802.11b/g Wireless LAN
USB 2.0 Adaptor

User’s Manual

REGULATORY STATEMENTS

FCC Certification

The United States Federal Communication Commission (FCC) and the Canadian Department of Communications have established certain rules governing the use of electronic equipment.

Part15, Class B

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interface, and

2) This device must accept any interface received, including interface that may cause undesired operation. 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 off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the distance between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

CAUTION:

1) To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

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

Per FCC 15.21, you are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user’s authority to operate the equipment.

Information for OEM integrator

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 manual of the end product.

The user manual which is provided by OEM integrators for end users must include the following information in a prominent location.

“To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

Label for end product must inclode "Contains FCC ID: RFHWUG2700"

Table of Contents

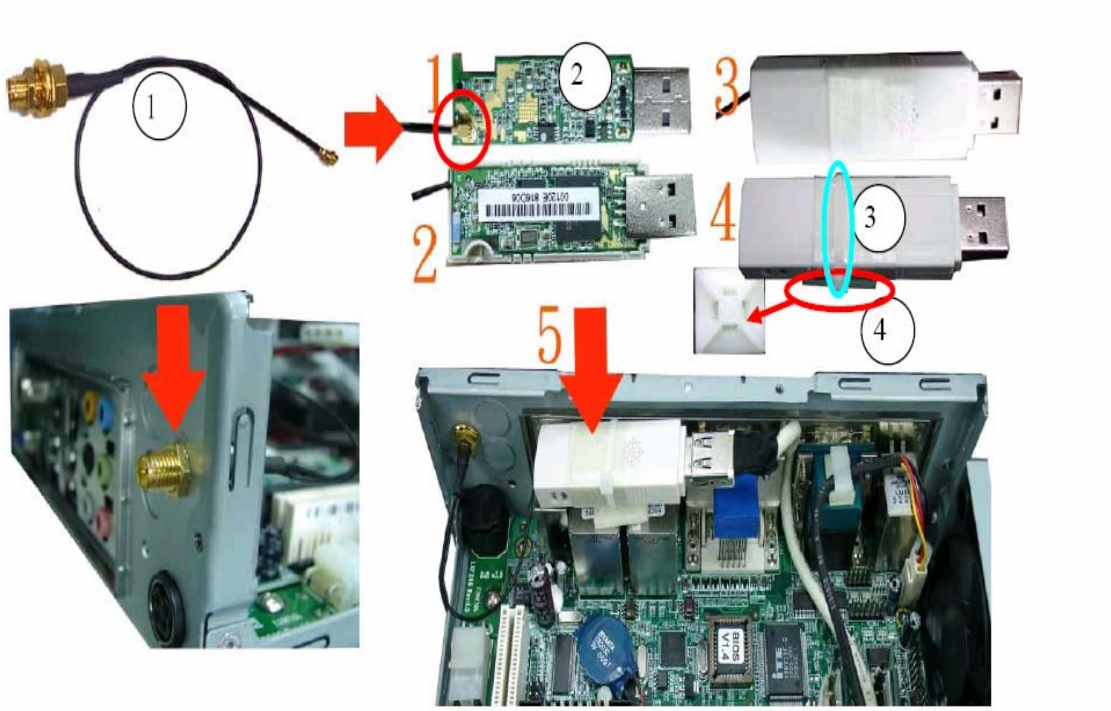
INTRODUCTION

The **802.11b/g High Gain Wireless LAN USB Adapter** is designed for a USB type A port of a laptop or desktop computer for creating a wireless workstation. It is USB 2.0 compliant, which connects to any available USB port on a notebook or desktop computer.

The **802.11b/g High Gain Wireless LAN USB Adapter** complies with **IEEE 802.11g** standard that offers a data rate up to **54Mbps** in a wireless LAN environment. It is backward compliant with IEEE 802.11b specification. The high-speed wireless network card can plug into your notebook or desktop PC and accesses to the LAN or peer-to-peer networking easily without wires or cables. Whether you're at your desk or in the boardroom, it allows you to share printers, files, and other network resources.

Features

- Complies with IEEE 802.11g standard for 2.4GHz Wireless LAN
- USB 2.0 compliant
- USB Plug & Play
- Interoperable with existing network infrastructure
- Secure information transmission
- Freedom to roam while staying connected
- Compatible with specialty wireless products and services
- Up to 54 Mbps data rate
- Antenna is built in the card with LED indication
- Low power consumption
- Easy to install and configure



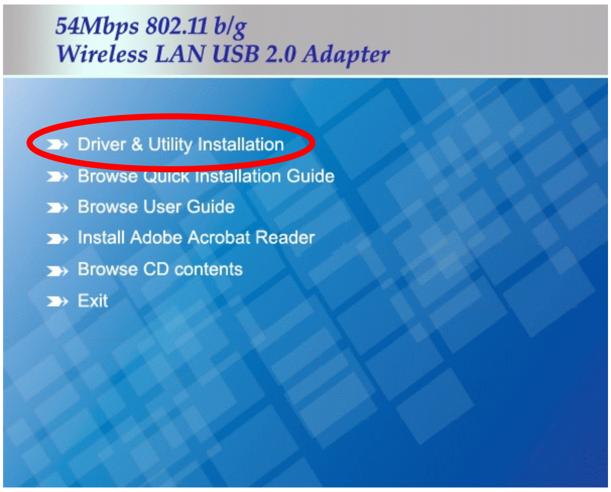
1. The RF Cable is connected and finally sat first.
2. The RF Cable is connected to AE04WUG27HRS.
3. Use one bunch of threads area and tie fixing and sitting.
4. Paste it on the main board.

Windows 2000/XP Installation

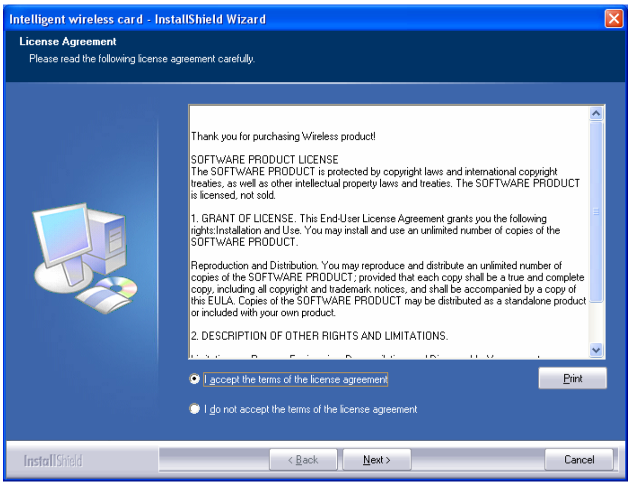
Install the Software

Do not insert the wireless LAN adapter into your computer until the procedures in "Driver& Utility Installation" have been performed.

1. Insert the included CD-ROM into the CD-ROM drive of your computer.
2. When the Main Menu screen appears, click **"Driver & Utility Installation"** to start the software installation.


54Mbps 802.11 b/g
Wireless LAN USB 2.0 Adapter
Driver & Utility Installation
Browse Quick Installation Guide
Browse User Guide
Install Adobe Acrobat Reader
Browse CD contents
Exit

3. 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.



Intelligent wireless card - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Thank you for purchasing Wireless product!

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

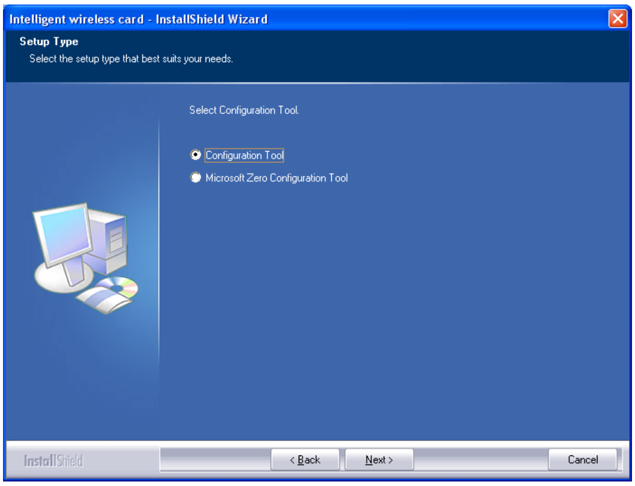
● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

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

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

Click **Next** to continue.



Intelligent wireless card - InstallShield Wizard

Setup Type

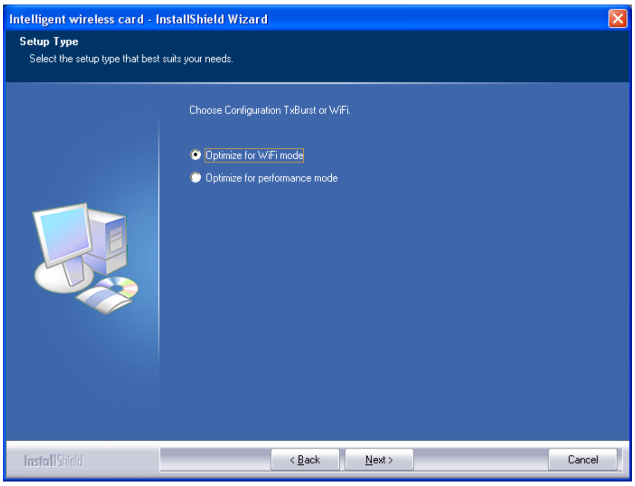
Select the setup type that best suits your needs.

Select Configuration Tool.

● Configuration Tool

○ Microsoft Zero Configuration Tool

5. There are two modes for you to choose in this screen, either choose **Optimize for WiFi mode** or **Optimize for performance mode (Tx Burst mode)**. This mode selection screen is set for the default mode shown in the utility screen; you can still change its mode later in the utility screen. Click **Next** to continue.



Intelligent wireless card - InstallShield Wizard

Setup Type

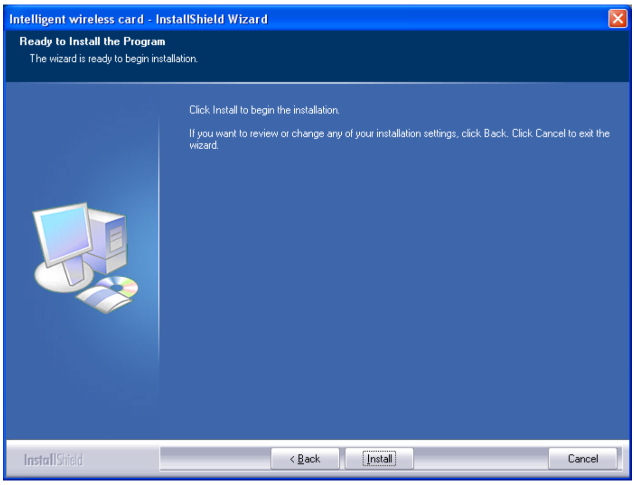
Select the setup type that best suits your needs.

Choose Configuration TxBurst or WiFi.

● Optimize for WiFi mode

○ Optimize for performance mode

6. When you are prompted the following message, please click **Install** to begin the installation.



Intelligent wireless card - InstallShield Wizard

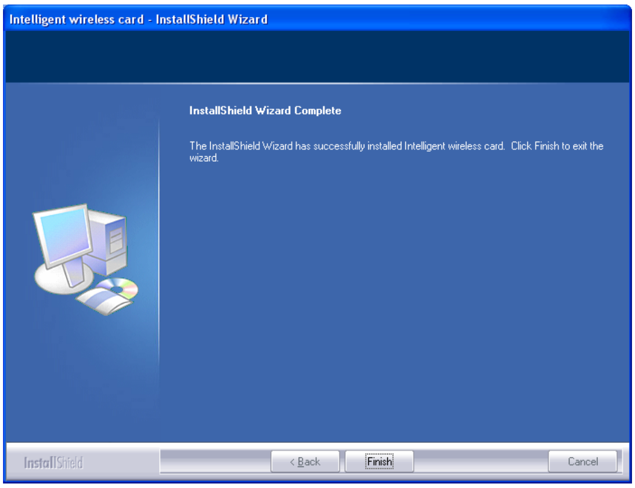
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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



Intelligent wireless card - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Intelligent wireless card. Click Finish to exit the wizard.

Install the Hardware

Note: Insert the Wireless USB card when you finished your software installation.

Insert the USB Adapter into the USB Port of your computer. The system will automatically detect the new hardware.

Windows Vista Installation

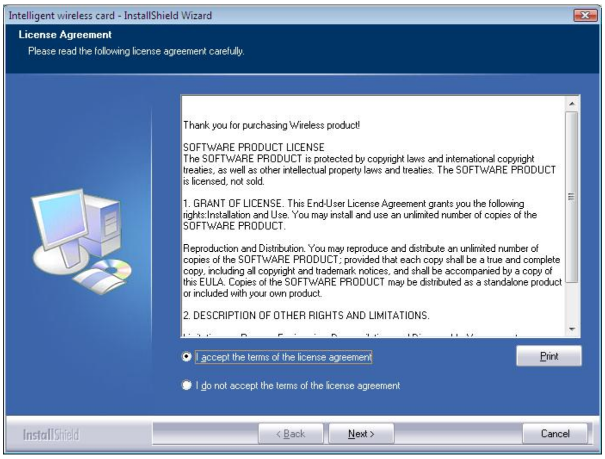
Install the Software

Do not insert the wireless LAN adapter into your computer until the procedures in "Driver& Utility Installation" have been performed.

1. Insert the included CD-ROM into the CD-ROM drive of your computer.

2. When the Main Menu screen appears, click "Driver & Utility Installation" to start the software installation.

3. 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.



Intelligent wireless card - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Thank you for purchasing Wireless product!

SOFTWARE PRODUCT LICENSE
The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This End-User License Agreement grants you the following rights:Installation and Use. You may install and use an unlimited number of copies of the SOFTWARE PRODUCT.

