



Users Manual

Mvix Nubbin

802.11n Wireless USB2.0 Adapter

SPECIFICATIONS

Standards	IEEE 802.11 b/g/n standards compliant
Antenna	Chip antenna (2dBi) *1 (Peak Gain)
Supported OS	Windows 2000, XP, Vista, Mac OS, Linux OS
Security	WEP 64/128, WPA, WPA2
Frequency Range	802.11b/g/n USA (FCC): 2.412GHz ~ 2.462GHz Europe (ETSI): 2.412GHz ~ 2.472 GHz Japan (TELEC): 2.412GHz ~ 2.472GHz
Selectable Channels	802.11b/g/n: USA (FCC) 11 channels; EU (ETSI) 13 channels; Japan (TELEC) 13 channels
Data Rate	802.11b: 1, 2, 5.5, 11Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps 802.11n(20MHz):MCS0~7, up to 72.22Mbps 802.11n(40MHz):MCS0~7, up to 150Mbps
Transmit Power (EIRP)	802.11b : 16+/-1.5 dBm (Typical) 802.11g : 12+/-1.5 dBm (Typical) Wireless-N : 12+/-1.5 dBm (Typical)
Receiver Sensitivity	11b 11Mbps :-76dBm 11g 54Mbps :-65dBm 11n-HT20 72.22Mbps :- 62dBm 11n-HT40 150Mbps :-59dBm
Physical Specifications Environment Specifications	Weight : 2.7 g Dimension : 30.0(L)*14.00(W)*7.0(H) mm Operating Temp : 0° to 45° Operating Humidity : 10% to 90% Non- Condensing
Power Requirement	DC 5V
Certifications:	FCC, CE
Model No	MS-811N



Supports Wi-Fi Multimedia
QoS
(WMM® and WMM-PS®)

Small, Unobtrusive Size
Protrudes less than 2cm
from USB Port

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. Other channel Selections are 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:

This device is in compliance with the essential requirement and other relevant provisions of the R&TTE Directive 1999/5/EC.

Table of Contents

CHAPTER 1: INTRODUCTION	4
FEATURES	4
CHAPTER 2: INSTALLATION	5
FOR WINDOWS 2000/XP	5
Installing Software	5
Installing Hardware	7
FOR WINDOWS VISTA	9
Installing Software	9
Installing Hardware	10
INSTALLATION VERIFICATION	8
NETWORK CONNECTION	11
IP Address	11
CHAPTER 3: UTILITY CONFIGURATION	12
FOR WINDOWS 2000/XP	12
Station Model	13
Profile	14
Network	19
Link Status	22
Advanced	23
Statistics	24
WMM / QoS	26
WPS	27
Radio On/Off	29
Utility Menu List	31
Soft AP Mode	32
Config	32
Access Control	35
MAC Table	36
Event Log	37
Statistics	38
FOR WINDOWS VISTA	39
Station Model	40
Profile	40
Network	45
Link Status	48
Advanced	49
Statistics	50
WMM / QoS	51
WPS	52
Radio On/Off	54
Utility Menu List	55
Soft AP Mode	56
Config	56
Access Control	58
MAC Table	59
Event Log	60
Statistics	60
CHAPTER 4: UN INSTALL DRIVER and APPLICATION	62

Chapter I

Introduction

Mvix Nubbin (MS-811N) is an IEEE802.11b/g/n mini-size USB adapter that can connect notebook, handheld or desktop PC equipped with USB2.0 interface to a wireless-N network. It brings the freedom of staying connected to the network at blazing-fast Wireless-N speeds while maintaining access to the Internet, e-mail, networked applications, and print services. The “nubbin” is a perfect companion for your notebook -providing access to the internet-enabled world anytime - anywhere.

The MS-811N fully complies with IEEE 802.11n draft 3.0 and IEEE 802.11b/g standards, delivering reliable, cost-effective, feature rich, wireless connectivity at high throughput from an extended distance. It supports WMM and WMM-PS (IEEE802.11e QoS standard) and has an innovative, built-in, WPS (Wi-Fi Protected Setup) feature which auto-builds a connection between the wireless router (access-point) and.

Features

- USB2.0 Wireless-N (150Mbps) Adapter
- Mini-footprint, Protrusion: Less than 2cm
- Compliance: IEEE 802.11n draft 3.0, IEEE 802.11b/g
- Supports WMM and WMM-PS (IEEE 802.11e QoS Standard)
- Innovative WPS (Wi-Fi Protected Setup) - auto-builds connection, synchronizes settings.
- Reliable, cost-effective, wireless connectivity at high throughput

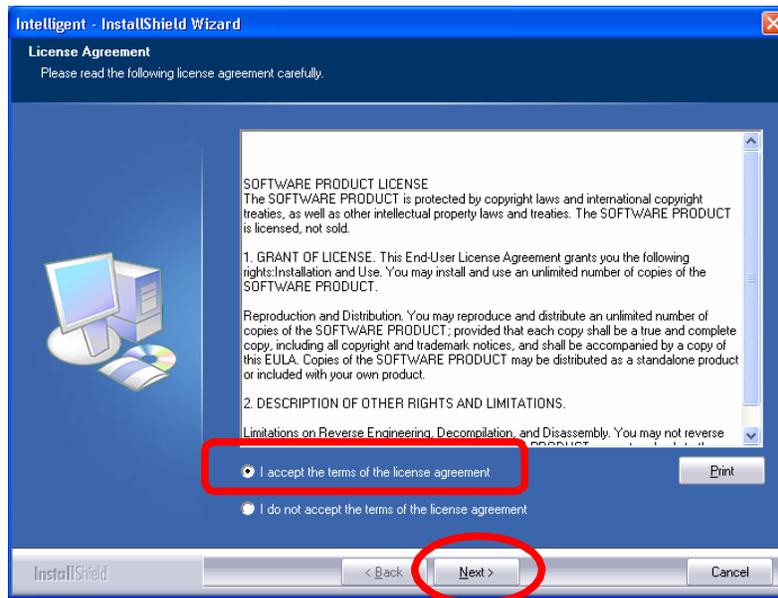
Chapter 2:

Installation

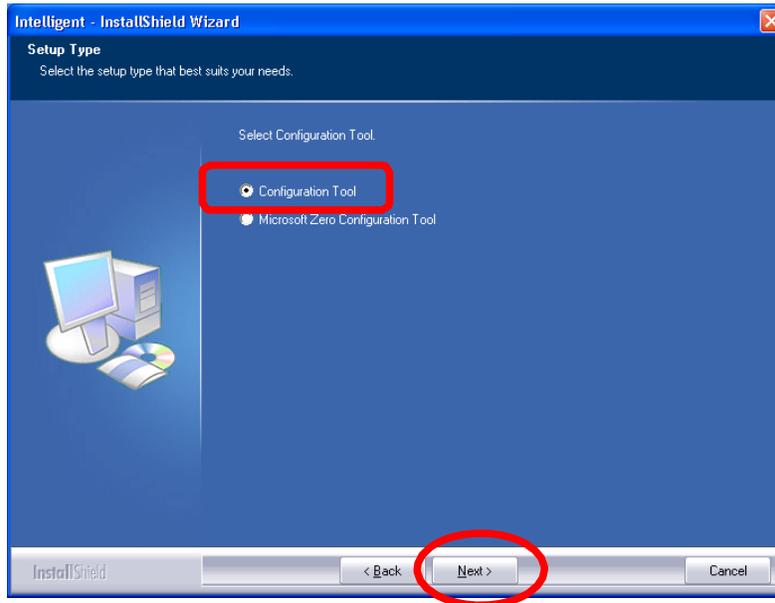
For Windows 2000/XP Installing Software

Note: Do not insert the Wireless LAN USB Adapter into your computer until the Install Shield Wizard has finished installing the software.

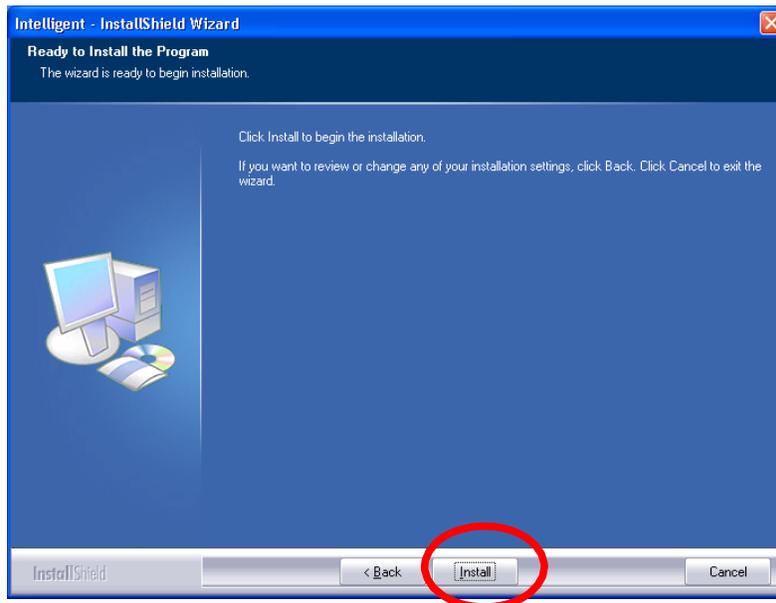
1. Exit all Windows programs. Insert the included Installation CD into the computer. The SETUP application will run automatically.
2. The License Agreement screen appears as below, please read the contents and select “I accept the terms of the license agreement “ then click **Next** to continue.



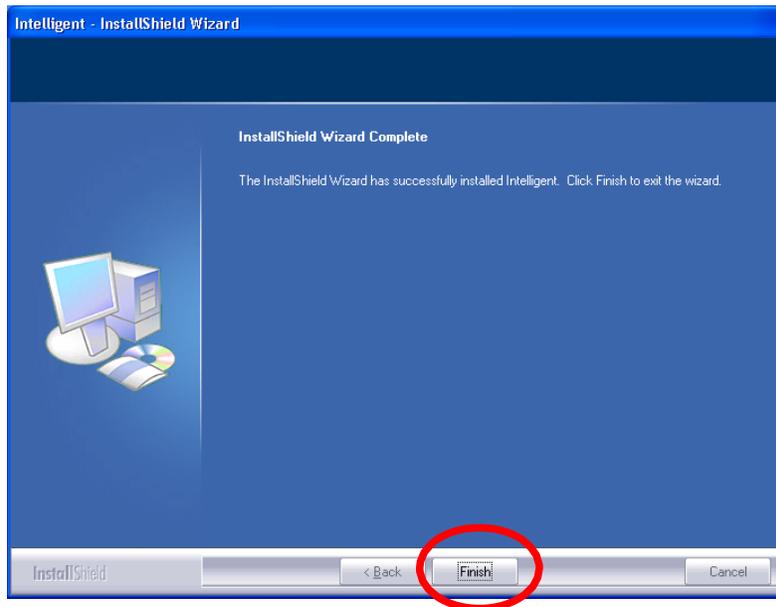
3. Select the check box to choose a Configuration Tool from the listed two choices.
- Configuration Tool: Choose to use the configuration utility.
 - Microsoft Zero Configuration Tool: Choose to use Windows XP's built-in Zero Configuration Utility (ZCU). Click **Next** to continue.



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



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



For Windows 2000/XP Installing Hardware

Note: Insert the Mvix Nubbin (MS-811N) Wireless LAN USB Adapter when software installation is completed.

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 has been correctly installed in your computer.

