Wireless Mini PCI Adapter
WL561MSI

Manual

FCC Information

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

1. This device may not cause harmful interference.
2. This device must accept any interference received; including interference that may cause undesired operation.

Federal Communications Commission (FCC) 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 or more 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 RF Radiation Exposure Statement:

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

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

End Product Labeling

This transmitter module is authorized only for use in devices where the antenna may be installed such that 20 cm may be maintained between the antenna and users (for example access points, routers, wireless ADSL modems, and similar equipment). The final end product must be labeled in visible area with the following:
“Contains TX FCC ID: PBLWL561MSI”

End Product Manual Information

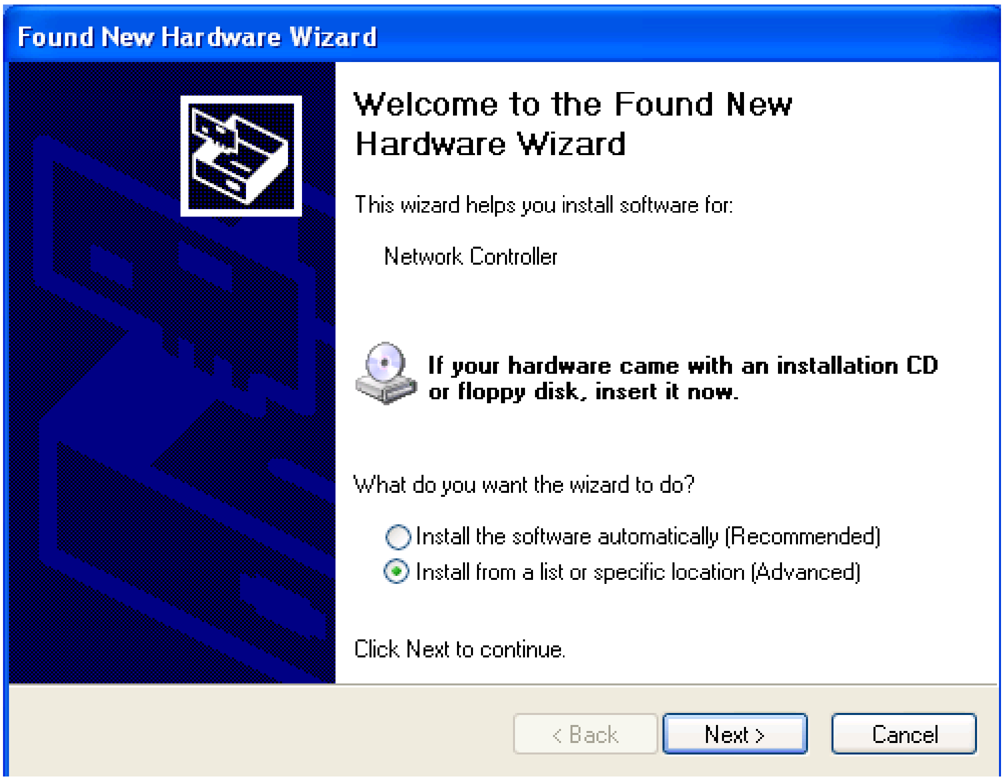
The user manual for end users must include the following information in a prominent location “IMPORTANT NOTE: To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.”

Other important note:

1. The end user may not be provided with instructions to remove or install the device.
2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
3. This device is authorised for OEM integration only.

Installation

- Power down your computer. (for Mini PCI adapter, you don't need to do that)
- Insert the wireless adapter into the Mini PCI slot for PCI adapter.
- Power up your computer.
- Select "**Cancel**" to ignore the "**Found New Hardware Wizard**" window after Windows been started up.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

Network Controller

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

○ Install the software automatically (Recommended)
● Install from a list or specific location (Advanced)

Click Next to continue.

- Insert the Product CD into the CD-ROM drive.
- Execute "Setup.exe" in the root directory of the CD, it will guide you to install the Driver and Utility.

Management

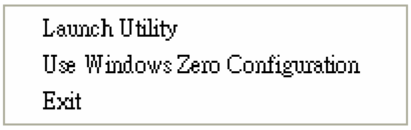
Load up utility

After the installation, one utility will be run and minimized on Windows system tray bar.

:Indicate wireless adapter detected, and connected to one site.

