802.11 b/g/n Mini Wireless LAN USB 2.0 Adapter

USER'S MANUAL

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

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.

To maintain compliance with FCC RF exposure requirements, use only belt-clips, holsters or similar accessories that do not contain metallic components in its assembly. The use of accessories that do not satisfy these requirements may not comply with FCC RF exposure requirements, and should be avoided.

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 2.5cm 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

CHAPTER 1: INTRODUCTION	1
FEATURES	1
CHAPTER 2: INSTALLATION	1
FOR WINDOWS 2000/XP	2
INSTALL THE SOFTWARE INSTALL THE HARDWARE	
FOR WINDOWS VISTA	6
INSTALL THE SOFTWARE INSTALL THE HARDWARE VERIFICATION	8
NETWORK CONNECTION	9
IP Address	9
CHAPTER 3: UTILITY CONFIGURATION	9
FOR WINDOWS 2000/XP	10
FOR WINDOWS 2000/XP	
	11
STATION MODE	11
STATION MODE Profile	11
STATION MODE Profile Network	11
STATION MODE Profile Network Link Status	11 11 17 19 21
STATION MODE Profile Network Link Status Advanced	11 11 17 19 21 22
STATION MODE Profile Network Link Status Advanced Statistics	11 11 17 19 21 22 23
STATION MODE Profile Network Link Status Advanced Statistics WMM / QoS	11 11 17 19 21 22 23 23 24
STATION MODE Profile Network Link Status Advanced Statistics WMM / QoS WPS	11 11 17 19 21 22 23 23 24 27
STATION MODE Profile Network Link Status Advanced Statistics WMM / QoS WPS Radio On/Off	11 11 17 19 21 22 23 23 24 27 28
STATION MODE Profile Network Link Status Advanced Statistics WMM / QoS WPS Radio On/Off About	11 11 17 19 21 22 23 23 24 27 28 28
STATION MODE Profile Network Link Status Advanced Statistics WMM / QoS WPS Radio On/Off About UTILITY MENU LIST	11 11 11 17 19 21 22 23 23 24 27 28 28 28 29
STATION MODE Profile Network Link Status Advanced Statistics WMM / QoS WPS Radio On/Off About UTILITY MENU LIST SOFT AP MODE	11 11 17 19 21 22 23 23 24 27 28 28 28 29 29
STATION MODE Profile Network Link Status Advanced Statistics WMM / QoS WPS Radio On/Off About UTILITY MENU LIST SOFT AP MODE Config	11 11 11 17 19 21 22 23 23 24 24 27 28 28 28 29 31

Statistics	
About	
FOR WINDOWS VISTA	36
STATION MODE	37
Profile	
Network	
Link Status	
Advanced	
Statistics	
WMM / QoS	
WPS	
Radio On/Off	
About	
UTILITY MENU LIST	54
SOFT AP MODE	55
Config	
Access Control	
MAC Table	
Event Log	
Statistics	
About	
CHAPTER 4: UNINSTALLATION	62
FOR WINDOWS 2000/XP	62
FOR WINDOWS VISTA	64

CHAPTER 1: INTRODUCTION

The **WU5214** (Wireless LAN USB Adapter) is an IEEE802.11b/g/n USB adapter that connects your notebook to a wireless local area network. The **WU5214** 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 **WU5214** is a very small adapter that can connect 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 bits, 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 2000, XP, and Vista operating systems.

CHAPTER 2:

INSTALLATION

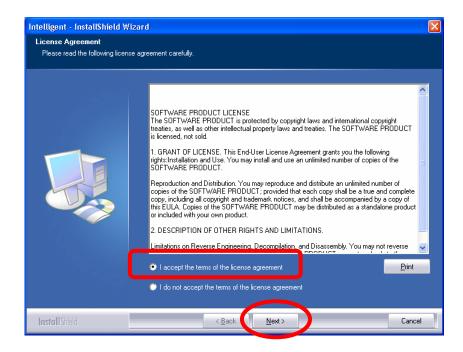
FOR WINDOWS 2000/XP

INSTALL THE SOFTWARE

Note:

Do not insert the Wireless LAN USB Adapter into the computer until the InstallShield Wizard finished installing.

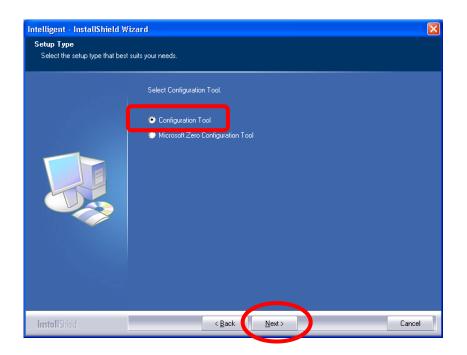
- 1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically.
- 2. When the License Agreement screen appears, please read the contents and select "I accept the terms of the license agreement " then click Next to continue.



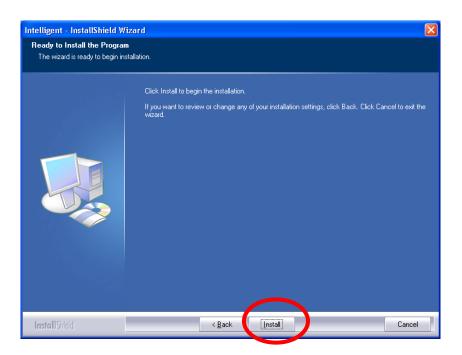
- 3. Select the check box to choose a Configuration Tool from the listed two choices.
 - **Configuration Tool**: Choose to use the configuration utility.

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

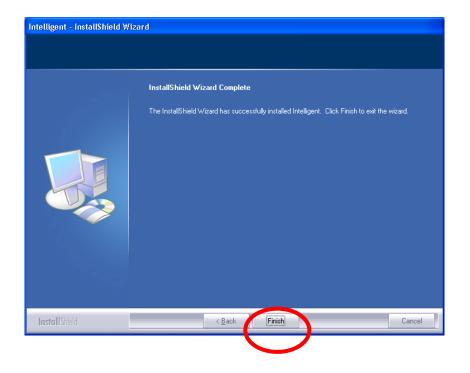
Click Next to continue.



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



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



INSTALL THE HARDWARE

Note:

Insert the Wireless LAN USB Adapter when finished software installation.

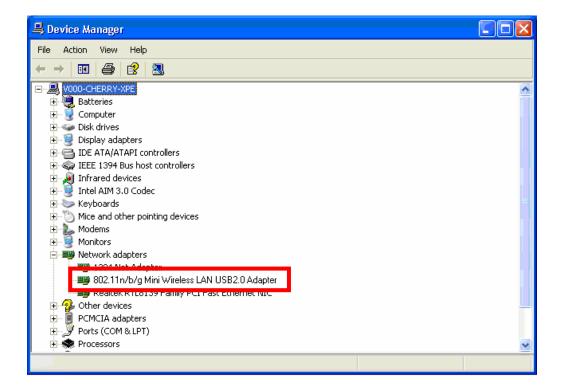
Insert the Wireless LAN USB Adapter into the USB Port of the computer. The system will automatically detect the new hardware.



To verify if the device is active in the computer. Go to Start > Setting > Control Panel > System

> Hardware > Device Manager. Expand the Network Adapters category. If the 802.11n/b/g

Mini Wireless LAN USB2.0 Adapter is listed here, it means that the device is properly installed and enabled.



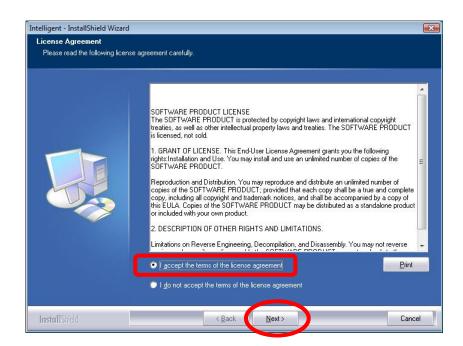
FOR WINDOWS VISTA

INSTALL THE SOFTWARE

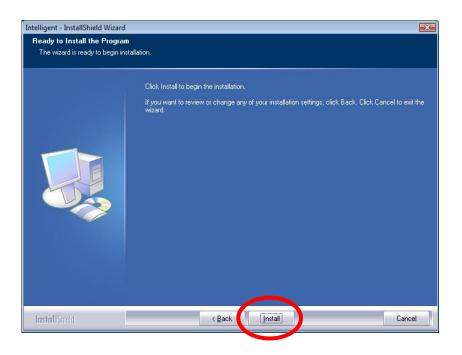
Note:

Do not insert the Wireless LAN USB Adapter into the computer until the InstallShield Wizard finished installing.