Go to

Start >

Setting >

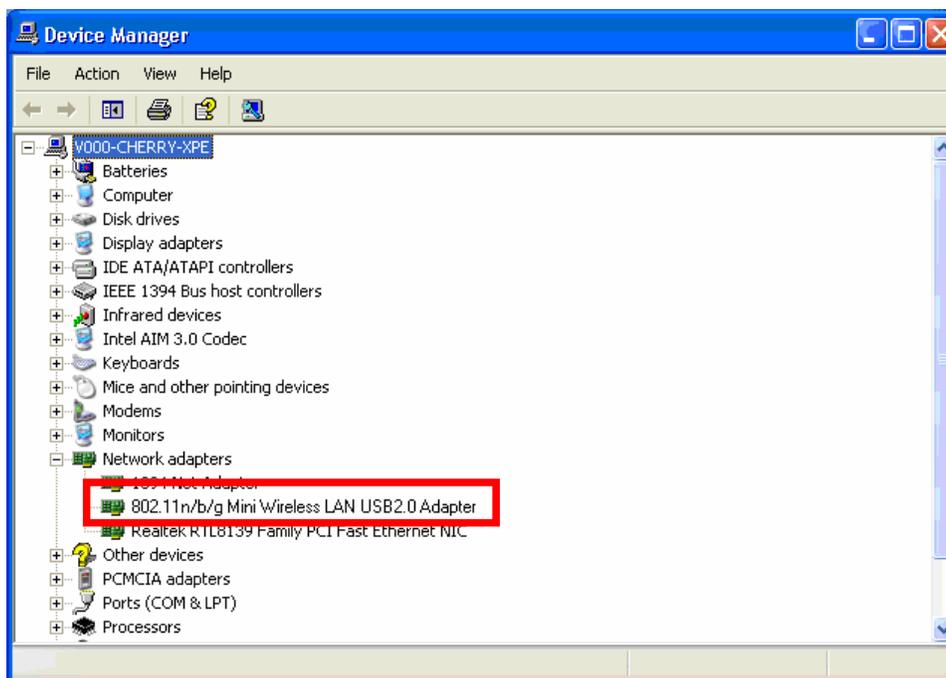
Control Panel >

System >

Hardware >

Device Manager.

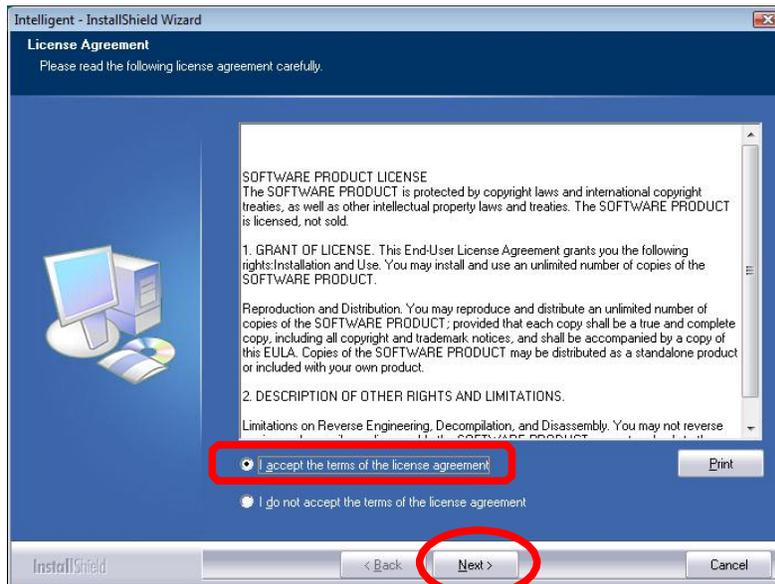
Expand the Network Adapters category. If the 802.11n/b/g Mini Wireless LAN USB2.0 Adapter is listed here, it means that the device is properly installed and enabled.



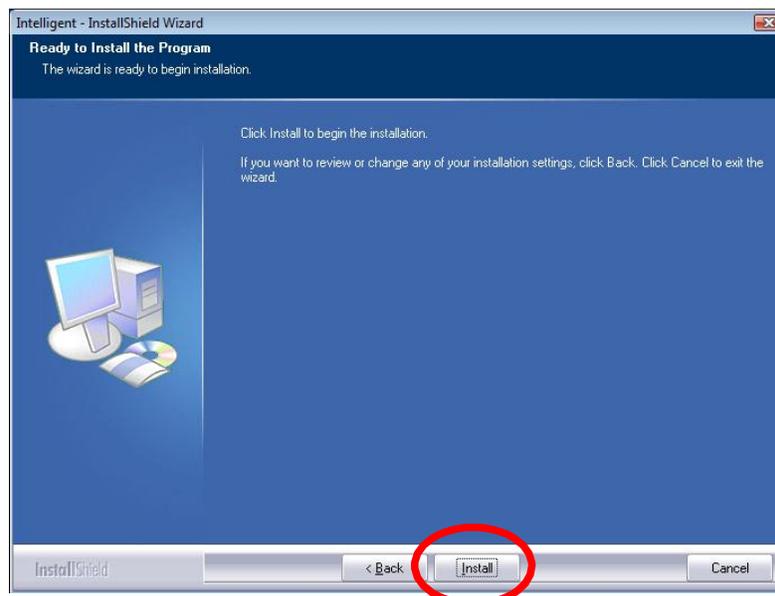
For Windows Vista Installing Software

Note: Do not insert the Wireless LAN USB Adapter into your computer until the Install Shield Wizard has finished installing the software.

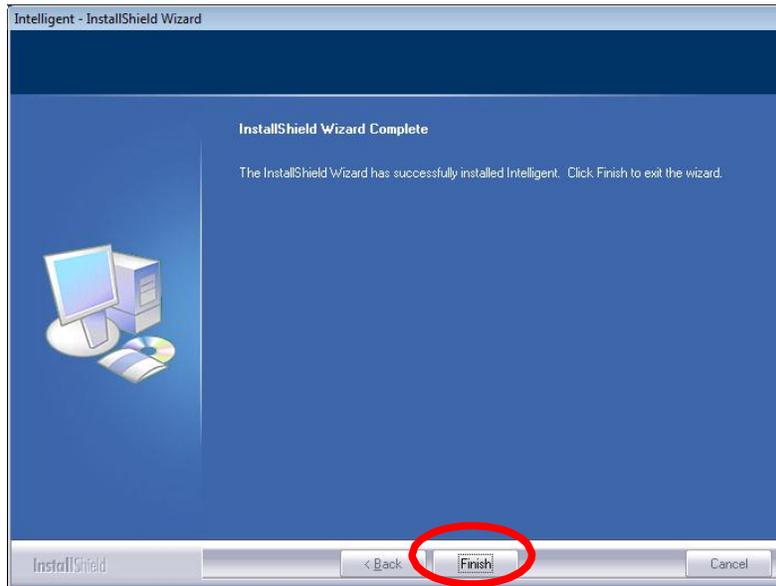
1. Exit all Windows programs. Insert the included Installation CD into the computer. The SETUP application will run automatically.
2. The License Agreement screen appears as below, please read the contents and select "I accept the terms of the license agreement " then click **Next** to continue.



3. When prompt, click Install to begin the installation.



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



For Windows 2000/XP Installing Hardware

Note: Insert the Mvix Nubbin (MS-811N) Wireless LAN USB Adapter when software installation is completed.

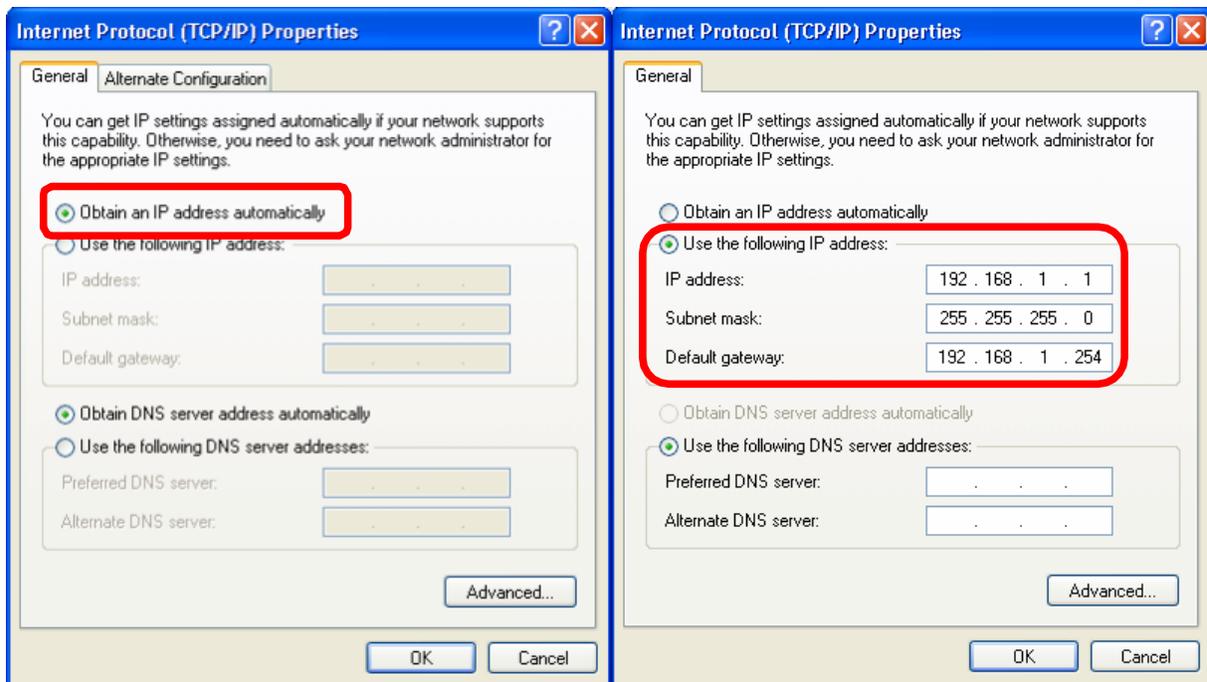
Insert the Wireless LAN USB Adapter into the USB Port of the computer. The system will automatically detect the new hardware.

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 DHCP server is enabled on your broadband Router), check the **Obtain an IP address automatically** option.
2. 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

192.168.1.110 in the IP address field,
255.255.255.0 for the Subnet Mask, and
192.168.1.1 for the default gateway.



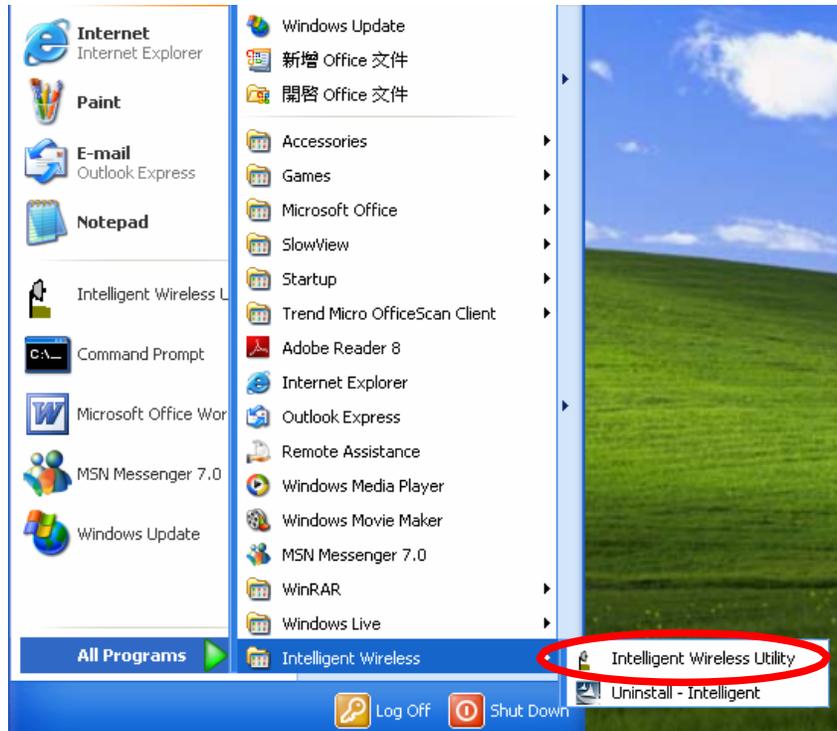
Chapter 3:

Utility Configuration

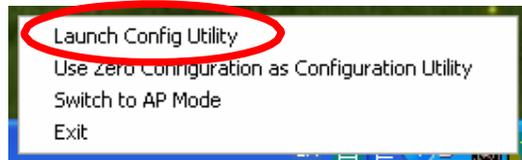
For Windows 2000/XP

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

Go to Start > (All) Program > Intelligent Wireless > 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**.