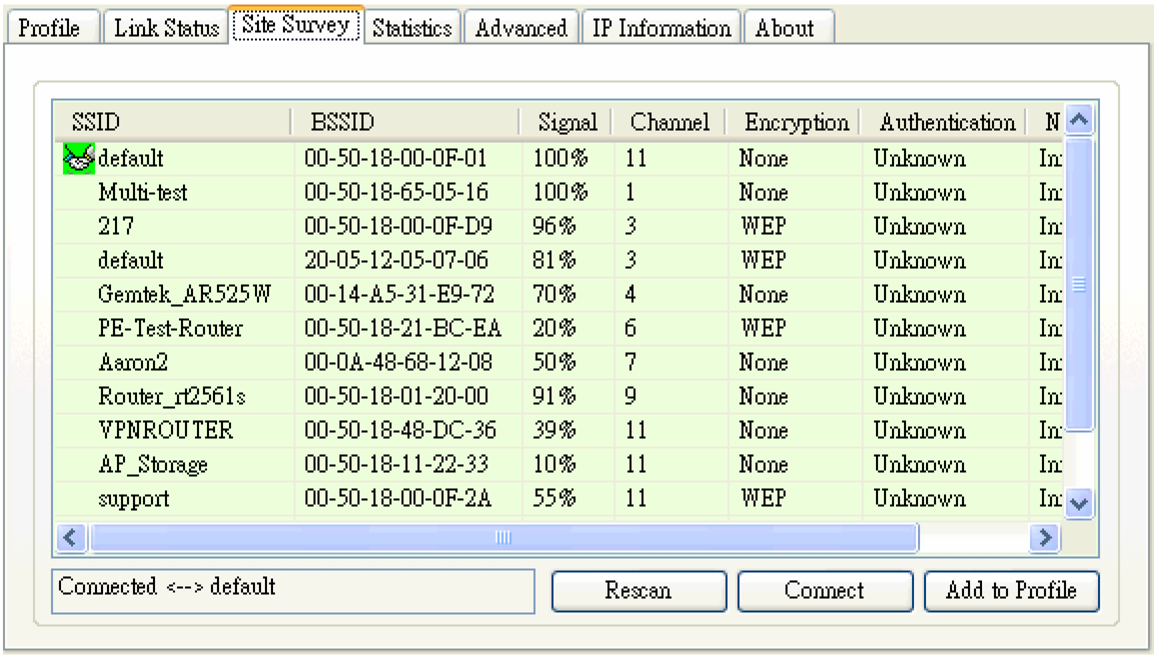
:Indicated wireless adapter not detected, or not connected to one site.

You may double click it to bring up the main menu. You may also use mouse right button to launch or to close it. For Windows XP, the utility provides one option to manage the wireless adapter with Windows Zero Configuration.



Site Survey Page

Under the site survey page, system will display the information of surrounding APs from last scan result. List information include SSID, BSSID, Signal, Channel, Encryption algorithm, and Network type.



SSID	BSSID	Signal	Channel	Encryption	Authentication	N
default	00-50-18-00-0F-01	100%	11	None	Unknown	In
Multi-test	00-50-18-65-05-16	100%	1	None	Unknown	In
217	00-50-18-00-0F-D9	96%	3	WEP	Unknown	In
default	20-05-12-05-07-06	81%	3	WEP	Unknown	In
Gemtek_AR525W	00-14-A5-31-E9-72	70%	4	None	Unknown	In
PE-Test-Router	00-50-18-21-BC-EA	20%	6	WEP	Unknown	In
Aaron2	00-0A-48-68-12-08	50%	7	None	Unknown	In
Router_rt2561s	00-50-18-01-20-00	91%	9	None	Unknown	In
VPNROUTER	00-50-18-48-DC-36	39%	11	None	Unknown	In
AP_Storage	00-50-18-11-22-33	10%	11	None	Unknown	In
support	00-50-18-00-0F-2A	55%	11	WEP	Unknown	In

Connected <--> default

Definition of each field

- SSID: Name of BSS of IBSS network.
- BSSID: MAC address of AP or randomly generated of IBSS.
- Signal: Receive signal strength of specified network.
- Channel: Channel in use.
- Encryption: Encryption algorithm used within than BSS or IBSS. Valid value includes WEP, TKIP, AES, and Not Use.
- Authentication: Authentication mode used within the network, including Unknown, WPA-PSK, WPA2-PSK, WPA and WPA2.
- Network Type: Network type in use, Infrastructure for BSS, Ad-Hoc for IBSS network.

