802.11 b/g/n Mini Wireless LAN USB2.0 Adapter

User's Manual

Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

Country Code Statement

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

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

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

Federal Communication Commission (FCC) Radiation Exposure Statement

This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. This equipment should be installed and operated with minimum distance 2.5 cm between the radiator & your body.

CE Statement:

Hereby, AboCom, declares that this device is in compliance with the essential requirement and other relevant provisions of the R&TTE Driective 1999/5/EC.



Table of Contents

INTRODUCTION1
Features1
Windows 2000/XP Installation2
INSTALL THE SOFTWARE
INSTALL THE HARDWARE
Windows Vista Installation
INSTALL THE SOFTWARE
INSTALL THE HARDWARE
VERIFICATION
NETWORK CONNECTION9
IP Address
UTILITY CONFIGURATION FOR WINDOWS 2000/XP10
UTILITY CONFIGURATION FOR WINDOWS 2000/XP
STATION MODE
STATION MODE
STATION MODE
STATION MODE

WPS
Radio On/Off
About
UTILITY MENU LIST
SOFT AP MODE
Config
Access Control
MAC Table40
Event Log41
Statistics
About
UTILITY CONFIGURATION FOR WINDOWS VISTA
STATION MODE
STATION MODE

SOFT AP MODE	SOFT
Config	
Access Control71	
MAC Table72	
Event Log73	
Statistics74	
About	
UNINSTALLATION FOR WINDOWS 2000/XP76	UNINS
UNINSTALLATION FOR WINDOWS VISTA78	UNINS

INTRODUCTION

The WU5204/GW-USMini2N is an IEEE802.11b/g/n USB adapter that connects your notebook to a wireless local area. The WU5204/GW-USMini2N fully complies with IEEE 802.11n draft 3.0 and IEEE 802.11 b/g standards, delivers reliable, cost-effective, feature rich wireless connectivity at high throughput from an extended distance. The WU5204/GW-USMini2N is a very small adapter that can connects notebook, handheld or desktop computer equipped with USB interface for wireless network applications. 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

- > 1T1R Mode with 150Mbps PHY Rate for both.
- > Complies with IEEE 802.11n draft 3.0 and IEEE 802.11 b/g standards.
- > Supports WEP 64/128, WPA, WPA2.
- > Supports WMM and WMM-PS.
- > Supports WPS configuration.
- > Supports USB 2.0/1.1 interface.
- Portable and mini-size design.
- > Compatible with Microsoft Windows Vista, XP, 2000.

- 1 -

Windows 2000/XP Installation

Install the Software

Caution!

Do not insert the wireless card into your computer until the InstallShield Wizard finish installing.

- 1. Exit all Windows programs. Insert the included CD-ROM into your 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.

SOFTWARE PRODUCT LICENSE The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, are well as other intellectual property laws and treates. The SOFTWARE PRODUCT is locensed, not sold. In GRANT OF LICENSE. This End User License Agreement grants you the following night: Installation and User. 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. Reproduction and Distribution. You may reproduce and distribute as a unlimited number of copies of the SOFTWARE PRODUCT. Tray be distributed as a standione product or included with your own product. 2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS. Limitations on Reverse Engineering. Decompliation, and Disassembly. You may not reverse I accept the terms of the license agreement I do not accept the terms of the license agreement	License Agreement Please read the following licer	se agreement carefully.
		 The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaters, as well as other intellectual property laws and treaters. The SOFTWARE PRODUCt is licensed, not sold. GRANT OF LICENSE. This End-User License Agreement grants you the following mgkr. Installation and User You may install and use an unimited number of copies of the SOFTWARE PRODUCT. The SOFTWARE PRODUCT. The SOFTWARE PRODUCT. The SOFTWARE PRODUCT. The SOFTWARE PRODUCT. Reproduction and Distribution. You may reproduce and distribute an unimited number of copies of the SOFTWARE PRODUCT. Involved that each copy halb be a true and complete copy. Including all copyright and trademark notices, and shall be accompanied by a copy of the SOFTWARE PRODUCT. may be distributed as a standalone product or included with your own product. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS. Limitations on Reverse Engineering. Decompliation, and Disassembly. You may not reverse of a copy of a copy of the license agreement.

- 2 -

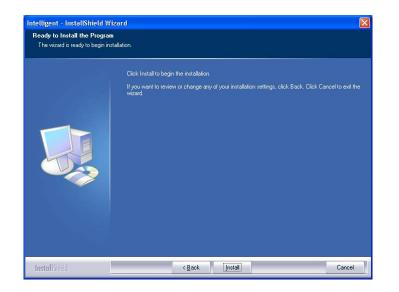
- 3. Select the check box to choose a **Configuration Tool** from the listed two choices.
 - **Configuration Tool**: Choose to use our configuration utility.
 - Microsoft Zero Configuration Tool: Choose to use Windows XP's built-in Zero Configuration Utility (ZCU).

Click Next to continue.

Intelligent - InstallShield Wi	izard	×
Setup Type Select the setup type that best	suits your needs.	
	Select Configuration Tool.	
	 Configuration Tool 	
	Microsoft Zero Configuration Tool	
InstallShield	< Back Next > Cancel	

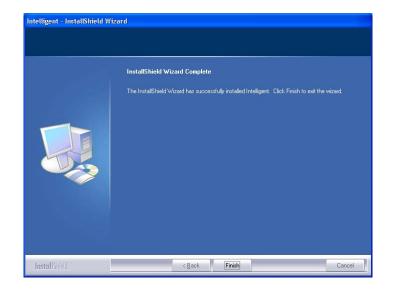
5. When you are prompted the following message, please click **Install** to begin the installation.

- 3 -



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

- 4 -



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.

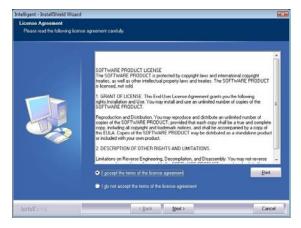
- 5 -

Windows Vista Installation

Install the Software

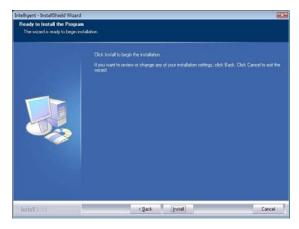
Do not insert the wireless LAN adapter into your computer until the procedures in "Driver& Utility Installation" have been performed.