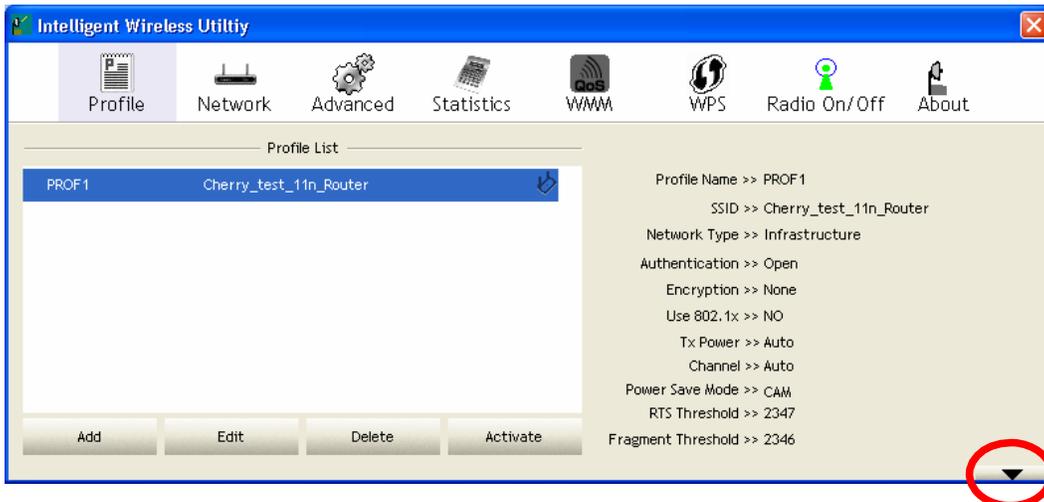
Station Mode

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 allows users to record their favorite wireless settings for home, office, and other public hot-spot. Users may save multiple profiles. 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	Use 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.

Click to add a profile from the drop-down screen.

System Configuration tab:

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 of modes:

Infrastructure and **Ad-hoc**. 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.

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.

Power Save Mode: Select between CAM (Constantly Awake Mode) or PSM (Power Saving Mode).

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

Add

exceeds the values that have been set. This value should remain at its default setting of 2347. Should users encounter inconsistent data flow, only minor modifications of this value are recommended.

Fragment Threshold: Users can adjust the Fragment threshold number by sliding the bar or key in the value directly. (The default value is 2346.) The mechanism of Fragmentation Threshold is used to improve the efficiency when high traffic flows along in the wireless network. If the Wireless LAN 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 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.

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

LEAP: Light Extensible Authentication Protocol. It is an EAP authentication type used primarily in Cisco Aironet WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication (only with CCX mode enabled.)

WPA/ WPA-PSK/ WPA2/ WPA2-PSK: WPA or WPA-PSK authentications offer two encryption methods, TKIP and AES. For WPA-PSK, select the type of algorithm TKIP or AES and then enter a WPA Shared Key of 8-64 characters in the WPA Pre-shared Key field.

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

WEP Key: Only valid when using WEP encryption algorithm. The key must match with the AP's key. There

are four formats to enter the keys.

ASCII (64 bits): 5 ASCII characters (case sensitivity).

ASCII (128 bits): 13 ASCII characters (case sensitivity).

Hexadecimal (64 bits): 10 Hex characters (0~9, a~f).

Hexadecimal (128 bits): 26 Hex characters (0~9, a~f).

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

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

802.1x tab:

EAP Method:

PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.

TLS / Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

TTLS: Tunnelled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

EAP-FAST: Flexible Authentication via Secure Tunnelling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-

band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication now.

MD5-Challenge: Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network. (Only Open and Shared authentication mode can use this function.)

Tunnel Authentication:

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

Tunnel Identity: Identity for tunnel.

Tunnel Password: Password for tunnel.

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

ID/PASSWORD tab:

The screenshot shows the 'System Config' dialog box with the 'Auth. \ Encry.' tab selected. The 'EAP Method' is set to 'PEAP' and 'Tunnel Authentication' is set to 'EAP-MSCHAP v2'. The 'ID \ PASSWORD' tab is active, showing fields for 'Authentication ID / Password' (Identity, Password, Domain Name) and 'Tunnel ID / Password' (Tunnel ID, Tunnel Password, Show Password). The 'Session Resumption' checkbox is unchecked. 'OK' and 'Cancel' buttons are at the bottom.

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.

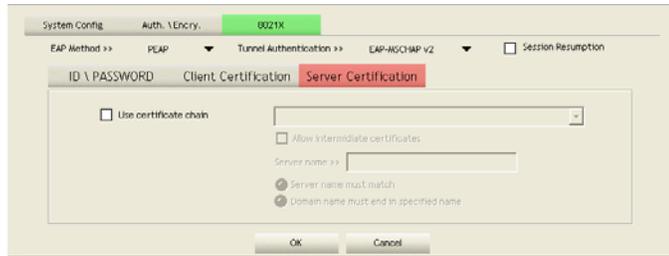
Client Certification tab:

The screenshot shows the 'System Config' dialog box with the 'Auth. \ Encry.' tab selected. The 'EAP Method' is set to 'PEAP' and 'Tunnel Authentication' is set to 'EAP-MSCHAP v2'. The 'Client Certification' tab is active, showing a 'Use Client certificate' checkbox and a dropdown menu. Below the dropdown are fields for 'Issued To', 'Issued By', 'Expired On', and 'Friendly Name'. The 'Session Resumption' checkbox is unchecked. 'OK' and 'Cancel' buttons are at the bottom.

Use Client certificate: Choose to enable server authentication.

OK: Click to save settings and exit this page.
Cancel: Click to call off the settings and exit.

Server Certification tab:



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

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

Server name: Enter an authentication sever.

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

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

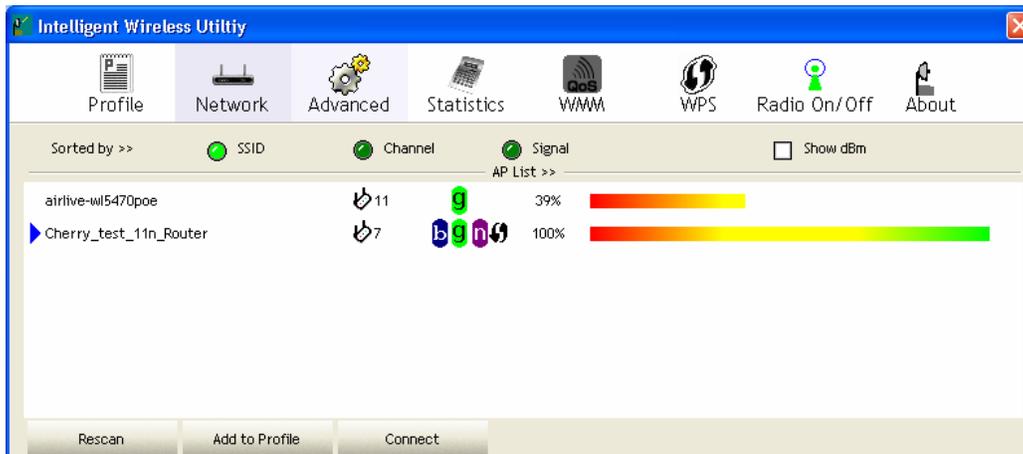
OK: Click to save settings and exit this page.

Cancel: Click call off the settings and exit

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

Network

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



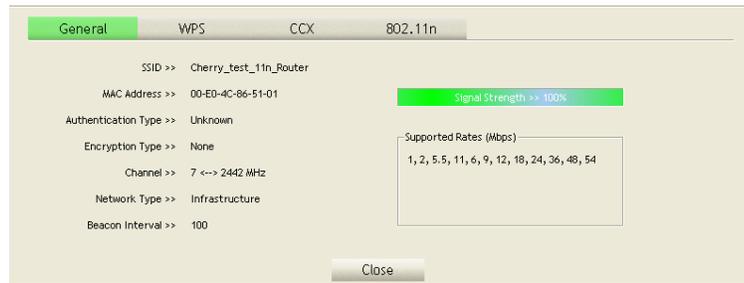
Network Tab

Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.
Show dBm	Check the box to show the dBm of the AP list.
SSID	Shows the name of BSS network.
Network Type	Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS
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
Connect	Select an item (SSID) on the list and then click to make a

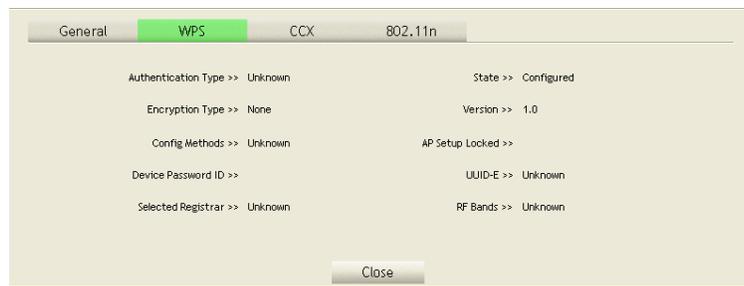
Access Point (AP) Information

Double click on the intended AP to see detailed information about that specific Access Point

General



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



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

WPS

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."

CCX



CCX information contains CCKM, Cmic and Ckip information.

802.11n



This tab will show up if the selected access point supports 11n mode. Here shows the connected access point 802.11n related information.

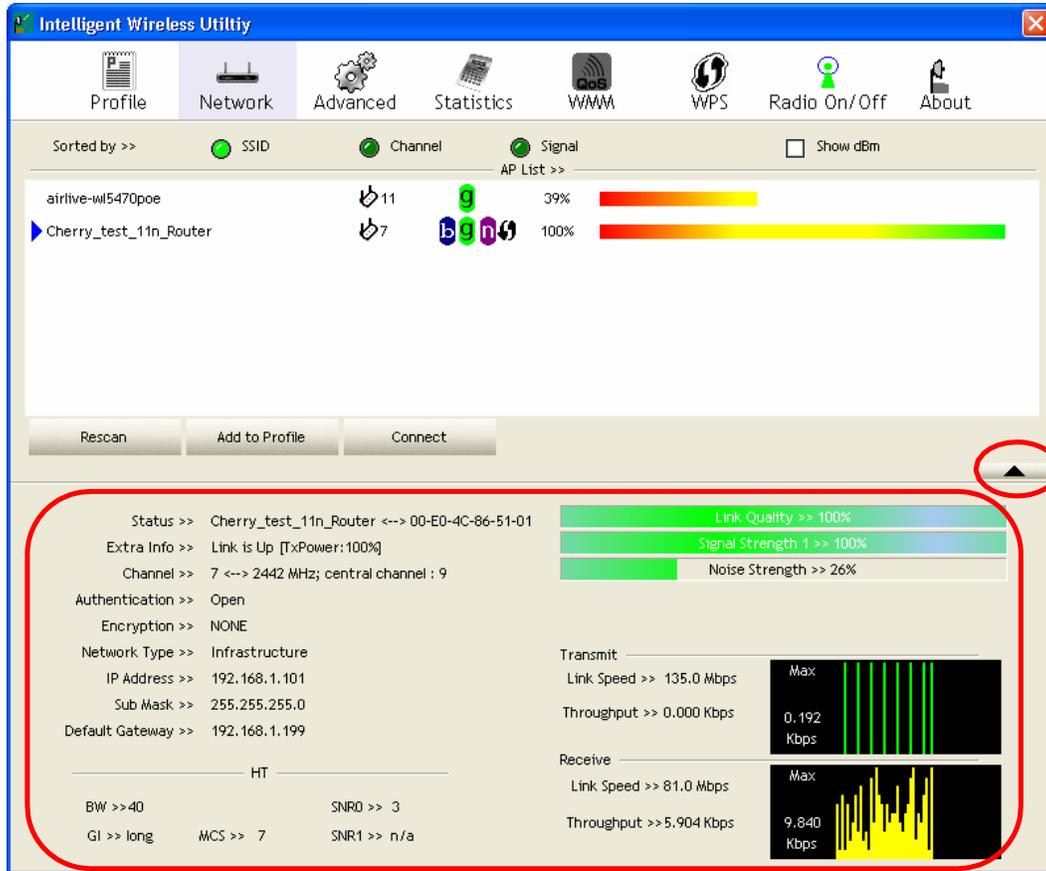
Link Status

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.

