IEEE802.b/g/n Wireless LAN USB 2.0 Client Adapter

User’s Manual

Version: 1.0

Table of Contents

Revision History

Version	Date	Notes
1.0	October 17, 2007	Initial Version

1 Introduction

The high-speed wireless USB 2.0 client adapter is the most convenient way to let you put a desktop/notebook computer almost anywhere without the hassle of running network cables. Now you don't need to suffer from drilling holes and exposed cables. Once you are connected, you can do anything, just like the wired network. This USB client adapter operates seamlessly in 2.4GHz frequency spectrum supporting the 802.11b, 802.11g, and 802.11nwireless standards. It's the best way to add wireless capability to your existing wired network or simply surf the web.

To protect your wireless connectivity, the high-speed wireless USB 2.0 client adapter can encrypt all wireless transmissions through 64/128-bit WEP, WPA, WPA-PSK and WPA-AES encryption and authentication allowing you to experience the most secure wireless connectivity available.

The Engenius 802.11n USB Adapter (EUB-9702) implements the latest 11n 2.0 technology which extremely improves wireless signal for your computer than existing wireless 802.11g technology. It supports the 1T2R MIMO architecture with fully forward compatibility with IEEE802.11n. The incredible speed of EUB-9702 USB adapter makes heavy traffic networking activities more flexible and takes the wireless into practical road. You could enjoy the racing speed of wireless connection, surfing on Internet without string wires.

Adding Engenius EUB-9702 to your Notebook or Computer, it provides an excellent performance and cost-effective solution for doing media-centric activities such as streaming video, gaming, and enhances the QoS (WMM) without any reduction of performance. It extends 3 times network coverage and boosts 6 times transmission throughput than existing 11g product. Advanced power management and low power consumption among 11n products.

For more security-sensitive application, EUB-9702 supports Hardware-based IEEE 802.11i encryption/decryption engine, including 64-bit/128-bit WEP, TKIP, and AES. Also, it supports Wi-Fi alliance WPA and WPA2 encryption and is Cisco CCX V1.0, V2.0 and V3.0 compliant.

1.1 Features & Benefits

Features	Benefits
Racing Speed up to 300Mbps Rx PHY rate (2.4GHz 11N technology)	Enjoy the Internet connection in crazy-fast speed, without the bottleneck of stringing wires.
Advanced power management	Low power consumption
WPA/WPA2 (IEEE 802.11i), WEP 64/128 Support	Powerful data security.
Support 1Tx * 2Rx Radios	With Intelligent Antenna enables

WMM (IEEE 802.11e) standard support	Wireless Multimedia Enhancements Quality of Service support (QoS) / enhanced power saving for Dynamic Networking
USB 2.0/1.1	USB 2.0 interface and compatible with USB 1.1

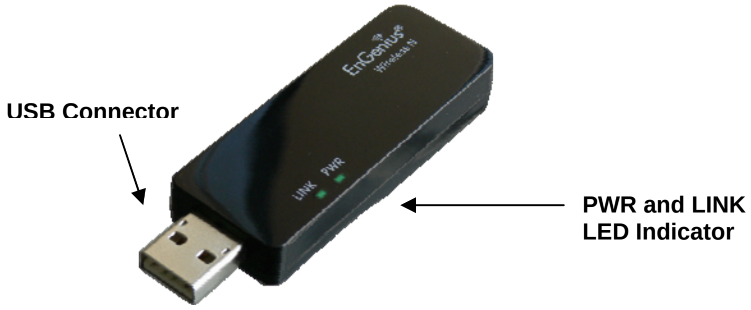
1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- One Wireless LAN USB Adapter
- One CD-ROM with Drivers and User's Manual Included
- One Quick Installation Guide

1.3 USB Adapter Description

The USB adapter is a standard USB adapter that fits into any USB interface. The USB adapter has two LED indicators and a built-in antenna.



1.4 System Requirements

The following are the minimum system requirements in order to use the USB adapter.

- PC/AT compatible computer with a USB interface.
- Windows 2000/XP/Vista or MAC OS operating system.
- 30 MB of free disk space for installing the USB adapter driver and utility program.

1.5 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) **Difficult-to-wire environments**
There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) **Temporary workgroups**
Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) **The ability to access real-time information**
Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) **Frequently changed environments**
Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) **Small Office and Home Office (SOHO) networks**
SOHO users need a cost-effective, easy and quick installation of a small network.

f) **Wireless extensions to Ethernet networks**
Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) **Wired LAN backup**
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) **Training/Educational facilities**
Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

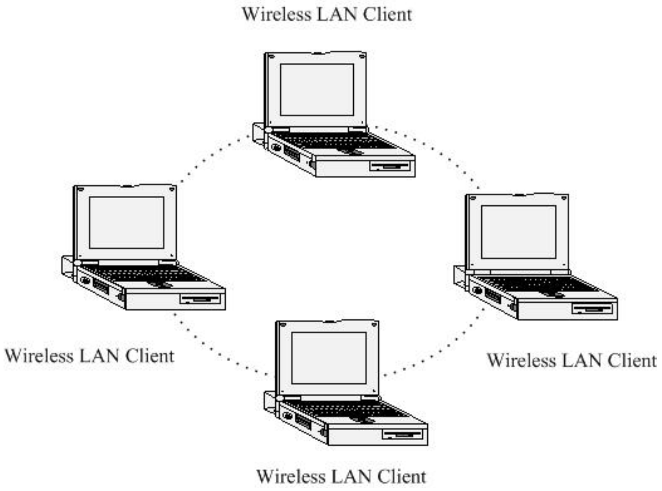
1.6 Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
b) Infrastructure for enterprise LANs.

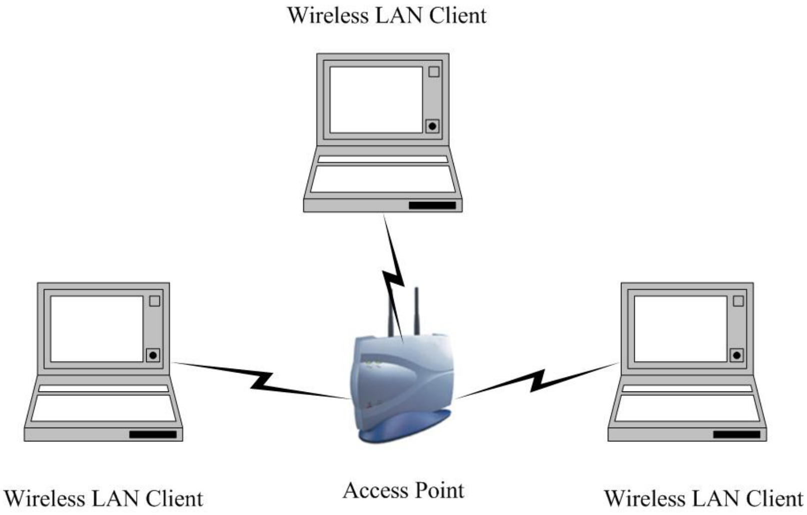
a) Ad-hoc (peer-to-peer) Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.



b) Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



2 USB Adapter for Windows Vista

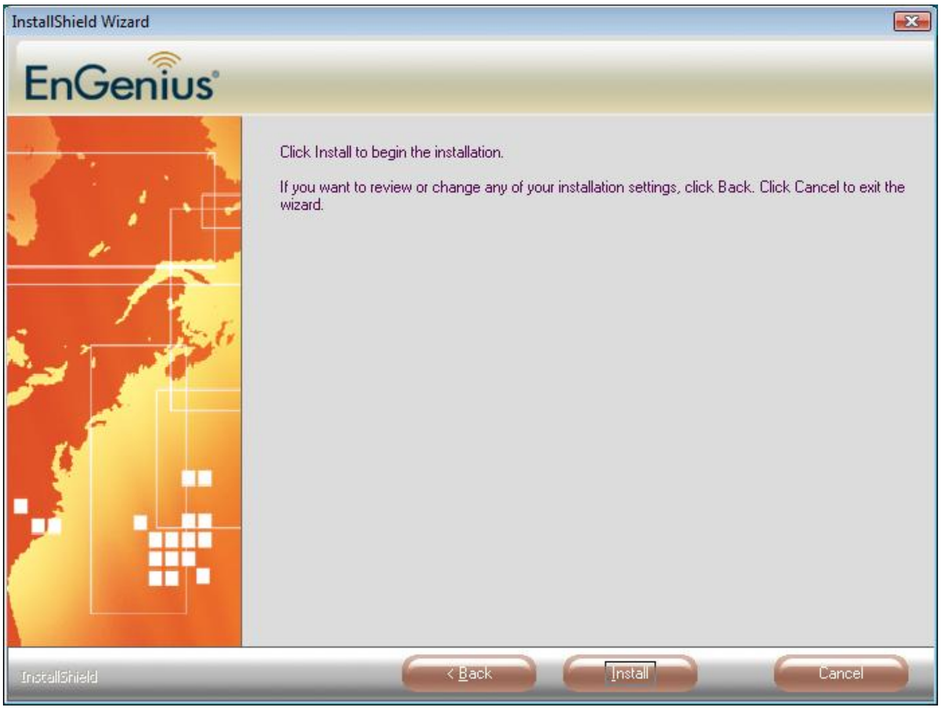
2.1 Before You Begin

During the installation, Vista may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers.