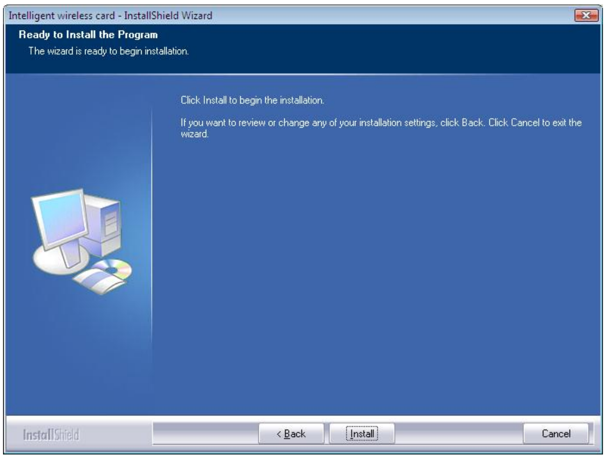
Reproduction and Distribution. You may reproduce and distribute an unlimited number of copies of the SOFTWARE PRODUCT; provided that each copy shall be a true and complete copy, including all copyright and trademark notices, and shall be accompanied by a copy of this EULA. Copies of the SOFTWARE PRODUCT may be distributed as a standalone product or included with your own product.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

4. When you are prompted the following message, please click **Install** to begin the installation.



Intelligent wireless card - InstallShield Wizard

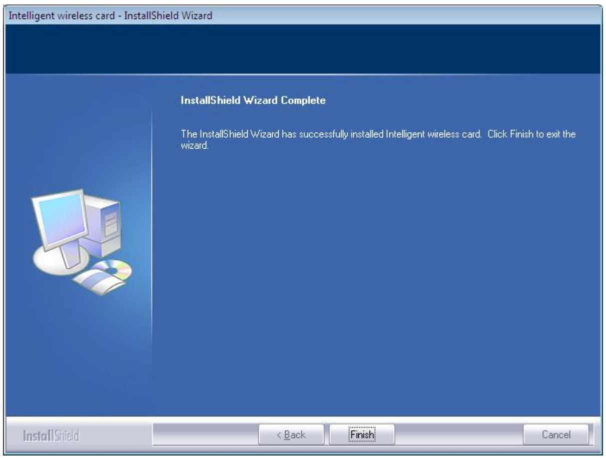
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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



Intelligent wireless card - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Intelligent wireless card. Click Finish to exit the wizard.

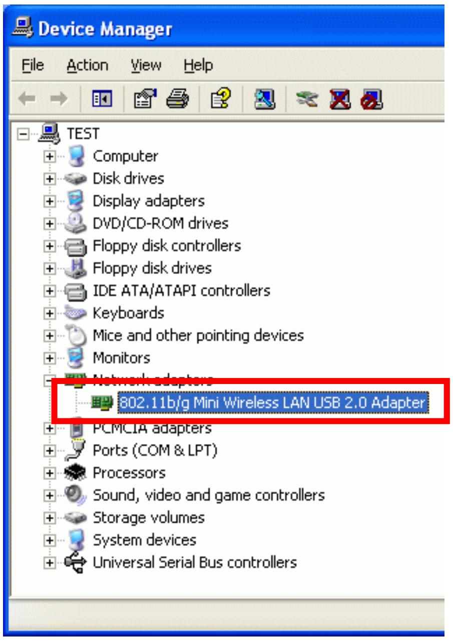
Install the Hardware

Note: Insert the Wireless USB card when you finished your software installation.

Insert the USB Adapter into the USB Port of your computer. The system will automatically detect the new hardware.

Verification

To verify if the device exists in your computer and is enabled, go to **Start > Control Panel** > **System** (> **Hardware)** > **Device Manager**. Expand the **Network Adapters** category. If the **802.11b/g Mini Wireless LAN USB 2.0 Adapter** is listed here, it means that your device is properly installed and enabled.



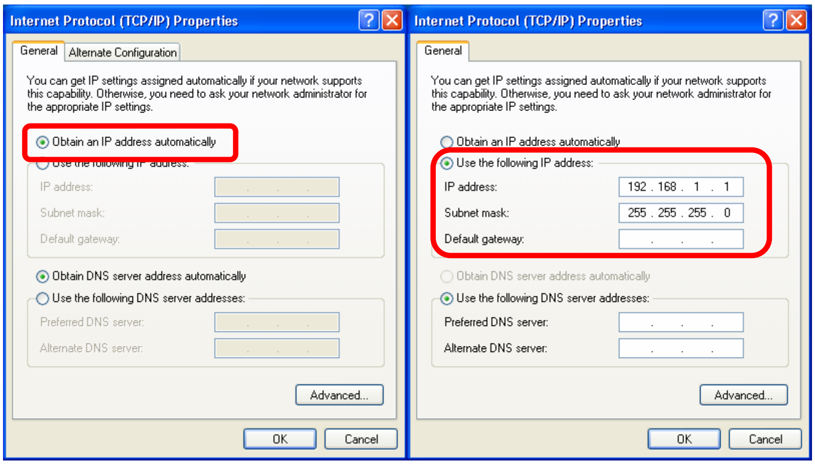
Device Manager

TEST
- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Floppy disk controllers
- Floppy disk drives
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network adapters
  - 802.11b/g Mini Wireless LAN USB 2.0 Adapter
- PCMCIA adapters
- Ports (COM & LPT)
- Processors
- Sound, video and game controllers
- Storage volumes
- System devices
- Universal Serial Bus controllers

IP Address

***Note**: When assigning IP Addresses to the computers on the network, remember to have the IP address for each computer set on the same subnet mask. If your Broadband Router use DHCP technology, however, it won't be necessary for you to assign Static IP Address for your computer.*

1. To configure a dynamic IP address (i.e. if your broadband Router has the DHCP technology), check the **Obtain an IP address automatically** option.
2. To configure a fixed IP address (if you broadband Router is not DHCP supported, or when you need to assign 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, and ***255.255.255.0*** for the Subnet mask.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically
○ Use the following IP address:
IP address: . . .
Subnet mask: . . .
Default gateway: . . .

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

Internet Protocol (TCP/IP) Properties

General

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

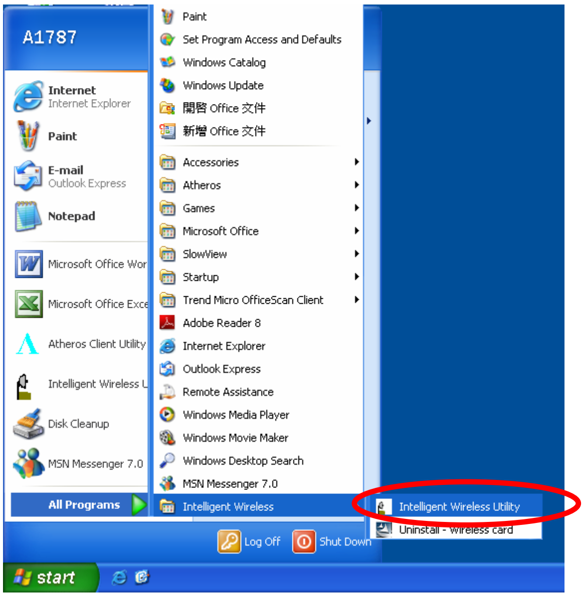
○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

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

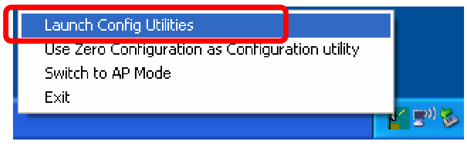
Utility Configuration for Windows 2000/XP

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

Go to **Start→ (All) Programs→Intelligent Wireless → Intelligent Wireless Utility**



You can also open the Configuration Utility by double clicking the icon or right clicking to select **Launch Config Utilities**.



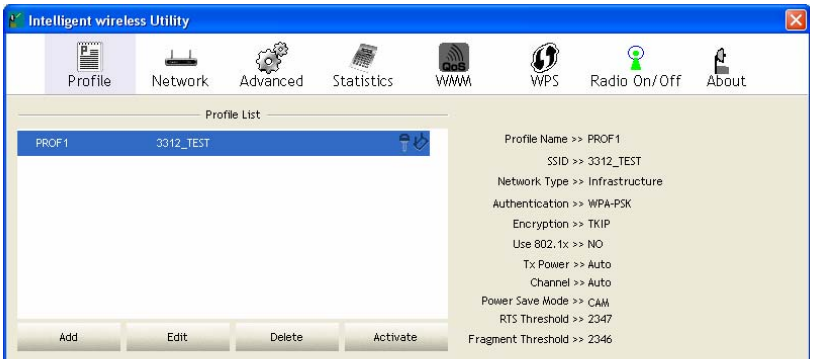
Station Mode

Profile

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

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

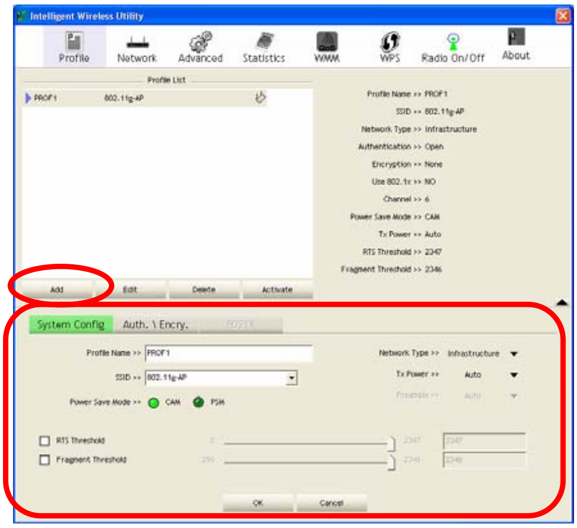
▲ Click this button to hide the information of Status Section.



PROF1 3312_TEST

Profile Name >> PROF1
SSID >> 3312_TEST
Network Type >> Infrastructure
Authentication >> WPA-PSK
Encryption >> TKIP
Use 802.1x >> NO
Tx Power >> Auto
Channel >> Auto
Power Save Mode >> CAM
RTS Threshold >> 2347
Fragment Threshold >> 2346

Profile Tab	
Profile Name	You 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 points in your wireless network.
Network Type	Shows the network type of the device, including infrastructure and Ad-Hoc.
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. (There are 14 channels available, depending on the country.)
Power Save Mode	Choose from CAM (Constantly Awake Mode) or Power Saving Mode.
RTS Threshold	Shows the RTS Threshold of the device.
Fragment Threshold	Shows the Fragment Threshold of the device.
Add	Click to add a profile from the drop-down screen. **System Configuration tab:**  Intelligent Wireless Utility Profile Network Advanced Statistics WMM WPS Radio On/Off About Profile List Add Edit Delete Activate System Config Auth. \ Encry. 802.1X OK Cancel PROF1 802.11g-AP Profile Name >> PROF1 SSID >> 802.11g-AP Network Type >> Infrastructure Authentication >> Open Encryption >> None Use 802.1x >> NO Channel >> 6 Power Save Mode >> CAM Tx Power >> Auto RTS Threshold >> 2347 Fragment Threshold >> 2346 Profile Name >> PROF1 SSID >> 802.11g-AP Power Save Mode >> ● CAM ○ PSM Network Type >> Infrastructure Tx Power >> Auto Preamble >> Auto □ RTS Threshold 0 2347 2347 □ Fragment Threshold 256 2346 2346 **Profile Name**: User can enter profile name, or use default name defined by system. The default is PROF# (# 1, #2, #3....). **SSID**: The **SSID** is the unique name shared among all points in your wireless network. The name must be identical for all devices and points attempting to connect to the same network. User can use pull-down menu to select from available APs.

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.
- **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.

Network Type: There are two types, Infrastructure and Ad hoc modes. Under Ad hoc mode, user can also choose the preamble type, the available preamble type includes **Auto** and **Long**. In addition to that, the channel field will be available for setup in Ad-hoc mode.

- The **Infrastructure** is intended for the connection between wireless network cards and an Access Point. With the wireless adapter, you can connect wireless LAN to a wired global network via an Access Point.
- The **Ad hoc** lets you set a small wireless workgroup easily and quickly. Equipped with the wireless adapter, you can share files and printers between each PC and laptop.

Tx Power: Select the Tx power percentage from the pull-down list including **Auto, 100%, 75%, 50%, 25%, 10%** and **Lowest.**

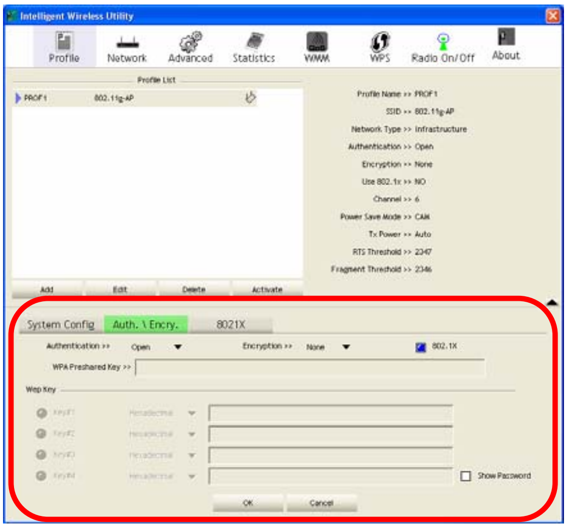
Preamble: A preamble is a signal used in wireless environment to synchronize the transmitting timing including Synchronization and Start frame delimiter. Select from the pull-down menu to change the Preamble type into **Auto** or **Long**.

RTS Threshold: User 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 you set.*

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

Fragment Threshold: User 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 your Wireless LAN Adapter often transmits large files in wireless network, you can enter new Fragment Threshold value to split the packet. The value can be set from 256 to 2346.