- 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.

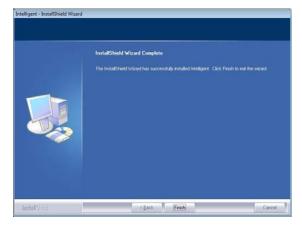


- 6 -

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



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



- 7 -

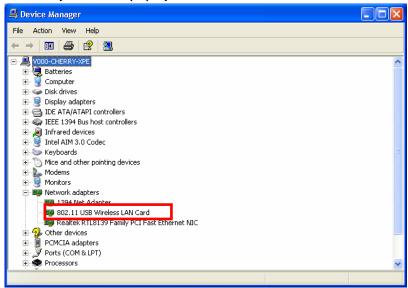
Install the Hardware

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 802.11 USB Wireless LAN Card is listed here, it means that your device is properly installed and enabled.



- 8 -

NETWORK CONNECTION

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.
- 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.

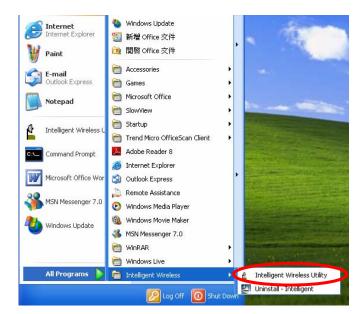
Internet Protocol (TCP/IP) Properties	Internet Protocol (TCP/IP) Properties
General Alternate Configuration	General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	You can get 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	Obtain as the address automatically
Use the following IP address:	Use the following IP address:
IP address:	IP address: 192.168.1.1
Subnet mask:	Subnet mask: 255 . 255 . 255 . 0
Default gateway:	Default gewiner
Obtain DNS server address automatically	Obtain DNS server address automatically
O Use the following DNS server addresses:	Use the following DNS server addresses:
Preferred DNS server:	Preferred DNS server:
Alternate DNS server:	Alternate DNS server:
Advanced	Advanced
OK Cancel	DK Cancel

- 9 -

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) Program→ Intelligent Wireless→ Intelligent Wireless Utility.



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

Launch Config Utility
Use Zero Configuration as Configuration Utility
Switch to AP Mode
Exit

- 10 -

Station Mode

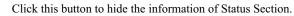
Notice: Under screen resolution 800 x 600 pixels, click the triangle button at the right down corner of the utility to expand the information of the station, the information will not be displayed completely.

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.



🖌 Ini	elligent Wirele	ss Utiltiy							X
	Profile	Land Network	Advanced	Statistics	Cos WMM	Ø WPS	Radio On/Off	A About	
		Pro	file List						
P	ROF1	Cherry_test_	11n_Router		6	Profile Name :	PROF1		
						SSID	>> Cherry_test_11n_Ro	uter	
						Network Type	>> Infrastructure		
						Authentication	>> Open		
						Encryption	>> None		
						Use 802.1x	>> NO		
						Tx Power	>> Auto		
						Channel	>> Auto		
					Po	wer Save Mode			
						RTS Threshold	>> 2347		-
	Add	Edit	Delete	Activat	Frag	ment Threshold	>> 2346	(_	

Profile Tab	
Profile Name	You can see 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.

- 11 -

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 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	Click to add a profile from the drop-down screen. System Configuration tab:		

- 12 -

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 : 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.
Preamble : This function will show up when Ad-hoc network type be selected. 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

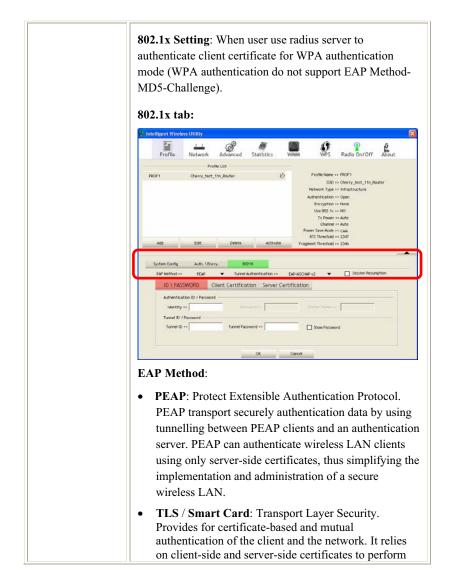
- 13 -

o Auto or Long.	
User can adjust the RT g the bar or key in the 347. RTS/CTS Thresh revent the " Hidden N c" problem is an issue, s size. <u>The RTS/CTS m</u> ta size exceeds the val	value directly. The old is a mechanism ode" problem. If users have to <u>bechanism will be</u>
remain at its default s inter inconsistent data his value are recommo	flow, only minor
by sliding the bar or k ult value is 2346. The reshold is used to imp flows along in the wir N Adapter often trans you can enter new Fra backet. The value can	key in the value mechanism of prove the efficience reless network. If mits large files in agment Threshold
nd Security tab:	
enter v	002.1x 004 Pactment
	47. RTS/CTS Thresh revent the "Hidden N " problem is an issue, size. <u>The RTS/CTS m</u> ta size exceeds the val remain at its default s unter inconsistent data his value are recomm hold: User can adjust by sliding the bar or H ult value is 2346. The reshold is used to imp flows along in the wir N Adapter often trans you can enter new Fr backet. The value can nd Security tab:



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 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 several formats to enter the keys.
 Hexadecimal (128bits): 26 Hex characters (0~9, a~f). ASCII (128bits): 13 ASCII characters.
Show Password : Check this box to show the password you en02tered.

- 15 -



- 16 -

•	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.)
Tu •	nnel Authentication: Protocol: Tunnel protocol, List information including EAP-MSCHAP v2, EAP-TLS/ Smart Card, and Generic Token Card.
•	Tunnel Identity: Identity for tunnel.

