Length: Only valid when using **Open** authentication mode and **WEP** encryption. There are key lengths 5, 10, 13 and 26.

Key Index: Only valid when using **Open** authentication mode and **WEP** encryption. There are 1~4 key index.

Key Material: The key material can be used to ensure the security of the wireless network. Fill in the appropriate value or phrase in **Key Material** field.

Show Password: Check this box to show the passwords that have been entered.

OK: Click to save and apply the new settings.

Cancel: Click to leave and discard the settings.

Connect

Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.

Rotate

Command to rotate to connect to the next network inside credentials.

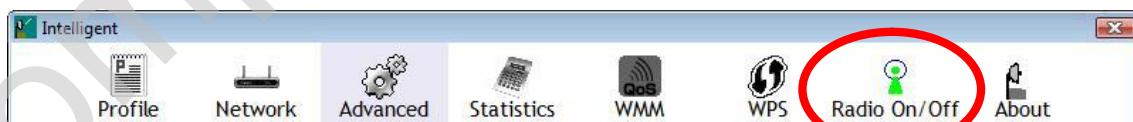
Disconnect

Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.

Export Profile	Export all credentials to Profile.
Delete	Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.
PIN	<p>Registrar: Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in two minutes and get IP address.</p> <p>Enrollee: Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address.</p>
PBC	Start to add to AP using PBC (Push Button Configuration) method. Click this button to connect the AP which supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.
Note:	
After the users click PIN or PBC, please do not rescan within two minutes of the connection. If users want to stop this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.	
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Progress Bar	Display rate of progress from Start to Connected status.
Status Bar	Display currently WPS Status.

Radio On/Off

Click this button to turn on or off radio function.



This icon shows radio is On.



This icon shows radio is Off.

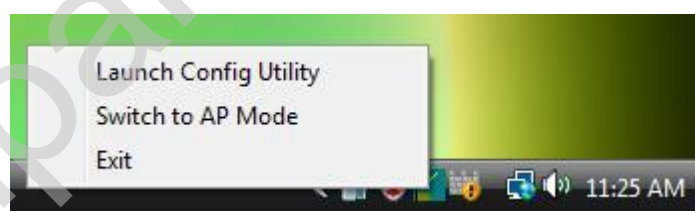
About

This page displays the information of the Wireless LAN Module including, RaConfig Version/ Date, Driver Version/ Date, EEPROM Version and Phy_Address.



Utility Menu List

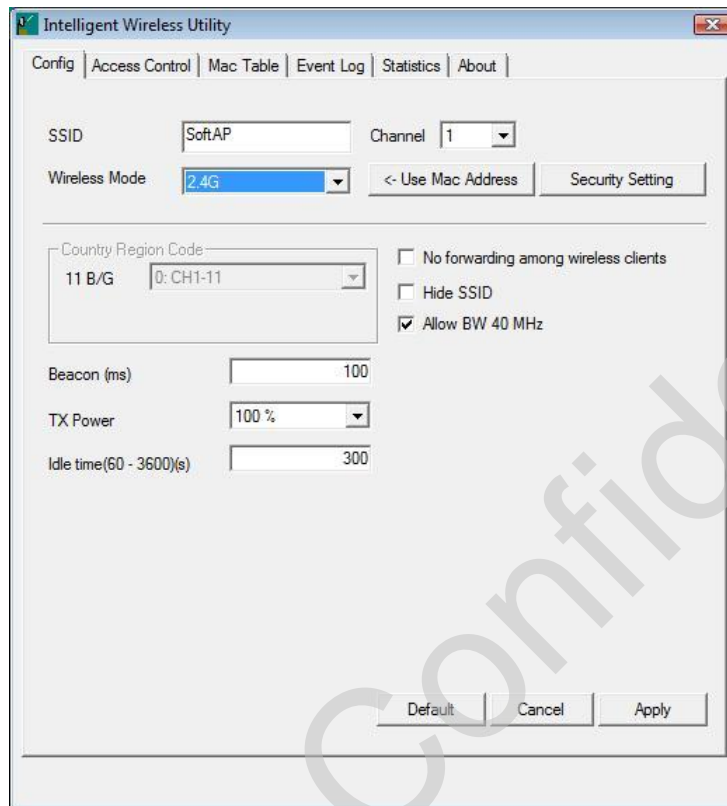
To access Windows Vista utility menu list, please right click the utility icon on the task bar.