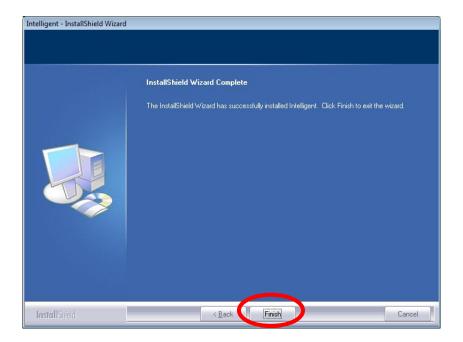
- 1. Exit all Windows programs. Insert the included Installation CD into the computer. The CD-ROM will run automatically.
- 2. When the License Agreement screen appears, please read the contents and select "I accept the terms of the license agreement " then click Next to continue.



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



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



INSTALL THE HARDWARE

Note:

Insert the Wireless LAN USB Adapter when finished software installation.

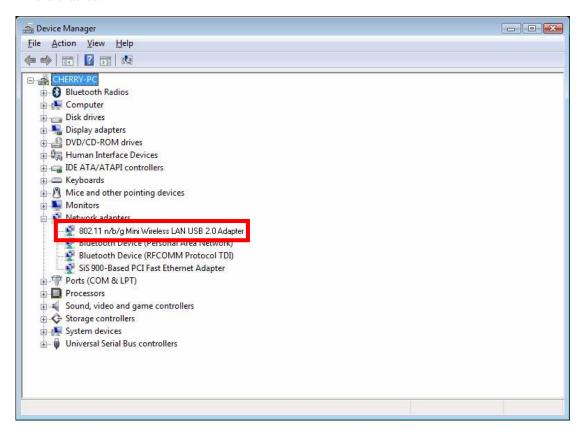
Insert the Wireless LAN USB Adapter into the USB Port of the computer. The system will automatically detect the new hardware.

VERIFICATION

To verify if the device is active in the computer. Go to **Start > Setting > Control Panel > System**

> Hardware > Device Manager. Expand the Network Adapters category. If the 802.11n/b/g Mini Wireless LAN USB2.0 Adapter is listed here, it means that the device is properly installed

and enabled.



NETWORK CONNECTION

IP ADDRESS

Note:

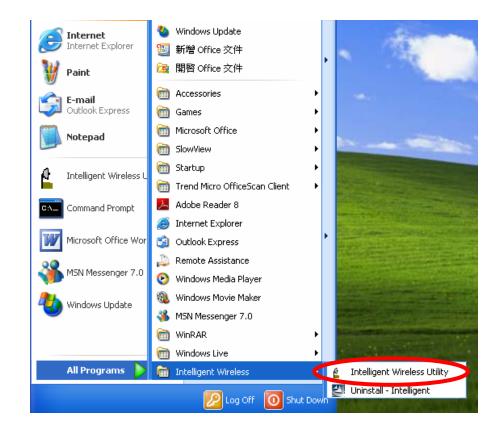
When assigning IP address(es) to computers on the network, remember to have IP address for each computer set on the same subnet mask. If the Broadband Router has been enabled DHCP server function, it won't be necessary to assign static IP address for PC.

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

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 an IP address automatically
Use the following IP address:	O Use the following IP address:
IP address:	IP address: 192.168.1.1
Subnet mask:	Subnet mask: 255 . 255 . 0
Default gateway:	Default gateway: 192 . 168 . 1 . 254
Obtain DNS server address automatically	O 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	OK Cancel

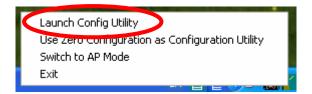
CHAPTER 3: UTILITY CONFIGURATION FOR WINDOWS 2000/XP

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



Go to Start \rightarrow (All) Program \rightarrow Intelligent Wireless \rightarrow Intelligent Wireless Utility.

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



STATION MODE

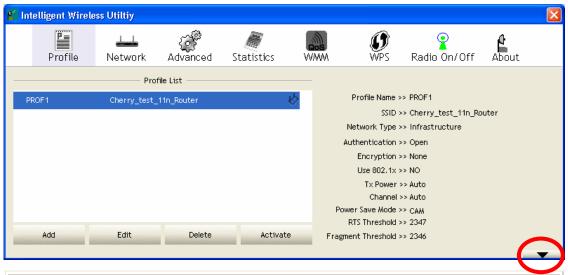
IMPORTANT NOTICE:

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

Profile

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

- Click this button to show the information of Status Section.
- Click this button to hide the information of Status Section.



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

1 Int	telligent Wirele	ss Utiltiy							
	Profile	Network	Advanced	Statistics	WAWA	Ø WPS	Radio On/Off	About	
		Pro	file List						
P	ROF1	Cherry_test_	11n_Router		6	Profile Name >>	PROF1		
							Cherry_test_11n_R	outer	
						Network Type >>			
						Authentication >> Encryption >>			
						Use 802.1x >>			
						Tx Power >>	• Auto		
						Channel >>			
					Po	wer Save Mode >> RTS Threshold >>			
-	Add	Edit	Delete	Activa		wer Save Mode >> RTS Threshold >> ment Threshold >>	2347		
	Add	Edit	Delete	Activa		RTS Threshold >>	2347	_	•
	2	-				RTS Threshold >>	2347		•
	Add System Config	Edit Auth. \ Enc		Activa 121X		RTS Threshold >>	2347		^
	System Config	Auth. \ Enc			ate Frag	RTS Threshold >> ment Threshold >>	2347 • 2346) =	
	System Config Profile Nam	Auth. \ Enc	ny. 83		ate Frag Network Type >	RTS Threshold >> ment Threshold >> > Infrastru	2347 2346 cture 💌) -	^
	System Config Profile Nam	Auth. \ Enc	ny. 83		ate Frag Network Type > T× Power >:	RTS Threshold >> ment Threshold >> > Infrastru > Auto	2347 2346 cture 💌		•
	System Config Profile Nam SSI	Auth. \ Enc e >> PROF1 D >> Cherry_tes	ry. 81 t_11n_Router	21X	ate Frag Network Type >	RTS Threshold >> ment Threshold >> > Infrastru > Auto	2347 2346		^
	System Config Profile Nam SSI	Auth. \ Enc	ry. 81 t_11n_Router	21X	ate Frag Network Type > T× Power >:	RTS Threshold >> ment Threshold >> > Infrastrue > Auto	2347 2346		
	System Config Profile Nam SSI Power Sav	Auth, \Enc e >> PROF1 D >> Cherry_tes e Mode >> @ C	ny. 80 t_11n_Router AM @ PSM	21X	Ate Frag Network Type > Tx Power >: Preamble >:	RTS Threshold >> ment Threshold >> > Infrastrue > Auto	2347 2346		•
	System Config Profile Nam SSI Power Sav	Auth. \ Enc e >> PROF1 D >> Cherry_tes	ny. 80 t_11n_Router AM @ PSM	21X	Ate Frag Network Type > Tx Power >: Preamble >:	RTS Threshold >> ment Threshold >> > Infrastrue > Auto	2347 2346		
	System Config Profile Nam SSI Power Sav	Auth, \Enc e >> PROF1 D >> Cherry_tes e Mode >> @ C	ny. 80 t_11n_Router AM @ PSM	21X	Ate Frag Network Type > Tx Power >: Preamble >:	RTS Threshold >> ment Threshold >> > Infrastrue > Auto	2347 2346		^
	System Config Profile Nam SSI Power Sav	Auth. \Enc e >> PROF1 D >> Cherny_tes e Mode >> O C	ry. 90 t_11n_Router AM @ PSM	21X	Network Type > Tx Power >: Preamble >: 2347	RTS Threshold >> ment Threshold >> > Infrastru > Auto 2347	2347 2346		•

Profile Name: Users 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 wireless access points in the wireless network. The name must be identical for all devices and wireless access points attempting to connect to the same network. Users can use pull-down menu to select from available access points.

Network Type: There are two types, **Infrastructure** and **Ad-hoc** modes. Under Ad-hoc mode users 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 LAN USB Adapter, users can connect wireless LAN to a wired global network via an access point.

• The **Ad-hoc** lets users set a small wireless workgroup easily and quickly. Equipped with the Wireless LAN USB Adapter, users 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 Preamble type into **Auto** or **Long**.