2.2 Installing the Drivers

Follow the steps below in order to install the USB adapter drivers:

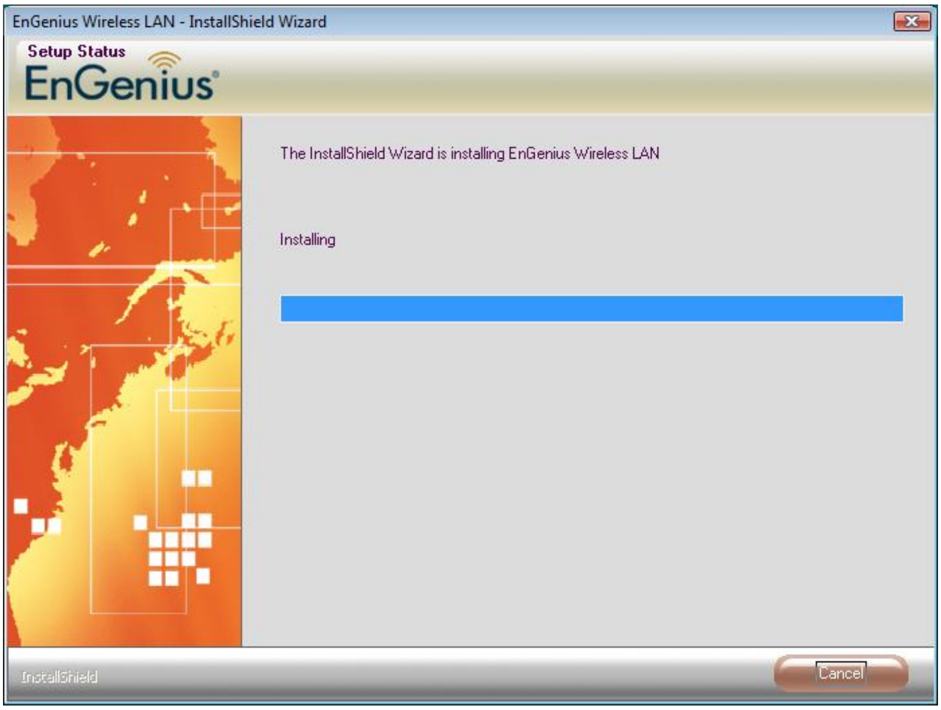
1. Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.



Click Install to begin the installation.

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

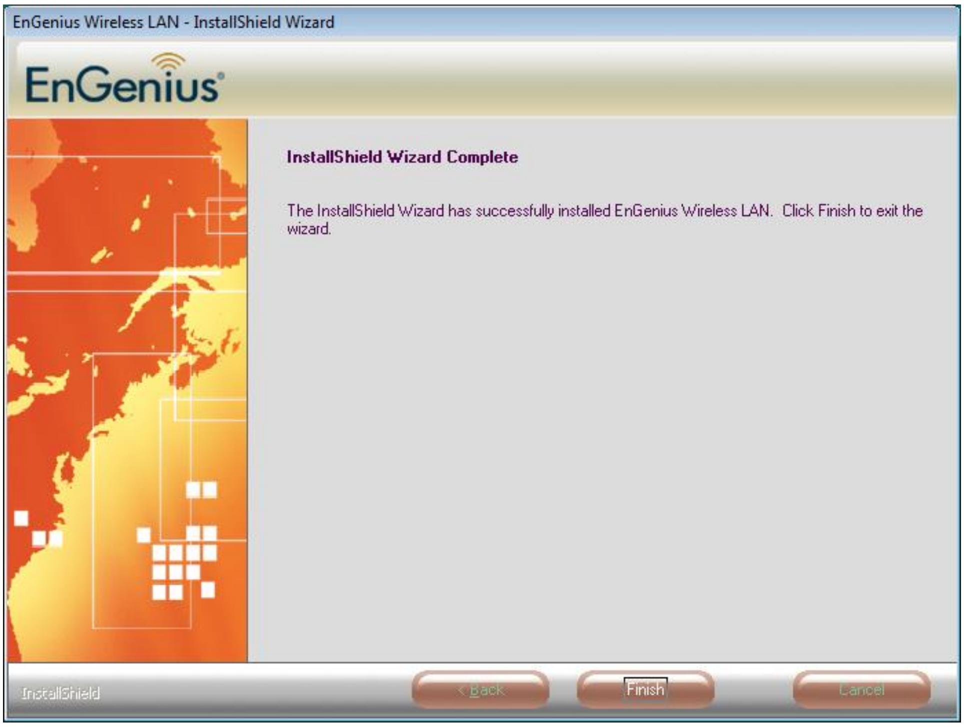
2. Once the setup begins you will see the **InstallShield Wizard**. Select **EnGenius Configuration Tool** and then click on the **Next>** button.



The InstallShield Wizard is installing EnGenius Wireless LAN

Installing

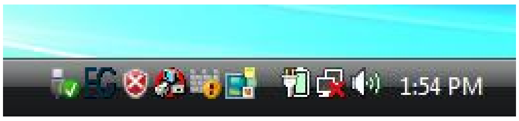
3. Click on the **Install** button to begin the installation.



InstallShield Wizard Complete

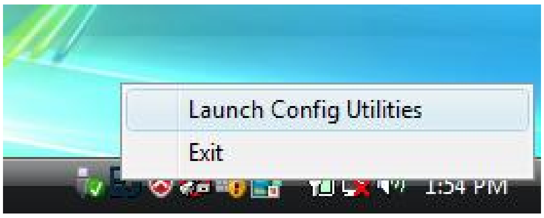
The InstallShield Wizard has successfully installed EnGenius Wireless LAN. Click Finish to exit the wizard.

4. The installation is complete. Click on the **Finish** button.
5. Carefully insert the USB adapter into the USB port. Windows will then detect and install the new hardware.



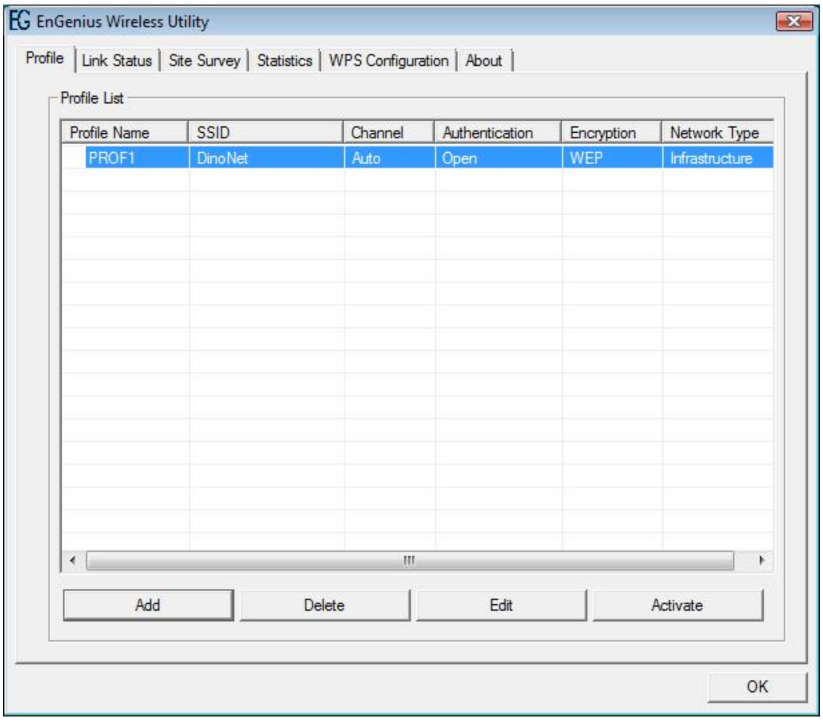
6. An **EG** icon will then appear in the system tray. Right click on the **EG** icon and then click on **Launch Config Utilities**.

Note: Click on **Use Zero Configuration as Configuration Utility** if you would like to use Windows Zero Config.