Connected network

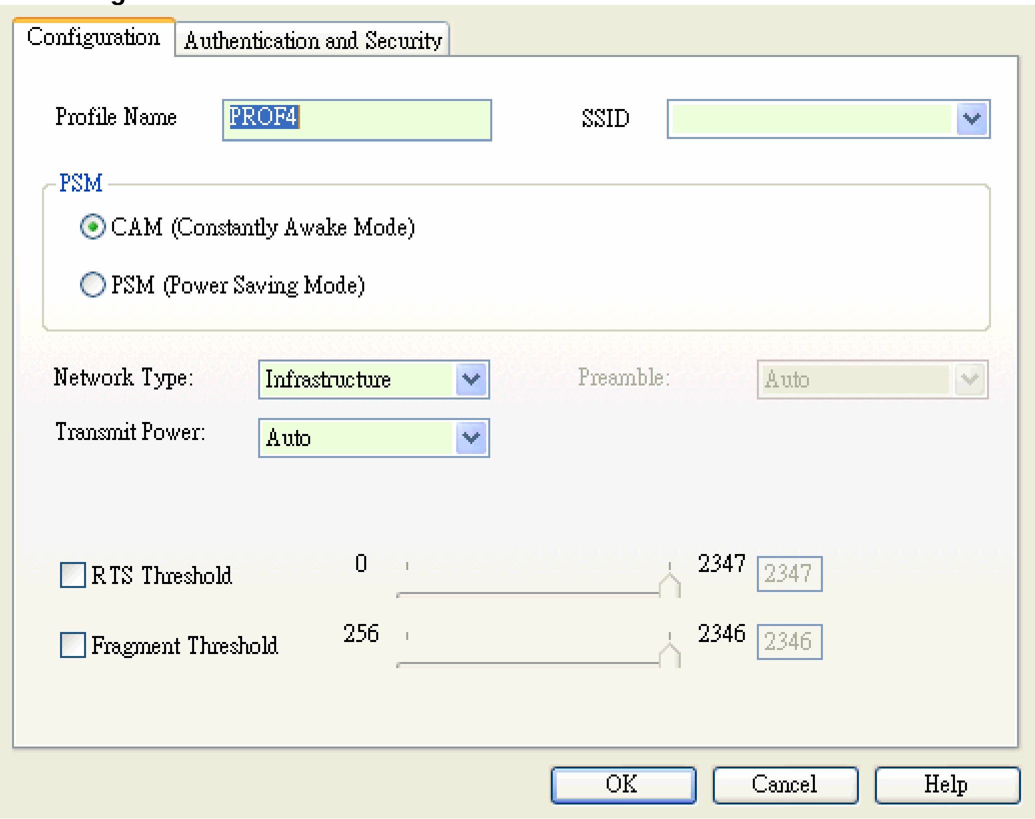
When utility first ran, it will select the best AP to connect automatically. It is available to connect to other site by double click the intended item. If the intended network has encryption other than " Not Use " or “Unknown”, the security page will pop up for you to setup the appropriate information to make the connection.

✓ : This icon indicates the change is successful.

- Connection box: Indicate connection status, the connected network SSID will show up here.
- Rescan: Issue an rescan command to wireless NIC to update information on surrounding wireless network.
- Connect: Command to connect to the selected network.
- Add to Profile: Add the selected AP to profile setting. It will bring up profile page and save the setting to a new profile.

Add/Edit Profile

System Configuration



Profile Name: PROF4

SSID:

PSM

● CAM (Constantly Awake Mode)

○ PSM (Power Saving Mode)