Power Save Mode:

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

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

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

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

Authentication and Security tab:

Authentication >>	Open	•	Encryption >> None	802.1X
WPA Preshared Key >>				
Wep Key				
Key#1	Hexadecimal	-		Show Password
	Hexadecimal	-		
	Hexadecimal	- F		
Key#4	Hexadecimal	- T		

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

• **Open**: If the access point or wireless router is using "**Open**" authentication, then the Wireless LAN USB Adapter will need to be set to the same authentication type.

• 11	ecret key.	
au en an	EAP: Light Extensible Authentication Protocol. It is an EA athentication type used primarily in Cisco Aironet WLANs acrypts data transmissions using dynamically generated WI and supports mutual authentication (only with CCX mode en	s. It EP keys, nabled.)
au W	/PA/ WPA-PSK/ WPA2/ WPA2-PSK: WPA or WPA-PS athentications offer two encryption methods, TKIP and AE /PA-PSK, select the type of algorithm TKIP or AES and the /PA Shared Key of 8-64 characters in the WPA Pre-shared	ES. For nen enter a
selec WPA	ryption Type : For Open and Shared authentication mode ction of encryption type are None and WEP . For WPA , W A-PSK and WPA2-PSK authentication mode, the encryption ports both TKIP and AES .	PA2,
STA.	A Pre-shared Key : This is the shared secret key betwee For WPA-PSK and WPA2-PSK authentication mode t be filled with character longer than 8 and less than 64 len	e, this field
must • AS • AS • He	P Key : Only valid when using WEP encryption algorithm. t match with the AP's key. There are four formats to enter SCII (64 bits) : 5 ASCII characters (case sensitivity). SCII (128 bits) : 13 ASCII characters (case sensitivity). exadecimal (64 bits) : 10 Hex characters (0~9, a~f). exadecimal (128 bits) : 26 Hex characters (0~9, a~f).	
	w Password: Check this box to show the passwords that	t have been
enter	red.	
enter 802.1	red. 1x Setting : When users use radius server to authent ficate for WPA authentication mode (WPA authenticat	
enter 802.1 certif suppo	1x Setting : When users use radius server to authent ficate for WPA authentication mode (WPA authenticat port EAP Method- MD5-Challenge).	
enter 802.1 certif suppo 802.1	1x Setting : When users use radius server to authent ficate for WPA authentication mode (WPA authenticat port EAP Method- MD5-Challenge). 1x tab:	tion do not
enter 802.1 certif supp 802.1	1x Setting : When users use radius server to authent ficate for WPA authentication mode (WPA authenticat out EAP Method- MD5-Challenge). 1x tab: Highernt Wireless Utility Image: Ima	
enter 302.1 certif supp 302.1	1x Setting : When users use radius server to authent ficate for WPA authentication mode (WPA authentication teap Method- MD5-Challenge). 1x tab: 1x tab: Weynt Wireless Utility Wireless Utility Network Advanced Statistics WWWA Work Advanced Statistics WWWA	tion do not
enter 302.1 certif supp 302.1	1x Setting: When users use radius server to authent ficate for WPA authentication mode (WPA authenticate bort EAP Method- MD5-Challenge). 1x tab: Ist tab: Intervent Mode MD5-Challenge). Ist tab: Intervent Mode MD5-Challenge). Intervent MD5-Challenge). Intervent MD5-Challenge). Intervent MD5-Challenge). Intervent MD5-Challenge). Intervent Mode Mode MD5-Challenge). Intervent Mode Mode Mode MD5-Challenge). Intervent Mode Mode Mod Mode Mode Mode Mode Mode	tion do not
enter 802.1 certif supp 802.1 Potelli PROF	1x Setting: When users use radius server to authent ficate for WPA authentication mode (WPA authentication ort EAP Method- MD5-Challenge). 1x tab: 1x tab: Ivent Wireless Utility Profile Advanced Statistics WWW Profile Advanced Statistics WWW Profile Statistics Profile Cherry_test_1in_Bouter F1 Cherry_test_1in_Bouter Profile Statistics SID > Cherry_test_1in_Bouter SiD > Cherry_test_1in_Bouter Side 2.1x > Note Use B02.1x > Note	tion do not
enter 802.1 certif suppo 802.1 P Intell PROF	Ix Setting: When users use radius server to authentificate for WPA authentication mode (WPA authentication or EAP Method- MD5-Challenge). Ix tab: If the set of the	tion do not
enter 802.1 certif suppo 802.1 % Intell PROF	1x Setting: When users use radius server to authent ficate for WPA authentication mode (WPA authentication teap Method- MD5-Challenge). 1x tab: Import Method- MD5-Challenge). Import Method- Method:	tion do not
enter 802.1 certif suppo 802.1 % Intell PROF	1x Setting: When users use radius server to authent ficate for WPA authentication mode (WPA authentication or EAP Method- MD5-Challenge). Ist tab: Ist tab: Import Wireless Utility	tion do not
enter 802.1 certif suppo 802.1 entett	1x Setting: When users use radius server to authentificate for WPA authentication mode (WPA authentication or EAP Method- MD5-Challenge). Ist tab: Ist tab: Import Wireless Utility	tion do not

EAP Method:

- **PEAP**: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- TLS / Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
- **TTLS**: Tunnelled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- **EAP-FAST**: Flexible Authentication via Secure Tunnelling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication now.
- **MD5-Challenge**: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication there is no mutual authentication of wireless client and the network. (Only Open and Shared authentication mode can use this function.)

Tunnel Authentication:

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

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

ID\PASSWORD tab:

ID \ PASSWORD Client Certification Server Certification Authentication ID / Password Identity >> Password >> Domath Name >> Domath Name >>
Identity ss Domain Name >>
Tunnel ID / Password
Tunnel ID >> Tunnel Password >> Show Password

ID/ PASSWORD: Identity and password for server.

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

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

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

Client Certification tab:

AP Method >> PEAP	 Tunnel Auther 	ntication >> EAP-MSCHAP v2	 Session Resumption
ID \ PASSWORD	Client Certification	Server Certification	
🔲 Use Client ce	rtificate		~
	issued By >>		
	Friendly Name >>		

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:

EAP Method >> PEAP 🔻	Tunnel Authentication >> EAP-MSCHAP v2 Session Resumption
ID \ PASSWORD Client C	ertification Server Certification
Use certificate chain	
	Allow intermidiate certificates
	Server name >>
	Server name must match
	Opmain 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.

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

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

OK: Click to save settings and exit this page.

Cancel: Click call off the settings and exit.

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

Network

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

🖌 Intelligent Wirele	ess Utiltiy							×
Profile	LLL Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
Sorted by >>	SSID	🖉 Cha	nnel 🥝	Signal		Show dBm		
airlive-wI5470poe	outer	ゆ11 ゆ7	9 99 94 9	39%				•
Rescan	Add to Profi	le 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 search and refresh the access point list.					

Add to Profile	Select an item (SSID) on the list and then click to add it into the profile list.
Connect	Select an item (SSID) on the list and then click to make a connection.

Access Point (AP) Information

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

General	General WPS CCX 802.11n						
	SSID >> Cherry_test_11n_Router MAC Address >> 00-E0-4C-86-51-01 Authentication Type >> Unknown Encryption Type >> None Channel >> 7 <>> 2442 MHz Network Type >> Infrastructure Beacon Interval >> 100						
	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	General WPS CCX 802.11n Authentication Type >> Unknown State >> Configured Encryption Type >> None Version >> 1.0 Config Methods >> Unknown AP Setup Looked >> Device Password ID >> UUID-E>> Unknown Selected Registrar >> Unknown RF Bands >>						
	Close 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, WPA securities, WPA2-PSK and WPA2.						
	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 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.									
ССХ	General WPS CCX 802.11n									
	COKM >> FALSE Onic >> FALSE Okip >> FALSE									
	Close									
	CCX information contains CCKM, Cmic and Ckip information. Close : Click this button to exit the information screen.									
802.11n	General WPS CCX 802.11n									
	Secondary Channel Offset element 0 Secondary Channel Offset element 0 Extended Capabilities information element FALSE Highbor Report element FALSE High Throughput FALSE High Throughput FALSE HT Capabilities element FALSE HT Capability Selement FALSE HT Capability Selement FALSE HT Capability Selement FALSE HT Capability Selement FALSE HT Capability TRUE LDPC Coding Capability Supported Channel Width Set 1									
	Close									
	This tab will show up if the selected access point supports 11n mode. Here shows the connected access point 802.11n related information.									