Authentication and Encryption tab:



PROF1 802.11g-AP

Profile Name >> PROF1
SSID >> 802.11g-AP
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Channel >> 6
Power Save Mode >> CAM
Tx Power >> Auto
RTS Threshold >> 2347
Fragment Threshold >> 2346

Authentication >> Open
Encryption >> None
☑ 802.1X
WPA Preshared Key >>
□ Show Password

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

- **Open**: If your access point/wireless router is using "**Open”** authentication, then the wireless adapter 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-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 is the shared secret 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 32 lengths.

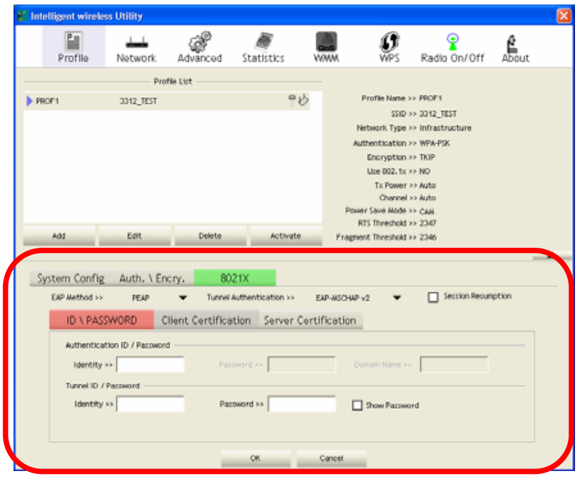
WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP’s key. There are several formats to enter the keys.

- Hexadecimal (40bits): 10 Hex characters.
- Hexadecimal (128bits): 32Hex characters.
- ASCII (40bits): 5 ASCII characters.
- ASCII (128bits): 13 ASCII characters.

Show Password: Check this box to show the password you entered.

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

802.1x tab:



PROF1 3312_TEST

Profile Name >> PROF1
SSID >> 3312_TEST
Network Type >> Infrastructure
Authentication >> WPA-PSK
Encryption >> TKIP
Use 802.1x >> NO
Tx Power >> Auto
Channel >> Auto
Power Save Mode >> CAM
RTS Threshold >> 2347
Fragment Threshold >> 2346

EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
☐ Session Resumption

Identity >>
Password >>
Domain Name >>

Identity >>
Password >>
☐ Show Password

EAP Method:

- **PEAP**: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunneling 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**: Tunneled 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.

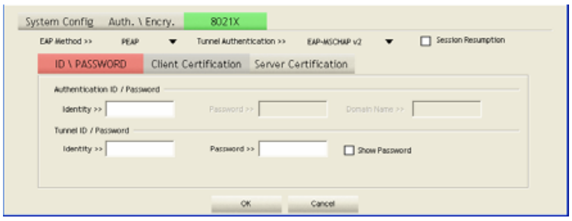
- **EAP-FAST**: Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed 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.

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: User can click the box to enable or disable this function.

ID\PASSWORD tab:



EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
☐ Session Resumption
☐ Show Password

ID/ PASSWORD: Identity and password for server.

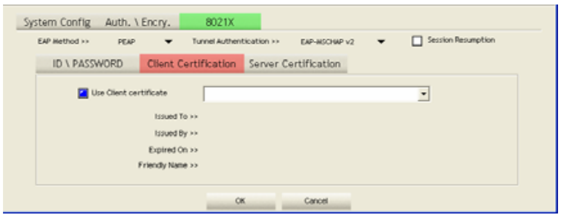
- **Authentication ID / Password**: Identity, password and domain name for server. Only "EAP-FAST" and "LEAP" authentication can key in domain name. Domain name can be keyed in blank space.
- **Tunnel ID / Password:** Identity and Password for server.

Show Password: Check this box to show the password you entered.

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

Client Certification tab:



EAP Method >> PEAP
Tunnel Authentication >> EAP-MSCHAP v2
☐ Session Resumption
☑ Use Client certificate

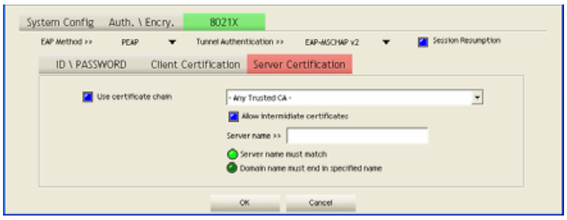
Client Certification: Client certificate for server authentication.

Use Client certificate: Choose to enable server authentication.

OK: Click to save settings and exit this page.

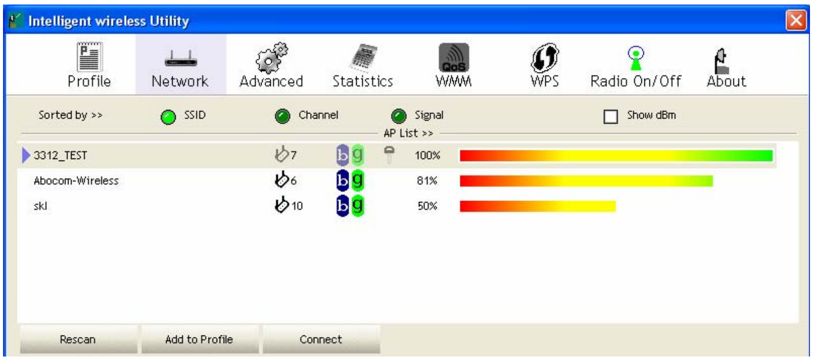
Cancel: Click to call off the settings and exit.

Server Certification tab:

	 System Config Auth. \ Encry. 8021X ID \ PASSWORD Client Certification Server Certification OK Cancel EAP Method >> PEAP Tunnel Authentication >> EAP-MSCHAP v2 ☑ Session Resumption ☑ Use certificate chain - Any Trusted CA - ☑ Allow intermidiate certificates Server name >> ● Server name must match ● Domain name must end in specified name **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 root. **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 to 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.

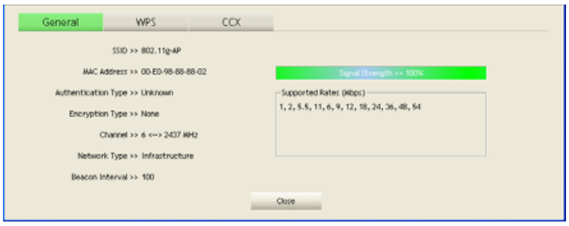
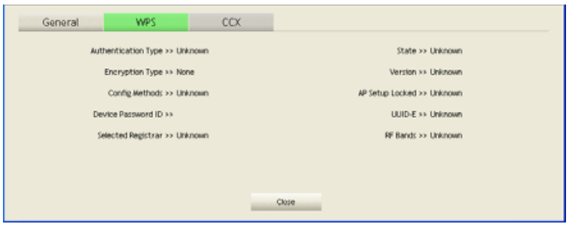


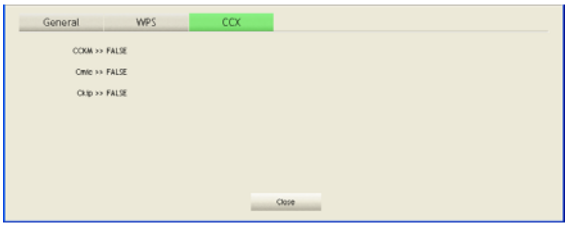
3312_TEST	7	bg	100%	
Abocom-Wireless	6	bg	81%	
skl	10	bg	50%	

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, Ad-Hoc for IBSS network.
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.
Connect	Select an item on the list and then click to make a connection.
Add to Profile	Select an item on the list and then click to add it into the profile list.

AP information

When you double click on the intended AP, you can see AP's detail information that divides into three parts. They are General, WPS, CCX information. The introduction is as following:

General	 SSID >> 802.11g-AP MAC Address >> 00-E0-98-88-88-02 Authentication Type >> Unknown Encryption Type >> None Channel >> 6 <--> 2437 MHz Network Type >> Infrastructure Beacon Interval >> 100 Signal Strength >> 100% Supported Rates (Mbps) 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54 General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates. **Close**: Click this button to exit the information screen.
WPS	 Authentication Type >> Unknown Encryption Type >> None Config Methods >> Unknown Device Password ID >> Selected Registrar >> Unknown State >> Unknown Version >> Unknown AP Setup Locked >> Unknown UUID-E >> Unknown RF Bands >> Unknown WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands. **Authentication Type**: There are four types of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system. **Encryption Type**: For open and shared authentication mode, the selection of encryption type are None and WEP.

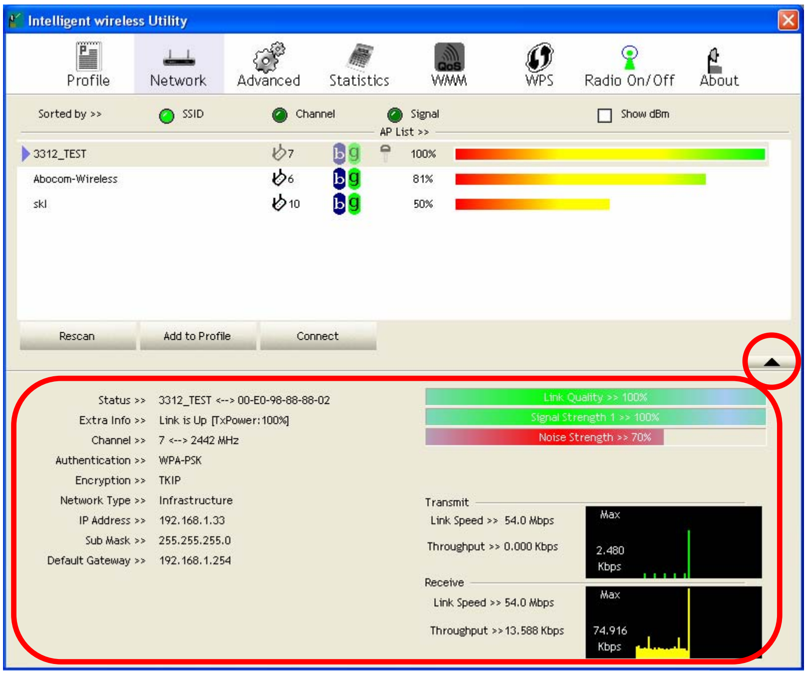
	For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES. **Config Methods**: Correspond to the methods the AP supports as an Enrollee for adding external Registrars. **Device Password ID**: Indicate the method or identifies the specific password that the selected Registrar intends to use. **Selected Registrar**: Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE". **State**: The current configuration state on AP. The values are "Unconfigured" and "Configured". **Version**: WPS specified version. **AP Setup Locked**: Indicate if AP has entered a setup locked state. **UUID-E**: The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes. **RF Bands**: Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz". **Close**: Click this button to exit the information screen.
CXX	 CCKM >> FALSE Cmic >> FALSE Ckip >> FALSE CCX information contains CCKM, Cmic and Ckip information. **Close**: Click this button to exit the information screen.

Link Status

Click the triangle button at the right 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 of Status Section.

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



SSID	Channel		Signal
3312_TEST	7	b g	100%
Abocom-Wireless	6	b g	81%
skl	10	b g	50%

Status >> 3312_TEST <--> 00-E0-98-88-88-02
Extra Info >> Link is Up [TxPower:100%]
Channel >> 7 <--> 2442 MHz
Authentication >> WPA-PSK
Encryption >> TKIP
Network Type >> Infrastructure
IP Address >> 192.168.1.33
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.254

Link Quality >> 100%
Signal Strength 1 >> 100%
Noise Strength >> 70%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps

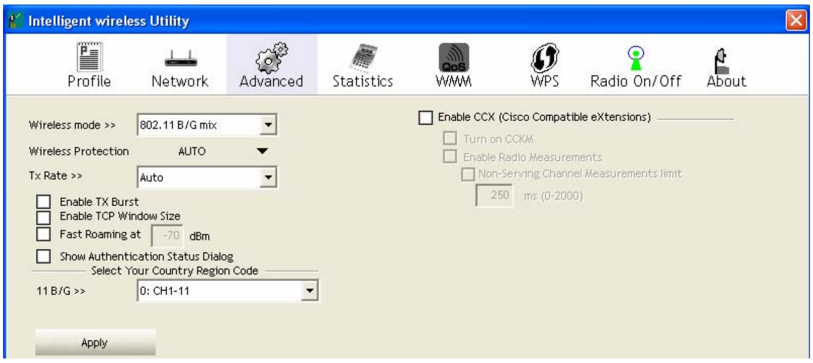
Receive
Link Speed >> 54.0 Mbps
Throughput >> 13.588 Kbps

Link Status Tab	
Status	Shows the current connection status. If there is no connection existing, it will show Disconnected.
Extra Info	Shows the link status.

Channel	Shows the current channel in use.
Authentication	Authentication mode used within the network, including Unknown, 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, Ad-Hoc for IBSS network.
IP Address	Shows the IP address information.
Sub Mask	Shows the Sub 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, you can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength.
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 throughput in the unit of K bits/sec.

Advanced

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



Wireless mode >> 802.11 B/G mix

Wireless Protection AUTO

Tx Rate >> Auto

□ Enable TX Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

□ Show Authentication Status Dialog

Select Your Country Region Code

11 B/G >> 0: CH1-11

□ Enable CCX (Cisco Compatible eXtensions)

□ Turn on CCKM

□ Enable Radio Measurements

□ Non-Serving Channel Measurements limit

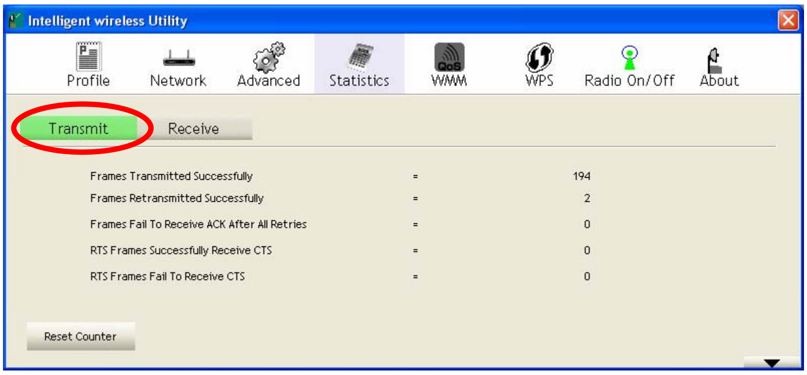
250 ms (0-2000)

Advanced Tab	
Wireless mode	Select wireless mode. There are two modes, 802.11B/G mix and 802.11B only supported. Default mode is 802.11B/G mix.
Wireless Protection	There are three modes can be selected. AUTO, ON and OFF.
Tx Rate	Select the transmitting rate you preferred. Default is Auto.
Enable TX Burst	Check this box to enable this function.
Enable TCP Window Size	Check to increase the transmission quality.
Fast Roaming at	Check to set the roaming interval, fast to roaming, setup by transmits power.
Show Authentication Status Dialog	When you connect AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog displays the process about 802.1x authentications.
Select Your Country Region Code	Select your country region code from the pull-down menu.