Network Type: Infrastructure

Preamble: Auto

Transmit Power: Auto

□ RTS Threshold 0 2347 2347

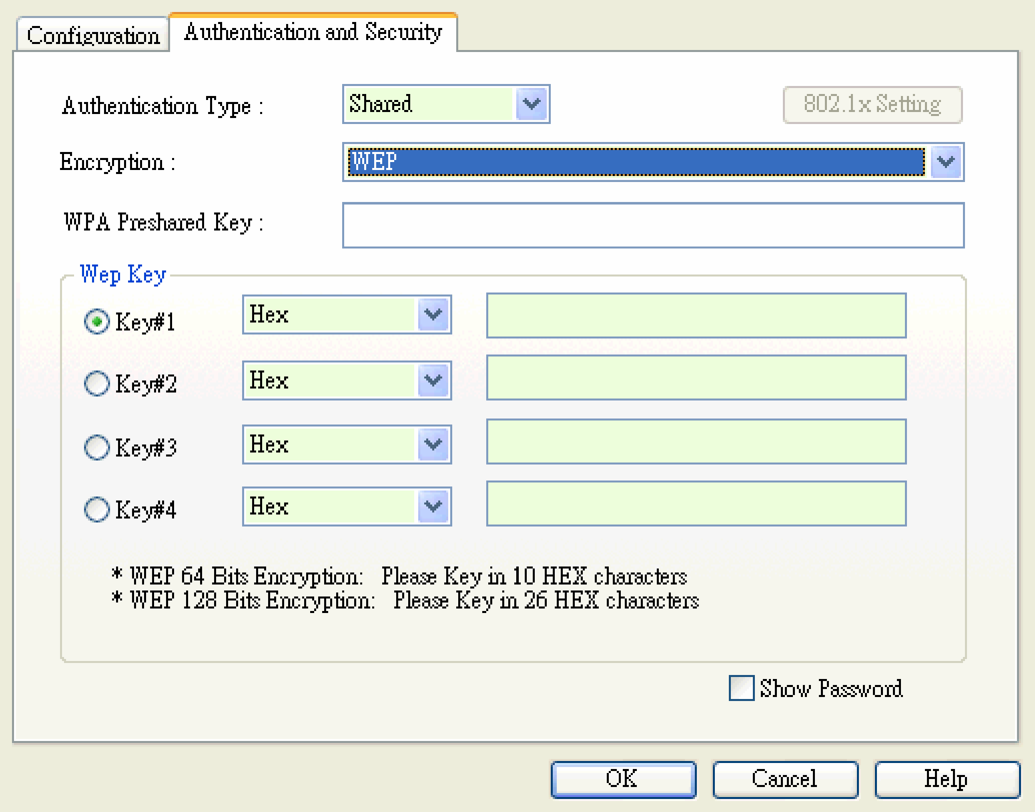
□ Fragment Threshold 256 2346 2346

- Profile Name: User chose name for this profile.
- SSID: User can key in the intended SSID name or use pull down menu to select from available APs.
- Power Save Mode: Choose from CAM (Constantly Awake Mode) or Power Saving Mode. There is a check box for CAM when AC power. When this is checked, the wireless NIC will stay full power when AC power cord is plug into power outlet.
- Network Type: There are two types, infrastructure and 802.11 ad-hoc modes. Under ad-hoc mode, user can also choose the preamble type; the available preamble type includes short and long. In addition to that, the channel and Ad hoc wireless mode 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. User can choose power value by sliding the bar.
- Preamble: There are three types, Auto, Long and Short are supported.
- Ad hoc wireless mode: 802.11b only, 802.11b/g mixed and 802.11g only modes are supported.
- RTS Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2347.
- Fragment Threshold: User can adjust the RTS threshold number by sliding the bar or key in the value directly. The default value is 2346.
- Channel: Only available for setting under ad-hoc mode. User can choose the channel frequency to start their ad-hoc network.

Profile function is based on the needs to set up the most linkable AP in order to record the system configuration and to set up the authentication security. The function of each session is shown below

Authentication & Security

When the Encryption feature is enabled, the other setups are same as the WEP setting.



Authentication Type : Shared

Encryption : WEP

WPA Preshared Key :

Wep Key

● Key#1 Hex

○ Key#2 Hex

○ Key#3 Hex

○ Key#4 Hex

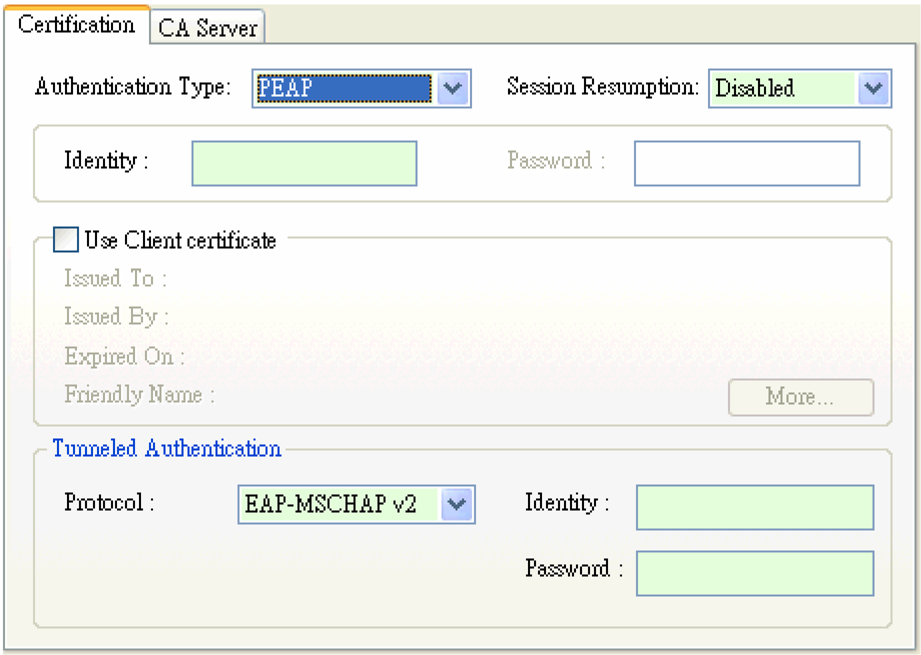
* WEP 64 Bits Encryption: Please Key in 10 HEX characters
* WEP 128 Bits Encryption: Please Key in 26 HEX characters

□ Show Password

- Authentication Type: There are three type of authentication modes supported. They are open, Shared, WPA-PSK and WPA system.
- 802.1x Setting: It will display to set when user use radius server to authenticate client certificate for WPA authentication mode.
- Encryption Type: For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.
- WPA Pre-shared Key: This is the shared secret between AP and STA. For WPA-PSK and WPA2-PSK authentication mode, this field must be filled with character longer than 8 and less than 32 length.
- WEP Key: Only valid when using WEP encryption algorithm. The key must matched AP key. There are several formats to enter the keys.

  i -- Hexadecimal?40bits:10 Hex characters.
  ii -- Hexadecimal?128bits:32Hex characters.
  iii -- ASCII?40bits:5 ASCII characters.
  iv -- ASCII?128bits:13 ASCII characters.

802.1x Setting



Certification | CA Server

Authentication Type: PEAP

Session Resumption: Disabled

Identity :

Password :

□ Use Client certificate

Issued To :

Issued By :

Expired On :

Friendly Name :

More...

Tunneled Authentication

Protocol : EAP-MSCHAP v2

Identity :

Password :

802.1x is a authentication for ?WPA?and ?WPA2?certificate to server.

- Authentication type:
  - i PEAP: Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
  - ii 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.
  - iii TTLS: Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
  - iv 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.
  - v 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.