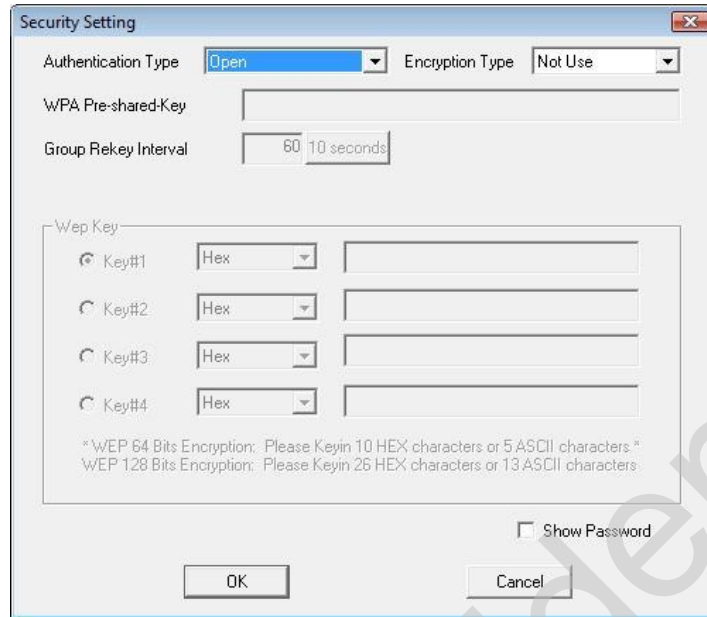
- I **Launch Config Utility:** Select to open the utility screen.
- I **Switch to AP Mode:** Select to make the Wireless LAN Module act as a wireless AP.
- I **Exit:** Select to close the utility program.

Soft AP mode

Config



Config	
SSID	AP name of user type. Users also can click Use Mac Address button to display it.
Channel	Manually force the AP using the channel. (The system default is CH 1.)
Wireless Mode	Here supports 2.4G (included 802.11b/g) wireless mode.
Use Mac Address	Click this button to replace SSID by MAC address.
Security Setting	Authentication mode and encryption algorithm used within the AP. (The system default is no authentication and encryption.)



Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. (System authentication type default is Open.)

Encryption Type: For **Open** and **Shared** authentication mode, the selections of encryption type are **Not Use** and **WEP**. For **WPA-PSK**, **WPA2-PSK**, and **WPA-PSK/ WPA2-PSK** authentication mode, the encryption type supports both **TKIP** and **AES**. (System authentication type default is Not Use.)

WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK and WPA-PSK/ WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

Group Re-key Interval: Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode to renew key. Users can set to change by seconds or packets. (Default is 600 seconds.)

WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys.

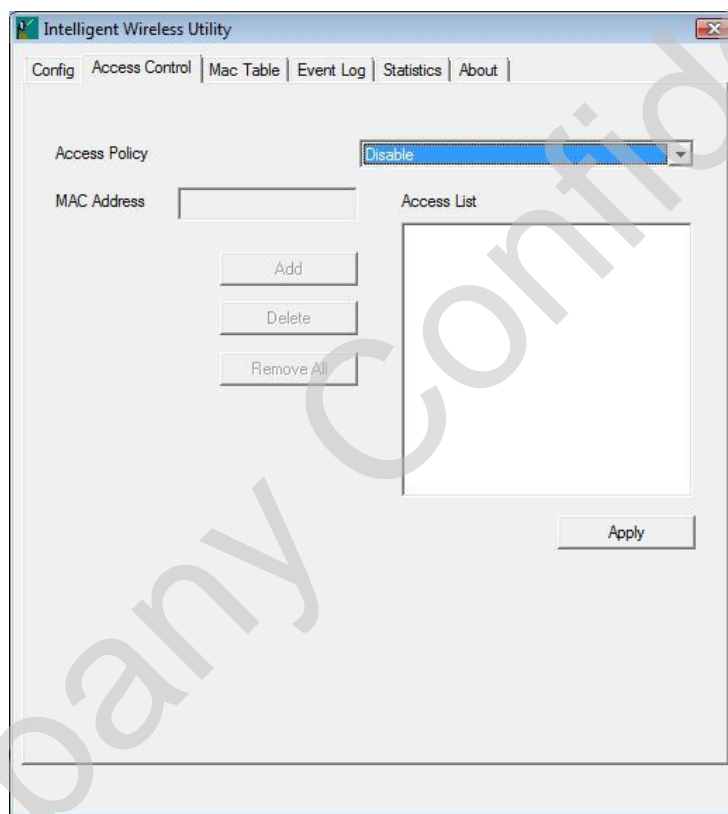
- [ASCII \(64 bits\): 5 ASCII characters](#) (case sensitivity).
- [ASCII \(128 bits\): 13 ASCII characters](#) (case sensitivity).
- [Hexadecimal \(64 bits\): 10 Hex characters](#) (0~9, a~f).
- [Hexadecimal \(128 bits\): 26 Hex characters](#) (0~9, a~f).

Show Password: Check this box to show the passwords that have been entered.

Beacon (ms)	The time between two beacons. (The system default is 100 ms.)
TX Power	Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and Lowest. (The system default is 100%.)
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. (Default value of idle time is 300 seconds.)

No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. (The system default is no forwarding.)
Hide SSID	Do not display AP name. (System default no hide.)
Default	Use the system default value.
Apply	Click to apply the above settings.