- 17 -

• Tunnel Password: Password for tunnel.
Session Resumption : Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. User can click the box to enable or disable this function.
ID\PASSWORD tab:
System Config Auth. Liberry. B2214 EUP Aeros >> Fga Funnet Authentication >> EuP-acroup v2 Session Reamption ID \PASSWORD Client Cortification Server Certification Authentication Di /Passeod Seekity >> Turnet Di /Passeod Turnet Passeord >> Turnet Passeord >> Secure 10 >>
OK Canoti
 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 password you entered. OK: Click to save settings and exit this page. Cancel: Click to call off the settings and exit.
Bytem Genta Muth. \Dicry; BOX Set Method >> FSAP Turnel Authentication >> Cate ACCINP +2 Cate Set Set Set Set Set Set Set Set Set S

- 18 -

	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
	EAP Method >> PGAP Turnel Addrentication >> EAP-ADCHAP v2 Section Resumption ID \ PASSWORD Client Certification Server Certification
	Use certificate chain
	About Antomotoria con Oficianos serviror ramino ere
	General instant match Constrict and in proceeding name
	OK Canot
	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 call off the settings and exit.
Delete	Click to delete an existing profile.
Edit	Click to edit a profile.

- 19 -

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.

Intelligent Wirele	ss Utiltiy						
Profile	Land Network	ر Advanced	Statistics	WMM	Ø WPS	Radio On/Off	About
Sorted by >>	🙆 SSID	🙆 Cha	nnel 🖉	Signal		Show dBm	
airlive-wl5470poe		11	g AP LI:	39%			
Cherry_test_11n_R	outer	107	B 9 0 0	100%		-	
D	Add to Durd						
Rescan	Add to Profi	ie Con	nect				

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, 802.11g or 802.11n 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 refresh the AP list.		
Add to Profile	Select an item on the list and then click to add it into the profile list.		

- 20 -

Connect	Select an item on the list and then click to make a
	connection.

AP Information

When you double click on the intended AP, you can see AP's detail information that divides into four parts. They are General, WPS, CCX and 802.11n information. The introduction is as following:

General][
General	General WPS CCX 802.11n	
	SSD >> Cherry_test_1th, Florter MAC Address >> 00 ED-42-66-51-01 Authentication Type >> Unicount Docryption Type >> Nome Outment >> 7	4,54
	General information contain AP's SSID, M	AC address
	Authentication Type, Encryption Type, Ch	
	Type, Beacon Interval, Signal Strength and	Supported
	Rates.	
	Close : Click this button to exit the information	tion screen.
WPS	General WPS CCX 802,11n	
	Authentication Type >> Uninteen State >> Configur	ed
	Encryption Type >> None Version >> 1.0	
	Config Methods >> Unknown AP Setup Locked >>	
	Device Password ID >> UUD-E >> Unknown	
	Selected Registrar >> Unknown RF Band: >> Unknown	N.
	Close	
	WPS information contains Authentication	Type, Encryption
	Type, Config Methods, Device Password I	D, Selected
	Registrar, State, Version, AP Setup Locked	l, UUID-E and
	RF Bands.	-

- 21 -

	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".
	Close : Click this button to exit the information screen.
CXX	General WPS CCX 802.11n C004 >> FALSE Gale >> FALSE Gale >> FALSE Gale >> FALSE
	Clore

- 22 -

	information. Close : Click this butto	on to exit the informat	ion screen.
802.11n	General WPS (CX 802.11n	
	Secondary Channel Offset element		2
	Secondary Channel Offset Extended Capabilities information element	0	
	HT Information Exchange Support	FALSE	
	Neighbor Report element		
	Mobility Domain	FALSE	
	High Throughput	FALSE	
	HT Capabilities element HT Capability	TOF	
	LDPC Coding Capability	FALSE	
	Supported Channel Width Set	1	
	Con Reason Concer		<u>M</u>
		Close	

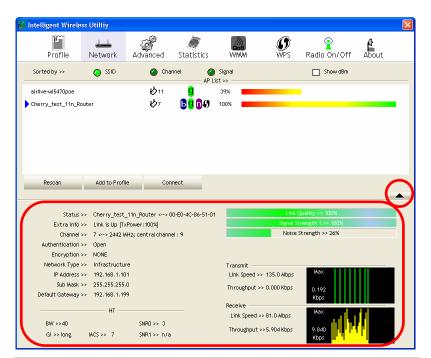
Link Status

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 of Status Section.

Click this button to hide the information of Status Section.



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, WPA-PSK, WPA2-PSK, WPA and WPA2.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.

- 24 -

1			
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 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, you 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 your wireless network.

- 25 -

🖌 Intelligent Wireless Utiltiy						
Profile Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	About
Wireless mode >> 2.4G	•		Non-	i CCKM Radio Measurei Serving Chann	nents el Measurements limit	
Enable TX Burst Enable TX Burst Enable TCP Window Size Fast Roaming at -70 dBm Show Authentication Status Dial Select Your Country Regi 11 B/G		-	21	i0 ms (0-200	0)	•
Advanced Tab						
Wireless mode	Here sup	oports 2.4	IG (includ	ed 802.	11b/g/n) wii	reless mode.
Enable TX Burst	Check to enable this function. This function enables the adapter 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 you connect AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog displays the process about 802.1x authentications.					
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. 					

- 26 -

Statistics

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

Y Intelligent Wireless Utility			X			
Profile Network Advanced Statis	tics WWW	WPS Radio On/	Off About			
Transmit Receive						
Frames Transmitted Successfully Frames Retransmitted Successfully	=	30836 30836				
Frames Fail To Receive ACK After All Retries	=	= 174				
RTS Frames Successfully Receive CTS	-	0				
RTS Frames Fail To Receive CTS	=	0				
Transmit Frames Transmitted Successfully	Shows inform	mation of frames	successfully			
Frames Retransmitted Successfully		mation of frames e or more reties.	successfully			
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 bu	tton to reset cou	nters to zero.			

- 27 -

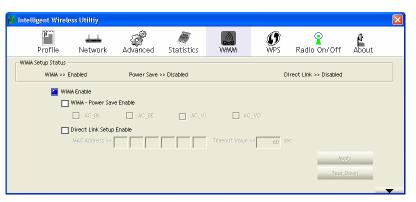
Intelligent Wirel Image: Control of the second seco	Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	2
Transmit	Receive	>						
Frames R	=		15	1541				
Frames Received With CRC Error			= 627					
Frames Dropped Due To Out-of-Resource			= 0					
Duplicate Frames Received				-		0		
Reset Counter								•

Receive Statistics	
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 frames 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 your wireless network quality.

- 28 -



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 which ACs you want to enable the power saving mode. AC_BK (Access Category Background) AC_BE (Access Category Best Effort) AC_VI (Access Category Video) AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	 The setting of DLS(Direct Link Setup) 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. 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.