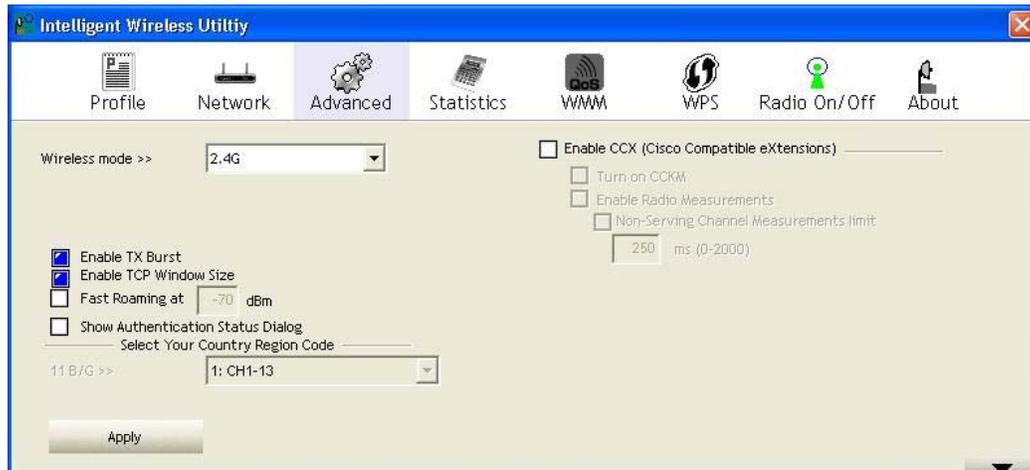
▲ Click this button to hide the information of Status Section.

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



Advanced

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



Advanced Tab

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

Statistics

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

The screenshot shows the 'Intelligent Wireless Utility' application window. The 'Statistics' tab is selected in the top navigation bar. Below the navigation bar, there are two buttons: 'Transmit' (highlighted with a red circle) and 'Receive'. The main area displays a table of statistics:

Frames Transmitted Successfully	=	30836
Frames Retransmitted Successfully	=	30836
Frames Fail To Receive ACK After All Retries	=	174
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0

At the bottom left, there is a 'Reset Counter' button.

Transmit

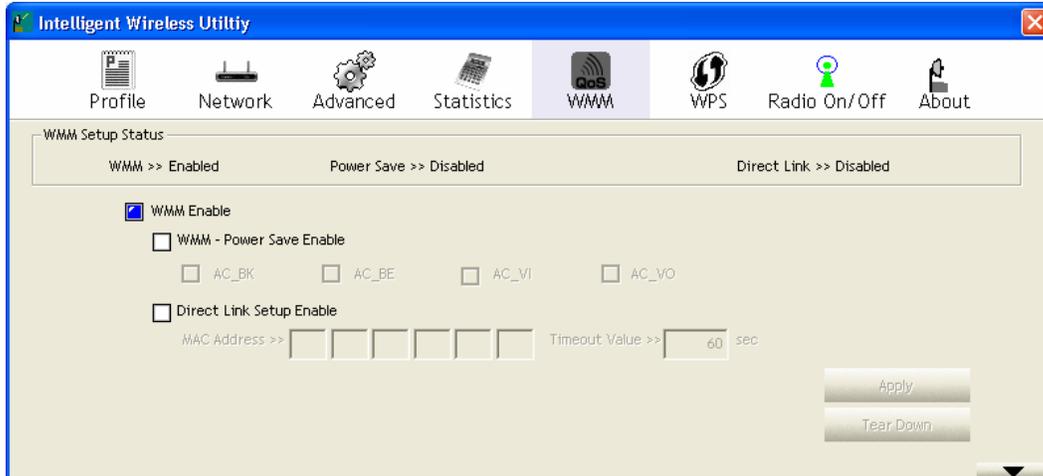
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Retransmitted Successfully	Shows information of packets successfully sent with one or more retries.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.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

Receive Statistics

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

WMM/ QoS

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

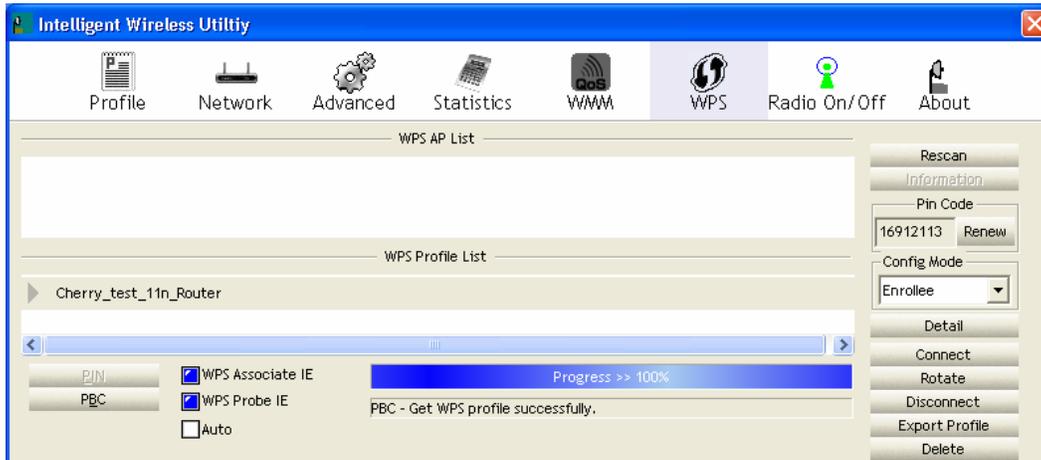


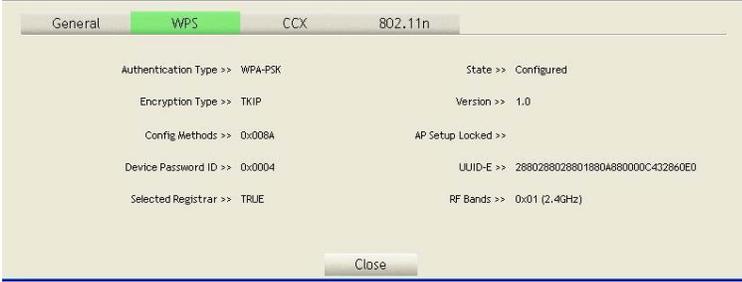
WMM/QoS Tab

WMM Enable	Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.
WMM- Power Save Enable	<p>Select a power save mode that preferred.</p> <ul style="list-style-type: none"> • 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	<p>The setting of DLS(Direct Link Setup) indicates as follow :</p> <p>Fill in the blanks of Direct Link with MAC Address of target STA, and the STA must conform to two conditions:</p> <ul style="list-style-type: none"> • 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.)
Tear Down	Select a direct link STA MAC address, then click "Tear Down" button to disconnect the STA.

WPS

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



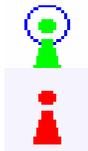
WPS Tab	
WPS AP List	Display the information of surrounding APs with WPS IE from last scan result. List information included SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.
Rescan	Issue a rescan command to wireless NIC to update information on surrounding wireless network.
Information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

Detail	<p>Click the Detail button to show the information about Security and Key:</p> <p>If selected the AP that listed in the WPS Profile List field, users can click the Detail button to see more AP information.</p> <p><i>SSID</i>: Shows the connected AP network name.</p> <p><i>BSSID</i>: The MAC address of the connected AP. Fixed and cannot be changed.</p> <p><i>Authentication Type</i>: The authentication type support Open, WPA-PSK and WPA2-PSK.</p> <p><i>Encryption Type</i>: 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.</p> <p><i>Key Length</i>: Only valid when using Open authentication mode and WEP encryption. There are key lengths 5, 10, 13 and 26.</p> <p><i>Key Index</i>: Only valid when using Open authentication mode and WEP encryption. There are 1~4 key index.</p> <p><i>Key Material</i>: 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.</p> <p><i>Show Password</i>: Check this box to show the passwords that have been entered</p>
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 a Profile File.
Delete	Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.
PIN	<p><i>Registrar</i>: Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in two minutes and get IP address.</p> <p><i>Enrollee</i>: Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the</p>

	device will connect to AP in two minutes and get IP address.
PBC	Start to add to AP using PBC (Push Button Configuration) method. Click this button to connect the AP which supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously.
<i>Note:</i> After the users click PIN or PBC, please do not rescan within two minutes of the connection. If users want to stop this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action.	
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Auto	Check this box the device will connect the AP automatically.

Radio On/Off

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

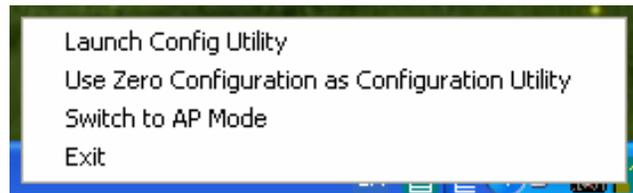


This icon shows radio on, click to turn it off.

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

Utility Menu List

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



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

Soft AP Mode

Config

The screenshot shows the 'Intelligent Wireless Utility' window with the 'Config' tab selected. The configuration fields are as follows:

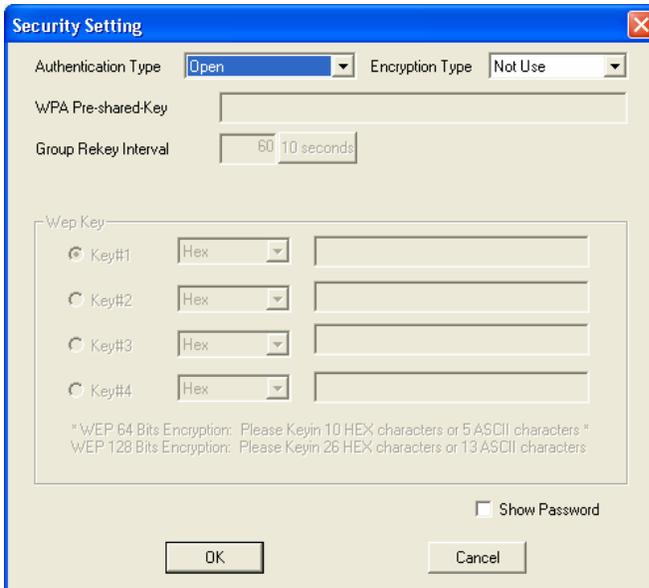
- SSID: SoftAP
- Channel: 1
- Wireless Mode: 2.4G
- Country Region Code: 11 B/G, 0: CH1-11
- Beacon (ms): 100
- TX Power: 100 %
- Idle time(60 - 3600)(s): 300

Checkboxes and buttons:

- No forwarding among wireless clients
- Hide SSID
- Allow BW 40 MHz
- Tx BURST
- Buttons: < Use Mac Address, Security Setting, Default, Cancel, Apply

SSID	AP name of user type. Users also can click Use Mac Address button to display it.
Channel	Manually Configure the AP using the channel. (The system default is CH 1.)
Wireless Mode	Support for 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.

Authentication mode and encryption algorithm used within the AP. (The system default is no authentication and encryption.)



Security Setting

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.)