- Session Resumption: user can choose “ Disable ”, “ Reauthentication ”, “ Roaming ”, “ SameSsid ” and “ Always ”.
- Identity and Password: Identity and password for server.
- Use Client Certicate: Client Certicate for server authentication.
- Tunnel Authentication

  Protocol: Tunnel protocol, List information include “ EAP-MSCHAP ”, “ EAP-MSCHAP v2 ”, “ CAHAP ” and “ MD5 ”

  Tunnel Identity: Identity for tunnel.

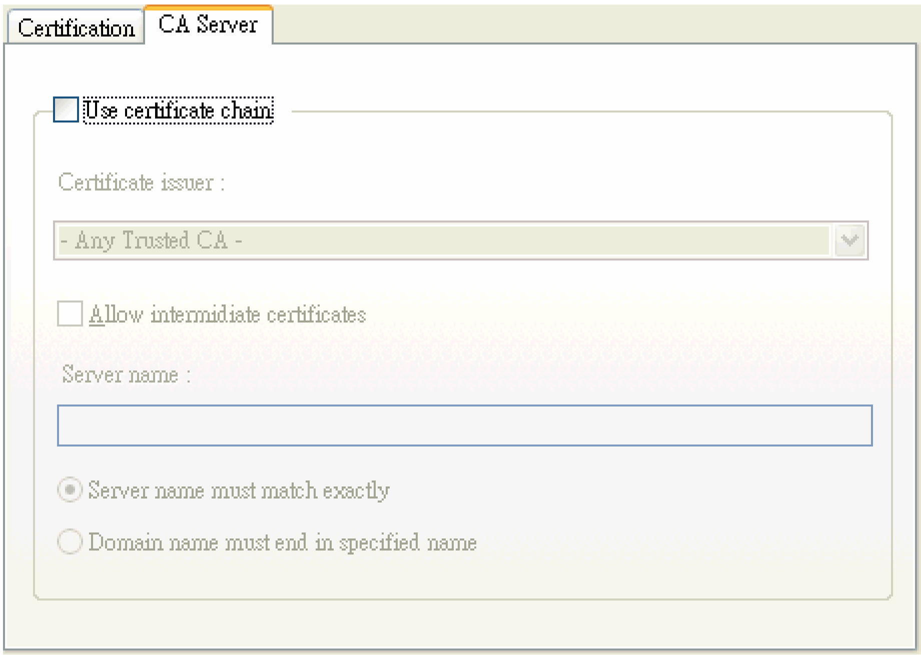
  Tunnel Password: Password for tunnel.
- CA Server: Certificate Authority Server. Each certificate is signed or issued by it.

CA Server

Depending on the EAP in use, only the server or both the server and client may be authenticated and require a certificate. Server certificates identify a server, usually an authentication or RADIUS server to clients. Most EAPs require a certificate issued by a root authority or a trusted commercial CA. Show as the figure.

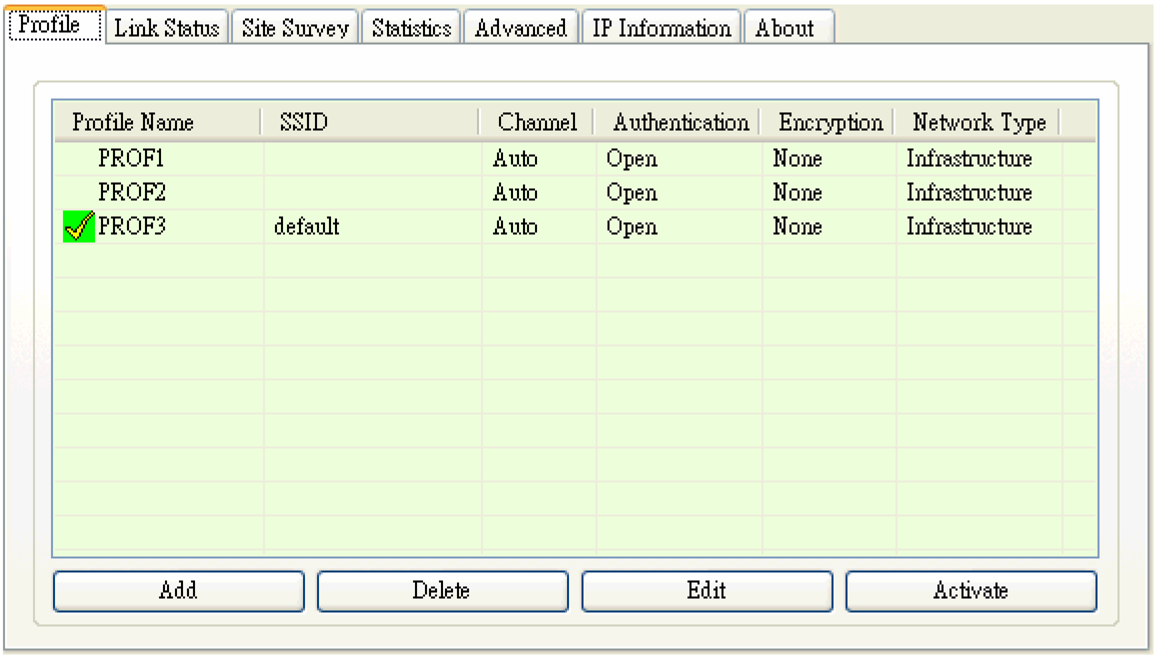
1. Certificate issuer: Choose use server that issuer of certificates.