2.3 Profiles

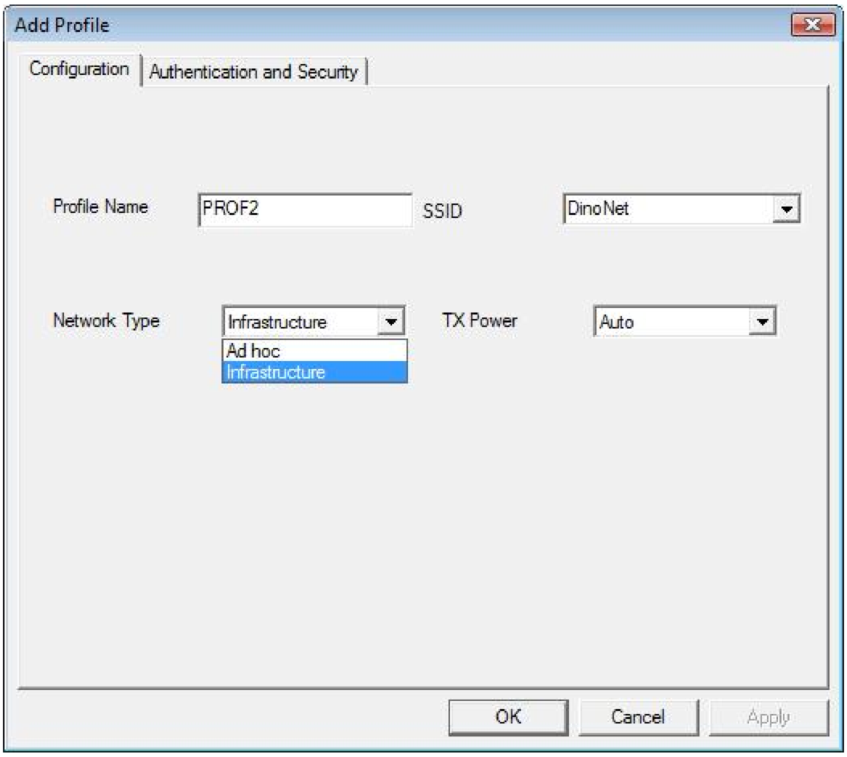
The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and encryption/authentication settings. A profile can be configured as **Infrastructure** or **Ad-hoc** mode. The configuration settings for each mode are described below.



Profile Name	SSID	Channel	Authentication	Encryption	Network Type
PROF1	DinoNet	Auto	Open	WEP	Infrastructure

2.3.1 Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.


Add Profile

Profile Name: PROF2

SSID: DinoNet

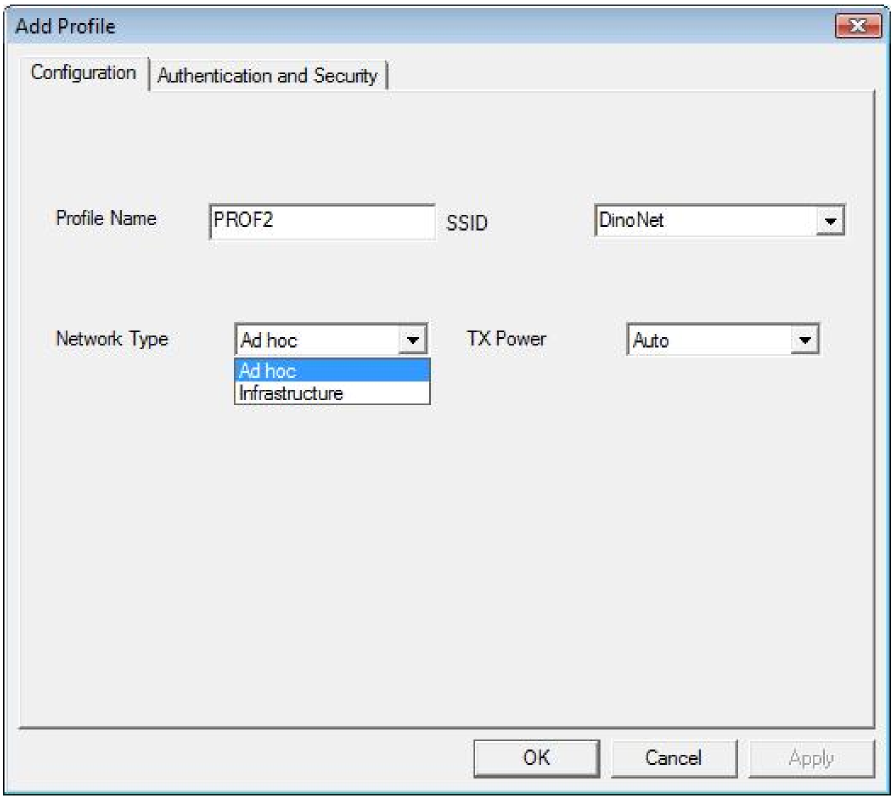
Network Type: Infrastructure

TX Power: Auto

- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Network Type:** Select **Infrastructure** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100**% or **auto**, if not, select one of the lower values for power saving.
- Click on the **Apply** button to save the changes.

2.3.2 Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.



Add Profile

Profile Name: PROF2

SSID: DinoNet

Network Type: Ad hoc

TX Power: Auto

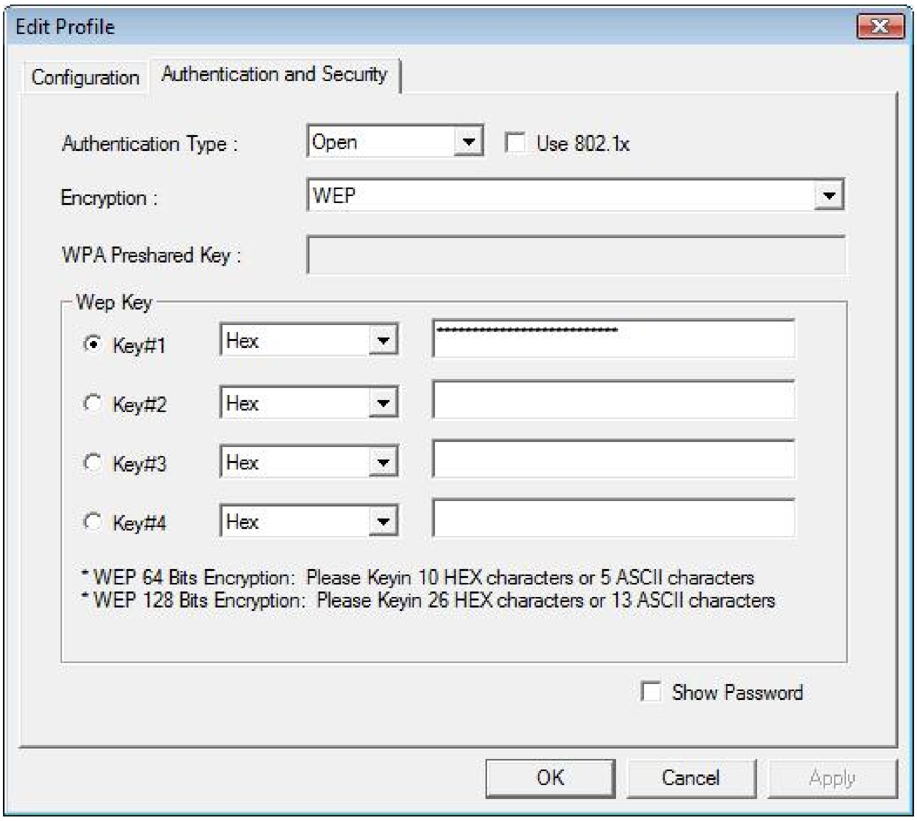
- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Network Type:** Select **Ad-hoc** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100**% or **auto**, if not, select one of the lower values for power saving.
- Click on the **Apply** button to save the changes.

2.4 Authentication and Security

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK. Each security option is described in detail below.

2.4.1 WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.



Authentication Type : Open □ Use 802.1x

Encryption : WEP

WPA Preshared Key :

Wep Key

● Key#1 Hex

○ Key#2 Hex

○ Key#3 Hex

○ Key#4 Hex

* WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters
* WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters

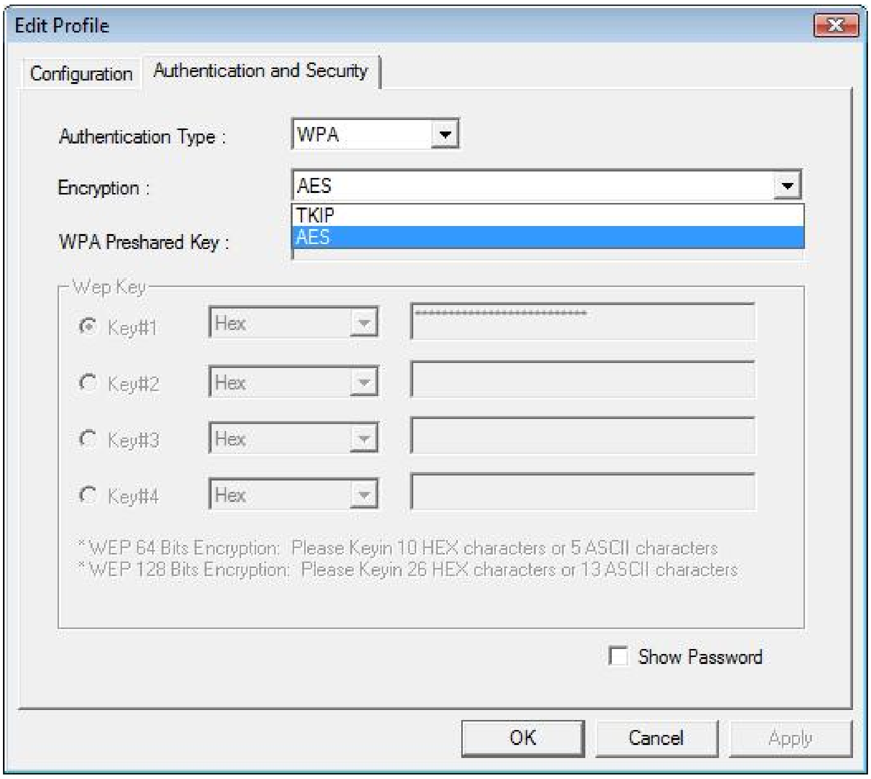
□ Show Password

- **Authentication Type:** Select **Open** or **Shared** from the drop-down list.
- **Encryption:** Select WEP from the drop-down list.
- **WEP Key:** Type a character string into the field. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.
- Click on the **Apply** button to save the changes.

- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

2.4.2 WPA, WPA2 Authentication & TKIP, AES Encryption

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't been tampered with. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



Edit Profile

Authentication Type : WPA

Encryption : AES

WPA Preshared Key :

Wep Key

○ Key#1 Hex ************************

○ Key#2 Hex

○ Key#3 Hex

○ Key#4 Hex

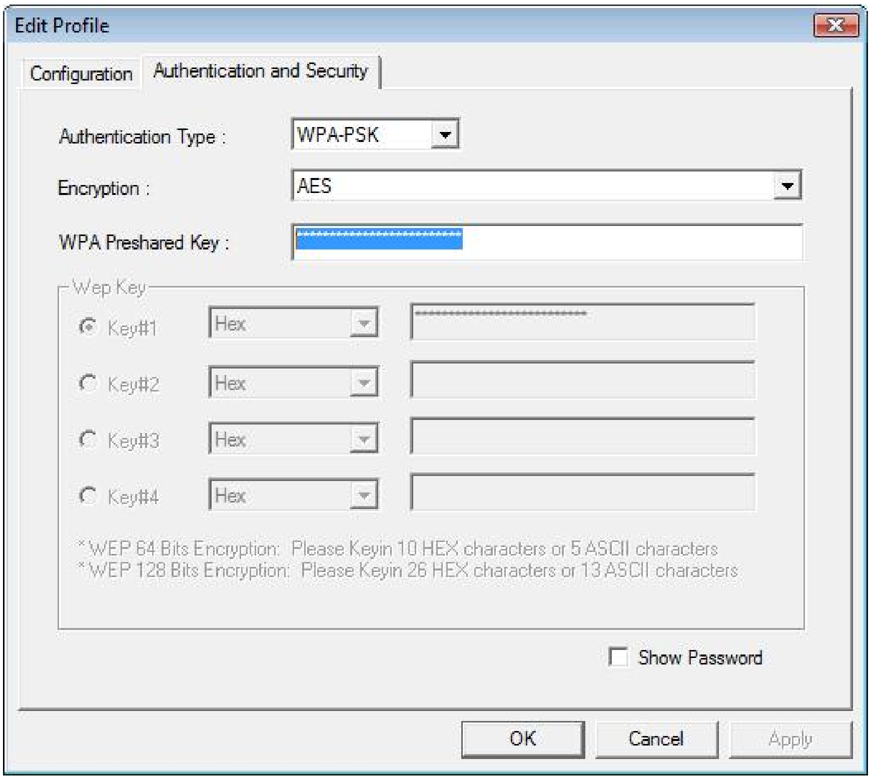
* WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters
* WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters

□ Show Password

- **Authentication Type**: Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

2.4.3 WPA-PSK Authentication & TKIP, AES Encryption

WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



Authentication Type : WPA-PSK

Encryption : AES

WPA Preshared Key : ************************

○ Key#1 Hex ****************************
○ Key#2 Hex
○ Key#3 Hex
○ Key#4 Hex

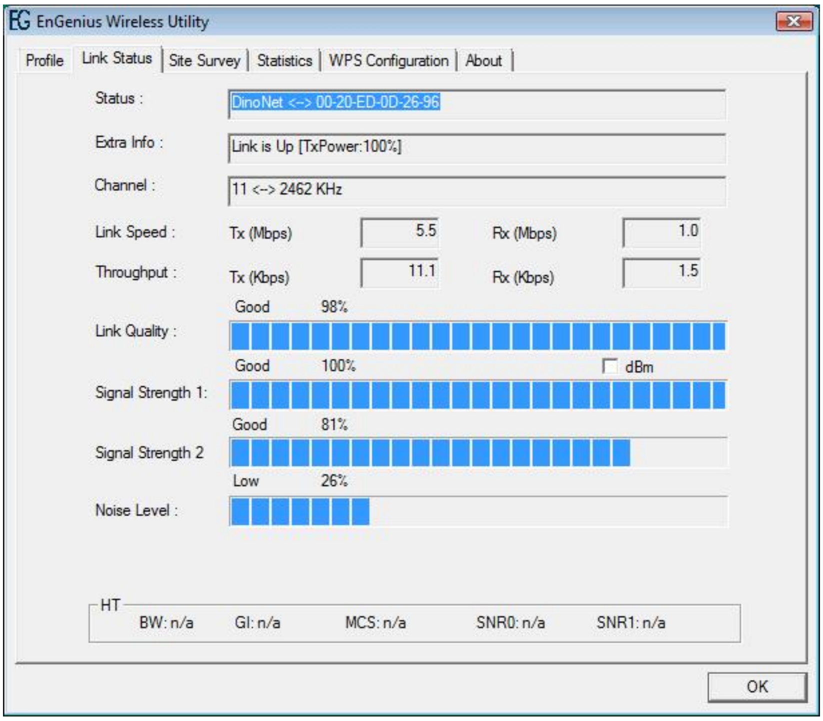
* WEP 64 Bits Encryption: Please Keyin 10 HEX characters or 5 ASCII characters
* WEP 128 Bits Encryption: Please Keyin 26 HEX characters or 13 ASCII characters

□ Show Password

- **Authentication Type**: Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- **WPA Preshared key:** Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

2.5 Link Status

The **Link Status** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.



Status : DinoNet <--> 00-20-ED-0D-26-96

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

Channel : 11 <--> 2462 KHz

Link Speed : Tx (Mbps) 5.5 Rx (Mbps) 1.0

Throughput : Tx (Kbps) 11.1 Rx (Kbps) 1.5

Link Quality : Good 98%

Signal Strength 1: Good 100% □ dBm

Signal Strength 2 Good 81%

Noise Level : Low 26%

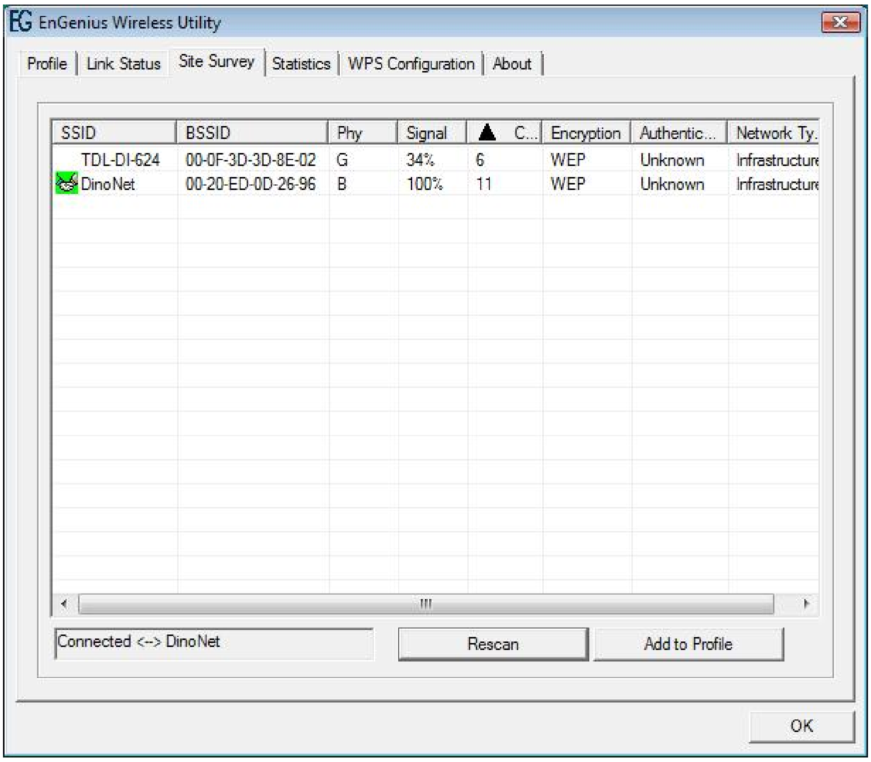
HT BW: n/a GI: n/a MCS: n/a SNR0: n/a SNR1: n/a

- **Status:** This indicates the state of the client. There are three options:
    - **Associated:** Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
    - **Scanning:** Indicates that the wireless client is searching for an AP in the area.
    - **Disconnected:** Indicates that there are no APs or clients in the area.
- **Extra Info:** Displayed here are information about the link stats and the percent of output power.
- **Current Channel:** The operating frequency channel that the client is using (infrastructure mode).
- **Link Speed**: The current rate at which the client is transmitting and receiving.
- **Throughput (bytes/sec):** Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- **Link Quality:** In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- **Signal Strength:** This bar displays the strength of the signal received from an AP or client.
- **Noise Level:** Displays the background noise level; a lower level indicates less interference.