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.

ntelligent Wirele		ംര്മ	Jan .				~
P		6		Gos	9	2	4
Profile	Network	Advanced	Statistics	WWW	₩PS	Radio On/Off	About
Sorted by >>	🧿 SSID	🥝 Cha	annel 🥝	Signal		Show dBm	
airlive-wl5470poe		1 /2	g	39%			
Cherry_test_11n_R	uter	107	b g n ø	100%			
Rescan	Add to Profile	e Cor	nnect				
Rescan	Add to Profile	e Cor	nnect				
Rescan					Link (Quality >> 100%	-
_	>> Cherry_test_	11n_Router <> (nnect 00-E0-4C-86-51-01			Quality >> 100% trength 1 >> 100%	-
Status Extra Info	>> Cherry_test_	,11n_Router <> (Power:100%)	00-E0-4C-86-51-01		Signal St		
Status Extra Info	 >> Cherry_test_ >> Link is Up [Txl >> 7 <> 2442 MI 	,11n_Router <> (Power:100%)	00-E0-4C-86-51-01		Signal St	trength 1 >> 100%	
Status Extra Info Channel	 >> Cherry_test_ >> Link is Up [Txl >> 7 <> 2442 MI >> Open 	,11n_Router <> (Power:100%)	00-E0-4C-86-51-01		Signal St	trength 1 >> 100%	
Status Extra Info Channel Authentication	 >> Cherry_test_ >> Link is Up [Tx] >> 7 <> 2442 Mi >> Open >> NONE 	11n_Router <> (Power:100%) Hz; central chanr	00-E0-4C-86-51-01	Transmit	Signal St	trength 1 >> 100%	
Status Extra Info Channel Authentication Encryption Network Type	 >> Cherry_test_ >> Link is Up [Tx] >> 7 <> 2442 Mi >> Open >> NONE 	11n_Router <> (Power:100%) Hz; central chanr e	00-E0-4C-86-51-01	Transmit —— Link Speed >>	Signal St Noise	trength 1 >> 100%	
Status Extra Info Channel Authentication Encryption Network Type IP Address	 >> Cherry_test_ >> Link is Up [Txl >> 7 <> 2442 Ml >> Open >> NONE >> Infrastructur 	11n_Router <> (Power:100%) Hz; central chanr e 1	00-E0-4C-86-51-01	Link Speed >>	Signal St Noise	Strength 1 >> 100% Strength >> 26%	
Status Extra Info Channel Authentication Encryption Network Type IP Address Sub Mask	 >> Cherry_test_ >> Link is Up [Txl >> 7 <> 2442 Ml >> Open >> NONE >> Infrastructur >>> 192.168.1.10 	11n_Router <> (Power:100%) Hz; central chanr e 1 D	00-E0-4C-86-51-01		Signal St Noise	trength 1 >> 100% Strength >> 26%	
Status Extra Info Channel Authentication Encryption Network Type IP Address Sub Mask	 >> Cherry_test_ >>> Link is Up [Txl >> 7 <> 2442 Ml >>> Open >>> NONE >>> Infrastructur >>>>>>>> 192.168.1.10 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	11n_Router <> (Power:100%) Hz; central chanr e 1 D	00-E0-4C-86-51-01	Link Speed >> Throughput >> Receive	Signal Si Noise 135.0 Mbps 0.000 Kbps	Max 0.192 Kbps	
Status Extra Info Channel Authentication Encryption Network Type IP Address Sub Mask	 >> Cherry_test_ >> Link is Up [Txl >> 7 <> 2442 Mi >> Open >> NONE >> Infrastructur >> 192.168.1.10' >> 255.255.255. >> 192.168.1.19' 	11n_Router <> (Power:100%) Hz; central chanr e 1 D	00-E0-4C-86-51-01	Link Speed >> Throughput >>	Signal Si Noise 135.0 Mbps 0.000 Kbps	trength 1 >> 100% Strength >> 26% Max 0.192	

Link Status Tab						
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.					
Extra Info	Shows the link status and TX power percentage.					
Channel	Shows the current channel in use.					
Authentication	Authentication mode used within the network, including Unknown, Open, Shared, Leap, WPA-PSK, WPA2-PSK, WPA and WPA2.					
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.					
Network Type	Network type in use, Infrastructure for BSS, 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, users can choose to display as percentage or dBm format.				
Noise Strength	Shows the noise signal strength in the wireless environment.				
Transmit Shows the current Link Speed and Throughput of the transmit rate.					
Receive	Shows the current Link Speed and Throughput of receive rate.				
Link Speed	Shows the current transmitting rate and receiving rate.				
Throughput	Shows the transmitting and receiving speed of data.				

Advanced

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

A [©] Inte	🎦 Intelligent Wireless Utiltiy									
	Profile	Handreine Network	Advanced	Statistics	www.	Ø WPS	Radio On/Off	About		
Win	eless mode >>	2.4G	•		Turn on	CCKM Radio Measurer				
	Enable TX Burst Enable TCP Windo Fast Roaming at	ow Size			25		el Measurements limit J)			
11	Show Authentica Select You B/G >>	tion Status Dialo; r Country Regior 1: CH1-13		<u></u>						
	Apply								_	

Advanced Tab						
Wireless mode Here supports 2.4G (included 802.11b/g/n) wireless mode.						
Enable TX Burst	Check to enable this function. This function enables the Wireless LAN USB 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 connected AP with authentication, choose whether show "Authentication Status Dialog" or not. Authentication Status Dialog displays the process about 802.1x authentications.					

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

Statistics

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

🖌 Inte	elligent Wirele	ess Utiltiy							
	Profile	Network	کی Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
<	Transmit	Receive							
	Frames ⁻	Transmitted Succe	ssfully		=		30836		
	Frames F	Retransmitted Suc	cessfully		= 30836				
	Frames F	Fail To Receive AC	(After All Retries		=		174		
	RTS Fran	nes Successfully Re	ceive CTS		-		0		
	RTS Frames Fail To Receive CTS				=		0		
Re	eset Counter								-

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

Profile	↓ ⊥↓ Network	کی Advanced	Statistics	www.	Ø WPS	Radio On/Off	A bout	
Transmit	Receive							
Frames R	Received Successfu	lly		=	15	41		
Frames R	eceived With CRC	Error		-	é	27		
Frames D)ropped Due To Ou	t-of-Resource		=		0		
Duplicate	e Frames Received			-		0		

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

WMM/ QoS

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

🖌 Inte	elligent Wirele	ss Utiltiy							
	Profile	Lee Network	ر Advanced	Statistics	www.	Ø WPS	Radio On/Off	About	
_₩M	M Setup Status —								
	WMM >> E	nabled	Power Save >	> Disabled		D	irect Link >> Disabled		
	🔼 WM/	/ Enable							
		WMM - Power Sav	e Enable						
		AC_BK	AC_BE	AC_VI	AC	_VO			
		Direct Link Setup	Enable						
		MAC Address >>			Timeout Value >	>> 60 Se	20		
							Арр	ly	
							Tear I	Down	

WMM/QoS Ta	b
WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	 Select a power save mode that preferred. 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 (DLS). This function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.
MAC Address	 The setting of DLS(Direct Link Setup) indicates as follow : Fill in the blanks of Direct Link with MAC Address of target STA, and the STA must conform to two conditions: 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 setting of Timeout Value is 60 seconds.)
Apply	Click this button to apply the settings.
Tear Down	Select a direct link STA MAC address, then click "Tear Down" button to disconnect the STA.

WPS

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

Intelligent Wirele	ess Utiltiy						
Profile	LLL Network A	dvanced	Statistics	www.	Ø WPS	Radio On/Off	A About
		WF	S AP List				
						F	Rescan Information Pin Code 16912113 Renew
		WPS	Profile List			L	Config Mode
Cherry_test_11n_	Router						Enrollee 🗾
<			1111				Detail Connect
PIN	WPS Associate IE			Progress >> 10	0%		Rotate
PBC	WPS Probe IE	PBC - G	et WPS profile succ	cessfully.			Disconnect
	Auto					-	Export Profile
						10	Delete

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.					
	General WPS CCX 802.11n					
	Autrentication Type >> WPA-PSK State >> Configured					
	Encryption Type >> TKIP: Version >> 1.0					
	Config Methods >> 0x008A AP Setup Locked >>					
	Device Password ID >> 0x0004 UUID-E >> 2880288028801880A880000C432860E0					
	Selected Registrar >> TRUE RF Bands >> 0x01 (2,4GHz)					
	Clase					
PIN Code	8-digit numbers. It is required to enter PIN Code into Registrar when using PIN method. When STA is Enrollee, users can use " Renew " button to re-generate new PIN Code.					
Config Mode	Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.					
Detail	Click the Detail button to show the information about Security and Key in the credential.					