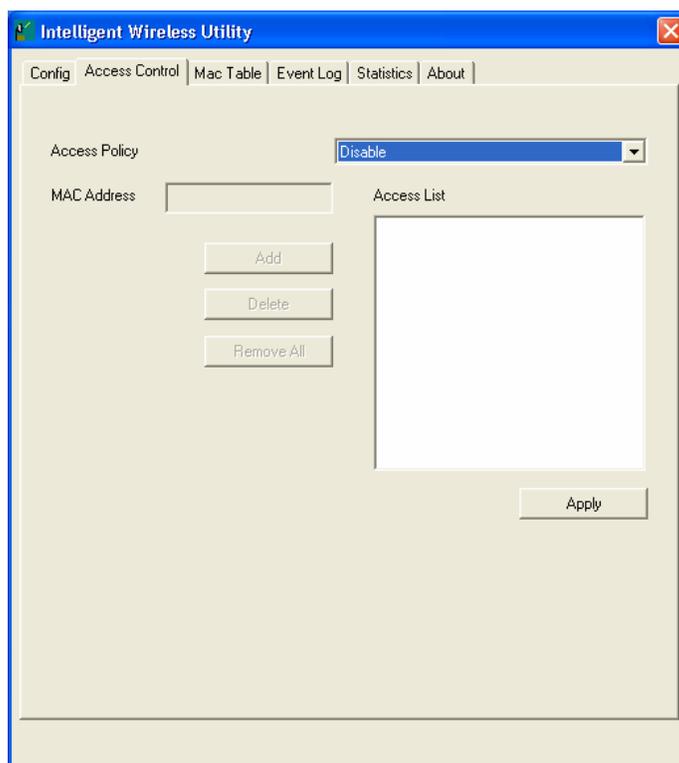
WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK and WPA-PSK/ WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 64 lengths.

Group Re-key Interval: Only valid when using WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK authentication mode

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.)
	Click to disable this function. (System default is enabled.)
Allow BW 40MHz	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. This function depends on the capability of device. Currently speed up to 150Mbps is supported (DOES 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.

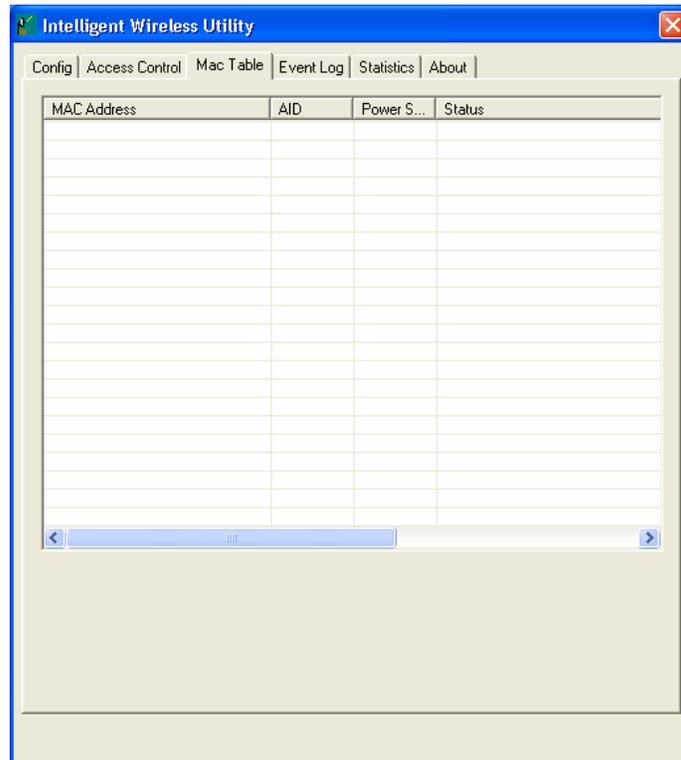
Access Control



Access Control

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

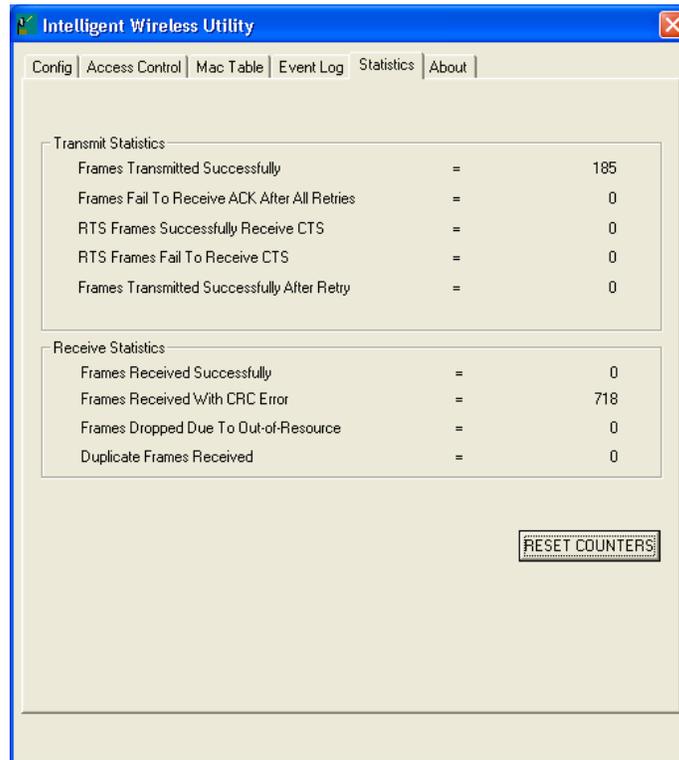
MAC Table



MAC Table

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

Statistics



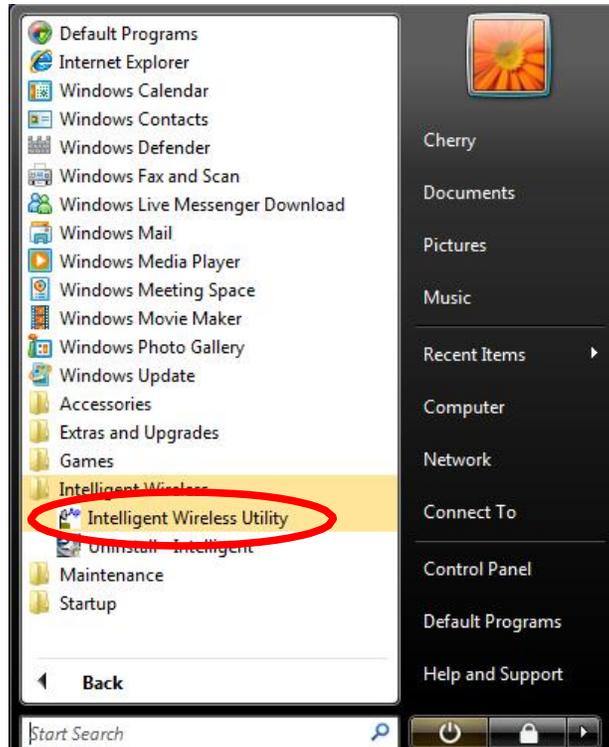
Duplicate Frames Received The number of duplicate packets received.

Reset Counter Reset counters to zero.

For Windows Vista

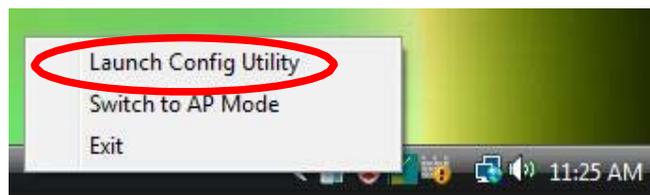
After successful installation of the Mvix Nubbing (MS-811N) Wireless-N LAN USB Adapter, Configuration the Wireless Connection Utility to set preference.

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.



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. Click to add a profile from the drop-down screen.

System Configuration tab:

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.

- 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.

Add

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. The RTS/CTS mechanism will be activated if the data size exceeds the value that have been set. This value should remain at its default setting of 2347. Should users encounter inconsistent data flow, only minor modifications of this value are recommended.

Fragment Threshold: Users can adjust the Fragment threshold number by sliding the bar or key in the value directly. (The default value is 2346.) The mechanism of Fragmentation Threshold is used to improve the efficiency when high traffic flows along in the wireless network. If the Wireless LAN 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:

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

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

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

WPA/ WPA-PSK/ WPA2/ WPA2-PSK: WPA-PSK offers two encryption methods, TKIP and AES. Select the type of algorithm, TKIP or AES and then enter a WPA Shared Key of 8-63 characters in the WPA Pre-shared Key field.

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

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

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

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

- Hexadecimal (128 bits): 26 Hex characters (0~9, a~f).

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

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

802.1x tab:

EAP Method:

PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunnelling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.

TLS / Smart Card: Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.

Tunnel Authentication:

- Protocol: Tunnel protocol, List information including
- EAP-MSCHAP v2 and EAP-TLS/ Smart Card.
- Tunnel Identity: Identity for tunnel.
- Tunnel Password: Password for tunnel.
- Session Resumption: Reconnect the signal while broken up, to reduce the packet and improve the transmitting speed. Users can click the box to enable or disable this function

ID / PASSWORD Tab:

The screenshot shows a configuration window titled '802.1x' with tabs for 'ID / PASSWORD', 'Client Certification', and 'Server Certification'. The 'ID / PASSWORD' tab is active. It contains two main sections: 'Authentication ID / Password' and 'Tunnel ID / Password'. The 'Authentication ID / Password' section has three input fields: 'Identity', 'Password', and 'Domain Name'. The 'Tunnel ID / Password' section has three input fields: 'Tunnel ID', 'Tunnel Password', and a checkbox labeled 'Show Password'. At the bottom of the window are 'OK' and 'Cancel' buttons.

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.

Client Certification tab:

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

Server Certification tab:



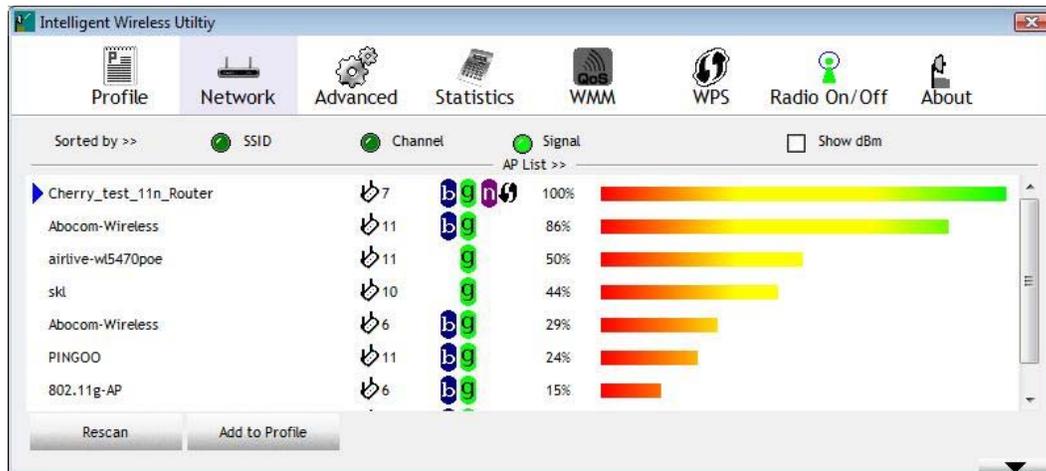
Use certificate chain: Choose use server that issuer of certificates.

Server name: Enter an authentication sever name.

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

Network

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



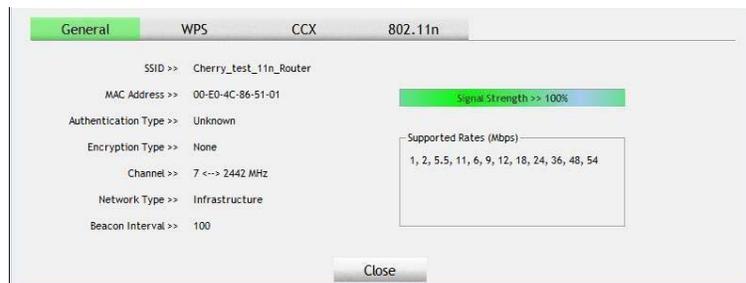
Network Tab

Sorted by	Indicate that AP list are sorted by SSID, Channel or Signal.
Show dBm	Check the box to show the dBm of the AP list.
SSID	Shows the name of BSS network.
Network Type	Network type in use, Infrastructure for BSS, 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: General, WPS, CCX and 802.11n

General



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

WPS

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".