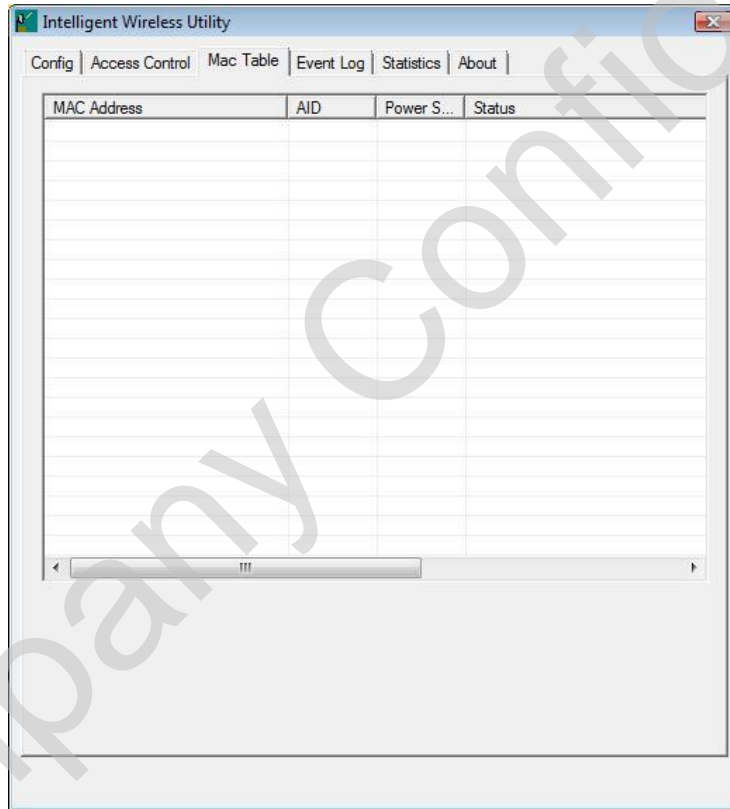
Access Control



Access Control	
Access Policy	<p>User chooses whether AP start the function or not. (System default is Disable.)</p> <ul style="list-style-type: none"> ! Disable: Do not use this access control function. ! Allow All: Only the MAC address listed in the Access List can connect with this soft AP. ! Reject All: Only the MAC address listed in the Access List can NOT connect with this soft AP.

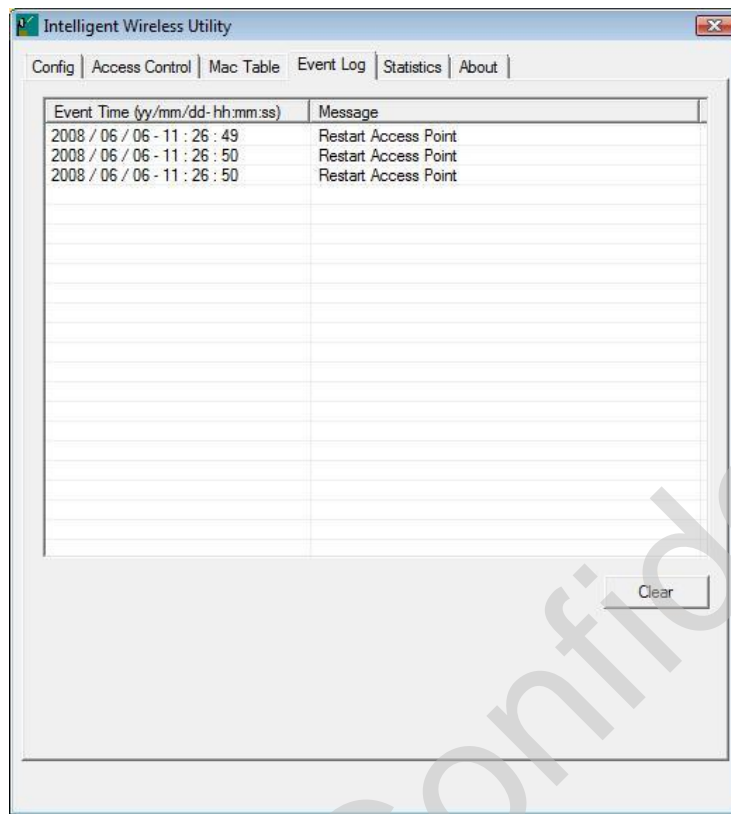
MAC Address	Manually force the Mac address using the function. Enter the MAC address in the column and click Add button, then the MAC address will be listed in the Access List pool.
Access List	Display all MAC Address that users have set.
Add	Add the MAC address that users would like to set.
Delete	Delete the MAC address that users have set.
Remove All	Remove all MAC address in the Access List.
Apply	Apply the above changes.

MAC Table



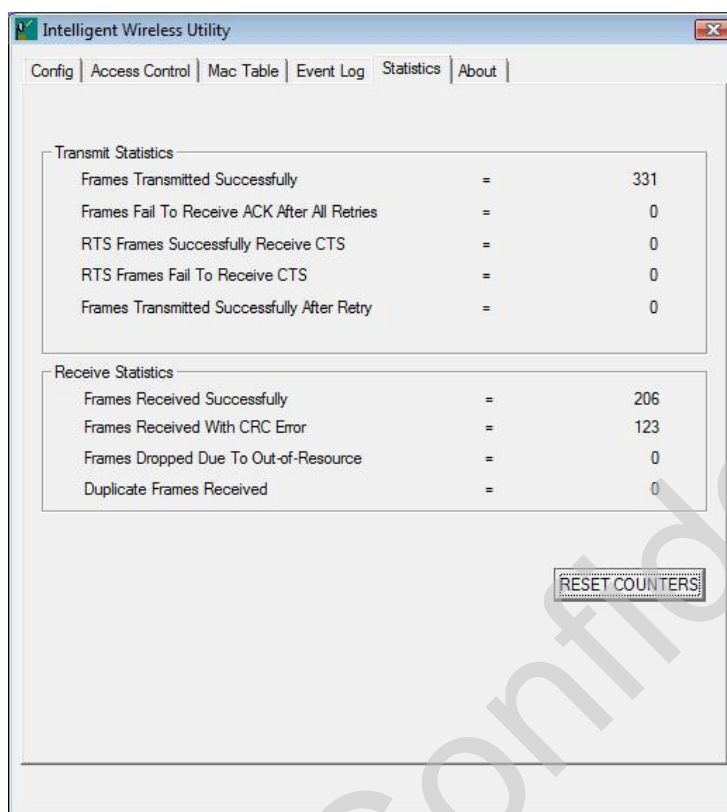
MAC Table	
MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	The station of current connect whether it have to support.
Status	The status of current connection.