Enable CCX (Cisco Compatible extensions)	Check to enable the CCX function. • Turn on CCKM • Enable Radio Measurements: Check to enable the Radio measurement function. • Non-Serving Measurements limit: User can set channel measurement every 0~2000 milliseconds. Default is set to 250 milliseconds.
Apply	Click to apply above settings.

Statistics

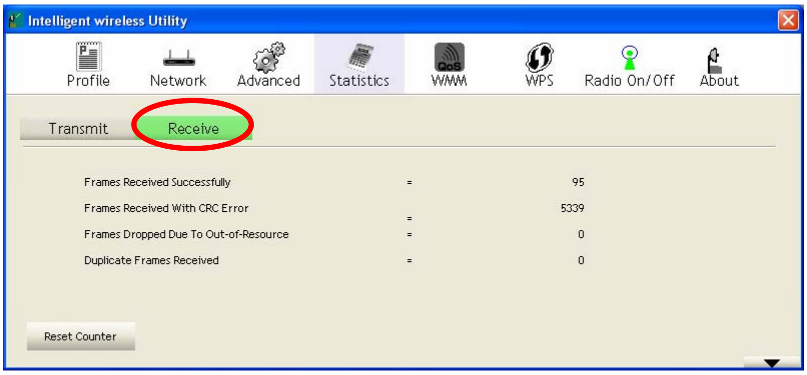
The Statistics screen displays the statistics on your current network settings.



```
Frames Transmitted Successfully                 =      194
Frames Retransmitted Successfully               =        2
Frames Fail To Receive ACK After All Retries    =        0
RTS Frames Successfully Receive CTS             =        0
RTS Frames Fail To Receive CTS                  =        0
```

Transmit Statistics Tab	
Frames Transmitted Successfully	Shows information of frames successfully sent.
Frames Retransmitted Successfully	Shows information of frames successfully sent with one or more reties.
Frames Fail To Receive ACK After All Retries	Shows information of frames failed transmit after hitting retry limit.
RTS Frames Successfully Receive	Shows information of successfully receive

CTS	CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Shows information of failed to receive CTS after sending RTS.
Reset Counter	Click this button to reset counters to zero.

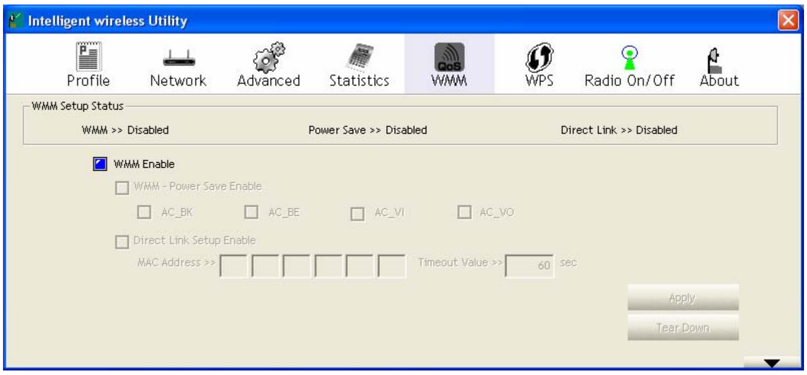


```
Frames Received Successfully              =       95
Frames Received With CRC Error            =     5339
Frames Dropped Due To Out-of-Resource     =        0
Duplicate Frames Received                 =        0
```

Receive Statistics Tab	
Frames Received Successfully	Shows information of frames Received Successfully.
Frames Received With CRC Error	Shows information of frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of frames dropped due to resource issue.
Duplicate Frames Received	Shows information of duplicate received frames.
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 your wireless network quality.



WMM Setup Status

WMM >> Disabled   Power Save >> Disabled   Direct Link >> Disabled

☑ WMM Enable

□ WMM - Power Save Enable

□ AC_BK □ AC_BE □ AC_VI □ AC_VO

□ Direct Link Setup Enable

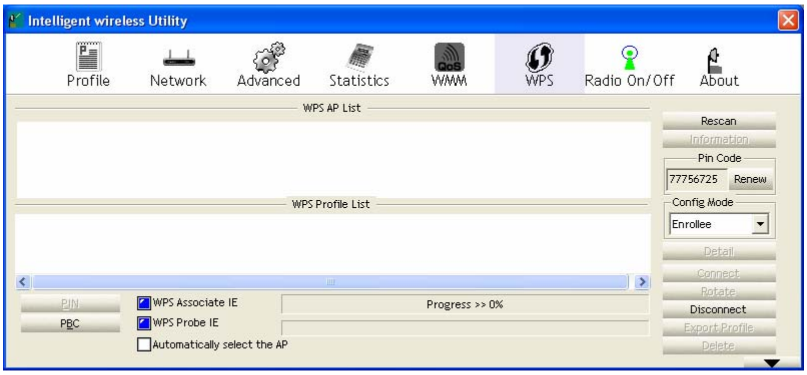
MAC Address >> □□□□□□ Timeout Value >> 60 sec

WMM/QoS Tab	
WMM Enable	Check the box to enable Wi-Fi Multi-Media function.
WMM- Power Save Enable	Select which ACs you want to enable.
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	The setting of DLS indicates as follow : Fill in the blanks of Direct Link with MAC Address of STA, and the STA must conform to two conditions: • Connecting with the same AP that supports DLS feature. • DSL 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.



Pin Code: 77756725

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

□ Automatically select the AP

Progress >> 0%

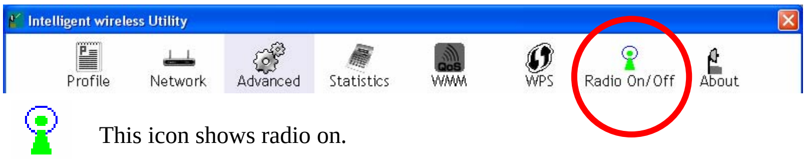
WPS Tab	
WPS AP List	Display the information of surrounding APs with WPS IE from last scan result. List information included SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.
Rescan	Issue a rescan command to wireless NIC to update information on surrounding wireless network.
Information	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 using PIN method. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.
Config Mode	Our station role-playing as an Enrollee or an external Registrar.
Detail	Information about Security and Key in the credential.
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	Start to add to Registrar using PIN (Personal Identification Number) configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
PBC	Start to add to AP using PBC (Push Button Configuration) method.
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.
Automatically	Check this box the device will connect the AP

select 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 button to turn on or off radio function.

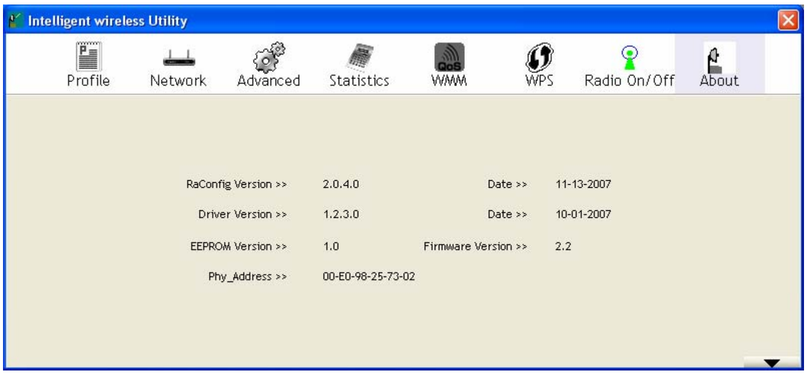


This icon shows radio on.

This icon shows radio off.

About

This page displays the information of the wireless card including, RaConfig Version/ Date, Driver Version/ Date, EEPROM Version, Firmware Version and Phy_Address.



RaConfig Version >> 2.0.4.0 Date >> 11-13-2007

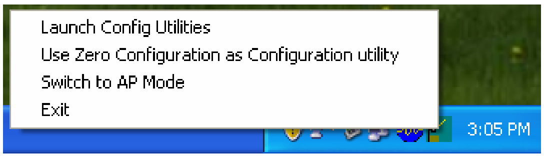
Driver Version >> 1.2.3.0 Date >> 10-01-2007

EEPROM Version >> 1.0 Firmware Version >> 2.2

Phy_Address >> 00-E0-98-25-73-02

Utility Menu list

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



- **Launch Config Utilities**: Select to open the utility screen.

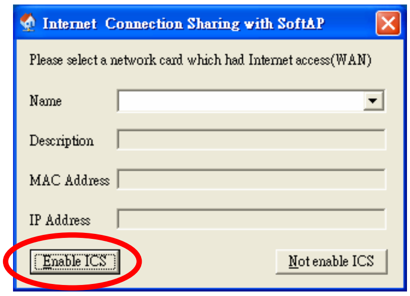
- **Use Zero Configuration as Configuration utility**: Select to use the Window XP built-in utility (Zero configuration utility).

- **Switch to AP Mode**: Select to make your wireless USB adapter act as a wireless AP.

- **Exit**: Select to close the utility program.

Soft AP mode

When device be switched to soft AP mode, the following screen will pop up, please select **Enable ICS** to enter soft AP configuration.



Please select a network card which had Internet access(WAN)

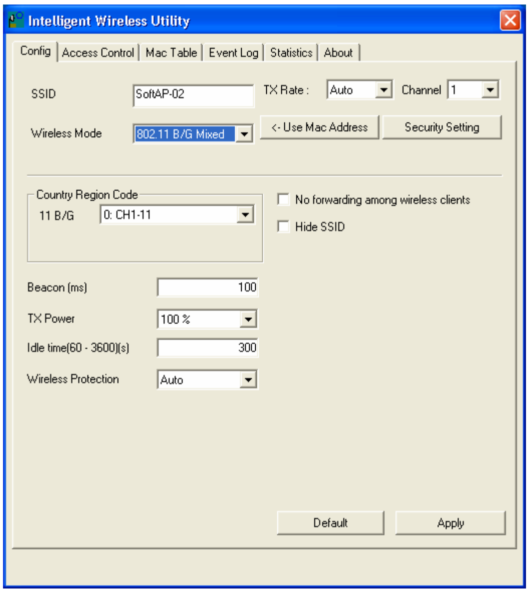
Name:

Description:

MAC Address:

IP Address:

Config



SSID: SoftAP-02

TX Rate : Auto

Channel: 1

Wireless Mode: 802.11 B/G Mixed

Country Region Code

11 B/G: 0: CH1-11

□ No forwarding among wireless clients

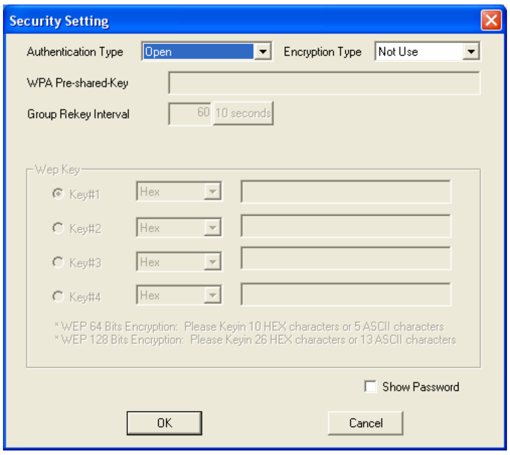
□ Hide SSID

Beacon (ms): 100

TX Power: 100 %

Idle time(60 - 3600)(s): 300

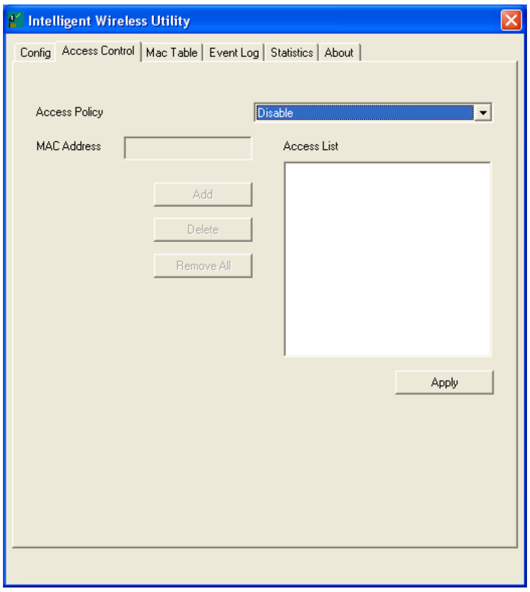
Wireless Protection: Auto

Config	
SSID	AP name of user type. User also can click **Use Mac Address** button to display it. System default is SoftAP-02.
TX Rate	Select the transmitting rate you preferred. Default is Auto.
Channel	Manually force the AP using the channel. The system default is CH 1.
Wireless mode	Select wireless mode. 802.11B/G Mixed, 802.11B only and 802.11G only modes are supported. System default is 802.11B/G Mixed.
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.  Security Setting Authentication Type: Open Encryption Type: Not Use WPA Pre-shared-Key: Group Rekey Interval: 60 10 seconds Wep Key ● Key#1 Hex ○ Key#2 Hex ○ Key#3 Hex ○ Key#4 Hex * WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters * WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters □ Show Password OK Cancel **Authentication Type**: There are five type of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. **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**. **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 32 lengths. **Group Rekey interval**: Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode to renew key. User 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 several formats to enter the keys. • Hexadecimal (64bits): 10 Hex characters. • Hexadecimal (128bits): 26 Hex characters. • ASCII (64bits): 5 ASCII characters. • ASCII (128bits): 13 ASCII characters. **Show Password**: Check this box to show the password you entered.
Country Region Code	Eight countries to choose. Country channel list: Classification Range 0: CH1 ~11 1: CH1 ~13 2: CH10 ~11 3: CH10 ~13 4: CH14 5: CH1 ~14 6: CH3 ~9 7: CH5 ~13
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.