	Intelligent Wireless Utility
	Profile Network Advanced Statistics WWW. WPS Radio On/Off About
	WPS AP List Rescan Information Pin Code
	WPS Profile List Config Made
	Cherry_test_11n_Router
	Pipe WPS Associate IE Progress >> 100x Rotate PBC @WPS Probe IE PBC - Get WPS profile successfully. Disconnect Auto Export Profile
	Delete
	SSID >> Cherry_test_11n_Router
	BSSID >> 00-0C-42-30-70-00 Authentication Type >> OPEN Encryption Type >> NONE
	Key Length >> Key Index >> Key Waterial >>
	Iney materia >>
	OK Cancel
	If selected the AP that listed in the WPS Profile List field, users can click the
	Detail button to see more AP information.
	SSID: Shows the connected AP network name.
	BSSID : The MAC address of the connected AP. Fixed and cannot be changed.
	Authentication Type : The authentication type support Open, WPA-PSK and WPA2-PSK.
	Encryption Type: For Open authentication mode, the selection of encryption type are NONE and WEP . For WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES .
	Key Length: Only valid when using Open authentication mode and WEP encryption. There are key lengths 5, 10, 13 and 26.
	Key Index: Only valid when using Open authentication mode and WEP encryption. There are 1~4 key index.
	Key Material: The key material can be used to ensure the security of the wireless network. Fill in the appropriate value or phrase in Key Material field.
	Show Password: Check this box to show the passwords that have been entered.
	OK : Click to save and apply the new settings.
	Cancel: Click to leave and discard the settings.
Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to rotate to connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.

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

Radio On/Off

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



About

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

💕 In	telligent Wirele	ss Utiltiy							
	Profile	44 Network	Advanced	Statistics	Cos WWM	() WPS	Radio On/Off	About	
		Config Ve	ersion >> 2.1.5	.0		Date >>	06-23-2008		
		Driver Ve	rsion >> 1.2.1	.0		Date >>	07-30-2008		
		EEPROM Ve	ersion >> 1.0		Firmware	Version >>	0.12		
		Phy_Ad	dress >> 00-1	2-0E-6B-58-3B					
									-

UTILITY MENU LIST

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

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

- 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 the Wireless LAN USB Adapter act as a wireless AP.
- **Exit**: Select to close the utility program.

SOFT AP MODE

Config

Intelligent Wireles	Mac Table Event Log	Statistics About	
SSID Sc Wireless Mode 2		Channel 1	Security Setting
Country Region Code	1	Hide SSID	ong wireless clients
Beacon (ms) TX Power Idle time(60 - 3600)(s)	100 % ▼ 100 % ▼ 300	₩ TxBURST	
	ļ	Default Car	ncel Apply

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

	Security Setting
	Authentication Type Open Encryption Type Not Use
	WPA Pre-shared-Key
	Group Rekey Interval 60 10 seconds
	Wep Key
	€ Key#1 Hex ▼
	C Key#2 Hex
	C Key#3 Hex
	C 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 several types of authentication modes
	including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/
	WPA2-PSK. (System authentication type default is Open.)
	Encryption Type: For Open and Shared authentication mode, the
	selections of encryption type are Not Use and WEP. For WPA-PSK,
	WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode, the encryption type supports both TKIP and AES. (System authentication
	type default is Not Use.)
	WPA Pre-shared Key : This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK and WPA-PSK/WPA2-PSK
	authentication mode, this field must be filled with character longer than 8
	and less than 64 lengths.
	Group Re-key Interval: Only valid when using WPA-PSK, WPA2-PSK,
	and WPA-PSK/ WPA2-PSK authentication mode to renew key. Users can set to change by seconds or packets. (Default is 600 seconds.)
	can set to change by seconds of packets. (Default is 600 seconds.)
	WEP Key : Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys
	must match with the AP's key. There are four formats to enter the keys.
	 ASCII (64 bits): 5 ASCII characters (case sensitivity). ASCII (128 bits): 13 ASCII characters (case sensitivity).
	• Hexadecimal (64 bits): 10 Hex characters (0~9, a~f).
	• Hexadecimal (128 bits): 26 Hex characters (0~9, a~f).
	Show Password: Check this box to show the passwords that have been
	entered.
Beacon (ms)	The time between two beacons. (The system default is 100 ms.)
TX Power	Manually force the AP transmits power from the pull-down list 100%, 75%, 50%, 25% and lowest. (The system default is 100%)
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. (Default value of idle time is 300 seconds.)

No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. (The system default is no forwarding.)
Hide SSID	Do not display AP name. (System default is disabled.)
Allow BW 40MHz	 Click to disable this function. (System default is enabled.) This function enables the adapter to deliver better throughput, enable this function the link speed will up to 300Mbps, disable this function the link speed will up to 150Mbps only. Note: This function depends on the capability of device. Here supports link speed up to 150Mbps only, DO NOT support link speed up to 300Mbps.
Tx BURST	This function enables the adapter to deliver better throughput during a period, it only takes effect when connecting with the AP that supports this function. (Default setting is enabled.)
Default	Use the system default value.
Apply	Click to apply the above settings.

Access Control

🖌 Intelligent Wireless	: Utility 🛛 🔁
Config Access Control	Mac Table Event Log Statistics About
Access Policy	Disable 🔽
MAC Address	Access List
	Add
	Delete
	Remove All
	Apply

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

MAC Table

MAC Address	 AID	Power S	Status	
<				
				>

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				
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.		

Statistics

🎸 Intelligent Wireless Utility		×
Config Access Control Mac Table Event Log	Statistics 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
		RESET COUNTERS

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

Duplicate Frames Received	The number of duplicate packets received.
Reset Counter	Reset counters to zero.

About

This page displays the Wireless LAN USB Adapter and driver version information.

Utility Version :	2.0.5.0	Date :	06-23-2008
Driver Version :	1.2.1.0	Date :	07-30-2008
EEPROM Version :	1.0	Firmware Version :	0.12
IP Address :	192.168.123.1	Phy_Address :	00-12-0E-6B-58-3B
Sub Mask :	255.255.255.0	Default Gateway :	

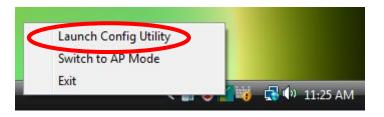
FOR WINDOWS VISTA

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

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



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



STATION MODE

Profile

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

- Click this button to show the information of Status Section.
- Click this button to hide the information of Status Section.

MIIntell	igent Wireless	Utiltiy							X
	Profile	Network	Advanced	Statistics	QoS WMM	() WPS	Radio On/Off	About	
		Pro	file List						
PRO)F1	Cherry_test_	11n_Router		5	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		
					1	Power Save Mode >:			
		10100	625425			RTS Threshold >:	> 2347		
	Add	Edit	Delete	Activate	Fra	gment Threshold >:	> 2346		\frown
								(-

Profile Tab	
Profile Name	Users may enter a distinctive name of profile in this column. The default is PROF# (#1, #2, #3)
SSID	The SSID is the unique name shared among all wireless access points in the wireless network.
Network Type	Shows the network type of the device, including Infrastructure 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.

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.					
	 The Infrastructure is intended for the connection between wireless network cards and an access point. With the Wireless LAN USB Adapter, users can connect wireless LAN to a wired global network via an access point. The Ad hoc lets users set a small wireless workgroup easily and quickly. Equipped with the Wireless LAN USB Adapter, users 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 Preamble type into **Auto** or **Long**.