Event Log



Event Log	
Event Time (yy/mm/dd-hh:mm:ss)	Records the event time.
Message	Records all the event messages.

Statistics



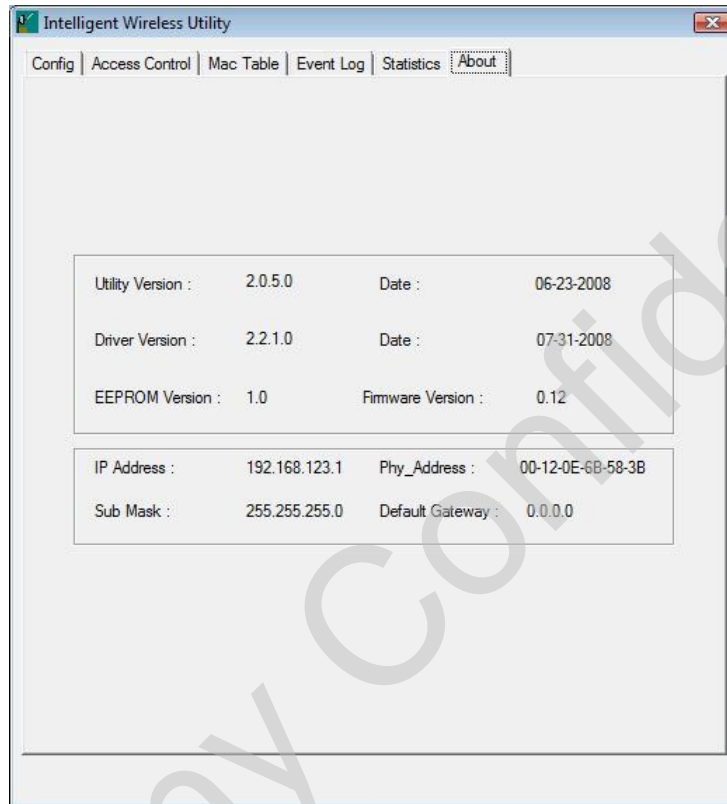
Transmit Statistics	
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS.
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Shows information of packets successfully sent with one or more retries.
Receive Statistics	
Frames Received Successfully	Shows information of packets received successfully.
Frames Received With CRC Error	Shows information of packets received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.
Duplicate Frames Received	The number of duplicate packets received.

Reset Counter

Reset counters to zero.

About

This page displays the Wireless LAN Module and driver version information.