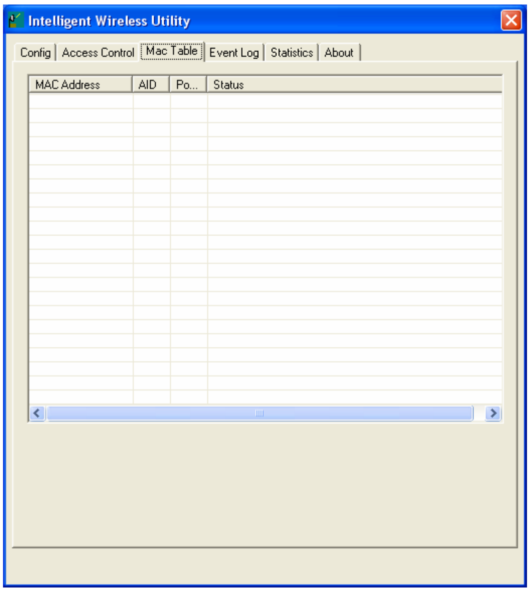
Access Control



Access Policy: Disable

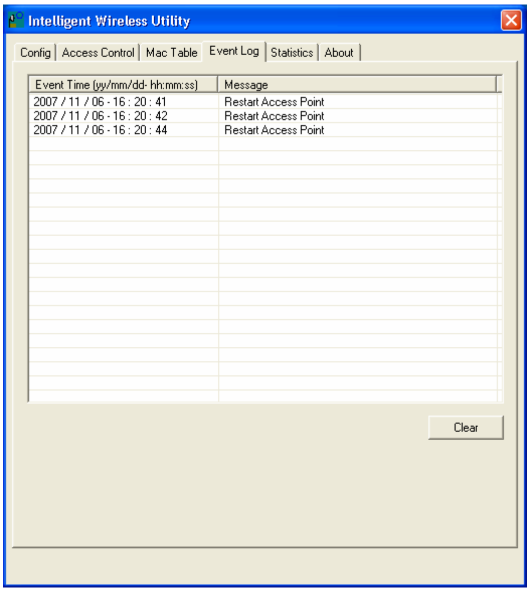
Access Control	
Access Policy	User chooses whether AP start the function or not. System default is Disable.
MAC Address	Manually force the Mac address using the function. Click Add and the MAC address will be listed in the Access List pool.
Access List	Display all MAC Address that you have set.
Add	Add the MAC address that you would like to set.
Delete	Delete the MAC address that you 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.

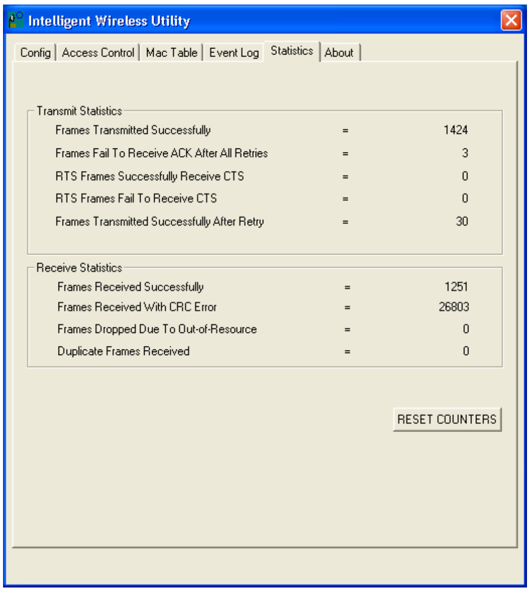
Event Log



Event Time (yy/mm/dd- hh:mm:ss)	Message
2007 / 11 / 06 - 16 : 20 : 41	Restart Access Point
2007 / 11 / 06 - 16 : 20 : 42	Restart Access Point
2007 / 11 / 06 - 16 : 20 : 44	Restart Access Point

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

Statistics



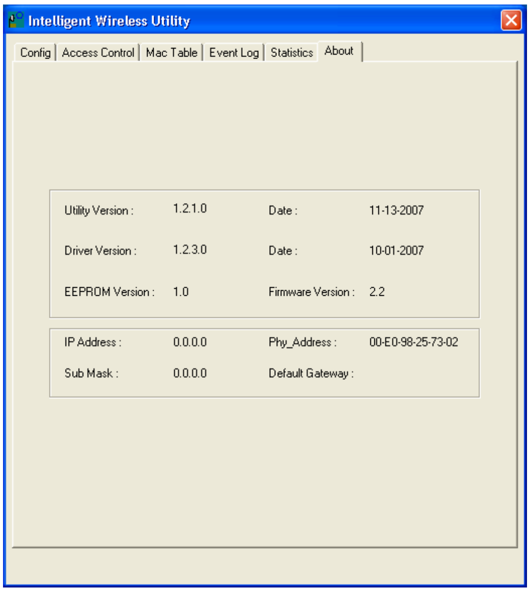
```
Transmit Statistics
    Frames Transmitted Successfully                 =        1424
    Frames Fail To Receive ACK After All Retries    =           3
    RTS Frames Successfully Receive CTS             =           0
    RTS Frames Fail To Receive CTS                  =           0
    Frames Transmitted Successfully After Retry     =          30

Receive Statistics
    Frames Received Successfully                    =        1251
    Frames Received With CRC Error                  =       26803
    Frames Dropped Due To Out-of-Resource           =           0
    Duplicate Frames Received                       =           0
```

Transmit Statistics	
Frames Transmitted Successfully	Frames successfully sent.
Frames Fail To Receive ACK After All Retries	Frames failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Frames successfully sent with one or more reties.

Receive Statistics	
Frames Received Successfully	Frames Received Successfully
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue
Duplicate Frames Received	Duplicate received frames.
Reset Counter	Reset counters to zero.

About

This page displays the wireless card and driver version information.



Utility Version : 1.2.1.0 Date : 11-13-2007

Driver Version : 1.2.3.0 Date : 10-01-2007

EEPROM Version : 1.0 Firmware Version : 2.2

IP Address : 0.0.0.0 Phy_Address : 00-E0-98-25-73-02

Sub Mask : 0.0.0.0 Default Gateway :

Utility Configuration for Windows Vista

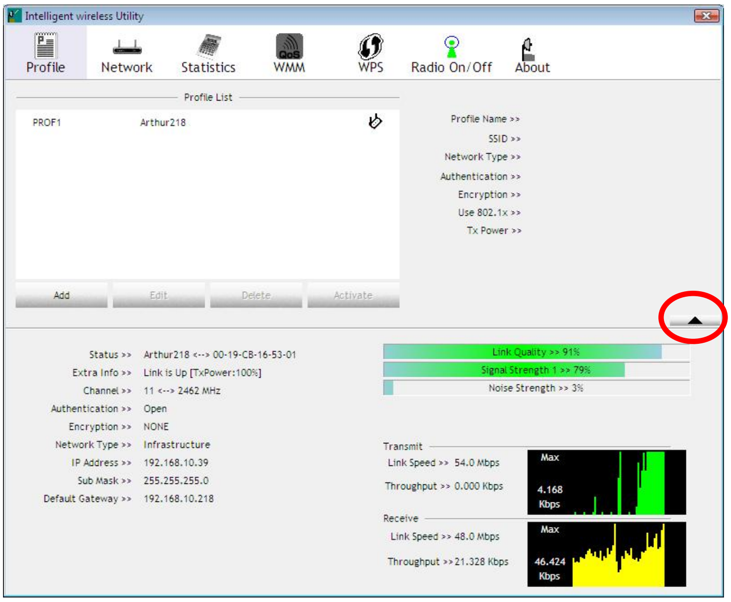
Station Mode

Profile

Profile can book keeping your favorite wireless setting among your home, office, and other public hot-spot. You may save multiple profiles, and activate the correct one at your preference. The Profile manager enables you 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.



PROF1 Arthur218

Status >> Arthur218 <--> 00-19-CB-16-53-01

Extra Info >> Link is Up [TxPower:100%]

Channel >> 11 <--> 2462 MHz

Authentication >> Open

Encryption >> NONE

Network Type >> Infrastructure

IP Address >> 192.168.10.39

Sub Mask >> 255.255.255.0

Default Gateway >> 192.168.10.218

Link Quality >> 91%

Signal Strength 1 >> 79%

Noise Strength >> 3%

Transmit

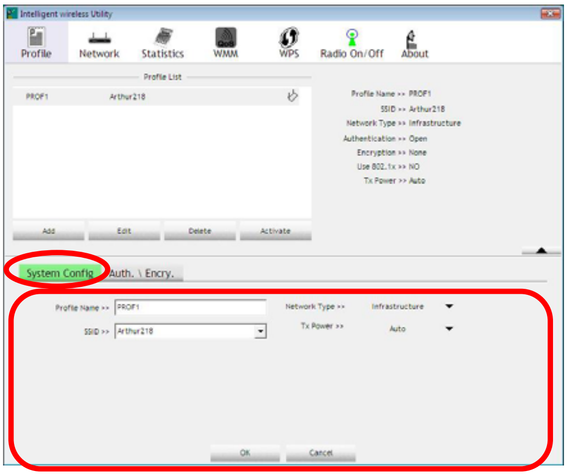
Link Speed >> 54.0 Mbps

Throughput >> 0.000 Kbps

Receive

Link Speed >> 48.0 Mbps

Throughput >>21.328 Kbps

Profile Tab	
Profile Name	You 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 points in your wireless network.
Network Type	Shows the network type of the device, including infrastructure and Ad-Hoc.
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.
Add	Click to add a profile from the drop-down screen. **System Configuration tab:**  Intelligent wireless Utility PROF1 Arthur218 Profile Name >> PROF1 SSID >> Arthur218 Network Type >> Infrastructure Authentication >> Open Encryption >> None Use 802.1x >> NO Tx Power >> Auto Profile Name >> PROF1 SSID >> Arthur218 Network Type >> Infrastructure Tx Power >> Auto Profile Network Statistics WMM WPS Radio On/Off About Profile List Add Edit Delete Activate System Config Auth. \ Encry. OK Cancel **Profile Name**: User can enter profile name, or use default name defined by system. The default is PROF# (# 1, #2, #3....). **SSID**: The **SSID** is the unique name shared among all points in your wireless network. The name must be

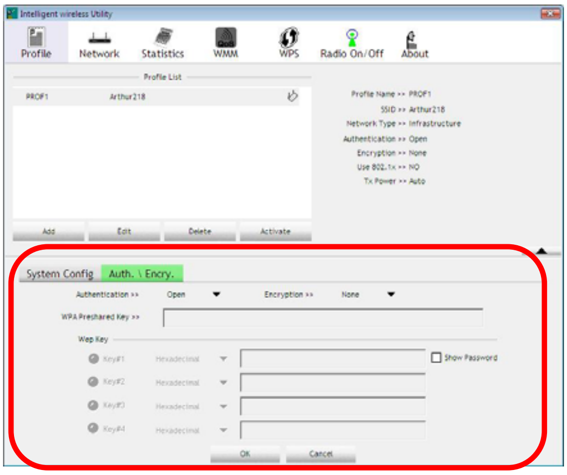
identical for all devices and points attempting to connect to the same network. User can use pull-down menu to select from available APs.

Network Type: There are two types, Infrastructure and Ad hoc modes.

- The **Infrastructure** is intended for the connection between wireless network cards and an Access Point. With the wireless adapter, you can connect wireless LAN to a wired global network via an Access Point.
- The **Ad hoc** lets you set a small wireless workgroup easily and quickly. Equipped with the wireless adapter, you can share files and printers between each PC and laptop.

Tx Power: Select the Tx power percentage from the pull-down list including **Auto, 100%, 75%, 50%, 25%, 10%** and **Lowest.**

Authentication and Encryption tab:



PROF1 Arthur218

Profile Name >> PROF1
SSID >> Arthur218
Network Type >> Infrastructure
Authentication >> Open
Encryption >> None
Use 802.1x >> NO
Tx Power >> Auto

Authentication >> Open
Encryption >> None
WPA Preshared Key >>
○ Key#1 Hexadecimal
○ Key#2 Hexadecimal
○ Key#3 Hexadecimal
○ Key#4 Hexadecimal
□ Show Password

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

- **Open**: If your access point/wireless router is using "**Open”** authentication, then the wireless adapter 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-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 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 32 length.

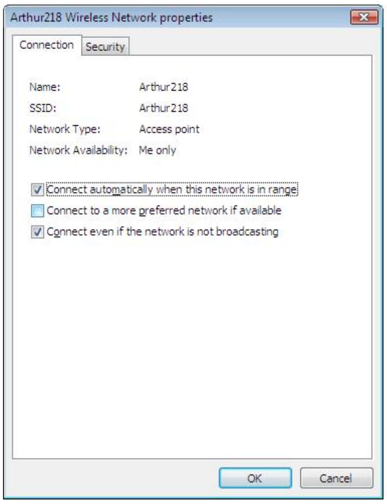
WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP’s key. There are several formats to enter the keys.

- Hexadecimal (40bits): 10 Hex characters.
- Hexadecimal (128bits): 32Hex characters.
- ASCII (40bits): 5 ASCII characters.
- ASCII (128bits): 13 ASCII characters.

Show Password: Check this box to show the password you entered.