- 29 -

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.

Profile	Land Network Ac	() Ivanced	Statistics	WWW	Ø WPS	Radio On/O	ff About
		WP	S AP List				Rescan Information Pin Code 16912113 Renew
Cherry_test_11r	n_Router	WPS F	Profile List				Config Mode
ein P <u>B</u> C	WPS Associate IE WPS Probe IE Auto	PBC - G	et WPS profile suc	Progress >> 100% ccessfully.) >	Detail Connect Rotate Disconnect Export Profile Delete

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				

- 30 -

	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, you 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.



	 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 your 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.

- 32 -

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.
РВС	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.
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 button to turn ON or OFF radio function.





i

This icon shows radio on, click to turn it off.

This icon shows radio off, click to turn it on.



About

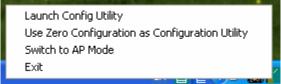
This page displays the information of the wireless card including, RaConfig Version/ Date, Driver Version/ Date, EEPROM Version, Firmware Version and Phy_Address.

Ľ	Intelligent Wirel	ess Utiltiy							
	Profile	Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
			ig Version >>	2.1.3.0			16-2008		
			er Version >> M Version >>	1.1.2.8 1.0	C Firmware Ver:		07-2008		
		Ph	y_Address >>	00-0C-43-30-70-I	00				
									-

- 34 -

Utility Menu List

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



- Launch Config Utility: 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.

- 35 -

Soft AP mode

Config

onfig Access Control	Mac Table Event	Log S	tatistics About	
SSID In	elligent	Ch	annel 1 💌	
Wireless Mode	4G 🗸	•	Use Mac Address	Security Setting
Country Region Code 11 B/G 0: CH1		•	 No forwarding among the second second	ong wireless clients
Beacon (ms)		100	▼ T×BURST	
TX Power	100 %	•		
Idle time(60 - 3600)(s)		300		
			Default	Apply

Config	
SSID	AP name of user type. User 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/n) 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.

- 36 -

Security				2
	itication Type Dpen	•	Encryption Type	Not Use 🔽
	Rekey Interval	60 10 seconds		
Toup	I lekey I literval	10 0000100		
-Wep	Key			
0	i Key#1 Hex			
C) Key#2 Hex	V		
0	0 Key#3 Hex	-		
	Key#4 Hex	-		
	WEP 64 Bits Encryption: F VEP 128 Bits Encryption: P	'lease Keyin 10 HE≯ 'lease Keyin 26 HE≻	K characters or 5 AS Characters or 13 A	CII characters * CII characters
			Г	Show Password
	OK		Cance	4
auther WPA- WPA2	entication Ty ntication mod -PSK, WPA2- 2-PSK. 2-PSK.	es includi -PSK, and	ng Open, S WPA-PS	Shared, K/
then PA- PA2 ICTY then De a PA2	ntication mod PSK, WPA2	es includi -PSK, and For Open e, the sele ad WEP . 1 VPA-PSK e, the encr	ng Open, S WPA-PS and Shar ctions of e For WPA-	Shared, K/ ed encryption PSK, PSK
her PA cry her e a PA her h T	ntication mod PSK, WPA2- 2-PSK. ption Type : ntication mod re Not Use ar 2-PSK , and V ntication mod FKIP and AE	es includi -PSK, and For Open e, the sele ad WEP . 1 VPA-PSK e, the enci S .	ng Open, 5 WPA-PS and Shar ctions of c For WPA - (WPA2 - yption typ	Shared, K/ ed encryption PSK , PSK be supports
her PA- PA2 cry her a PA2 her her h f h PA	ntication mod PSK, WPA2- 2-PSK. ption Type : ntication mod re Not Use ar 2-PSK , and V ntication mod (KIP and AE Pre-shared 1 en AP and ST	es includi -PSK, and For Open e, the sele ad WEP . I VPA-PSK e, the encr S . Key : This CA. For W	ng Open, 5 WPA-PS and Shar ctions of c For WPA- c/ WPA2- yption typ is the sha PA-PSK a	Shared, K/ ed encryption PSK , PSK be supports red secret and
her PA cry her e a PA her h T PA	ntication mod PSK, WPA2- 2-PSK. ption Type : ntication mod re Not Use ar 2-PSK , and V ntication mod (KIP and AE Pre-shared 1 en AP and ST 2-PSK and W	es includi -PSK, and For Open e, the sele ad WEP . I VPA-PSK e, the encr S . Key : This TA. For W PA-PSK/	ng Open, S WPA-PS and Shar ctions of c For WPA- (/ WPA2- yption typ is the sha PA-PSK a WPA2-PS	Shared, K/ ed encryption PSK , PSK be supports red secret and SK
her A- PA2 cry her e a PA2 her A2 her	ntication mod PSK, WPA2- 2-PSK. ption Type : ntication mod re Not Use ar 2-PSK , and V ntication mod (KIP and AE Pre-shared 1 en AP and ST	es includi -PSK, and For Open e, the sele ad WEP . I VPA-PSK e, the encr S . Key : This CA. For W PA-PSK/ e, this fiel	ng Open, S WPA-PS and Shar ctions of c For WPA- c/ WPA2- yption typ is the sha PA-PSK a WPA2-PS d must be	Shared, K/ ed encryption PSK , PSK be supports red secret and SK filled with
her PA- PA: cry her e a PA: her her PA we PA: her urac	ntication mod PSK, WPA2- 2-PSK. ption Type : ntication mod- re Not Use ar 2-PSK , and V ntication mod FKIP and AE Pre-shared 1 en AP and ST 2-PSK and W ntication mod cter longer tha p Re-key Int	es includi -PSK, and For Open e, the sele ad WEP . I VPA-PSK e, the encr S . Key : This CA. For W PA-PSK/ e, this fiel an 8 and lo erval: On	ng Open, S WPA-PS and Shar ctions of e For WPA- yption typ is the sha PA-PSK a WPA2-PS d must be ess than 64 ly valid w	Shared, K/ ed ncryption PSK , PSK be supports red secret and SK filled with l lengths. hen using
her PA Cry her e a PA her her PA her urac OU	ntication mod PSK, WPA2- 2-PSK. ption Type : ntication mod- re Not Use ar 2-PSK , and V ntication mod FKIP and AE Pre-shared 1 en AP and ST 2-PSK and W ntication mod cter longer that p Re-key Int -PSK, WPA2-	es includi -PSK, and For Open e, the sele ad WEP . I VPA-PSK e, the encr S . Key : This CA. For W PA-PSK/ e, this fiel an 8 and lo erval: On -PSK, and	ng Open, S WPA-PS and Shar ctions of e For WPA- / WPA2- yption typ is the sha PA-PSK a WPA2-PS d must be ess than 64 ly valid w	Shared, K/ ed ncryption PSK , PSK be supports red secret and SK filled with l lengths. hen using K/
en A- A2 ry en A2 en A2 en A2 A2 A2	ntication mod PSK, WPA2- 2-PSK. ption Type : ntication mod- re Not Use ar 2-PSK , and V ntication mod FKIP and AE Pre-shared 1 en AP and ST 2-PSK and W ntication mod cter longer tha p Re-key Int	es includi -PSK, and For Open e, the sele ad WEP . 1 VPA-PSK e, the encr S . Key : This CA. For W PA-PSK/ e, this fiel un 8 and lo erval: On -PSK, and tication m	ng Open, S WPA-PS and Shar ctions of e For WPA- C/WPA2- ryption typ is the sha PA-PSK a WPA2-PS d must be ess than 64 ly valid w WPA-PS node to rer	Shared, K/ ed encryption PSK , PSK be supports red secret and SK filled with lengths. hen using K/ uew key. U