Power Save Mode:

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

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

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

Authentication and Encryption tab:

Profile	Network	Advanced	Statistics	QoS WMM	() WPS	Radio On/Off	About
	Pr-	ofile List					
ROF1	Cherry_test	_11n_Router		6	Profile Name :	>> PROF1	
					SSID	<pre>>> Cherry_test_11n_Rc</pre>	outer
						>> Infrastructure	
					Authentication		
					Encryption Use 802.1x		
					Tx Power		
					Channel	>> Auto	
				1	Power Save Mode		
Add	Edit	Delete	Activate		RTS Threshold		
WPA P		'					1
0.000000	ер Кеу ————	Hexadecimal	▼			Show Pass	word
0.000000	ер Кеу		*			Show Pass	word
0.000000	ер Кеу ————	Hexadecimal Hexadecimal	× [Show Pass	word
0.000000	ер Кеу		×			Show Pass	word
0.000000	 Pep Key Key#1 Key#2 	Hexadecimal	×			Show Pass	word
0.000000	ep Key Key#1 Key#2 Key#3	Hexadecimal Hexadecimal	▼	Cancel		Show Pass	word
0.000000	ep Key Key#1 Key#2 Key#3	Hexadecimal Hexadecimal	▼	Cancel		Show Pass	word
0.000000	ep Key Key#1 Key#2 Key#3	Hexadecimal Hexadecimal	▼	Cancel		Show Pass	word
W	 Key#1 Key#2 Key#3 Key#4 	Hexadecimal Hexadecimal Hexadecimal			e of aut		
thentio	кер Кеу Кеу#1 Кеу#2 Кеу#3 Кеу#4 Key#4 Key#4	Hexadecimal Hexadecimal Hexadecimal	ere are s	ix typ		Show Pass	on mod

• **Shared**: Shared key is when both the sender and the recipient share a secret key.

authentication, then the Wireless LAN USB Adapter will need to be set

to the same authentication type.

WPA/ WPA-PSK/ WPA2/ WPA2-PSK: WPA-PSK offers two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES and then enter a WPA Shared Key of 8-63 characters in the WPA Pre-shared Key field.
ncryption Type: For Open and Shared authentication mode, the election of encryption type are None and WEP . For WPA , WPA2 , /PA-PSK and WPA2-PSK authentication mode, the encryption type apports both TKIP and AES .
VPA Pre-shared Key : This blank is the shared secret key between AP nd STA. For WPA-PSK and WPA2-PSK authentication mode, this eld must be filled with character longer than 8 and less than 64 lengths
WEP Key : Only valid when using WEP encryption algorithm. The key nust match with the AP's key. There are four formats to enter the keys.
 ASCII (64 bits): 5 ASCII characters (case sensitivity). ASCII (128 bits): 13 ASCII characters (case sensitivity). Hexadecimal (64 bits): 10 Hex characters (0~9, a~f). Hexadecimal (128 bits): 26 Hex characters (0~9, a~f).
how Password: Check this box to show the passwords that have bentered.
02.1x Setting : When users use radius server to authenticate client ertificate for WPA authentication mode.
02.1x tab:
Intelligent Wireless Utility
Profile Network Advanced Statistics WMM WPS Radio On/Off About
Profile List PROF1 Cherry_test_11n_Bouter V SID >> Cherry_test_11n_Bouter V SID >> Cherry_test_11n_Bouter V SID >> Cherry_test_11n_Bouter V Network Type >> Infrastructure Authentication >> Open Encryption >> None Use 802, 1x> NO Tx Power >> Auto Channel >> Auto Channel >> Auto Power Save Modes >> CAM RTS Threshold >> 2347 Add Edit Delete Activate
EAP Method >> PEAP
Authentication ID / Password
Tunnel ID >> Tunnel Password >> Show Password
OK Cancel
AP Method:
PEAP : Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
TLS / Smart Card: Transport Layer Security. Provides for

certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

Tunnel Authentication:

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

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

ID\PASSWORD tab:

EAP Method >> PE/	P Tunnel Authentication >>	EAP-MSCHAP v2 Session Resumption
ID \ PASSWORD	Client Certification Server Cer	tification
Authentication ID / Pa	ssword	
Identity >>	Password >>	Domain Name >>
- 1	1 033001 0 77	Domail Mano XX
Tunnel ID / Password		
Tunnel ID >>	Tunnel Password >>	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 passwords that have been entered.

OK: Click to save settings and exit this page.

Cancel: Click to call off the settings and exit.

Client Certification tab:

EAP	Method >> PEAP		el Authentication >>	EAP-MSCHAP v2	•	Session Resumption
-	ID \ PASSWORD	Client Certific	ation Server	Certification		
	Use a certificate on	this computer				~
		1				
		Issued To >>				
		Issued By >>				
		Expired On >>				
		Friendly Name >>				
	Use my smart card					
			ОК	Cancel		

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

	OK : Click to save settings and exit this page.
	Cancel: Click to call off the settings and exit.
	Server Certification tab:
	System Config Auth. \ Encry. 8021X
	EAP Method >> PEAP
	Server name >>
	OK Cancel
	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

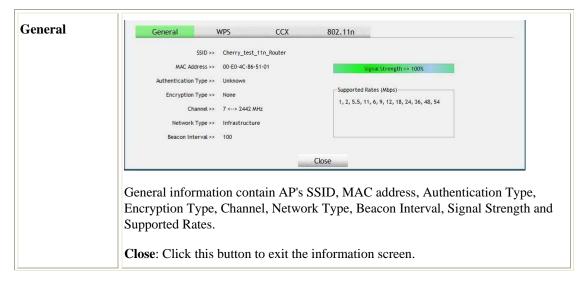
The Network page displays the information of surrounding APs from last scan result. The tab lists the information including SSID, Network type, Channel, Wireless mode, Security-Enabled and Signal.

Intelligent Wireless U		<u>_</u>	A	-	A	۲	A	
Profile	Network	Advanced	Statistics	WMM	WPS	Radio On/Off	About	
Sorted by >>	SSID	🖉 Cha		Signal		Show dBm		
Cherry_test_11n_R	outer	b 7	B910	100%				
Abocom-Wireless		11	bg	86%				
airlive-wl5470poe		11	g	50%				
skl		10	g	44%				
Abocom-Wireless		6	Ъg	29%				
PINGOO		11	bg	24%				
802.11g-AP		6	Bg	15%				
Rescan	Add to Profi	ile .						
Rescan	Add to Profi	ile						

Network Tal	0
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.

Access Point (AP) Information

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



WPS	General WPS CCX 802.11n								
	Authentication Type >> Unknown State >> Configured								
	Encryption Type >> None Version >> 1.0								
	Config Methods >> 0x0086 AP Setup Locked >>								
	Device Password ID >> UUID-E >> 6304125310192006122800E04C865101								
	Selected Registrar >> Unknown RF Bands >> Unknown								
	Close								
	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, WPA securities, WPA2-PSK and WPA2.								
	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.								
ССХ	General WPS CCX 802.11n								
	CCKM >> FALSE Cmic >> FALSE Ckip >> FALSE								
	Close								
	CCX information contains CCKM, Cmic and Ckip information.								
	Close: Click this button to exit the information screen.								

Tanana and a second		here in the second s
Secondary Channel Offset element		<u>^</u>
Secondary Channel Offset	0	E
Extended Capabilities information element		
HT Information Exchange Support	FALSE	
Neighbor Report element		
Mobility Domain	FALSE	
High Throughput	FALSE	
HT Capabilities element		
HT Capability	TRUE	
LDPC Coding Capability	FALSE	
Supported Channel Width Set	1	121
cu n c	2	
	Close	
	CIUSE	

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.

	Advanced	Statistics	WMM	WPS	Radio On/Off	About
SSID	🥝 Cha) Signal		Show dBm	
er	107		100%			
	1011		86%			
		a	50%			
		ä	assess and a			
			NELSER TO A			
	•					
		P a	24%			
	6	bg	15%	11		
Cherry_test_11	n_Router <> (00-E0-4C-86-51-01	1			
	; central chann	el : 9		Noise	strength >> 26%	
			10000			
				> 135.0 Mbps	Max	
					100 - 100 miles - 100 miles	
			inroughput >	> 0.000 Kbps	11.728 Kbps	
			Receive			
ні —			Link Speed >	> 135.0 Mbps	Max	
	SNRO >> 0		-	>21.484 Kbps	550.016	
	Link is Up [TxPo	Add to Profile Cherry_test_11n_Router <> 0 Link is Up [TxPower:100%] 7 <> 2442 MHz; central chann Open NONE Infrastructure 192.168.1.100 255.255.255.0 192.168.1.199 HT	er 07 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Unit Unit	er	er \$\begin{pmatrix} y 7 & y & y & y & y & y & y & y & y & y

Link Status Ta	ab
Status	Shows the current connected AP SSID and MAC address. If there is no connection existing, it will show Disconnected.
Extra Info	Shows the link status and Tx power percentage.
Channel	Shows the current channel in use.
Authentication	Authentication mode used within the network, including Unknown, Open, Shared, WPA-PSK, WPA2-PSK, WPA and WPA2.
Encryption	Shows the encryption type currently in use. Valid value includes WEP, TKIP, AES, and Not Use.
Network Type	Network type in use, Infrastructure for BSS, 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, users can choose to display as percentage or dBm format.
Noise Strength	Shows the noise signal strength in the wireless environment.
Transmit	Shows the current Link Speed and Throughput of the transmit rate.
Receive	Shows the current Link Speed and Throughput of receive rate.
Link Speed	Shows the current transmitting rate and receiving rate.
Throughput	Shows the transmitting and receiving speed of data.