CCX

CCX information contains CCKM, Cmic and Ckip information.

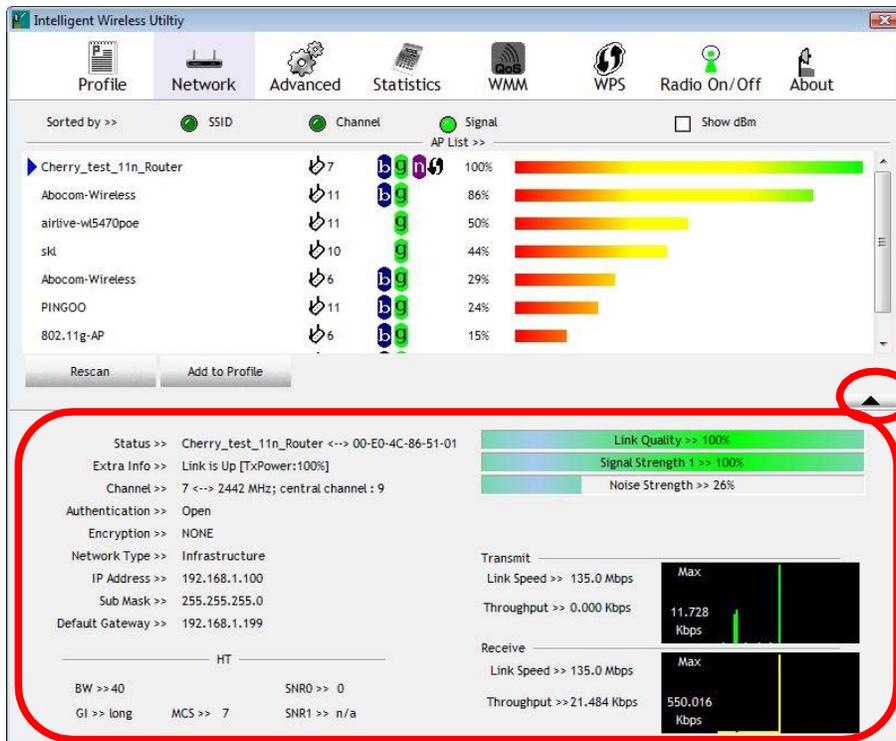
802.11n

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.



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

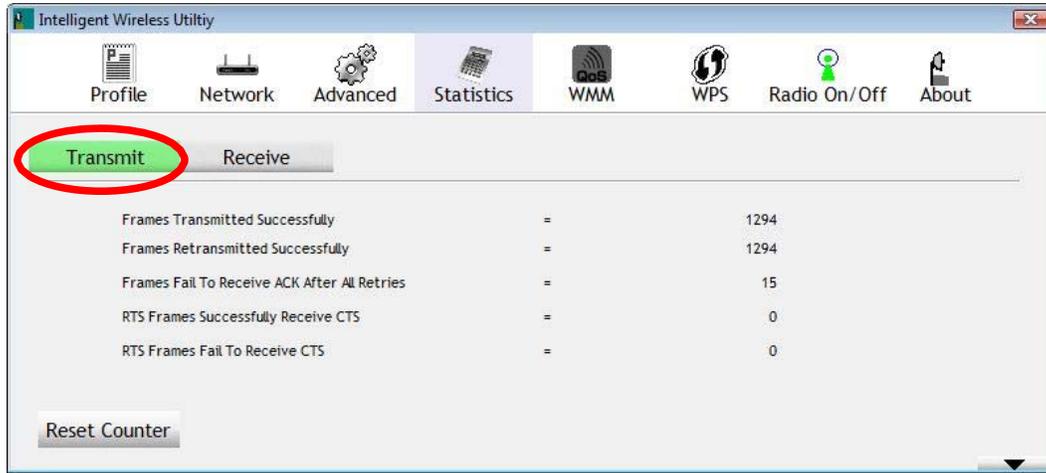
Advanced

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

Advanced Tab	
Wireless mode	Here supports 2.4G (included 802.11b/g/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.



Transmit Statistics Tab

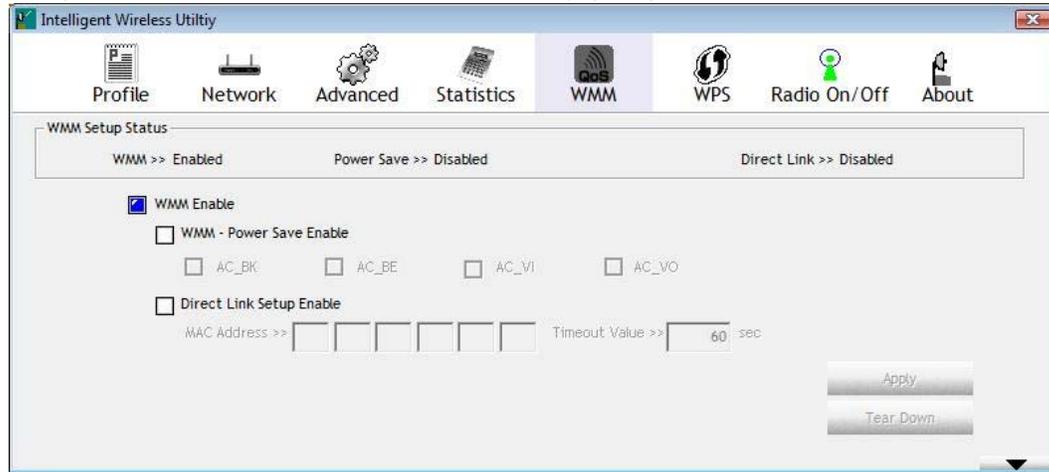
Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Retransmitted Successfully	Shows information of packets successfully sent with one or more retries.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.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

Receive Statistics Tab

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

WMM/ QoS

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



WMM / QoS Tab

WMM Enable

Check the box to enable Wi-Fi Multi-Media function that is meant to improve audio, video and voice applications transmitted over Wi-Fi.

WMM- Power Save Enable

Select a power save mode that preferred.

- 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

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

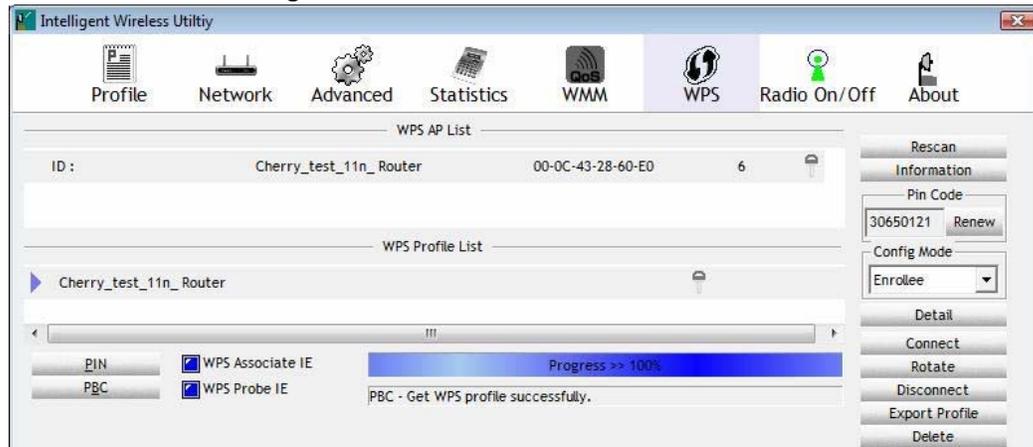
Click this button to apply the settings.

Tear Down

Select a direct link STA, then click "Tear Down" button to disconnect the STA.

WPS

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



WPS Tab

WPS AP List

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

Rescan

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

Information

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



PIN Code

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

Config Mode

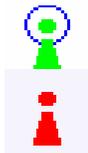
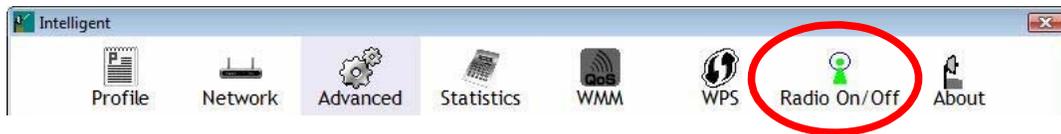
Select from the pull-down menu to decide the station role-playing as an Enrollee or an external Registrar.

Detail	<p>Click the Detail button to show the information about Security and Key in the credential. Click the Detail button to see more AP information.</p> <p><i>SSID</i>: Shows the connected AP network name.</p> <p><i>BSSID</i>: The MAC address of the connected AP. Fixed and cannot be changed.</p> <p><i>Authentication Type</i>: The authentication type support Open, WPA-PSK and WPA2-PSK.</p> <p><i>Encryption Type</i>: 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.</p> <p><i>Key Length</i>: Only valid when using Open authentication mode and WEP encryption. There are key lengths 5, 10, 13 and 26.</p> <p><i>Key Index</i>: Only valid when using Open authentication mode and WEP encryption. There are 1~4 key index.</p> <p><i>Key Material</i>: 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.</p> <p><i>Show Password</i>: Check this box to show the passwords that have been entered.</p>
Connect	Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.
Rotate	Command to rotate to connect to the next network inside credentials.
Disconnect	Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page. If there is an empty profile page, the driver will select any non-security AP.
Export Profile	Export all credentials to Profile.
Delete	Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP
PIN	<p><i>Registrar</i>: Add the AP's PIN code into the PIN code column, and press the device PIN button. It will connect with the AP in two minutes and get IP address.</p> <p><i>Enrollee</i>: Input the device's PIN code into the PIN code column of AP. Start AP WPS process and click device PIN button. Then, the device will connect to AP in two minutes and get IP address.</p>

PBC	Start to add to AP using PBC (Push Button Configuration) method. Click this button to connect the AP which supported WPS function within two minutes. Meanwhile, the AP should also click the PBC button simultaneously
<i>Note: After the users click PIN or PBC, please do not rescan within two minutes of the connection. If users want to stop this setup within the interval, restart PIN/PBC or click "Disconnect" to stop WPS action</i>	
WPS Associate IE	Send the association request with WPS IE during WPS setup. It is optional for STA.
WPS Probe IE	Send the probe request with WPS IE during WPS setup. It is optional for STA.
Progress Bar	Display rate of progress from Start to Connected status
Status Bar	Display currently WPS Status

Radio On/Off

Click this button to turn on or off radio function.

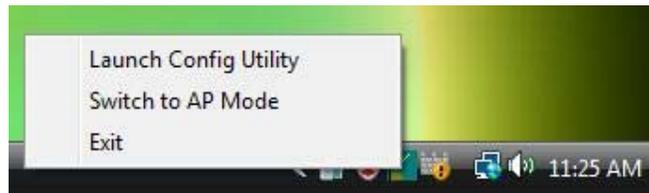


This icon shows radio on, click to turn it off.

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

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 Model

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.

The screenshot shows a 'Security Setting' dialog box with the following fields and options:

- Authentication Type:** Open (selected)
- Encryption Type:** Not Use (selected)
- WPA Pre-shared-Key:** [Empty text field]
- Group Rekey Interval:** 60 10 seconds
- Wep Key:** Four entries (Key#1 to Key#4), each with a 'Hex' dropdown and an empty text field.
- Show Password:** [Unchecked checkbox]
- Buttons:** OK and Cancel

Footnote text at the bottom of the dialog:

- * 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.