- 37 -

	 WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are two formats to enter the keys. Hexadecimal (128bits): 26 Hex 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.
Allow BW 40MHz	Click to disable this function. Default is enabled.
Tx BURST	Check to enable this function.
Default	Use the system default value.
Apply	Click to apply the above settings.

- 38 -

Access Control

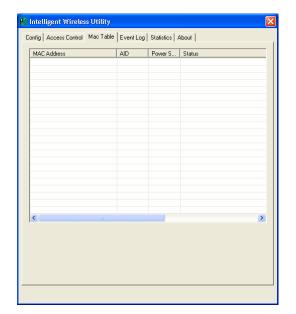
Config Access Control	Mac Table Event	Log Statistics About	
Access Policy		Disable	•
MAC Address		Access List	
	Add		
	Delete	1	
	Remove All		
			Apply
			мрру

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

- 39 -

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.

- 40 -

Event Log

Config Access Control Mac Table E	Event Log Statistics About
Event Time (yy/mm/dd-hh:mm:ss)	Message
2008 / 06 / 03 - 14 : 19 : 44	Restart Access Point
	Clear

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

- 41 -

Statistics

🌠 Intelligent Wireless Utility		
Config Access Control Mac Table Event Log Sta	tistics About	
Transmit Statistics		
Frames Transmitted Successfully	-	185
Frames Fail To Receive ACK After All Retries	=	0
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0
Frames Transmitted Successfully After Retry	=	0
Receive Statistics		
Frames Received Successfully	-	0
Frames Received With CRC Error	-	718
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0
	E I	ESET COUNTERS
	1	ESET COONTENS

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.

- 42 -

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.

×			s Utility	lligent Wireles	🖌 Inte
	atistics About	.og Statistics	Mac Table Event	Access Control	Config
18	ate : 05-16-2008	Date :	2.0.2.1	Utility Version :	
08	ate : 05-07-2008	Date :	1.1.2.8	Driver Version :	
	are Version : 0.9	Firmware Ver:	an: 1.0	EEPROM Versio	
0-70-00					
	afault Gateway :	Default G	255.255.255.0	Sub Mask :	
08	ate : 05-07-2008	Date : Firmware Ver: Phy_Addr	1.1.2.8	Driver Version : EEPROM Version IP Address :	

- 43 -

UTILITY CONFIGURATION FOR WINDOWS VISTA

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

Go to Start→ (All) Program→ Intelligent Wireless→ Intelligent Wireless Utility.



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



- 44 -

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.

P		68		200	ß	\mathbf{Q}	A
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About
	Pro	file List					
PROF1	Cherry_test_	_11n_Router		6	Profile Name	>> PROF1	
					SSID	>> Cherry_test_11n_Rd	outer
					Network Type	>> Infrastructure	
					Authentication	>> Open	
					Encryption	>> None	
					Use 802.1x	>> NO	
					Tx Power	>> <mark>Auto</mark>	
					Channel	>> Auto	
					Power Save Mode	>> CAM	
					RTS Threshold	>> 2347	
Add	Edit	Delete	Activat	P Fra	agment 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.

- 45 -

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	Click to add a profile from the drop-down screen.
	System Configuration tab:

- 46 -

Intelligent Wireless	Utiltiy						11.50
Profile	Network	Advanced) Statistics		Ø WPS	Radio On/Off	About
PROPT	Profile Cherry_test_11 East		Activat	J Pov		>> Cherry_test_tin_R >> Infrastructure >> Topen >> None >> NO >> Auto >> Auto >> CAM >> 2347	outer
System Config	Auth. \ Encry	y. no	215				
SI Power Sa	re Hode >> PEOF1 D >> Cherry_test, re Hode >> O CAP	а О 154	•	Network Type ** Tx Power ** Freatton **	λα 20 [13:0	to 👻	
□ fa	psent Threshold	296.5.4	OK		2346		J
3). SSID: Theoints in dentical	ne SSID your w for all one netwo) is the vireless device vork. U	e uniqu netwo s and p Jser ca	e nam ork. Th ooints a	e shar e narr attemj	ROF# (# red amor ne must l pting to o own mer	ng all be connect
Network Ad hoc r		There	are tw	o type	s, Infi	rastructu	re and
oetwe With 1	en wire he wire	less ne eless ac	etwork lapter,	cards a you ca	and and an an cor	e connec n Access nnect win Access	Point. reless
easily	and qui in share	ickly.	Equipp	bed wit	th the	ess work wireless en each l	adapter.