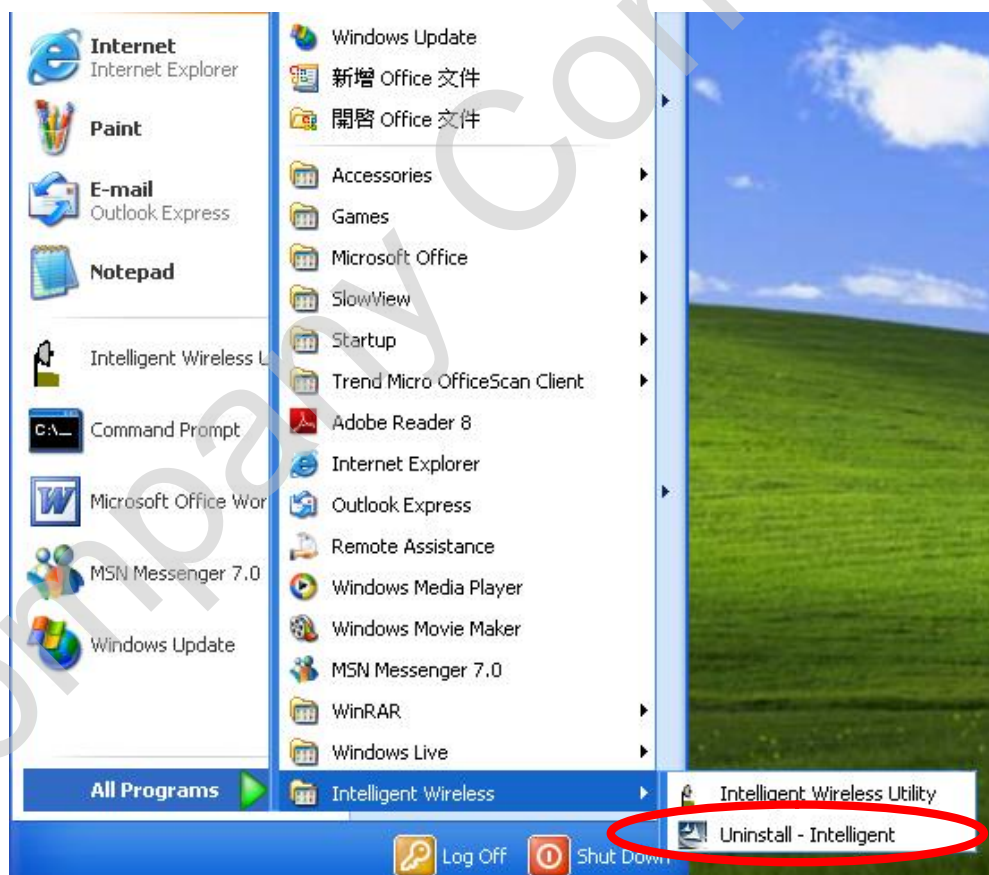


Chapter 4: Uninstallation

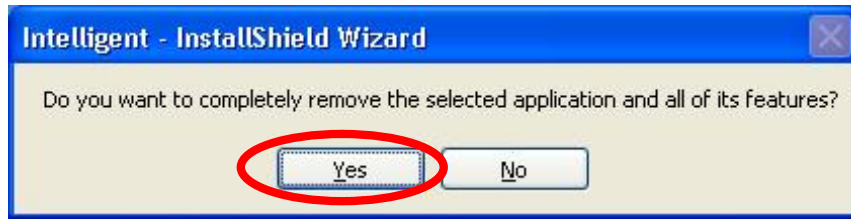
For Windows 2000/XP

To uninstall the utility and driver, please refer to below steps. (When uninstalling the utility, the driver will be uninstalled as well.)

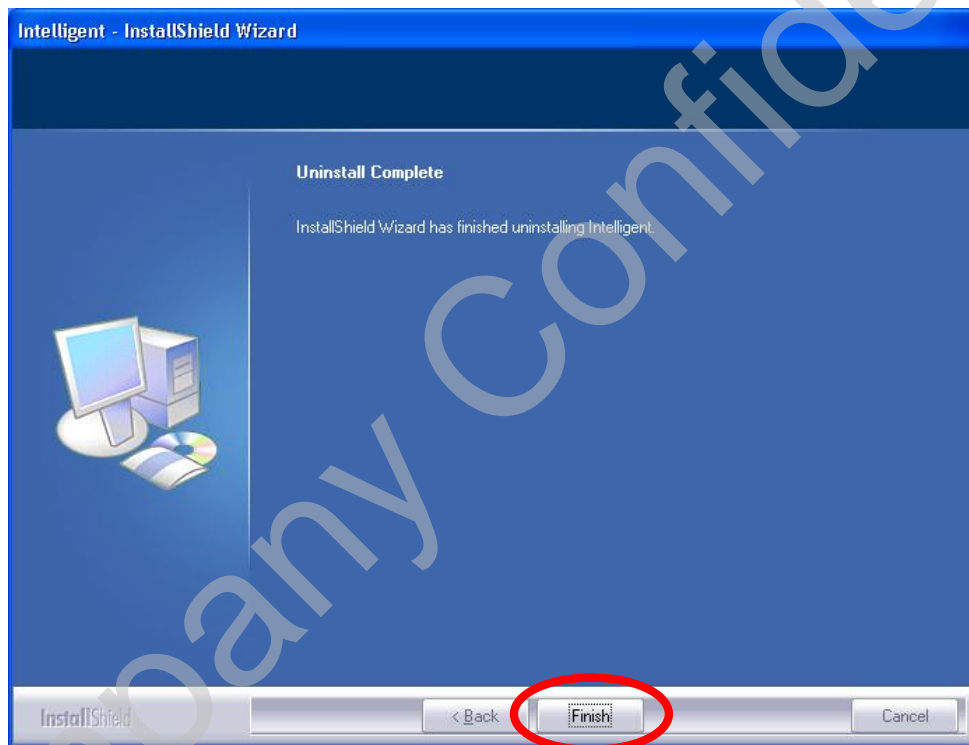
1. Go to **Start à All Programs à Intelligent Wireless à Uninstall –Intelligent.**