802.1x Setting: When user use radius server to authenticate client certificate for WPA authentication mode. When the profile being active with 802.1x security the wireless network properties screen will pop-up for setting.

Connection Tab:



Arthur218 Wireless Network properties

Connection | Security

Name: Arthur218

SSID: Arthur218

Network Type: Access point

Network Availability: Me only

☑ Connect automatically when this network is in range

□ Connect to a more preferred network if available

☑ Connect even if the network is not broadcasting

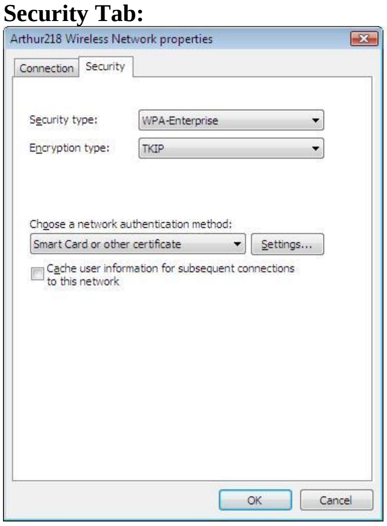
Name: The connected AP profile name.

SSID: The **SSID** is the unique name shared among all points in your wireless network.

Network Type: The network type of the connected device.

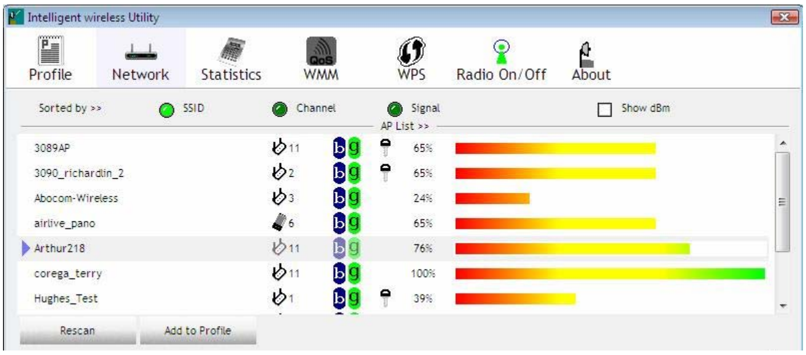
Network Availability: Shows the connected access point is available for the certificated device only.

* You can check the following three boxes to enable the functions that you preferred.

	Security Tab:  Arthur218 Wireless Network properties Connection Security Settings... OK Cancel Security type: WPA-Enterprise Encryption type: TKIP Choose a network authentication method: Smart Card or other certificate □ Cache user information for subsequent connections to this network **Security Type:** Select the security type form the pull-down menu, No authentication (Open), Shared, WPA2-Personal, WPA-Personal, WPA2-Enterprise, WPA-Enterprise and 802.1X. **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. **Choose a network authentication method:** Select from pull-down menu, either **Smart Card or other certificat**e or **Protected EAP (PEAP).** **Settings:** Click the settings button to set up further configuration management. **OK**: Click to save settings and exit this page. **Cancel:** Click to 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.

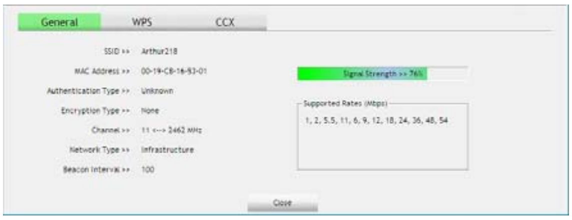


3089AP	11	bg	65%
3090_richardlin_2	2	bg	65%
Abocom-Wireless	3	bg	24%
airlive_pano	6	bg	65%
Arthur218	11	bg	76%
corega_terry	11	bg	100%
Hughes_Test	1	bg	39%

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, Ad-Hoc for IBSS network.
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.

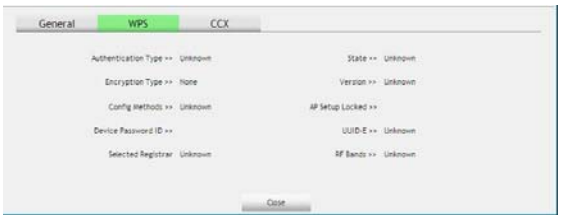
AP information

When you double click on the intended AP, you can see AP's detail information that divides into three parts. They are General, WPS, CCX information. The introduction is as following:

<table>
<tr>
<td><b>General</b></td>
<td>


SSID >> Arthur218
MAC Address >> 00-19-CB-16-93-01
Authentication Type >> Unknown
Encryption Type >> None
Channel >> 11 <--> 2462 MHz
Network Type >> Infrastructure
Beacon Interval >> 100
Signal Strength >> 76%
Supported Rates (Mbps)
1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54

General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates.

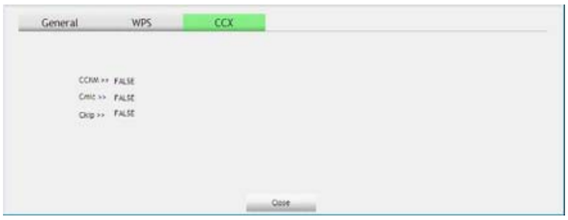
<b>Close</b>: Click this button to exit the information screen.
</td>
</tr>
<tr>
<td><b>WPS</b></td>
<td>


Authentication Type >> Unknown
Encryption Type >> None
Config Methods >> Unknown
Device Password ID >>
Selected Registrar Unknown
State >> Unknown
Version >> Unknown
AP Setup Locked >>
UUID-E >> Unknown
RF Bands >> Unknown

WPS information contains Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands.

<b>Authentication Type</b>: There are four types of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.

<b>Encryption Type</b>: For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK
</td>
</tr>
</table>

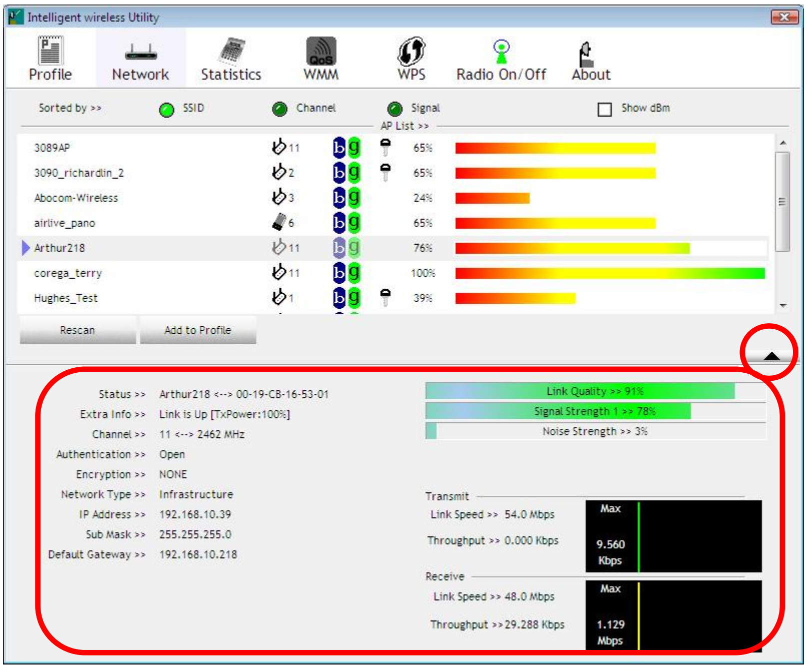
	authentication mode, the encryption type supports both TKIP and AES. **Config Methods**: Correspond to the methods the AP supports as an Enrollee for adding external Registrars. **Device Password ID**: Indicate the method or identifies the specific password that the selected Registrar intends to use. **Selected Registrar**: Indicate if the user has recently activated a Registrar to add an Enrollee. The values are "TRUE" and "FALSE". **State**: The current configuration state on AP. The values are "Unconfigured" and "Configured". **Version**: WPS specified version. **AP Setup Locked**: Indicate if AP has entered a setup locked state. **UUID-E**: The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes. **RF Bands**: Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are "2.4GHz" and "5GHz". **Close**: Click this button to exit the information screen.
CXX	 CCKM >> FALSE Cmic >> FALSE Ckip >> FALSE CCX information contains CCKM, Cmic and Ckip information. **Close**: Click this button to exit the information screen.

Link Status

Click the triangle button at the right 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 of Status Section.

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



Sorted by >> ● SSID ● Channel ● Signal □ Show dBm

AP List >>

3089AP	11	bg	65%
3090_richardlin_2	2	bg	65%
Abocom-Wireless	3	bg	24%
airlive_pano	6	bg	65%
Arthur218	11	bg	76%
corega_terry	11	bg	100%
Hughes_Test	1	bg	39%

Status >> Arthur218 <--> 00-19-CB-16-53-01
Extra Info >> Link is Up [TxPower:100%]
Channel >> 11 <--> 2462 MHz
Authentication >> Open
Encryption >> NONE
Network Type >> Infrastructure
IP Address >> 192.168.10.39
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.10.218

Link Quality >> 91%
Signal Strength 1 >> 78%
Noise Strength >> 3%

Transmit
Link Speed >> 54.0 Mbps
Throughput >> 0.000 Kbps
Max
9.560 Kbps

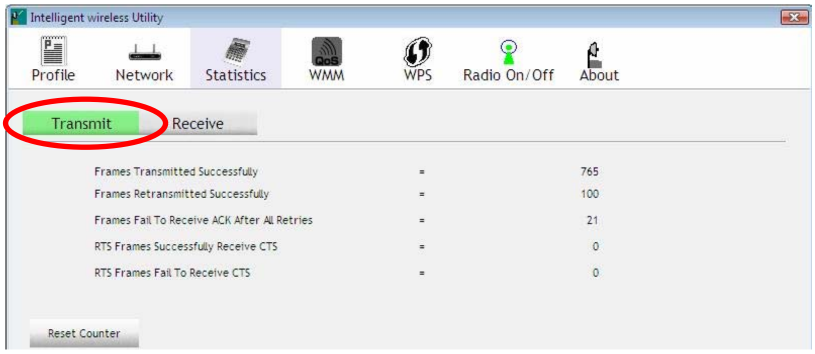
Receive
Link Speed >> 48.0 Mbps
Throughput >> 29.288 Kbps
Max
1.129 Mbps

Link Status Tab	
Status	Shows the current connection status. If there is no connection existing, it will show Disconnected.

Extra Info	Shows the link status.
Channel	Shows the current channel in use.
Authentication	Authentication mode used within the network, including Unknown, Open, 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, Ad-Hoc for IBSS network.
IP Address	Shows the IP address information.
Sub Mask	Shows the Sub 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, you can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength.
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 throughput in the unit of K bits/sec.

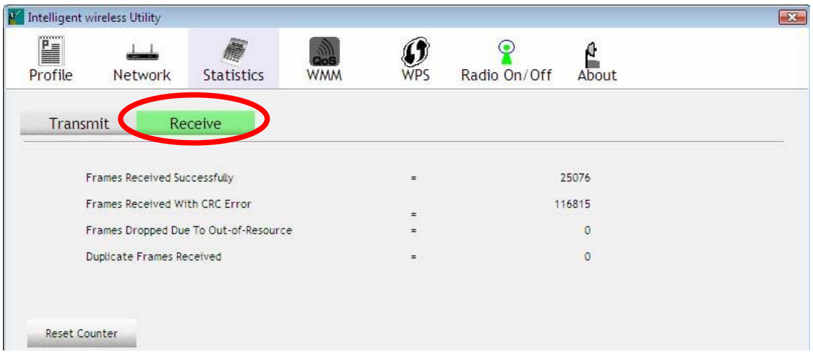
Statistics

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



```
Frames Transmitted Successfully              =     765
Frames Retransmitted Successfully            =     100
Frames Fail To Receive ACK After All Retries =      21
RTS Frames Successfully Receive CTS          =       0
RTS Frames Fail To Receive CTS               =       0
```

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

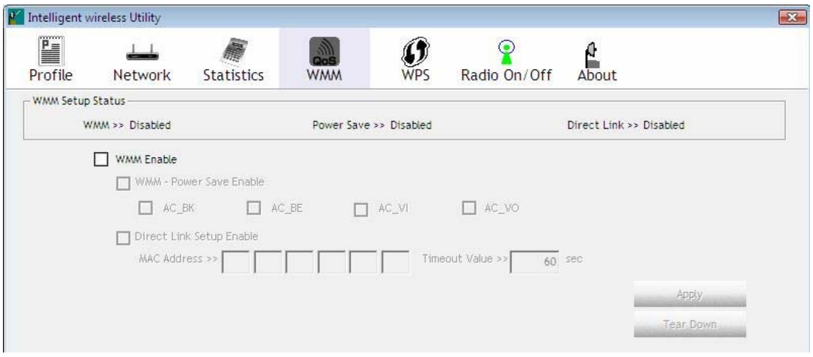


```
Frames Received Successfully                 =        25076
Frames Received With CRC Error               =       116815
Frames Dropped Due To Out-of-Resource        =            0
Duplicate Frames Received                    =            0
```

Receive Statistics Tab	
Frames Received Successfully	Shows information of frames Received Successfully.
Frames Received With CRC Error	Shows information of frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of frames dropped due to resource issue.
Duplicate Frames Received	Shows information of duplicate received frames.
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 your wireless network quality.