- 47 -

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 .
Preamble : This function will show up when Ad-hoc network type be selected. 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. <u>The RTS/CTS mechanism will be</u> <u>activated if the data size exceeds the value you set</u> . 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:

- 48 -

Profile	s Ubiny	a Statistics		0	Radio On/Off A
Prome	Profile List	i statistics	**/***	WPS	Radio On/Off A
PROPT	Cherry_test_11n_Boyter		N Ju Powe R		Cherry_test_11n_Router Infrastructure Open None NO Auto Auto CAM 2347
System Config	Auth. \ Encry.	1021X			
	eshared Key >>	• Encryp	Not >> No	• •	B02.1X
	() Key () KeyPt Herzidetinal	*			Show Password
	Key#2 Hexadecima Key#2 Hexadecima	*			_
	Keylet Heradecinal	~			-
		OK.	Cancel	ā	
"Ôper	: If your acco n" authentica to be set to th	ation, the	n the v	virele	ss adapter
	d: Shared ke	v is whe	n both	the se	ender and
recipie		2			
• WPA/ offers the typ WPA	/ WPA-PSK two encrypt pe of algorith Shared Key nared Key fig	<pre>/ WPA2 ion meth im, TKI of 8-63</pre>	/ WPA ods, T P or Al	. 2-PS KIP a ES an	nd AES. d then ent

- 49 -

bet aut	tween thentic	AP and	STA. ode, tł	For W	PA-P d mu	SK and st be fi	shared s d WPA2 lled with engths.	-PSK
alg are ●	gorithm e sever Hexad	n. The k al form	tey mu ats to e (128bi	st mate inter th ts): 26	ch wi ie key Hex	th the A ys. charac	encryptio AP's key ters (0~9	. There
	ow Pa u enter		I: Che	ck this	s box	to sh	ow the	password
aut		etting: ate clie					ver to thentica	tion
_	2.1x ta							
	Profile	Network	Advanced) Statistics		() WPS	Radio On/Off	About
,	Add	Prof Cherry_test_1	e List In_Bouter Detete		6		 Cherry_test_11n_lk Infrastructure Open None No Auto Auto CAM 2347 	suter
-		2.37/24	-	150200		agnerit meanoù	- 1.4	
-	System Config EAP Method +	Auth. \ Encr	Advantation of the second second	1X uthentication ++	EAP-MSC	JHAP Y2 🔻	Session Result	nption
	-		ient Certificat	tion Server	Certificati	ion		
	Authentic	ation ID / Password	- Peo	eerd >>	-	Domain Name >>		
	Turnel ID	/ Passward	Turret Pass	word >=	-	Show Passwo	rd	
				OK	Cancel			

- 50 -

• 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. User can click the box to enable or disable this function.
ID\PASSWORD tab:

- 51 -

	System Coefig Auth. \ Encry. 8021X
-	EAP Method >> PEAP - Tunnel Authentication >> EAP MSCHAP v2 - Session Resumption
	ID \ PASSWORD Client Certification Server Certification
	Authentication ID / Password
	Identity ++ Doministration ++ Doministration ++
	Tunnel ID / Password Tunnel Password >> Tunnel ID >>
	Comparison of Co
	Ol. Cancel
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.
Sh	ow Password: Check this box to show the password
	u entered.
,0	
o	K: Click to save settings and exit this page.
	K . Chek to save settings and exit this page.
C -	Incel: Click to call off the settings and exit.
Ľa	incer. Click to call off the settings and exit.
~	
Cli	ient Certification tab:
. 2	System Config Auth. \ Encry. 8021X
1	EAP Method ++ PEAP + Turnet Authentication ++ EAP-MSCHAP v2 + 🚆 Session Resumption
	ID \ PASSWORD Client Certification Server Certification
	Une a contribute on this computer
	lanet fa se
	Explored On +++
	Friendly Name >>
	Use my insurt card
	OK Cancel
va	an salast Use a contificate on this computer a
	bu can select Use a certificate on this computer, a
	ent certificate for server authentication. Or you can
el	ect 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:
	System Carring Adds., 1 Encry. BB21X ExP Method => PEUP Tunner Authentication => Exp-anglium Proceedings ID \ PASSWORD Client Certification Service Certification
	live certificate chain
	Use certificate chain: Choose use server that issuer of
	certificates.
	Server name: Enter an authentication sever name.
	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.

- 53 -

Profile		Advanced	Statistics	Qos WMM	Ø WPS	Radio On/Off	About
Sorted by >>	SSID	O Cha	nnel 🥑			Show dBm	110.000
Cherry_test_11n_R	outer	b 7	B9n0	100%			
Abocom-Wireless		1011	Bg	86%			
airlive-wl5470poe		11	g	50%			
skl		10	g	44%			
Abocom-Wireless		100	Bg	29%			
PINGOO		10 11	Ъg	24%			
802.11g-AP		100	B9	15%			

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 or 802.11n 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:

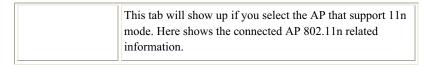
- 54 -

General	General WPS CCX 802.11n
	SUD -> Cherry_test_1 th, Rowber MAC. Address -> 00 E0-4C-46-51-01 Authentication Type -> Linknown Bicryptian Type -> Linknown Charmet +> 7> Hetwork Type -> Infrastructure Beacon Interval -> 100
	Close
	General information contain AP's SSID, MAC address, Authentication Type, Encryption Type, Channel, Network Type, Beacon Interval, Signal Strength and Supported Rates.
MIDO	Close : Click this button to exit the information screen.
WPS	General WPS CCX 802.11n
	Authentication Type >> Uninown State >> Configured
	Encryption Type >> None Version >> 1.0
	Config Methods ++ 0x0086 AP Setup Locked ++
	Device Password ID >> ULID-E >> 6304125310192006128800DHC665101 Selected Registrar >> Unknown RF Bands >> Unknown
	Clone
	WPS information contains Authentication Type, Encryptic 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.

- 55 -

	 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
	 Indicate in All 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". Close: Click this button to exit the information screen.
CXX	General WPS COX 802.11n COM >> FALSE Comp >> FALSE Comp >> FALSE Comp >> FALSE Comp >> FALSE Comp >> FALSE
	CCX information contains CCKM, Cmic and Ckip information. Close: Click this button to exit the information screen.
802.11n	General WPS CCX 802.11a Secondary Channel Offset element 0 Image: Channel Offset element Image: Channel Offset Im

- 56 -



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.

 \mathbf{v}

Click this button to show the information of Status Section.

Click this button to hide the information of Status Section.