- Click on the **OK** button to close this window.
- **dBm Check Box**. When you click on the check box as the drawing below. The signal strength and noise level will be shown as the dBm measurements.

2.6 Site Survey

The **Site Survey** tab displays a list of Access Points and Stations in the area, and allows you to connect to a specific one. The following information is included in this tab, as the image depicts below.



SSID	BSSID	Phy	Signal	▲ C...	Encryption	Authentic...	Network Ty.
TDL-DI-624	00-0F-3D-3D-8E-02	G	34%	6	WEP	Unknown	Infrastructure
DinoNet	00-20-ED-0D-26-96	B	100%	11	WEP	Unknown	Infrastructure

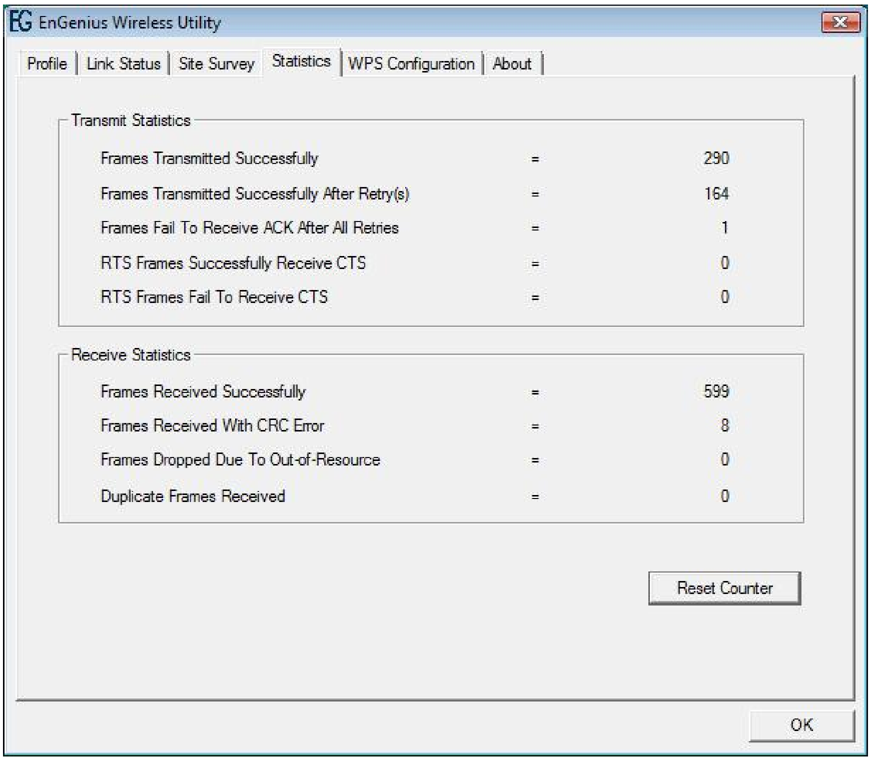
Connected <--> DinoNet

- **SSID**: Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **BSSID**: Displays the MAC address of the Access Point.
- **Signal**: Displays the receiving signal strength from the Access Point.
- **Channel**: Displays the channel number of the Access Point.
- **Encryption**: Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- **Authentication**: displays the authentication on the Access Point, this includes WPA, WPA-PSK, WPA2, or Unknown.
- **Network Type**: Indicates whether the SSID is a Station (Ad-hoc) or Access Point (Infrastructure).
- **Rescan:** Click on this button to view a list of Access Points in the area.
- **Connect**: to connect with a specific Access Point, select the SSID from the list, and then click on the **Connect** button.

- **Add to Profile**: Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

2.7 Statistics

The **Statistics** tab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after retry, received with CRC error, duplicate frames received, etc.



Transmit Statistics

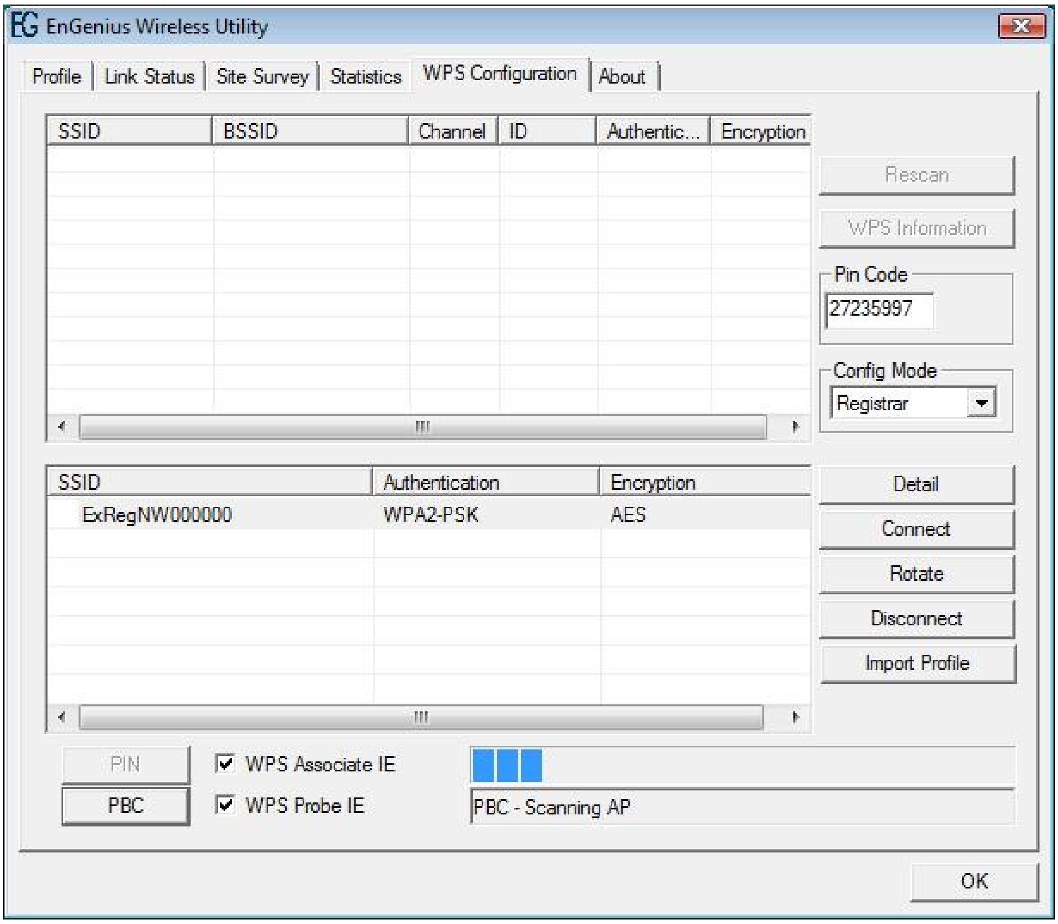
Frames Transmitted Successfully	=	290
Frames Transmitted Successfully After Retry(s)	=	164
Frames Fail To Receive ACK After All Retries	=	1
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0

Receive Statistics

Frames Received Successfully	=	599
Frames Received With CRC Error	=	8
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

2.8 WPS

Click on the WPS Configuration tab. WPS (Wireless Push Button) is used for WiFi Protected Setup. By pressing this button, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.