2. Click **Yes** to complete remove the selected application and all of its features.



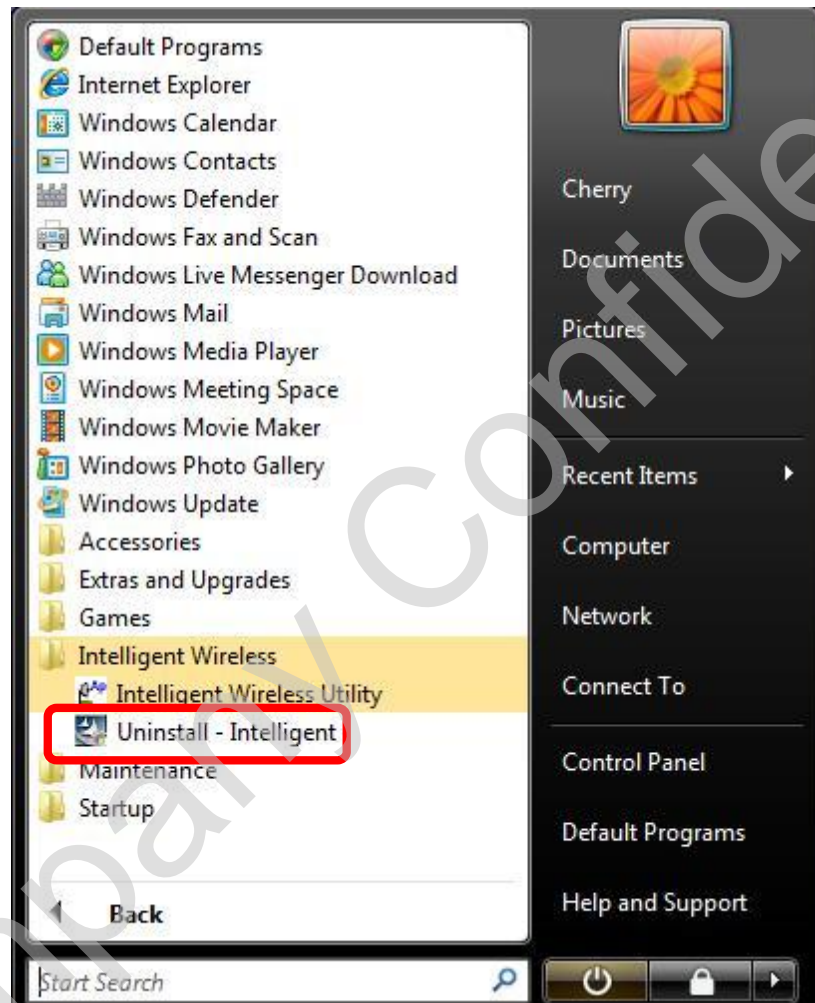
3. Then click **Finish** to complete the uninstallation.



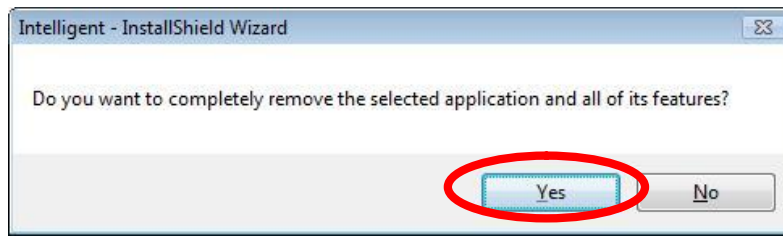
For Windows Vista

To uninstall the utility and driver, please refer to below steps. (When uninstalling the utility, the driver will be uninstalled as well.)

1. Go to **Start à Programs à Intelligent Wireless à Uninstall –Intelligent.**



2. Click **Yes** to complete remove the selected application and all of its features.

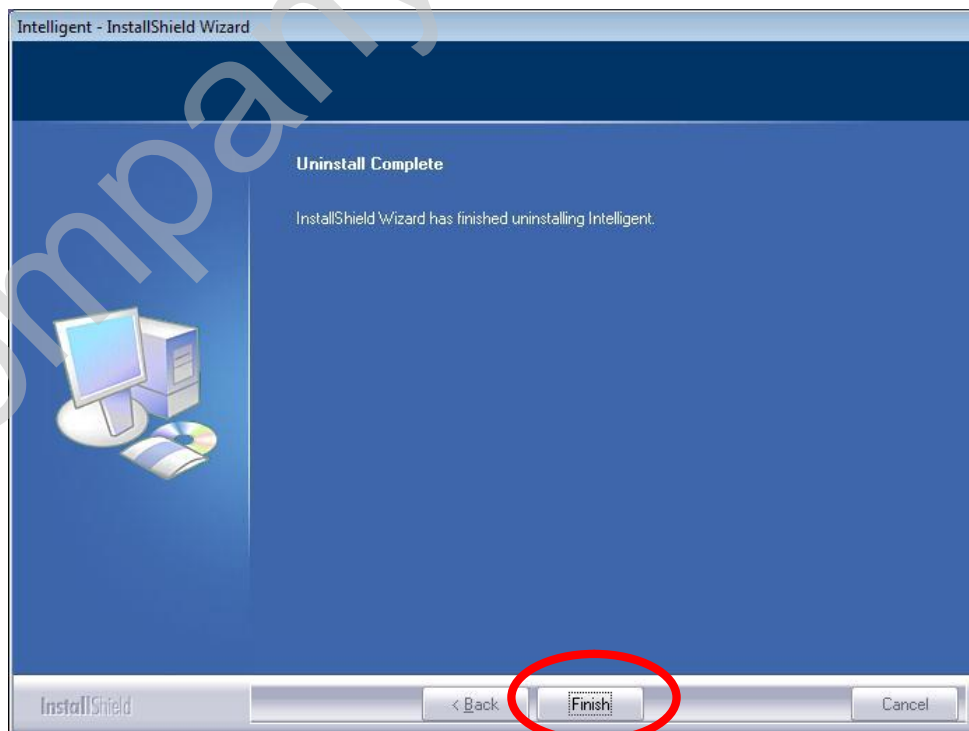


Caution:

Under Vista 64-bit operation system, when process uninstallation the following screen will show up and request to insert Wireless LAN Module to complete the uninstallation.