- 57 -

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, 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 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, you can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength in the wireless environment.

- 58 -

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 your wireless network.

Vireless mode >> 2.	-70 dBm	Advanced	Statistics	WMM	W PS	Radio On/Off	About
Enable TX Burst Enable TCP Window Siz Fast Roaming at Select Your Co	ize 70 dBm ountry Region						
Enable TCP Window Siz Fast Roaming at Fast Roaming at Select Your Content	-70 dBm ountry Regior	n Code					
	ountry Regior	n Code					
11 B/G >> 0	0: CH1-11						
			<u> </u>				
Apply							
dvanced Ta	h						
uvanceu ra	U						
vireless mode	e	Here sup	pports 2.4	G (includ	led 802.	11b/g/n) wir	eless mo

Enable TX Burst	Check to enable this function. This function enables the adapter to deliver better throughput during a period of

- 59 -

	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 your current network settings.

Profile Networ	k Advanced	Statistics	WMM	WPS	Radio On/Off	About
ansmit Rece	live					
Frames Transmitted S	iuccessfully				1294	
Frames Retransmitted Successfully				1294		
Frames Fail To Receiv	e ACK After All Retries	-		15		
RTS Frames Successfully Receive CTS			-		0	
RTS Frames Fail To Receive CTS			-		0	
et Counter						

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

- 60 -

	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.

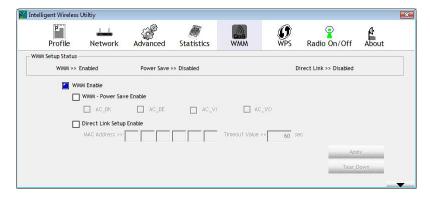
Profile	Network	ک Advanced	Statistics	WMM	() WPS	Radio On/Off	About
ansmit	Receive						
Frames I	Received Successfu	lly				452	
Frames Received With CRC Error					731		
Frames Dropped Due To Out-of-Resource			-		0		
Duplicate Frames Received					0		

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 frames received more than twice.			
Reset Counter	Click this button to reset counters to zero.			

- 61 -

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/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 which ACs you want to enable the power saving mode. AC_BK (Access Category Background) AC_BE (Access Category Best Effort) AC_VI (Access Category Video) AC_VO (Access Category Voice)
Direct Link Setup Enable	Check the box to enable Direct Link Setup.
MAC Address	 The setting of DLS(Direct Link Setup) 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.

- 62 -

	• 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.

Intelligent Wireless	Utiltiy					2		E
Profile	Network	رم) Advanced	Statistics	Ques WMM	Ø WPS	Radio On/Of	f Abo	ut
		wi	PS AP List				Resc	20
ID:	Cherr	y_test_11n_Route	r	00-E0-4C-86-51-01	7		Inform	1000
						Ī	Pin C	Renew
		WPS	Profile List —			Ľ	Config Mod	je
Cherry_test_11n	Router						Enrollee	-
								ail
•						•		tot
<u>P</u> IN	WPS Associate	IE		Progress >> 100	*		Rota	27. A
PBC	WPS Probe IE	PBC - C	Get WPS profile s	uccessfully.			Discon	
							Export F	
						-		
WPS Tab	I							
WPS AP L	ist			rmation of sult. List ir		•		

- 63 -

	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, you 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.			

- 64 -

Key Material: The key material can be used to ensure security of your wireless network. Fill in the appropriat
Key Material: The key material can be used to ensure
Key Index: Only valid when using Open authentication mode and WEP encryption. There are 1~4 key index.
Key Length: Only valid when using Open authenticati mode and WEP encryption. There are key lengths 5, 10 13 and 26.
selection of encryption type are NONE and WEP. For WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
Authentication Type: The authentication type support Open, WPA-PSK and WPA2-PSK. Encryption Type: For Open authentication mode, the
SSID : Shows the connected AP network name. BSSID : The MAC address of the connected AP. Fixed and cannot be changed.

- 65 -

	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.
РВС	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.





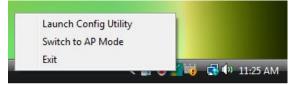
About

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

telligent Wireless		cia.	-			-	
P		6		Qos	0	8	6
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About
	Conf	ig Version >>	2.1.3.0	Dat	e >> 05	-16-2008	
	Drive	er Version >>	2.1.6.7	Dat	ə >> 05	-02-2008	
	EEPRO	M Version >>	1.0	Firmware Versio	n>> 0.9)	
	Ph	y_Address >>	00-0C-43-30-70-0	0			

Utility Menu List

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



- Launch Config Utility: 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.

- 67 -

Soft AP mode

Config

SSID	ligent	Channel 1	
Wireless Mode		<- Use Mac Address	Security Setting
Country Region Code- 11 B/G 0: CH1-1	1 💌	☐ No forwarding amo ☐ Hide SSID ☞ Allow BW 40 MHz	ong wireless clients
Beacon (ms)	100	i i	
TX Power	100 % 💌]	
Idle time(60 - 3600)(s)	300		
		Default	Apply

Config	
SSID	AP name of user type. User 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/n) 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.

- 68 -

Security Setting Authentication Type Open	Encryption Type Not Use
WPA Pre-shared-Key	
Group Rekey Interval 60 10 seco	nas
r-Wep Key	
€ Key#1 Hex ▼	
C Key#2 Hex -	
C Key#3 Hex -	
C Key#4 Hex 🗾	
*WEP 64 Bits Encryption: Please Keyin WEP 128 Bits Encryption: Please Keyin 2	0 HEX characters or 5 ASCII characters * 6 HEX characters or 13 ASCII characters
	Show Password
OK	Cancel
 Encryption Type: For OI authentication mode, the stype are Not Use and WE WPA2-PSK, and WPA-P authentication mode, the eboth TKIP and AES. WPA Pre-shared Key: T 	elections of encryption P. For WPA-PSK, SK/WPA2-PSK encryption type supports his is the shared secret
authentication mode, the s type are Not Use and WE WPA2-PSK , and WPA-F authentication mode, the e both TKIP and AES .	elections of encryption P. For WPA-PSK, PSK/WPA2-PSK encryption type supports his is the shared secret r WPA-PSK and K/WPA2-PSK field must be filled with d less than 64 lengths. Only valid when using

- 69 -

	 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.
Allow BW 40MHz	Click to disable this function. Default is enabling.
Default	Use the system default value.
Apply	Click to apply the above settings.