Security Settings

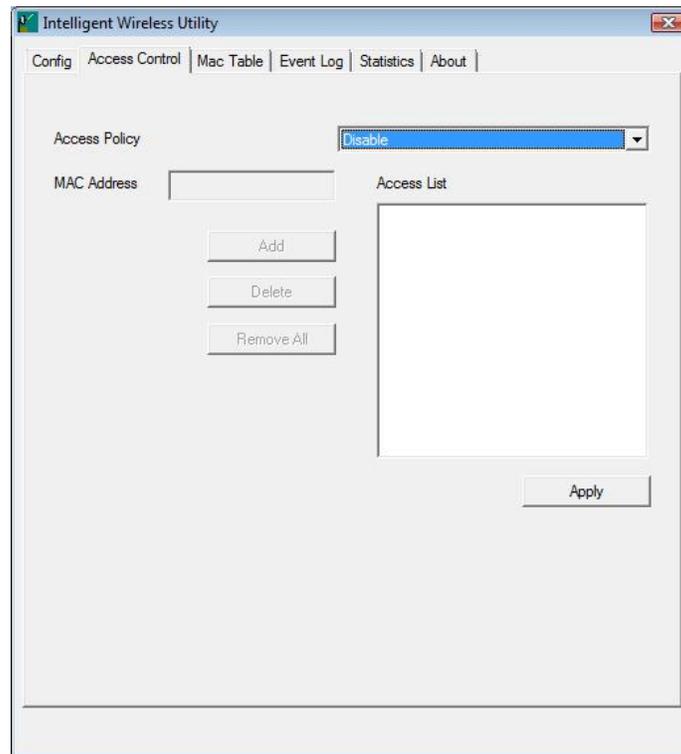
Authentication Type: There are several types of authentication modes including Open, Shared, WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK. (System authentication type default is Open.)

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. <ul style="list-style-type: none"> • ASCII (64 bits): 5 ASCII characters (case sensitivity). • ASCII (128 bits): 13 ASCII characters (case sensitivity). • Hexadecimal (64 bits): 10 Hex characters (0~9, a~f). • Hexadecimal (128 bits): 26 Hex characters (0~9, a~f).
	Show Password: Check this box to show the passwords that have been entered.
Beacon (ms)	The time between two beacons. (The system default is 100 ms.)
TX Power	Manually force the AP transmits power from the pull down list 100%, 75%, 50%, 25% and Lowest. (The system default is 100%.)
Idle time(60-3600)(s)	It represents that the AP will idle after few seconds. The time must be set between 60~3600 seconds. (Default value of idle time is 300 seconds.)
No forwarding among wireless clients	No beacon among wireless client, clients can share information each other. (The system default is no forwarding.)
Hide SSID	Do not display AP name. (System default no hide.)
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. <i>Supported link speed up to 150Mbps onl. Mvix Nubbin MS-811N, DOES NOT support link speed of 300Mbps.</i>
Default	Use the system default value.
Apply	Click to apply the above settings.

Access Control



Access Control

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

Access Policy

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

MAC Address

Manually force the Mac address using the function. Enter the MAC address in the column and click **Add** button, then the MAC address will be listed in the Access List pool.

Access List

Display all MAC Address that users have set.

Add

Add the MAC address that users would like to set.

Delete

Delete the MAC address that users have set.

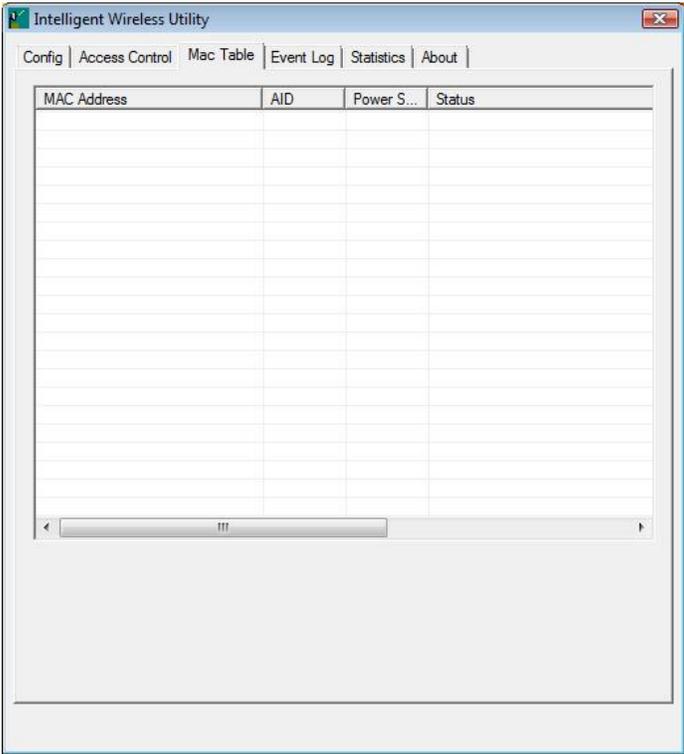
Remove All

Remove all MAC address in the Access List.

Apply

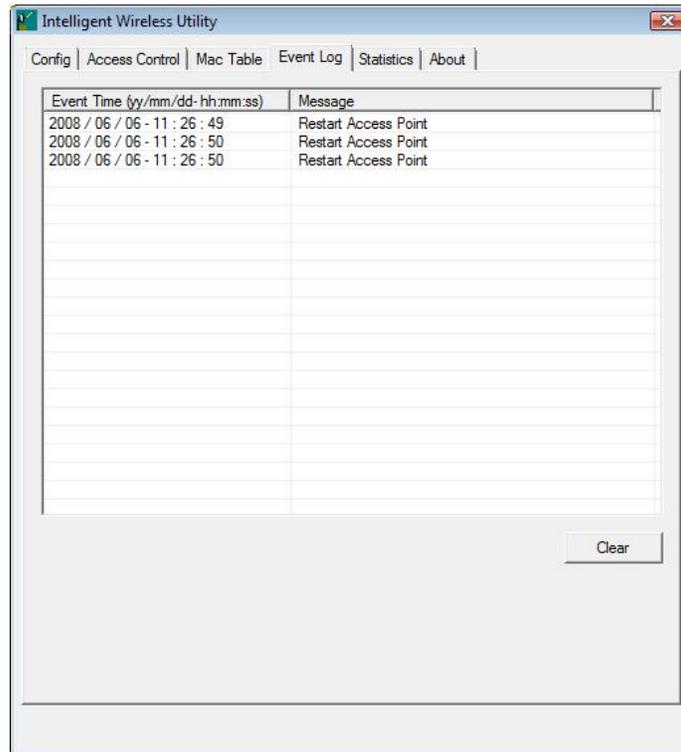
Apply the above changes.

MAC Table

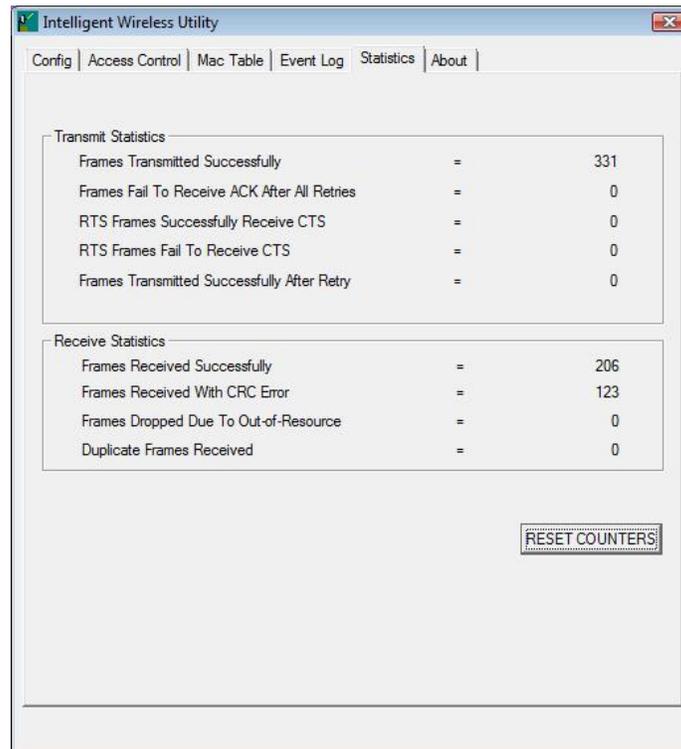


MAC Table	
MAC Address	The station MAC address of current connection.
AID	Raise value by current connection.
Power Saving Mode	The station of current connect whether it have to support.
Status	The status of current connection.

Event Log



Statistics



Transmit Statistics

Frames Transmitted Successfully	Shows information of packets successfully sent.
Frames Fail To Receive ACK After All Retries	Shows information of packets failed transmit after hitting retry limit.
RTS Frames Successfully Receive CTS	Shows information of packets successfully receive CTS after sending RTS.
RTS Frames Fail To Receive CTS	Shows information of packets failed to receive CTS after sending RTS.
Frames Transmitted Successfully After Retry	Shows information of packets successfully sent with one or more retries.

Receive Statistics

Frames Received Successfully	Shows information of packets received successfully.
Frames Received With CRC Error	Shows information of packets received with CRC error.
Frames Dropped Due To Out-of-Resource	Shows information of packets dropped due to resource issue.
Duplicate Frames Received	The number of duplicate packets received.
Reset Counter	Reset counters to zero.

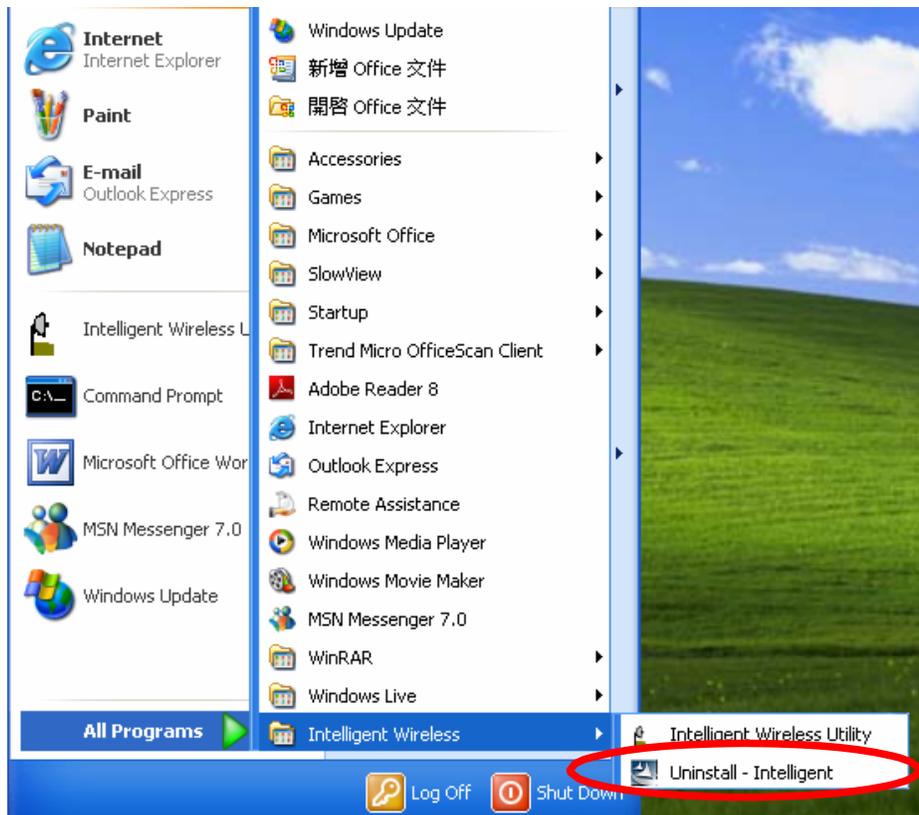
Chapter 4:

Uninstall Driver and Utility / Application

For Windows 2000/XP

To uninstall the utility and driver, please refer to steps below. (Driver is deleted automatically during un-installation of Utility / Application)

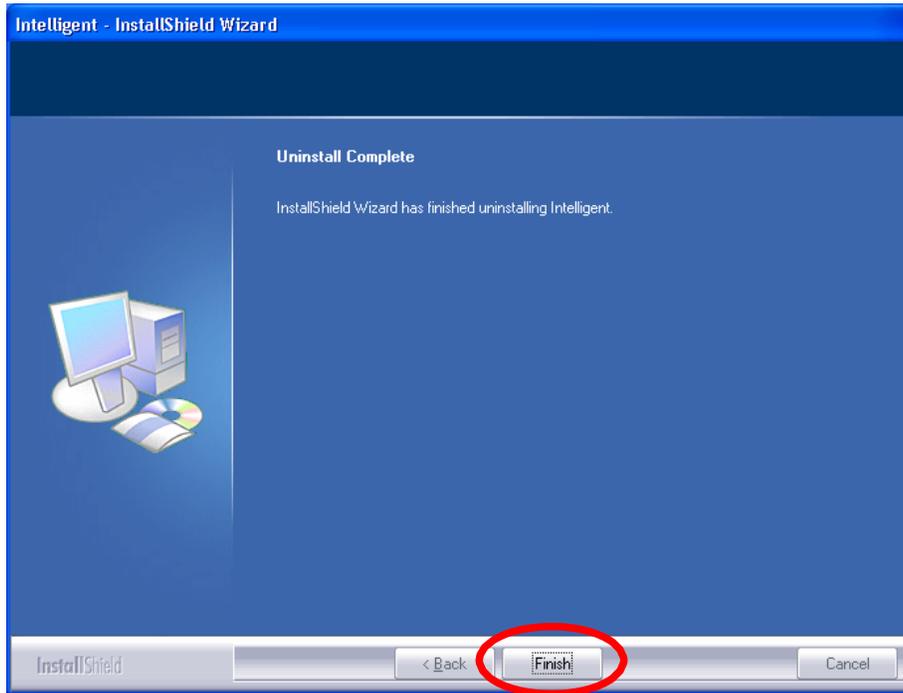
1. Go to Start > All Programs > Intelligent Wireless > Uninstall –Intelligent.