Advanced

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

M Intellig	gent Wireless Ut	tiltiy							
	Profile	Network	ک Advanced	Statistics	WMM	() WPS	Radio On/Off	About	
Wirele	ss mode >>	2.4G	•						
	Enable TX Burst Enable TCP Wind Fast Roaming at	low Size							
11 B)	G >>	ur Country Region	n Code	*					
-	Apply								•

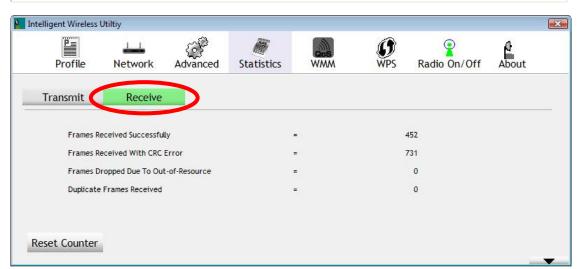
Advanced Tab					
Wireless mode	Here supports 2.4G (included 802.11b/g/n) wireless mode.				
Enable TX Burst	Check to enable this function. This function enables the Wireless LAN USB Adapter to deliver better throughput during a period of time, it only takes effect when connecting with the AP that supports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

Statistics

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

👔 Intelligent Wireless Uti	ltiy							X
Profile	Network	Advanced	Statistics	Gos WMM	() WPS	Radio On/Off	About	
Transmit	Receive							
Frames Tra	Frames Transmitted Successfully				1294			
Frames Ret	transmitted Succ	cessfully	=		1294			
Frames Fail	l To Receive ACK	After All Retries	=		15			
RTS Frames	s Successfully Re	ceive CTS	=		0			
RTS Frames	RTS Frames Fail To Receive CTS			=		0		
Reset Counter								•

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



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

WMM/ QoS

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

Profile	Network	Advanced	Statistics	Gos WMM	WPS	Radio On/Off	About
W Setup Status							
WMM >>	Enabled	Power Save :	> Disabled		D	irect Link >> Disabled	
WA	W Enable						
	WMM - Power Sav	e Enable					
	AC_BK	AC_BE	AC_VI	AC_VO			
	Direct Link Setup	Enable					
	MAC Address >>			Timeout Value >>	60 se	0	
						.Apj	niv.
						Tear	Down

WMM/QoS Tab					
WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.				
WMM- Power Save Enable	 Select a power save mode that preferred. 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 (DLS). This function will be enabled under the connection with AP which must support the DLS function. Direct Link Setup allows direct STA-to-STA frame transfer within a BSS (Basic Service Set). This is designed for consumer use, where STA-to-STA transfer is more commonly used.				
MAC Address	 The setting of DLS(Direct Link Setup) indicates as follow : Fill in the blanks of Direct Link with MAC Address of target STA, and the STA must conform to two conditions: 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.)				
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

Īī

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 Wirele	ess Utiltiy						
Profile	Network	Advanced	Statistics	Gos	W PS	Radio On/	Off About
		w	PS AP List				Constant and
ID :	Cherry	y_test_11n_ Rout	er	00-0C-43-28-60-E0	6	2	Rescan Information
							Pin Code
							30650121 Renew
		WPS	Profile List				Config Mode
Cherry_test_1	1n_Router				7		Enrollee 💌
							Detail
			III			•	Connect
PIN	WPS Associate	IE		Progress >> 100%			Rotate
PBC	WPS Probe IE	PBC - 0	Get WPS profile s	uccessfully.			Disconnect
				10000000000000000000000000000000000000			Export Profile
							Delete

surrounding wireless network.	ID (Device nation on twork. List ype, Config
Password ID), Security-Enabled. Rescan Issue a rescan command to wireless NIC to update inform surrounding wireless network. Information Display the information about WPS IE on the selected ne information included Authentication Type, Encryption Tymethods, Device Password ID, Selected Registrar, State, Locked, UUID-E and RF Bands. General WPS CCX 802.11n	nation on twork. List ype, Config
Rescan Issue a rescan command to wireless NIC to update inform surrounding wireless network. Information Display the information about WPS IE on the selected ne information included Authentication Type, Encryption Ty Methods, Device Password ID, Selected Registrar, State, Locked, UUID-E and RF Bands. General WPS CCX 802.11n	twork. List ype, Config
surrounding wireless network. Information Display the information about WPS IE on the selected ne information included Authentication Type, Encryption Ty Methods, Device Password ID, Selected Registrar, State, Locked, UUID-E and RF Bands. General WPS CCX 802.11n	twork. List ype, Config
Information Display the information about WPS IE on the selected ne information included Authentication Type, Encryption Ty Methods, Device Password ID, Selected Registrar, State, Locked, UUID-E and RF Bands. General WPS CCX 802.11n	ype, Config
information included Authentication Type, Encryption Ty Methods, Device Password ID, Selected Registrar, State, Locked, UUID-E and RF Bands.	ype, Config
information included Authentication Type, Encryption Ty Methods, Device Password ID, Selected Registrar, State, Locked, UUID-E and RF Bands.	ype, Config
Methods, Device Password ID, Selected Registrar, State, Locked, UUID-E and RF Bands.	
Locked, UUID-E and RF Bands.	
General WPS CCX 802.11n	
Authentication Type >> Unknown State >> Configured	
Encryption Type >> None Version >> 1.0	
Config Methods >> 0x0086 AP Setup Locked >>	
Device Password ID >> UUID-E >> 6304125310	192006122800E04C86510
Selected Registrar >> Unknown RF Bands >> Unknown	
Close	
PIN Code 8-digit numbers. It is required to enter PIN Code into Reg	-
PIN method. When STA is Enrollee, users can use "Rene	w" hutton to

	Enrollee or an external Registrar.									
Detail	Click the Detail button to show the information about Security and Key in the credential.									
	Market Intelligent Wireless Utility									
	Profile Network Advanced Statistics WMM WPS Radio On/Off About									
	WPS AP List Rescan ID: Cherry_test_11n_Router 00-E0-4C-86-51-01 7 Information									
	Pin Code 57055251 Renew WPS Profile List Confg Mode									
	Cherry_test_1in_Router									
	PBC - Get WPS profile successfully. Export Porfile Delete									
	SSID >> Cherry test 11n Router									
	SSID >> Cherry_test_11n_Router BSSID >> 00-E0-4C-86-51-01									
	Authentication Type >> OPEN Encryption Type >> NONE Key Length >> Key Index >>									
	Key Material >>									
	Show Password OK Cancel									
	SSID: Shows the connected AP network name.BSSID: The MAC address of the connected AP. Fixed and cannot be changed.									
	Authentication Type : The authentication type support Open, WPA-PSK and WPA2-PSK.									
	Encryption Type: For Open authentication mode, the selection of encryption type are NONE and WEP . For WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES .									
	Key Length: Only valid when using Open authentication mode and WEP encryption. There are key lengths 5, 10, 13 and 26.									
	Key Index: Only valid when using Open authentication mode and WEP encryption. There are 1~4 key index.									
	Key Material: The key material can be used to ensure the security of the wireless network. Fill in the appropriate value or phrase in Key Material field.									
	Show Password: Check this box to show the passwords that have be entered.									
	OK : Click to save and apply the new settings.									
	Cancel: Click to leave and discard the settings.									

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	Registrar : Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in two minutes and get IP address.
	Enrollee : Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address.
РВС	Start to add to AP using PBC (Push Button Configuration) method. Click this button to connect the AP which supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.
connection. If use	ck PIN or PBC, please do not rescan within two minutes of the rs want to stop this setup within the interval, restart PIN/PBC or " to stop WPS action.
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Progress Bar	Display rate of progress from Start to Connected status.
Status Bar	Display currently WPS Status.

Radio On/Off

Click this button to turn on or off radio function.

M Intellig	PLOATES.							E	x
	Profile	Network	Advanced	Statistics	WMM	W PS	Radio On/Off	About	
?	This i	con shows r	adio on, clic	k to turn it o	ff.				
i	This i	con shows r	adio off, clio	ck to turn it o	on.				