SSID	BSSID	Channel	ID	Authentic...	Encryption

Pin Code: 27235997

Config Mode: Registrar

SSID	Authentication	Encryption
ExRegNW000000	WPA2-PSK	AES

☑ WPS Associate IE

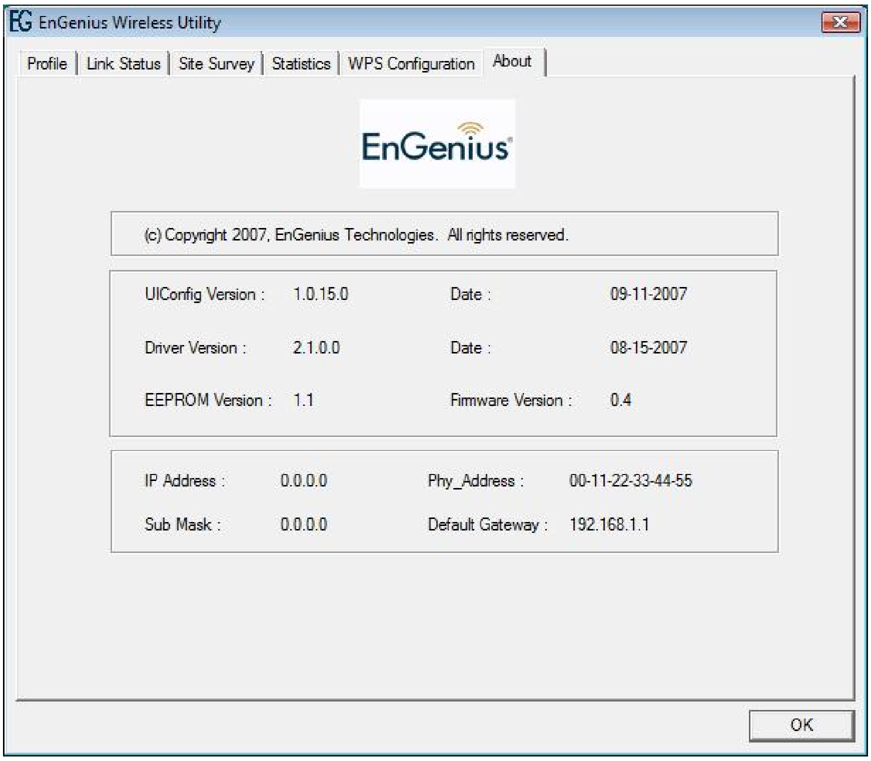
☑ WPS Probe IE

PBC - Scanning AP

- **Rescan:** Click on this button to view a list of Access Points in the area.
- **WPS Information:**
- **Pin Code:**
- **Config Mode:**
- **Detail:**
- **Connect:**
- **Rotate:**
- **Disconnect:**
- **Import Profile:**
- **PBC:**
- **WPS Associate IE:**
- **WPS Probe IE:**
- Click on the **OK** button if you have made any changes.

2.9 About

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.



(c) Copyright 2007, EnGenius Technologies. All rights reserved.

UIConfig Version : 1.0.15.0 Date : 09-11-2007

Driver Version : 2.1.0.0 Date : 08-15-2007

EEPROM Version : 1.1 Firmware Version : 0.4

IP Address : 0.0.0.0 Phy_Address : 00-11-22-33-44-55

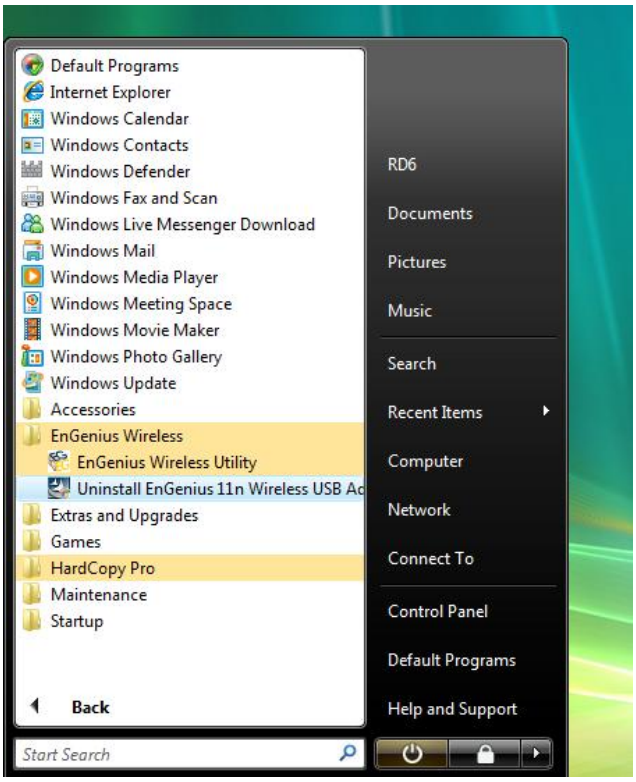
Sub Mask : 0.0.0.0 Default Gateway : 192.168.1.1

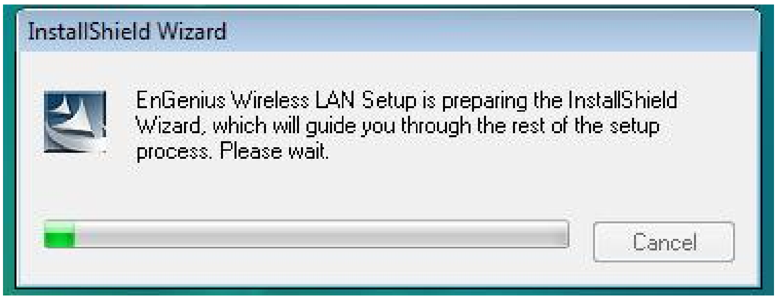
2.10 Uninstall the Drivers & Client Utility

If the USB client adapter installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the USB adapter and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the client utility:

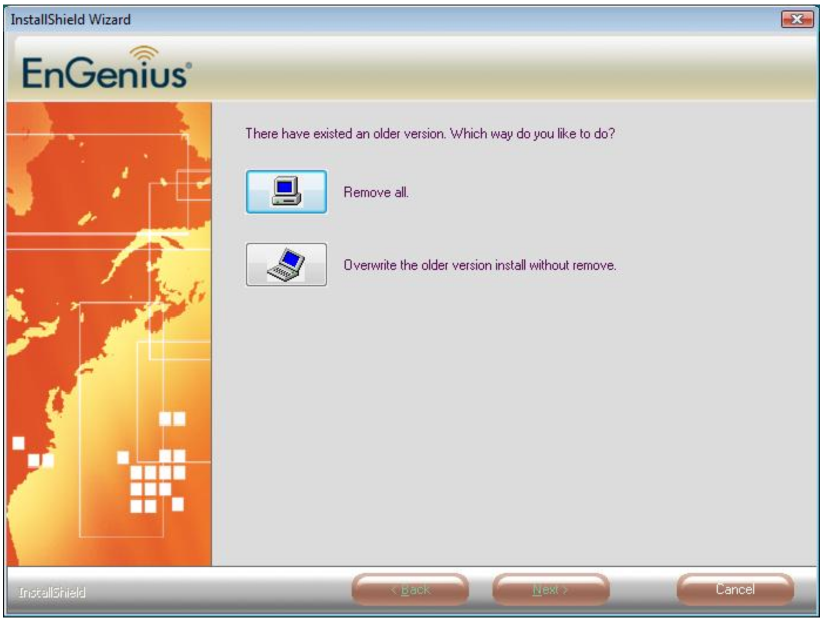
1. Click on **Start > EnGenius Wireless > Uninstall EnGenius Wireless USB Adapter**




InstallShield Wizard

EnGenius Wireless LAN Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

2. The un-installation process will then begin.

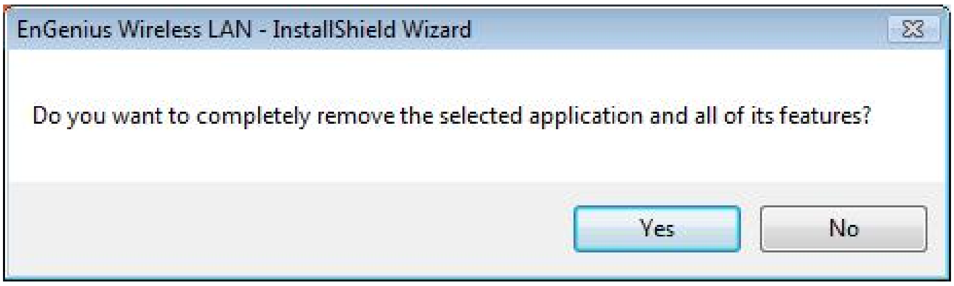


There have existed an older version. Which way do you like to do?

Remove all.