WMM Setup Status

WMM >> Disabled   Power Save >> Disabled   Direct Link >> Disabled

□ WMM Enable

□ WMM - Power Save Enable

□ AC_BK   □ AC_BE   □ AC_VI   □ AC_VO

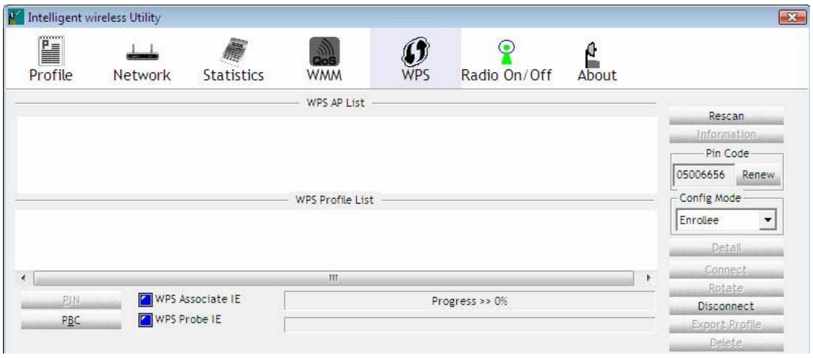
□ Direct Link Setup Enable

MAC Address >> □ □ □ □ □ □   Timeout Value >> 60 sec

WMM/QoS Tab	
WMM Enable	Check the box to enable Wi-Fi Multi-Media function.
WMM- Power Save Enable	Select which ACs you want to enable.
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	The setting of DLS indicates as follow : Fill in the blanks of Direct Link with MAC Address of STA, and the STA must conform to two conditions: • Connecting with the same AP that supports DLS feature. • DSL 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.



Pin Code: 05006656

Config Mode: Enrollee

☑ WPS Associate IE

☑ WPS Probe IE

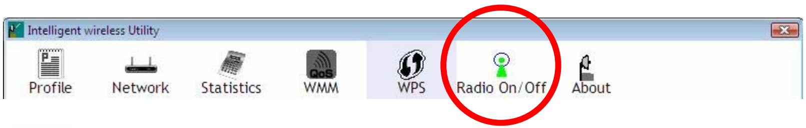
Progress >> 0%

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 using PIN method. When STA is Enrollee, you can use "Renew" button to re-generate new PIN Code.

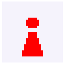
Config Mode	Our station role-playing as an Enrollee or an external Registrar.
Detail	Information about Security and Key in the credential.
Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to 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	Start to add to Registrar using PIN (Personal Identification Number) configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.
PBC	Start to add to AP using PBC (Push Button Configuration) method.
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.

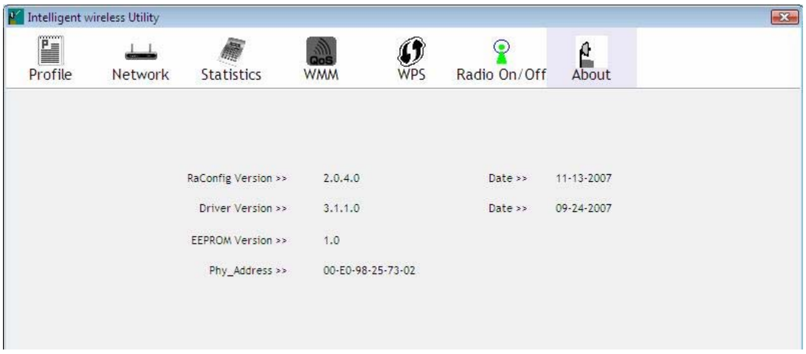


This icon shows radio on.


This icon shows radio off.

About

This page displays the information of the wireless card including, RaConfig Version/ Date, Driver Version/ Date, EEPROM Version and Phy_Address.



RaConfig Version >> 2.0.4.0 Date >> 11-13-2007

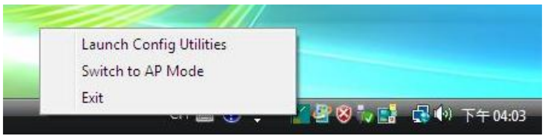
Driver Version >> 3.1.1.0 Date >> 09-24-2007

EEPROM Version >> 1.0

Phy_Address >> 00-E0-98-25-73-02

Utility Menu list

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

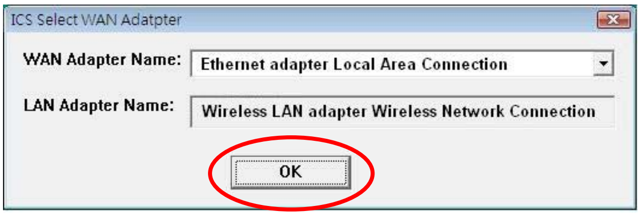


- **Launch Config Utilities**: Select to open the utility screen.
- **Switch to AP Mode**: Select to make your wireless USB adapter act as a wireless AP.
- **Exit**: Select to close the utility program.

Soft AP mode

When device be switched to soft AP mode, the following screen will pop up, please click **OK** to enter soft AP configuration.

Notice: This screen shows up in Windows Vista 32-bit Operating System only.

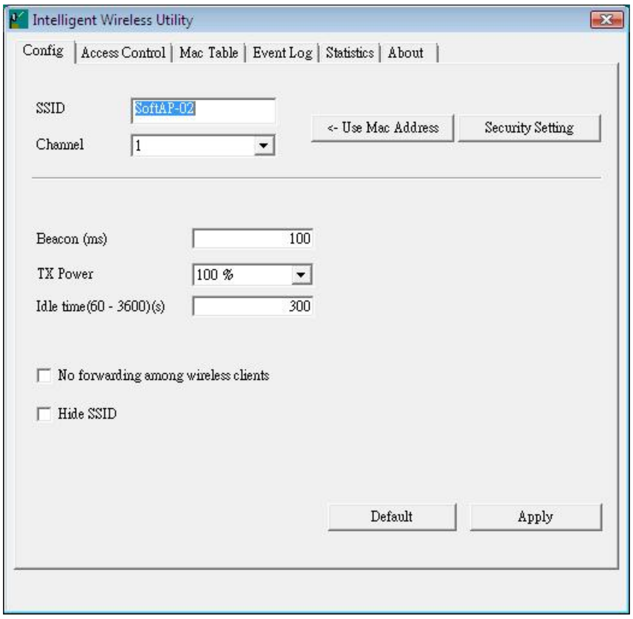


ICS Select WAN Adatpter

WAN Adapter Name: Ethernet adapter Local Area Connection

LAN Adapter Name: Wireless LAN adapter Wireless Network Connection

Config



Intelligent Wireless Utility

SSID: SoftAP-02

Channel: 1

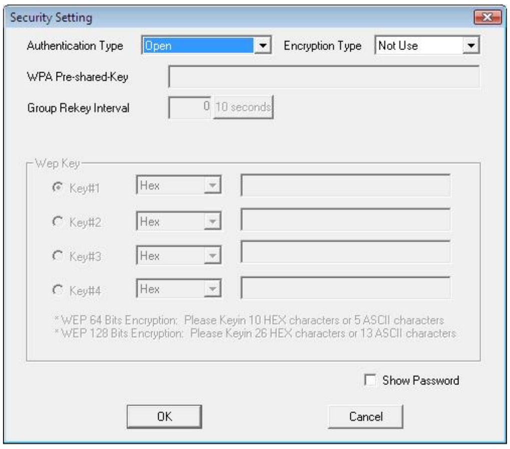
Beacon (ms): 100

TX Power: 100 %

Idle time(60 - 3600)(s): 300

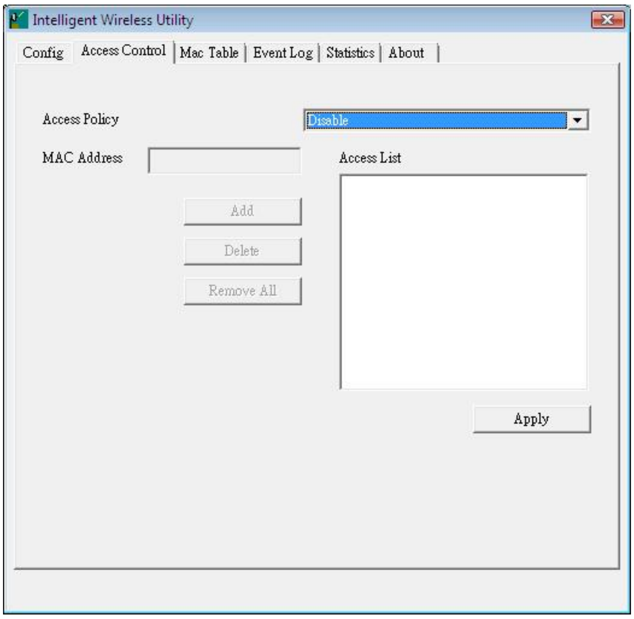
□ No forwarding among wireless clients

□ Hide SSID

Config	
SSID	AP name of user type. User also can click **Use Mac Address** button to display it. System default is SoftAP-02.
Channel	Manually force the AP using the channel. The system default is CH 1.
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.  Security Setting Authentication Type: Open Encryption Type: Not Use WPA Pre-shared-Key: Group Rekey Interval: 0 10 seconds Wep Key ● Key#1 Hex ○ Key#2 Hex ○ Key#3 Hex ○ Key#4 Hex * WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters * WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters □ Show Password OK Cancel **Authentication Type**: There are five type of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/WPA2-PSK. **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**. **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 32 lengths. **Group Rekey Interval**: Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode to renew key. User can set to change by seconds or packets. Default is 10 seconds. **WEP Key**: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are several formats to enter the keys. • Hexadecimal (64bits): 10 Hex characters. • Hexadecimal (128bits): 26 Hex characters. • ASCII (64bits): 5 ASCII characters. • ASCII (128bits): 13 ASCII characters. **Show Password**: Check this box to show the password you 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



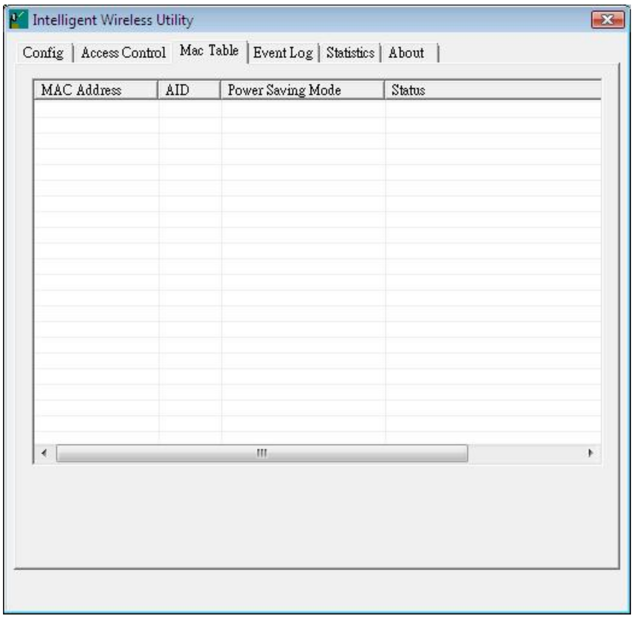
Access Policy: Disable

MAC Address

Access List

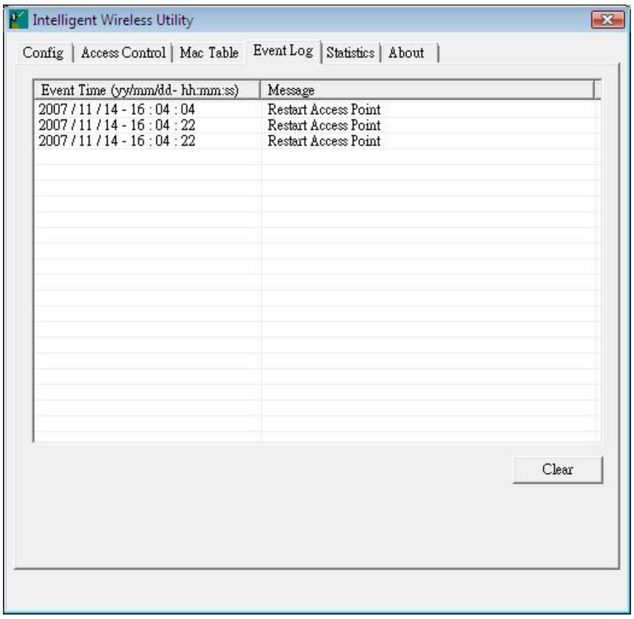
Access Control	
Access Policy	User chooses whether AP start the function or not. System default is Disable.
MAC Address	Manually force the Mac address using the function. Click Add and the MAC address will be listed in the Access List pool.
Access List	Display all MAC Address that you have set.
Add	Add the MAC address that you would like to set.
Delete	Delete the MAC address that you 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.