- 70 -

Access Control

Access Policy		Disable	-
MAC Address		Access List	
L			
	Add		
	Delete		
	Remove All	1	
			Apply

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

- 71 -

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 Address	AID	Power S	Contra 1	
MAC Address	AID	Power S	Status	
•	m			,

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.

- 72 -

Event Log

Event Time (yy/mm/dd-hh:mm:ss)	Message	
2008 / 06 / 06 - 11 : 26 : 49 2008 / 06 / 06 - 11 : 26 : 50 2008 / 06 / 06 - 11 : 26 : 50	Restart Access Point Restart Access Point Restart Access Point	
		Clear

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

- 73 -

Statistics

Access Control Mac Table Event Log Statistics About Transmit Statistics - Frames Transmitted Successfully = 331 Frames Fail To Receive ACK After All Retries = 0 RTS Frames Successfully Receive CTS = 0 RTS Frames Transmitted Successfully After Retry = 0 RTS Frames Transmitted Successfully After Retry = 0 Receive Statistics = Frames Received With CRC Error = 123 Frames Received With CRC Error = 0 Duplicate Frames Received = 0	Intelligent Wireless Utility		
Frames Transmitted Successfully = 331 Frames Fail To Receive ACK After All Retries = 0 RTS Frames Successfully Receive CTS = 0 RTS Frames Fail To Receive CTS = 0 Frames Transmitted Successfully After Retry = 0 Receive Statistics = 206 Frames Received Successfully = 206 Frames Received With CRC Eror = 123 Frames Dropped Due To Out of-Resource = 0 Duplicate Frames Received = 0	onfig Access Control Mac Table Event Log Si	tatistics About	
Frames Fail To Receive ACK After All Retries = 0 RTS Frames Successfully Receive CTS = 0 RTS Frames Fail To Receive CTS = 0 Frames Transmitted Successfully After Retry = 0 Receive Statistics = 206 Frames Received With CRC Error = 123 Frames Dropped Due To Out-of-Resource = 0 Duplicate Frames Received = 0	Transmit Statistics		
RTS Frames Successfully Receive CTS = 0 RTS Frames Fail To Receive CTS = 0 Frames Transmitted Successfully After Retry = 0 Receive Statistics = 206 Frames Received Successfully = 206 Frames Received With CRC Error = 123 Frames Droped Due To Out of-Resource = 0 Duplicate Frames Received = 0	Frames Transmitted Successfully	=	331
RTS Frames Fail To Receive CTS = 0 Frames Transmitted Successfully After Retry = 0 Receive Statistics = 206 Frames Received Successfully = 206 Frames Received With CRC Error = 123 Frames Dropped Due To Out of Resource = 0 Duplicate Frames Received = 0	Frames Fail To Receive ACK After All Retries	=	0
Frames Transmitted Successfully After Retry = 0 Receive Statistics = 206 Frames Received Successfully = 206 Frames Received With CRC Error = 123 Frames Dropped Due To Out-of-Resource = 0 Duplicate Frames Received = 0	RTS Frames Successfully Receive CTS	=	0
Receive Statistics = 206 Frames Received Successfully = 123 Frames Received With CRC Error = 123 Frames Dropped Due To Out-of-Resource = 0 Duplicate Frames Received = 0	RTS Frames Fail To Receive CTS	=	0
Frames Received Successfully = 206 Frames Received With CRC Error = 123 Frames Dropped Due To Out-of-Resource = 0 Duplicate Frames Received = 0	Frames Transmitted Successfully After Retry	=	0
Frames Received With CRC Error = 123 Frames Dropped Due To Out-of-Resource = 0 Duplicate Frames Received = 0	Receive Statistics		
Frames Dropped Due To Out-of-Resource = 0 Duplicate Frames Received = 0		-	
Duplicate Frames Received = 0		-	123
	Frames Dropped Due To Out-of-Resource	-	0
RESET COUNTER	Duplicate Frames Received	=	0
	Duplicate Frames Received		

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.	

- 74 -

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 :	2.0.2.1	Date :	05-16-2008
Driver Version :	2.1.6.7	Date :	05-02-2008
EEPROM Version :	1.0	Firmware Version :	0.9
IP Address :	192.168.123.1	Phy_Address :	00-0C-43-30-70-00
Sub Mask :	255.255.255.0	Default Gateway :	0.0.0.0

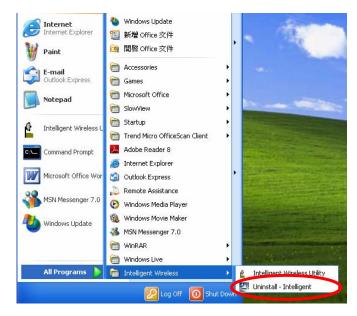
- 75 -

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 –Intelligent.

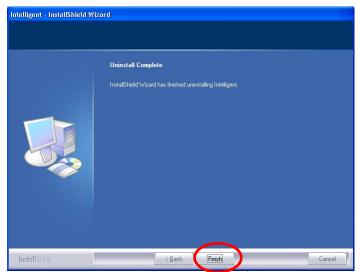


- 76 -

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



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



- 77 -

UNINSTALLATION FOR WINDOWS

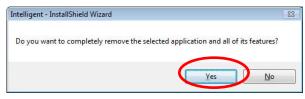
VISTA

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.)

- Default Programs
 Ø
 Internet Explorer Windows Calendar Windows Contacts Windows Defender Windows Fax and Scan Windows Fax and Scan
 Windows Fax and Scan
 Windows Live Messenger Download
 Windows Mail
 Windows Media Player
 Windows Meeting Space Documents Windows Meeting Space Windows Movie Maker Windows Photo Gallery Recent Items Windows Update Accessories Computer Extras and Upgrades Network Games Intelligent Wireless Connect To 🔄 Uninstall - Intelligent Control Panel Maintenance Startup Default Programs Help and Support Back <u>د</u> Start Search Q
- 1. Go to Start → Programs →Intelligent Wireless → Uninstall –Intelligent.



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



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

Intelligent - InstallShield Wizard	Uninstall Complete InstallShield Wizard has finished uninstalling Intelligent.
InstallShield	< Back Finish Cancel

- 79 -