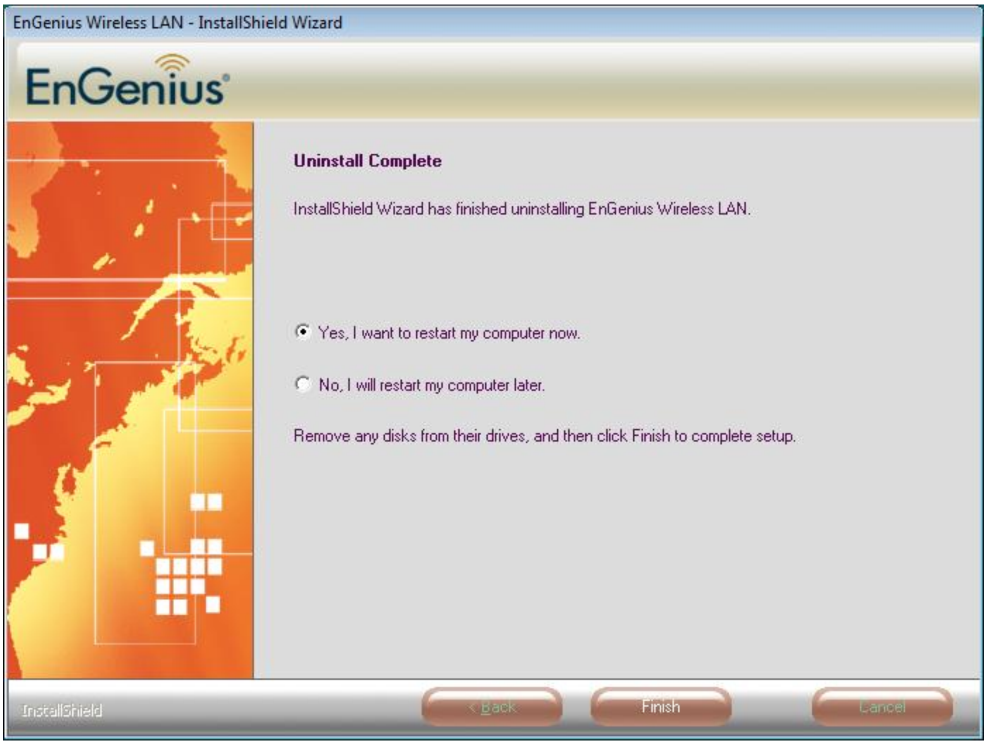
Overwrite the older version install without remove.

3. Select the **Remove all** button and then click on the **Next** button.



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

4. Click on the **Yes** button to confirm the un-installation process.



EnGenius Wireless LAN - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling EnGenius Wireless LAN.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

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

5. The un-installation process is complete. Select **Yes, I want to restart my computer now** radio button and then click on the Finish button. Then remove the USB adapter.

3 USB Adapter for Windows XP

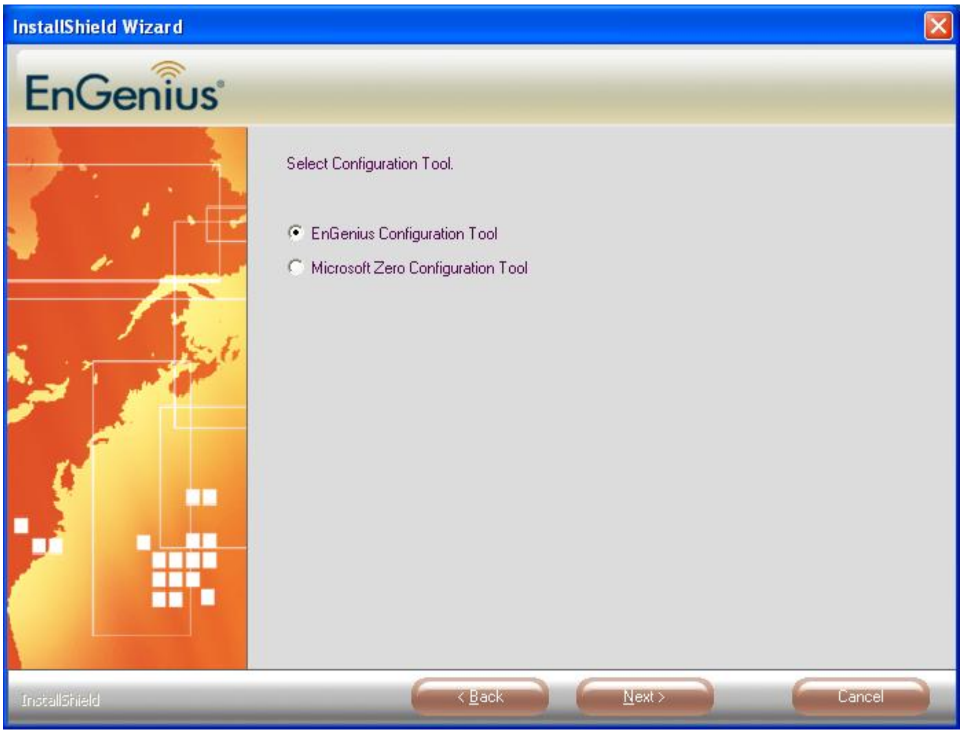
3.1 Before You Begin

During the installation, XP may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers. On many systems, instead of a CD, the necessary installation files are archived on the hard disk in C:\WINDOWS \OPTIONS\CABS directory.

3.2 Installing the Drivers

Follow the steps below in order to install the USB adapter drivers:

7. Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.

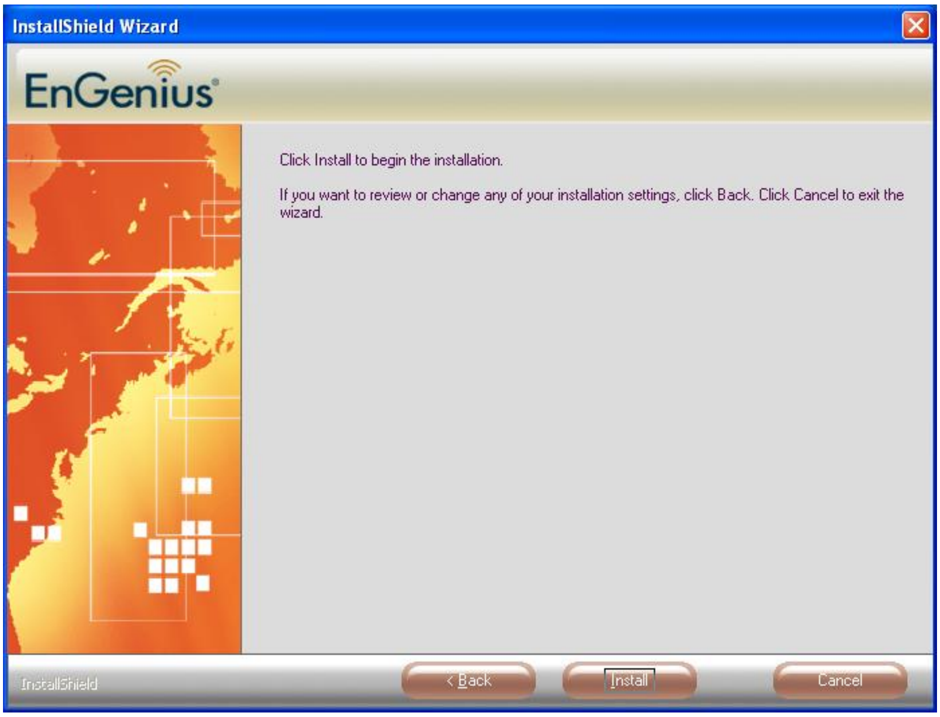


Select Configuration Tool.

● EnGenius Configuration Tool

○ Microsoft Zero Configuration Tool

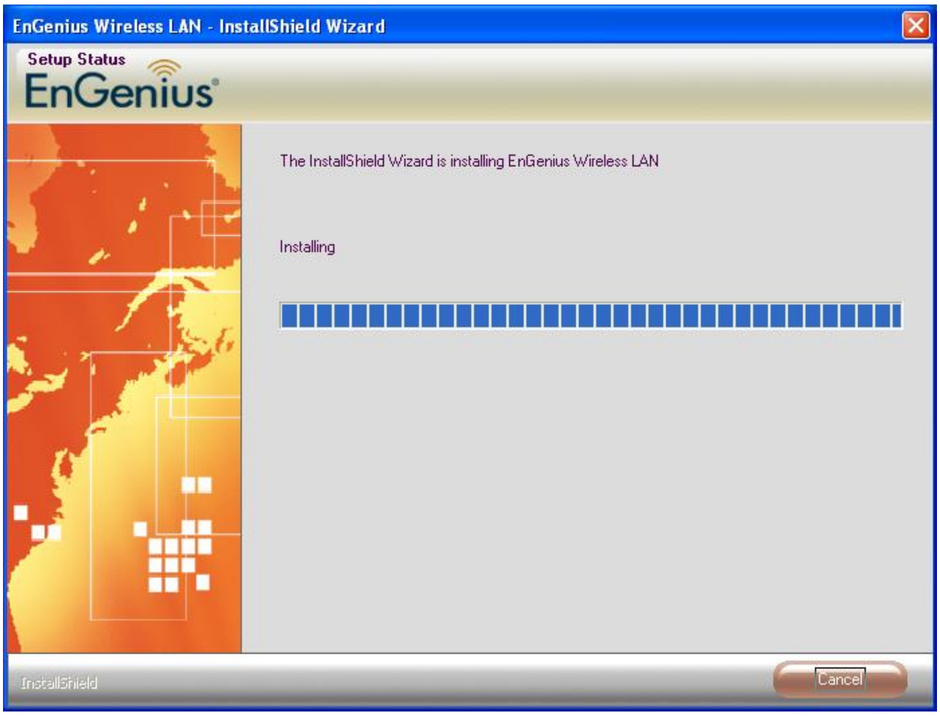
8. Once the setup begins you will see the **InstallShield Wizard**. Select **EnGenius Configuration Tool** and then click on the **Next>** button.