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



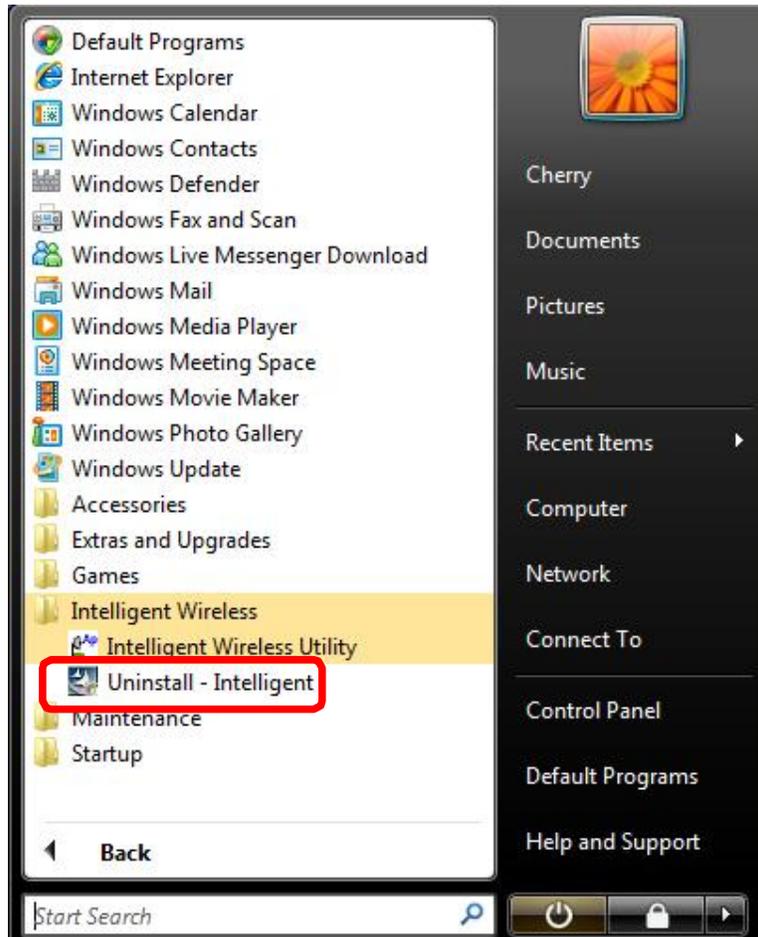
3. Then click Finish to complete the uninstallation process.



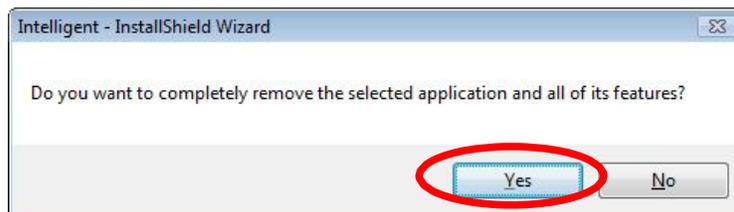
For Windows Vista

To uninstall the utility and driver, please refer to steps below. (Driver is deleted automatically during un-installation of Utility / Application)

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



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

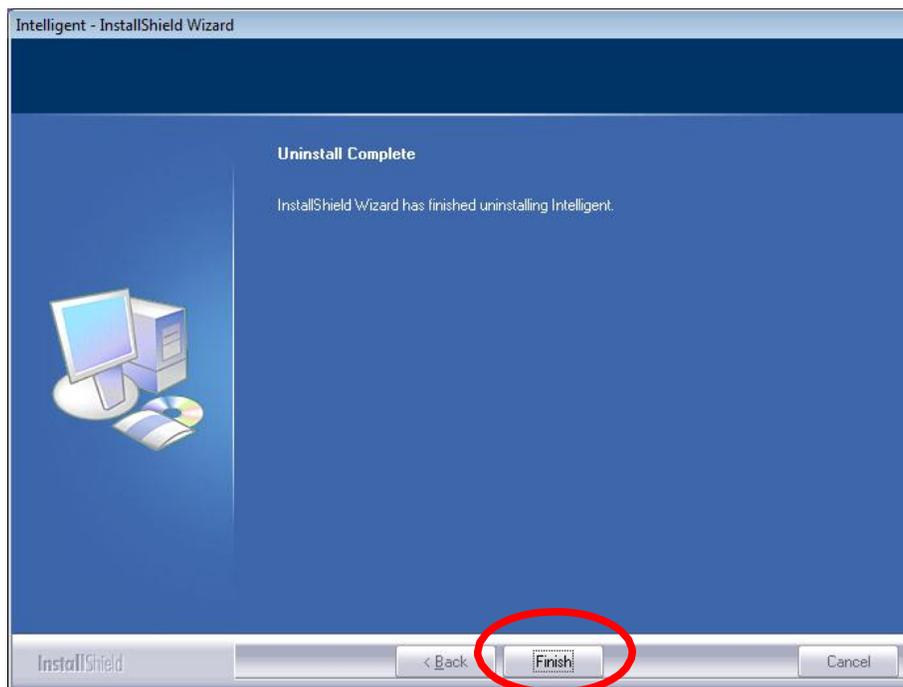


Caution:

During Un-installation process on Microsoft Vista 64-bit OS, the following popup request to insert Wireless LAN USB Adapter:.



3. Finally, click Finish to complete the uninstallation.



Limited Warranty

The Mvix Nubbin MS-811N Wireless-N USB2.0 Adapter comes with a full 1-yr manufacturer's warranty on parts and labor. The Warranty coverage on this player begins the day you buy your product. This warranty covers defects in manufacturing only, and expressly excludes coverage for excessive wear and tear, physical or accidental abuse, loss and theft. Kindly contact your local distributor for the warranty and service procedures. Warranty service is available in all countries where the product is officially distributed. The warranty covers any service or exchange required for a defective unit during the coverage period. The service / exchange opportunity ends one year after the date of purchase. The replacement product is covered only for the warranty period of the original product. When the warranty on the original product expires, the warranty on all replaced products also expires. When it is necessary for you to ship the product to distributor / service center for service / exchange, you will pay the shipping costs for shipment to the distributor. The distributor will pay the shipping costs when returning the product to you.

To receive warranty service, please be sure to have your proof of purchase and a barcode from the product's packaging. Warranty requests cannot be processed without proof of purchase. In no event shall MvixUSA's (or its distributors') liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its software, or its documentation.

MvixUSA does not offer refunds for any product. As a part of our warranty service, we offer to repair or replace the product. We offer cross shipments, a faster process for processing and receiving your replacement. MvixUSA and its distributor pay for ground shipping only. Please contact MvixUSA's Distributor in your country for more details.

Specifically, your warranty does not cover the following:

- Shipping charges to return defective product.
- Labor charges for installation or setup of the product, adjustment of customer controls on the product, and installation or repair of systems outside of the product.
- Product repair and/or part replacement because of improper installation, connections to improper voltage supply, abuse, neglect, misuse, accident, unauthorized repair or other cause not within our control.
- Damage occurring to product during shipping when improperly packaged or cost associated with packaging.
- Incidental or consequential damages resulting from the product.

Some states do not allow the exclusion of incidental or consequential damages, so the above exclusion may not apply to you. This includes, but is not limited to, prerecorded material, whether copyrighted or not.) Mvix(USA), Inc. and its other partners and distributors DO NOT assume any responsibility in any way for how you choose to use this product, associated firmware and this manual. By purchasing or receiving this product, you automatically agree to this disclaimer, and eliminate this company and any affiliates of any responsibility in this matter.

MvixUSA or ITS DISTRIBUTORS ARE NOT LIABLE UNDER ANY CIRCUMSTANCES FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, HOWSOEVER INCURRED, EVEN IF NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. TO THE EXTENT PERMITTED BY LOCAL LAW, THE REMEDIES PROVIDED IN THIS WARRANTY STATEMENT ARE YOUR SOLE AND EXCLUSIVE REMEDY. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE/PROVINCE TO STATE/PROVINCE.

REMEMBER...Please record below the model and serial numbers found on the product.

MODEL # _____

SERIAL # _____

Trademark and Legal Attributions

The trademarks of Mvix® and MvixUSA® are used in connection with products and services to signify the quality and excellence for which MvixUSA® is known.

Mvix® and MvixUSA® are trademarks or registered trademarks of Mvix(USA), Inc. in the United States. You may use a Mvix® trademark or product name to refer specifically to such Mvix® product in marketing and promotional materials, books, conferences, applications, demonstrations, and so on. You are permitted to use a Mvix® trademark referentially provided that:

- * You adhere to these Mvix™ Trademark Usage Guidelines.
- * You do not disparage Mvix(USA), Inc. or its products and services.
- * You display your name or logo more prominently than any Mvix™ trademark.
- * You include a disclaimer that Mvix™ does not sponsor, affiliate, or endorse your product, and/or services.

All other textual references, brands, logos or product names are the copyrights, trademarks or registered trademarks of their respective owners /holders. Use of these trademarks on our website, products, literature, communications, manuals, advertising material, press releases, etc. do not represent endorsements by the respective companies for Mvix(USA), Inc.'s products, services or brand, but merely reflect their possible compatibility with our products.

- Google is a trademark of Google Technology, Inc.
- HDMI is a trademark of HDMI Licensing LLC.
- iPod® is a registered trademark of Apple Computer, Inc.
- PSP™ (PlayStation Portable) is a trademark of Sony Computer Entertainment Inc.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Vista are trademarks of Microsoft Corporation.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- WI-FI, WPA, WPA2 and WMM are registered trademarks of Wi-Fi Alliance.

REFERENCES TO CORPORATIONS, THEIR SERVICES, PRODUCTS and BRANDS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL MVIX(USA), INC. BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS INFORMATION.

MVIX Products are not officially licensed or certified by DivX® Networks or Wifi Alliance.

Any MvixUSA, Inc. publication may include technical inaccuracies or typographical errors. The information presented here is intended for general information only and is subject to change without notice. ALL INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU.

Contact Information

Mvix(USA), Inc.

www.mvixusa.com

Tel. 866 . 310 . 4923
Fax 866 . 614 . 3880

sales@mvixusa.com

Technical Support: <http://support.mvixusa.com>