2. 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.
3. Server name: Enter an authentication sever root.


Certification
CA Server
□ Use certificate chain
Certificate issuer :
- Any Trusted CA -
□ Allow intermidiate certificates
Server name :
● Server name must match exactly
○ Domain name must end in specified name

Profile Page

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



Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1		Auto	Open	None	Infrastructure
PROF2		Auto	Open	None	Infrastructure
✓ PROF3	default	Auto	Open	None	Infrastructure

Definition of each field

- Profile: Name of profile, preset to PROF* (* indicate 1, 2, 3,).
- SSID: AP or Ad-hoc name.
- Channel: Channel in use for Ad-Hoc mode.
- Authentication: Authentication mode.
- Encryption: Security algorithm in use.
- Network Type: including infrastructure and Ad-Hoc.

Connection status

🟩 Indicate connection is successful on currently activated profile.

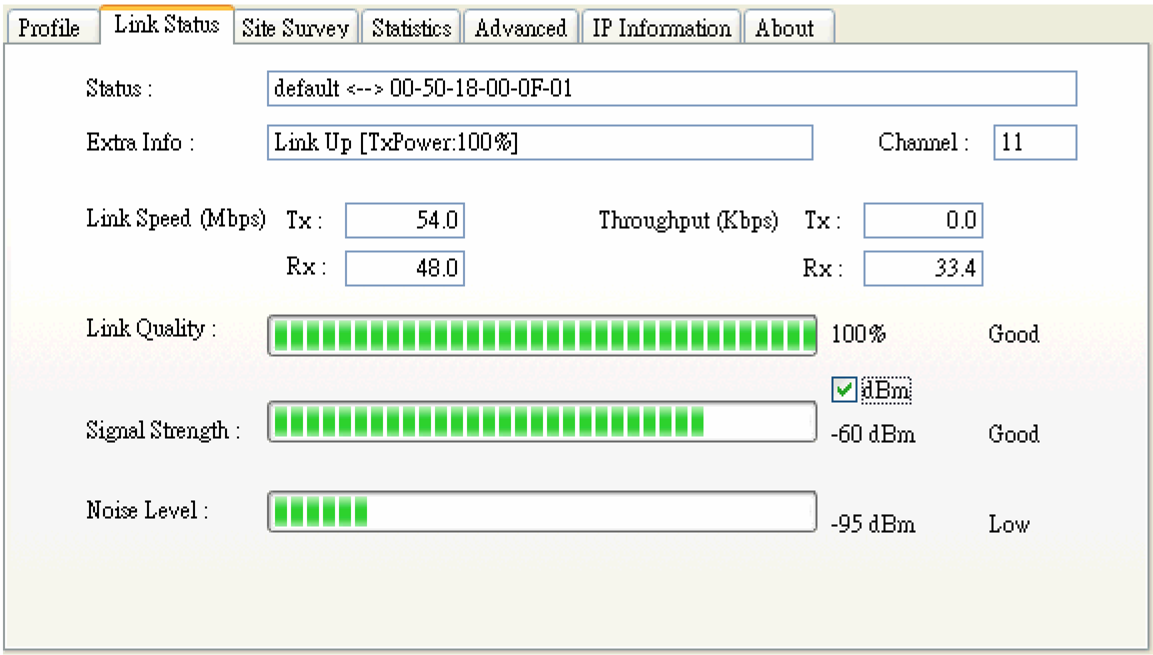
🟥 Indicate connection is failed on currently activated profile.

Note: When use site survey to make the connection. None of the profile will have the connection status icon.

- Add: Add a new profile.
- Delete: Delete an existing profile.
- Edit: Edit profile content.
- Activate: Activate selected profile.

Link Status Page

The page displays the detailed information of the current connection.



Status : default <--> 00-50-18-00-0F-01

Extra Info : Link Up [TxPower:100%]