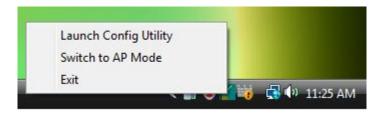
About

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

Profile	Network	Advanced	Statistics	Q.S.	WPS	Radio On/Off	About
	Config Ve	ersion >> 2.1.	5.0		Date >>	06-23-2008	
	Driver Ve	ersion >> 2.2.	1.0		Date >>	07-31-2008	
	EEPROM Ve	ersion >> 1.0		Firmware	Version >>	0.12	
	Phy_Ad	dress >> 00-	12-0E-6B-58-3B				

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 the Wireless LAN USB Adapter act as a wireless AP.
- **Exit**: Select to close the utility program.

SOFT AP MODE

Config

SID Soft Vireless Mode 2.4		Channel 1 <- Use Mac Address Security Set	ting
-Country Region Code- 11 B/G 0: CH1-		No forwarding among wireless clier Hide SSID Allow BW 40 MHz	nts
leacon (ms) 'X Power	100 %		
dle time(60 - 3600)(s)	300		
		Default Cancel Ap	ply

Config	
SSID	AP name of user type. Users also can click Use Mac Address button to display it.
Channel	Manually force the AP using the channel. (The system default is CH 1.)
Wireless Mode	Here supports 2.4G (included 802.11b/g/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.)

	Security Setting
	Authentication Type Open Encryption Type Not Use
	WPA Pre-shared-Key
	Group Rekey Interval 60 10 seconds
	Г Wep Key
	Key#1 Hex ✓
	C Key#2 Hex -
	C Key#3 Hex
	C 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
	Anthentioption Type: There are according to the structure of
	Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/
	WPA2-PSK. (System authentication type default is Open.)
	Encryption Type: For Open and Shared authentication mode, the
	selections of encryption type are Not Use and WEP . For WPA-PSK , WPA2-PSK , and WPA-PSK / WPA2-PSK authentication mode, the
	encryption type supports both TKIP and AES. (System authentication
	type default is Not Use.)
	WPA Pre-shared Key : This is the shared secret between AP and STA.
	For WPA-PSK and WPA2-PSK and WPA-PSK/WPA2-PSK authentication mode, this field must be filled with character longer than 8
	and less than 64 lengths.
	Group Re-key Interval: Only valid when using WPA-PSK, WPA2-PSK,
	and WPA-PSK/ WPA2-PSK authentication mode to renew key. Users can set to change by seconds or packets. (Default is 600 seconds.)
	WEP Key : Only valid when using WEP encryption algorithm. The key must match with the AP's key. There are four formats to enter the keys.
	• ASCII (64 bits): 5 ASCII characters (case sensitivity).
	 ASCII (128 bits): 13 ASCII characters (case sensitivity). Hexadecimal (64 bits): 10 Hex characters (0~9, a~f).
	 Hexadecimal (04 bits): 10 Hex characters (0~9, a~f). Hexadecimal (128 bits): 26 Hex characters (0~9, a~f).
	Show Password: Check this box to show the passwords that have been
	entered.
Beacon (ms)	The time between two beacons. (The system default is 100 ms.)
TX Power	Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and Lowest. (The system default is 100%.)
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. (Default value of idle time is 300 seconds.)

No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. (The system default is no forwarding.)
Hide SSID	Do not display AP name. (System default no hide.)
Allow BW 40MHz	 Click to disable this function. (System default is enabled.) This function enables the adapter to deliver better throughput, enable this function the link speed will up to 300Mbps, disable this function the link speed will up to 150Mbps only. Note: This function depends on the capability of device. Here supports link speed up to 150Mbps only, DO NOT support link speed up to 300Mbps.
Default	Use the system default value.
Apply	Click to apply the above settings.

Access Control

YIIII Intelligent Wireless Ut	ility		X
Config Access Control	Mac Table Event L	og Statistics About	
Access Policy		Disable	-
MAC Address		- Access List	
	Add		
	Delete		
	Remove All	1	
			Apply
-			

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

MAC Table

MAC Address	AID	Power S	Charles	
MAC Address	AID	Fower 5	Judius	
٠ III				,

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	
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.

Statistics

Config Act	cess Control Mac Table Event Log	Statistics About	
- Transmit	Statistics		
	es Transmitted Successfully	=	331
Fram	es Fail To Receive ACK After All Retries	=	0
RTS	Frames Successfully Receive CTS	=	0
RTS	Frames Fail To Receive CTS	=	0
Fram	es Transmitted Successfully After Retry	=	0
Receive	Statistics		
Fran	nes Received Successfully	=	206
Fran	nes Received With CRC Error	=	123
Fran	nes Dropped Due To Out-of-Resource	=	0
Dup	licate Frames Received	=	0
			RESET COUNTERS

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

Duplicate Frames Received	The number of duplicate packets received.
Reset Counter	Reset counters to zero.

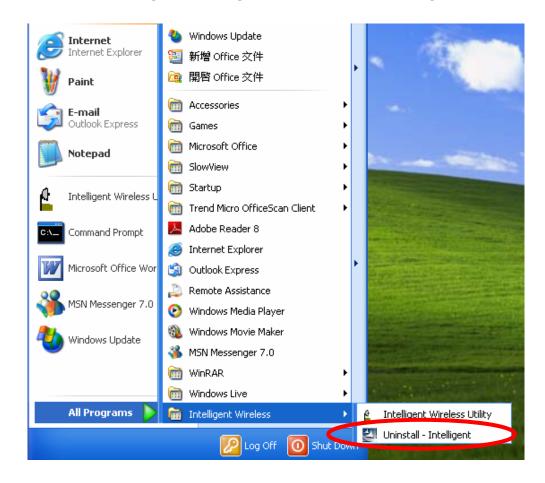
About

This page displays the Wireless LAN USB Adapter and driver version information.

Utility Version :	2.0.5.0	Date :	06-23-2008
Driver Version :	2.2.1.0	Date :	07-31-2008
EEPROM Version :	1.0	Firmware Version :	0.12
IP Address :	192.168.123.1	Phy_Address :	00-12-0E-6B-58-3B
Sub Mask :	255.255.255.0	Default Gateway :	0.0.0

CHAPTER 4: UNINSTALLATION FOR WINDOWS 2000/XP

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

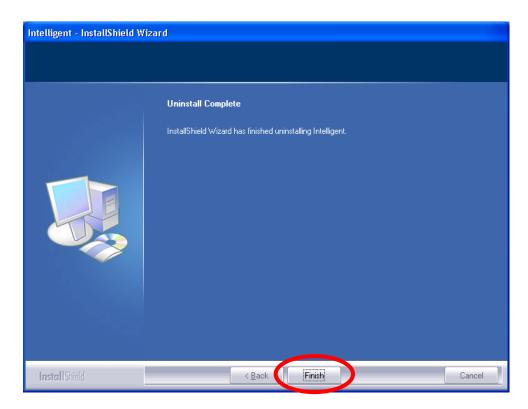


1. Go to Start →All Programs →Intelligent Wireless → Uninstall –Intelligent.

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



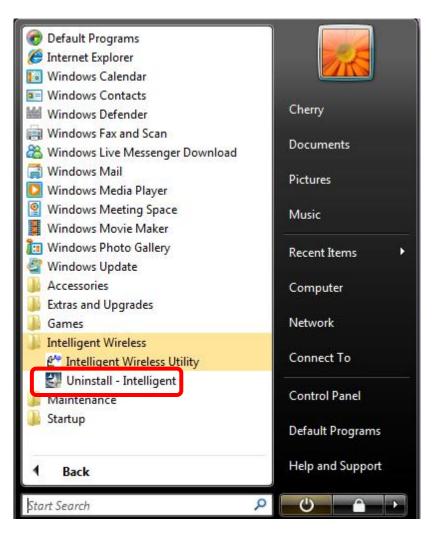
3. Then click **Finish** to complete the uninstallation.



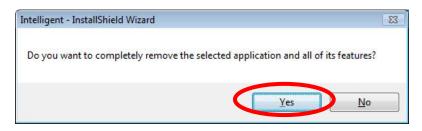
FOR WINDOWS VISTA

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

1. Go to Start → Programs →Intelligent Wireless → Uninstall –Intelligent.



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



Caution:

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



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

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

Free Manuals Download Website <u>http://myh66.com</u> <u>http://usermanuals.us</u> <u>http://www.somanuals.com</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.cc</u> <u>http://www.4manuals.com</u> <u>http://www.404manual.com</u> <u>http://www.luxmanual.com</u> <u>http://aubethermostatmanual.com</u> Golf course search by state

http://golfingnear.com Email search by domain

http://emailbydomain.com Auto manuals search

http://auto.somanuals.com TV manuals search

http://tv.somanuals.com