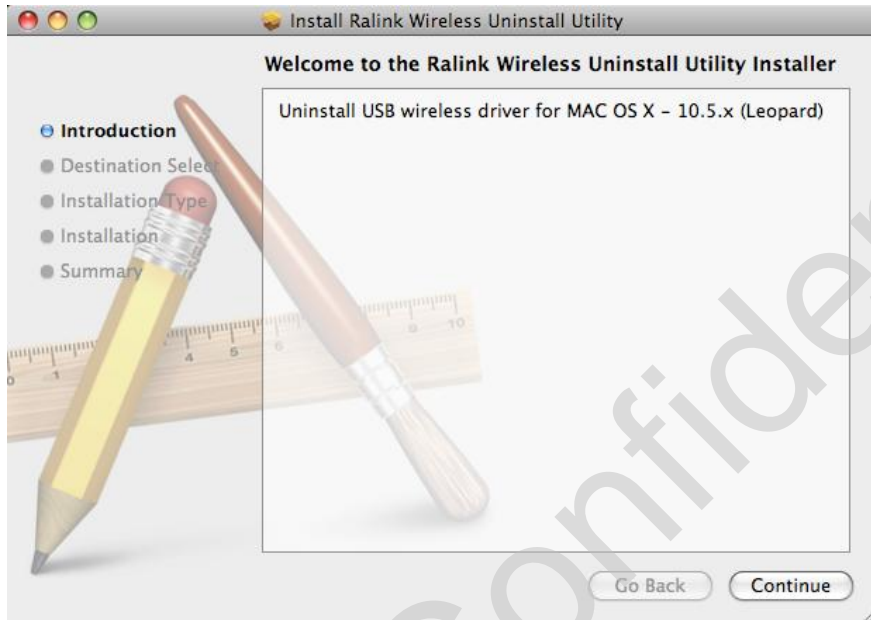
3. Finally, click **Finish** to complete the uninstallation.



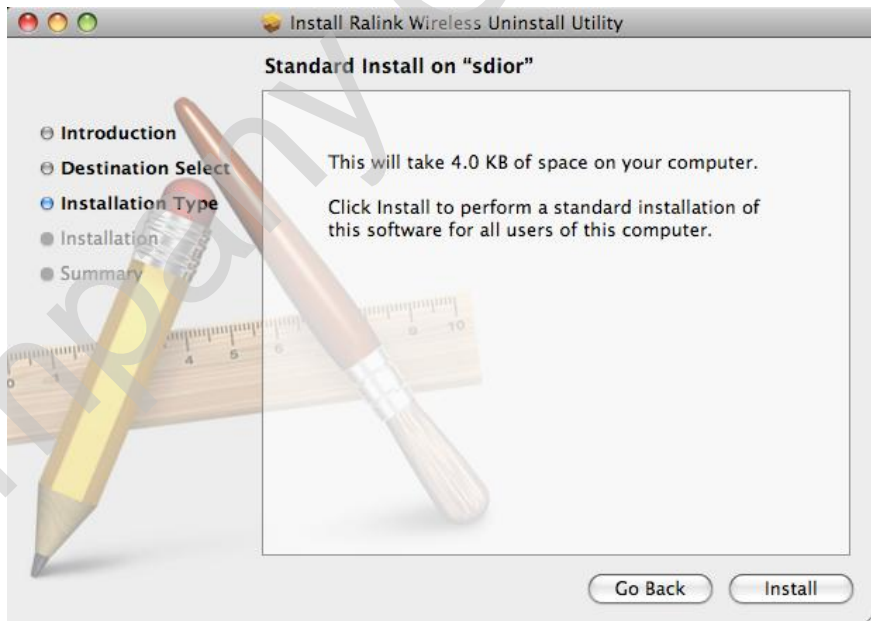
For Mac OS 10.5

To remove the Mac driver, please go to execute the Wireless- Leopard-Uninstall.pkg file to start.