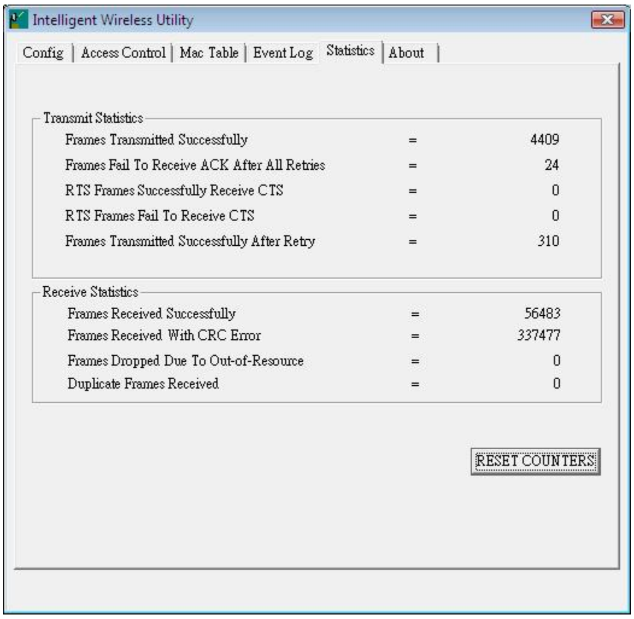
Event Log



Event Time (yy/mm/dd- hh:mm:ss)	Message
2007 / 11 / 14 - 16 : 04 : 04	Restart Access Point
2007 / 11 / 14 - 16 : 04 : 22	Restart Access Point
2007 / 11 / 14 - 16 : 04 : 22	Restart Access Point

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                =      4409
Frames Fail To Receive ACK After All Retries   =        24
RTS Frames Successfully Receive CTS            =         0
RTS Frames Fail To Receive CTS                 =         0
Frames Transmitted Successfully After Retry    =       310
```

Receive Statistics

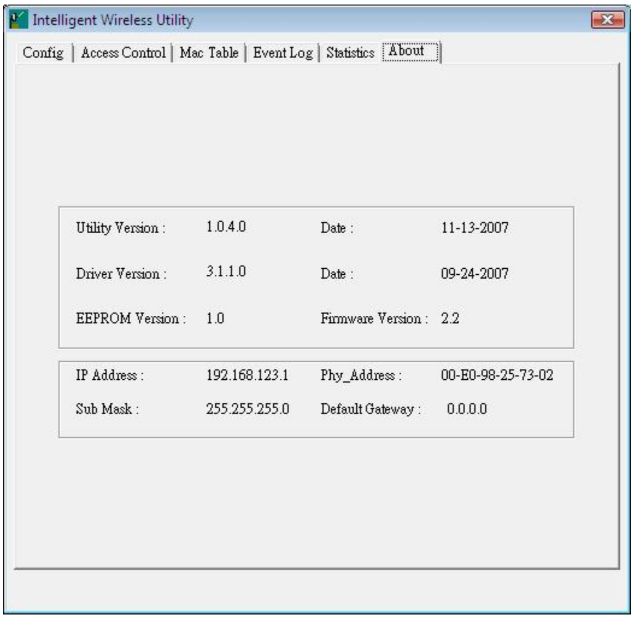
```
Frames Received Successfully                   =     56483
Frames Received With CRC Error                 =    337477
Frames Dropped Due To Out-of-Resource          =         0
Duplicate Frames Received                      =         0
```

Transmit Statistics	
Frames Transmitted Successfully	Frames successfully sent.
Frames Fail To Receive ACK After All Retries	Frames failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Successfully receive CTS after sending RTS frame
RTS Frames Fail To Receive CTS	Failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Frames successfully sent with one or more reties.

Receive Statistics	
Frames Received Successfully	Frames Received Successfully
Frames Received With CRC Error	Frames received with CRC error.
Frames Dropped Due To Out-of-Resource	Frames dropped due to resource issue
Duplicate Frames Received	Duplicate received frames.
Reset Counter	Reset counters to zero.

About

This page displays the wireless card and driver version information.



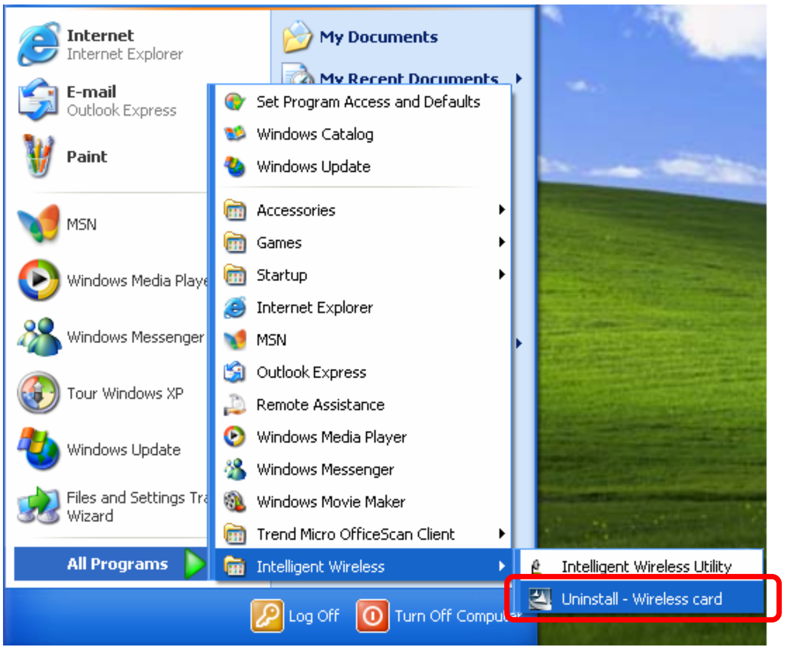
Utility Version :	1.0.4.0	Date :	11-13-2007
Driver Version :	3.1.1.0	Date :	09-24-2007
EEPROM Version :	1.0	Firmware Version :	2.2

IP Address :	192.168.123.1	Phy_Address :	00-E0-98-25-73-02
Sub Mask :	255.255.255.0	Default Gateway :	0.0.0.0

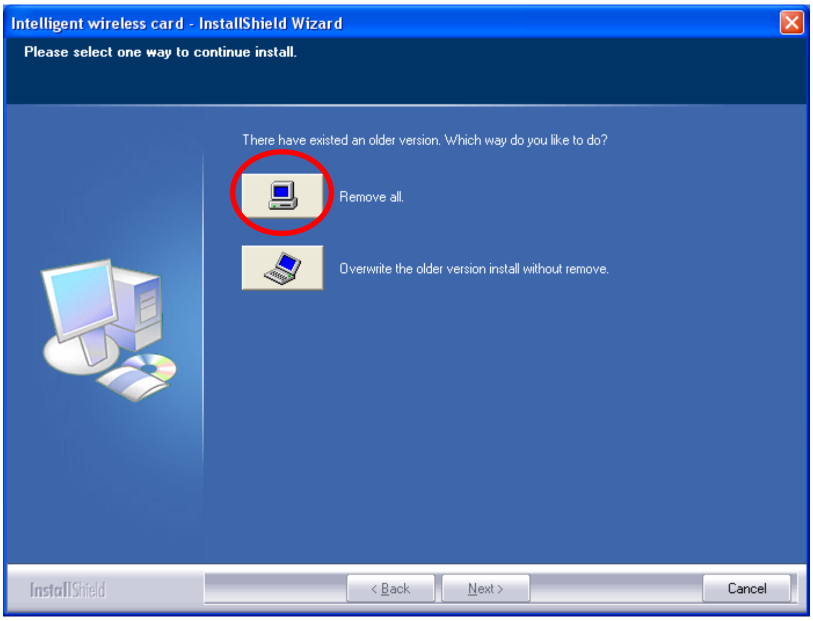
UNINSTALLATION FOR WINDOWS 2000/XP

In case you need to uninstall the utility and driver, please refer to below steps. (As you uninstall the utility, the driver will be uninstalled as well.)

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



2. Select **Remove all** button and click **Next** to start uninstalling.



Intelligent wireless card - InstallShield Wizard

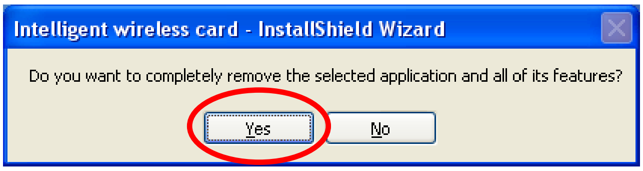
Please select one way to continue install.

There have existed an older version. Which way do you like to do?

Remove all.

Overwrite the older version install without remove.

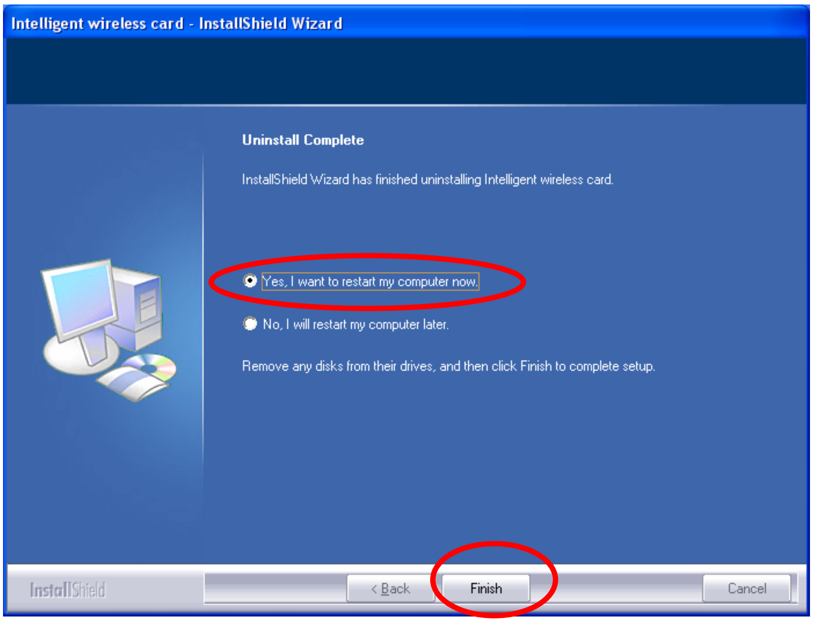
3. Click **Yes** to complete remove the selected application and all of its features.



Intelligent wireless card - InstallShield Wizard

Do you want to completely remove the selected application and all of its features?

4. Select “**Yes, I want to restart my computer now”** and then click **Finish** to complete the uninstallation.



Intelligent wireless card - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling Intelligent wireless card.

● Yes, I want to restart my computer now.

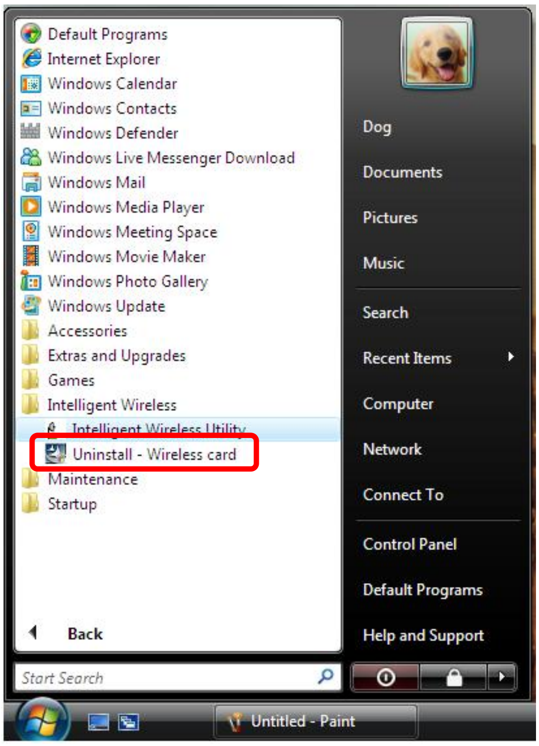
○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

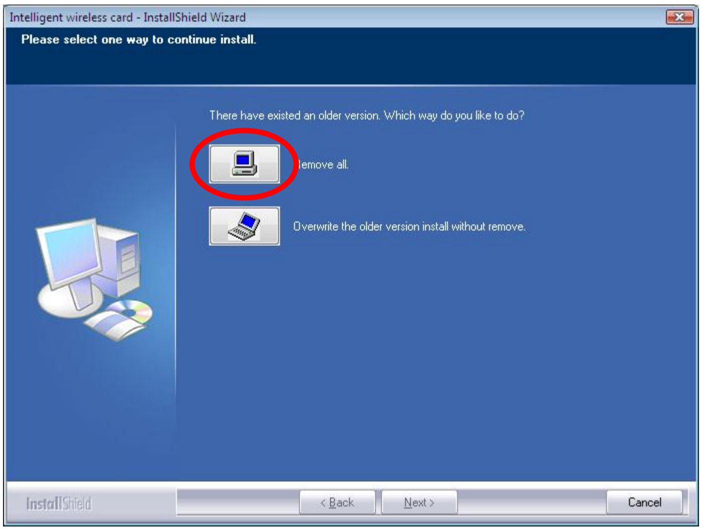
UNINSTALLATION FOR WINDOWS VISTA

In case you need to uninstall the utility and driver, please refer to below steps. (As you uninstall the utility, the driver will be uninstalled as well.)

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



2. Select **Remove all** button and click **Next** to start uninstalling.



Intelligent wireless card - InstallShield Wizard

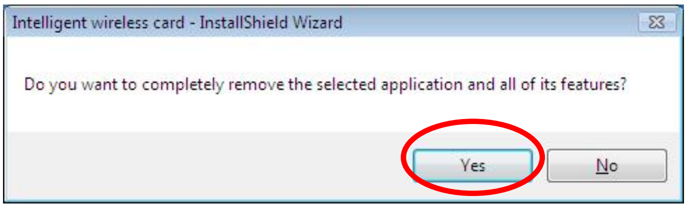
Please select one way to continue install.

There have existed an older version. Which way do you like to do?

Remove all.

Overwrite the older version install without remove.

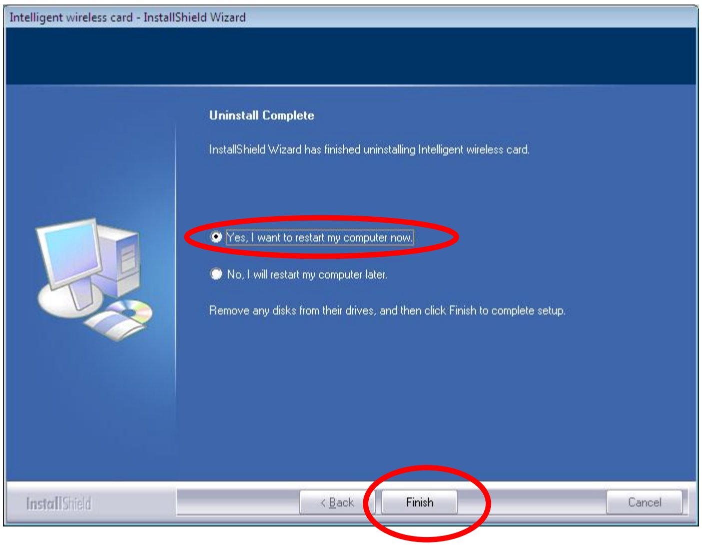
3. Click **Yes** to complete remove the selected application and all of its features.



Intelligent wireless card - InstallShield Wizard

Do you want to completely remove the selected application and all of its features?

4. Select “**Yes, I want to restart my computer now”** and then click **Finish** to complete the uninstallation.



Intelligent wireless card - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling Intelligent wireless card.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.