Channel : 11

Link Speed (Mbps) Tx : 54.0

Rx : 48.0

Throughput (Kbps) Tx : 0.0

Rx : 33.4

Link Quality : 100% Good

☑ dBm

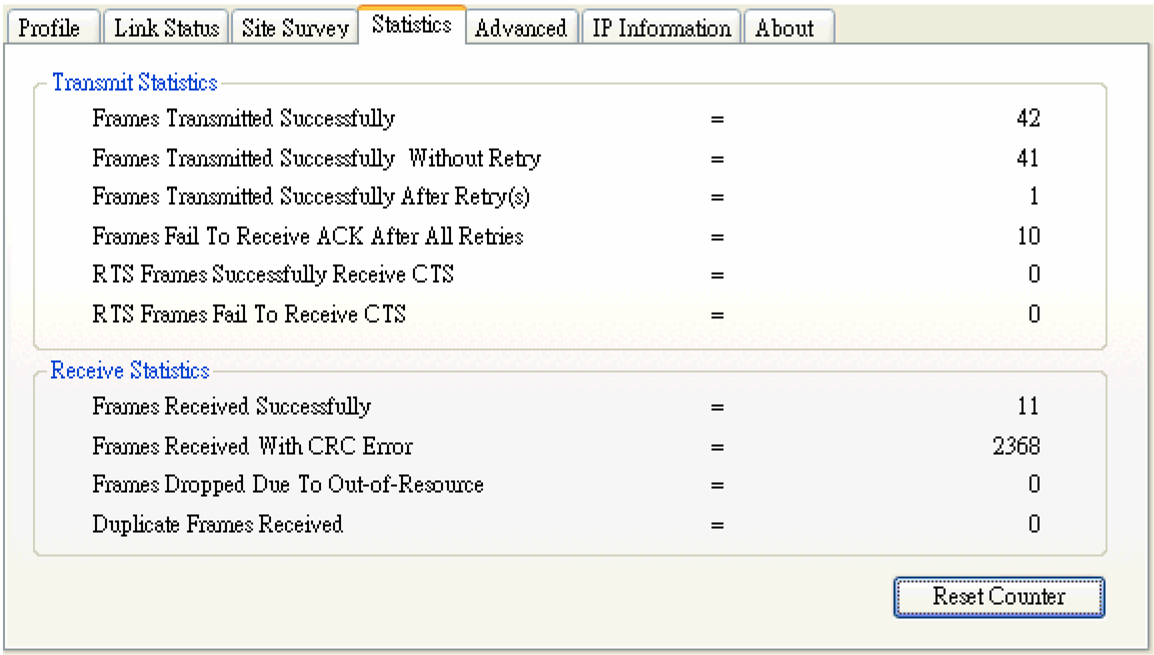
Signal Strength : -60 dBm Good

Noise Level : -95 dBm Low

- Status: Current connection status. If no connection, if will show Disconnected. Otherwise, the SSID and BSSID will show here.
- Extra Info: Display link status and current channel in use.
- Link Speed: Show current transmit rate and receive rate.
- Throughout: Display transmits and receive throughput in unit of K bits/sec.
- Link Quality: Display connection quality based on signal strength and Tx/Rx packet error rate.
- Signal Strength: Receive signal strength, user can choose to display as percentage or dBm format.
- Noise Level: Display noise signal strength.

Statistics Page

Statistics page displays the detail counter information based on 802.11 MIB counters. This page translates that MIB counters into a format easier for user to understand.



Transmit Statistics

Frames Transmitted Successfully	=	42
Frames Transmitted Successfully Without Retry	=	41
Frames Transmitted Successfully After Retry(s)	=	1
Frames Fail To Receive ACK After All Retries	=	10
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0

Receive Statistics

Frames Received Successfully	=	11
Frames Received With CRC Error	=	2368
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

Transmit Statistics

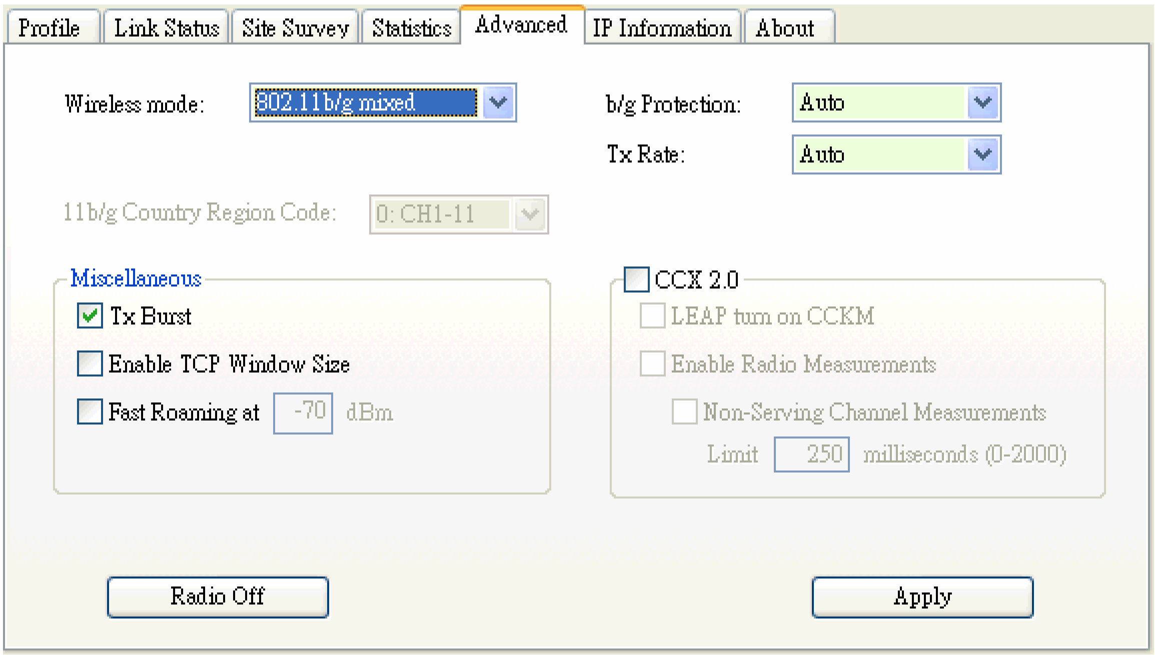
- Frames Transmitted Successfully: Frames successfully sent.
- Frames Transmitted Successfully Without Retry: Frames successfully sent without any retry.
- Frames Transmitted Successfully After Retry: Frames successfully sent with one or more reties.
- Frames Fail To Receive ACK After All Retries: Frames failed transmit after hitting retry limit.
- RTS Frames Successfully Receive CTS: Successfully receive CTS after sending RTS frame.
- RTS Frames Fail To Receive CTS: Failed to receive CTS after sending RTS.