1. When this Welcome screen shows, please click **Continue** to go on.



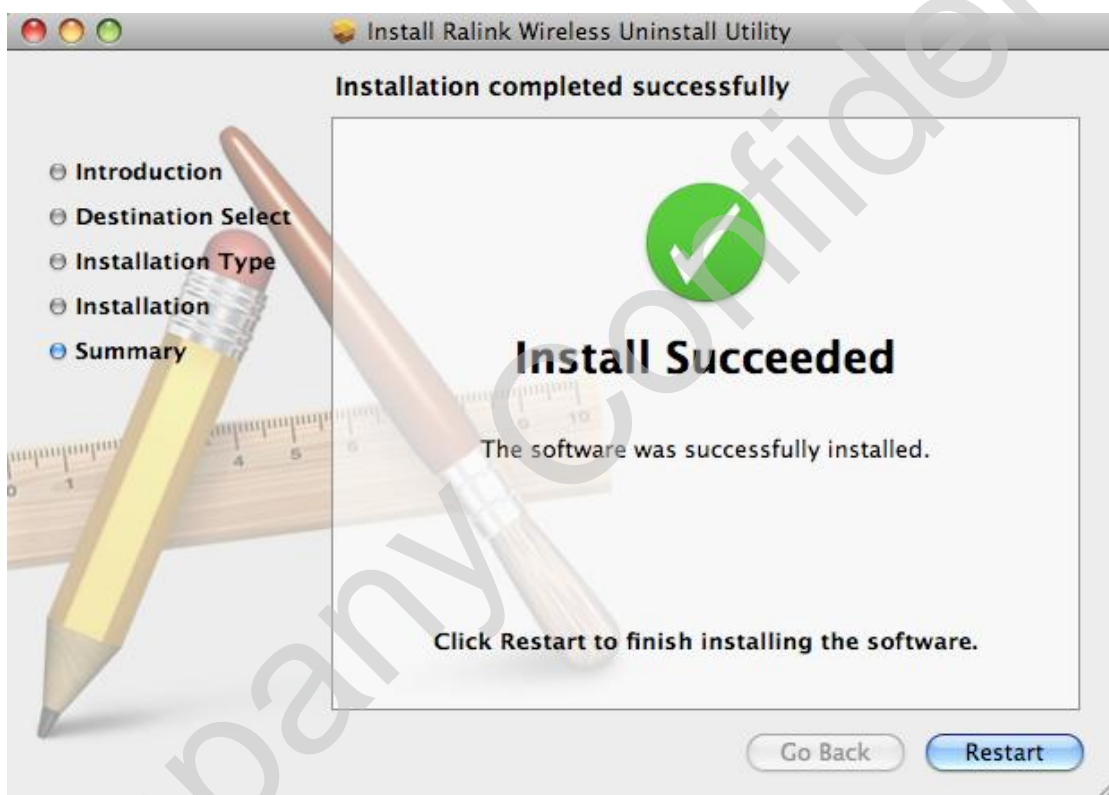
2. Click **Install** to perform the uninstallation.



3. The computer restart message will show up, please click **Continue Installation** to install.

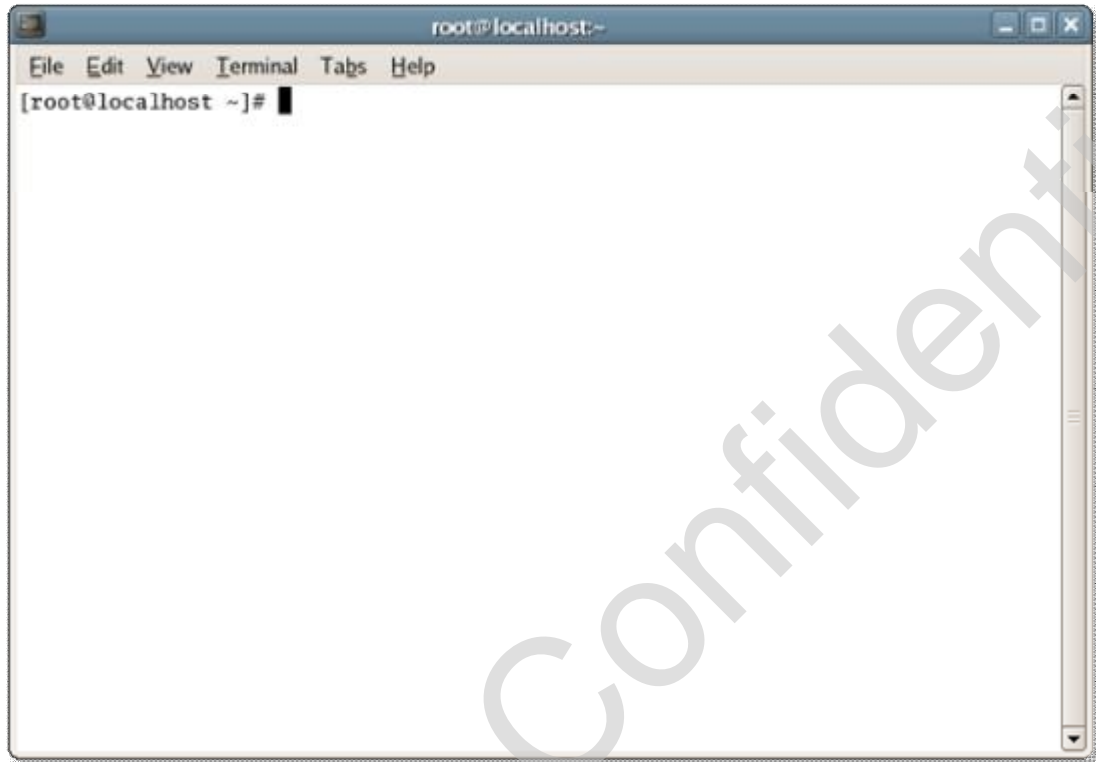


4. Click **Restart** to finish installing the software.



For Linux Kernel 2.4/2.6

To remove the Linux kernel driver, please enter the commands as following in the Terminal program.



1. unload driver

```
$/sbin/ifconfig ra0 down
```

```
$/sbin/rmmod rt3070sta
```