Receive Statistics

- Frames Received Successfully: Frames received successfully.
- Frames Received With CRC Error: Frames received with CRC error.
- Frames Dropped Due To Out-of-Resource: Frames dropped due to resource issue.
- Duplicate Frames Received: Duplicate received frames.

- Reset Counter: Reset all counters to zero.

Advance Page



Wireless mode: 802.11b/g mixed

b/g Protection: Auto

Tx Rate: Auto

11b/g Country Region Code: 0: CH1-11

Miscellaneous

☑ Tx Burst

□ Enable TCP Window Size

□ Fast Roaming at -70 dBm

□ CCX 2.0

□ LEAP turn on CCKM

□ Enable Radio Measurements

□ Non-Serving Channel Measurements

Limit 250 milliseconds (0-2000)

- Wireless mode: Select wireless mode. 802.11b only, 802.11 b/g mixed and 802.11g only modes are supported.
- 11b/g Protection: ERP protection mode of 802.11g definition.
  Auto: STA will dynamically change as AP announcement.
  On: Always send frame with protection.
  Off: Always send frame without protection.
- Tx Rate: Manually force the Transmit using selected rate. Default is auto.
- Tx Burst: Proprietary frame burst mode of this utility.
- Enable TCP Window Size:.
- Fast Roaming at: fast to roaming, setup by transmit power.
- 11b/g Country Region Code: country to choose. Country channel list: Country channel list

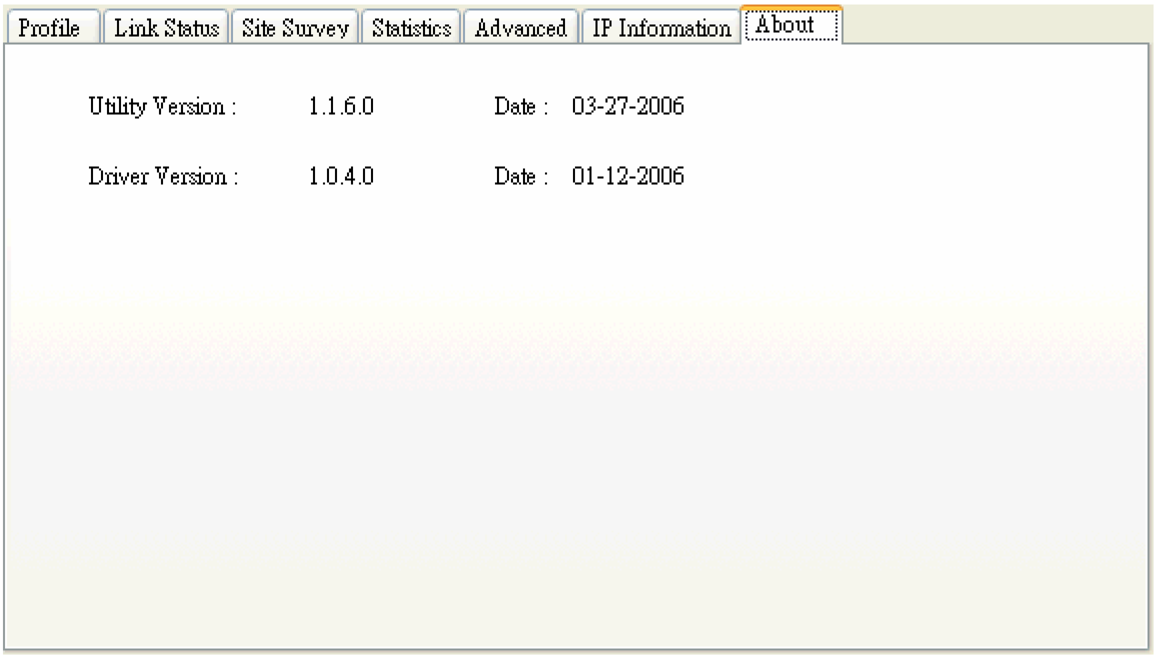
- CCX2.0: support Cisco Compatible Extensions function:
  LEAP turn on CCKM
  Enable Radio Measurement: can channel measurement every 0~2000 milliseconds.

- Radio On: To turn on radio.
- Radio Off: To turn off radio.

- Apply: Apply the above changes.

About Page

About page display the utility and driver version information of the wireless adapter.



Utility Version : 1.1.6.0 Date : 03-27-2006

Driver Version : 1.0.4.0 Date : 01-12-2006