Click Install to begin the installation.

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

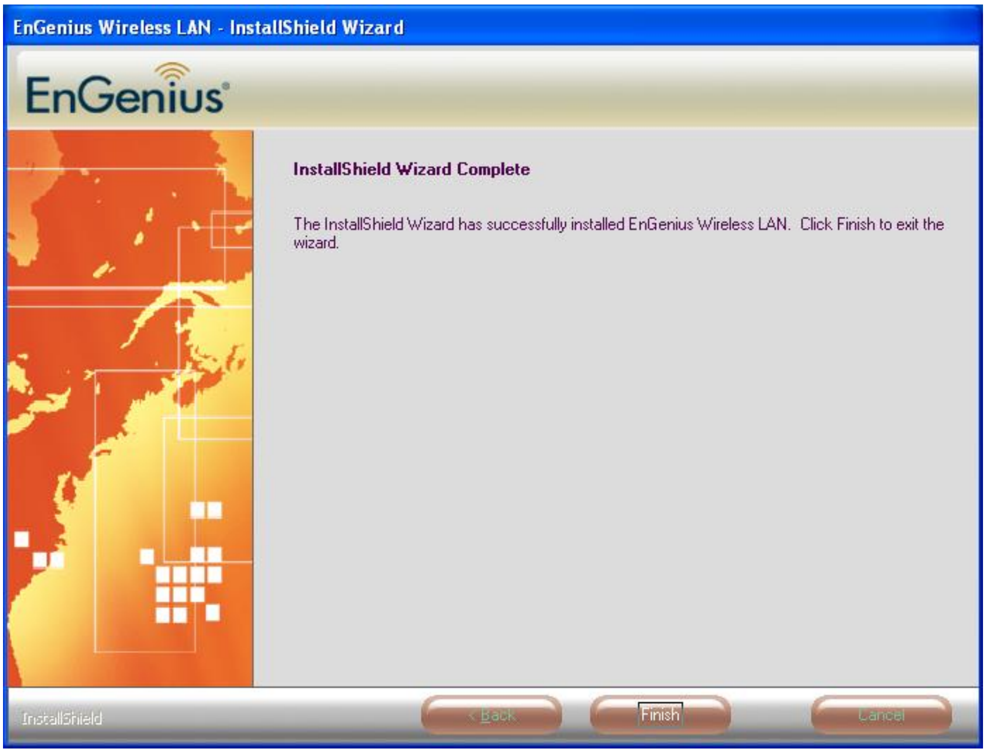
9. Click on the **Install** button to begin the installation.



The InstallShield Wizard is installing EnGenius Wireless LAN

Installing

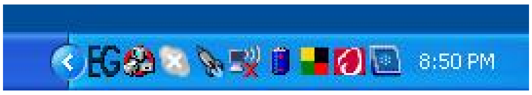
10. Wait for a few seconds until the driver and client utility is installed.



InstallShield Wizard Complete

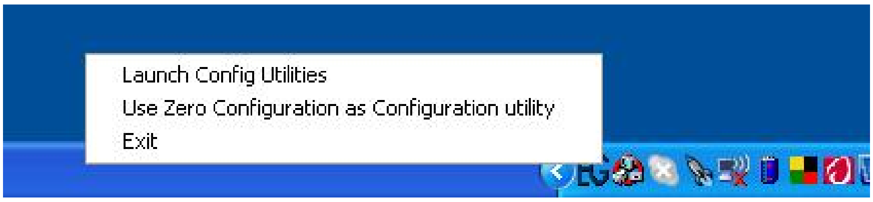
The InstallShield Wizard has successfully installed EnGenius Wireless LAN. Click Finish to exit the wizard.

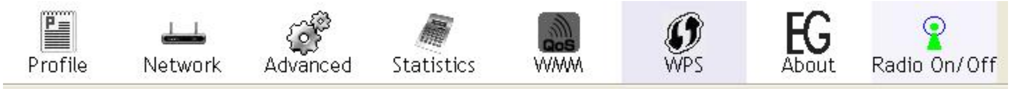
11. The installation is complete. Click on the **Finish** button.
12. Carefully insert the USB adapter into the USB port. Windows will then detect and install the new hardware.



13. An **EG** icon will then appear in the system tray. Right click on the **EG** icon and then click on **Launch Config Utilities**.

Note: Click on **Use Zero Configuration as Configuration Utility** if you would like to use Windows Zero Config.



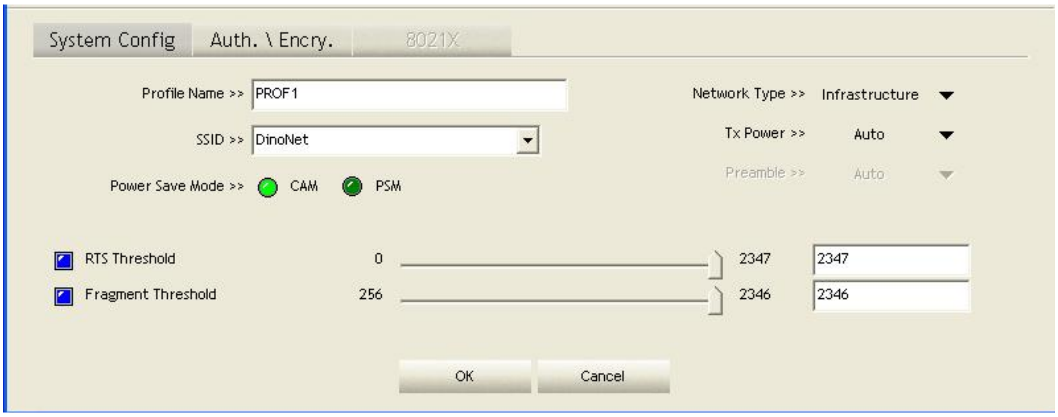


3.3 Profiles

The **Profile** tab is used to store the settings of multiple Access Points such as home, office, café, etc. When adding a profile you are required to enter a profile name and SSID as well as configure the power-saving mode, network type, RTS/fragmentation threshold and encryption/authentication settings. A profile can be configured as **Infrastructure** or **Ad-hoc** mode. The configuration settings for each mode are described below.

3.3.1 Infrastructure Mode

The infrastructure mode requires the use of an Access Point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations.



Profile Name >> PROF1

SSID >> DinoNet

Power Save Mode >> ● CAM ● PSM

Network Type >> Infrastructure

Tx Power >> Auto

Preamble >> Auto

☑ RTS Threshold 0 2347 2347

☑ Fragment Threshold 256 2346 2346

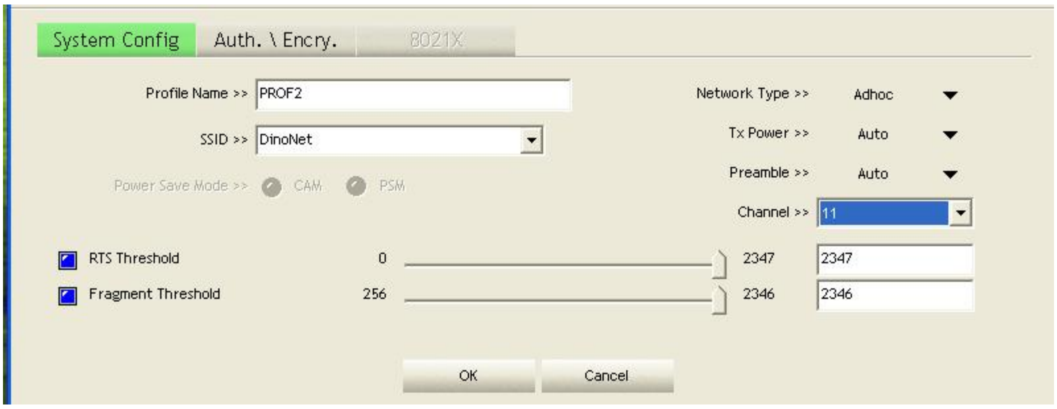
- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **PSM:** Select a power saving mode (PSM) option.
  - **CAM (Continuously Awake Mode)**: Select this option if your notebook is always connected to the power supply.
  - **PSM (Power Saving Mode)**: Select this option if your notebook uses its battery power. This option minimizes the battery usage while the network is idle.
- **Network Type:** Select **Infrastructure** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100**% or **auto**, if not, select one of the lower values for power saving.
- **RTS Threshold:** Place a check in this box if you would like to enable

RTS Threshold. Any packet in the RTS/CTS handshake larger than the specified value (bytes) will be discarded.

- **Fragment Threshold:** Place a check in this box if you would like to enable Fragment Threshold. Any packet larger than the specified value (bytes) will be discarded.
- Click on the **OK** button to save the changes.

3.3.2 Ad-hoc Mode

This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-to-peer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network.



Profile Name >> PROF2

SSID >> DinoNet

Power Save Mode >> ○ CAM ○ PSM

Network Type >> Adhoc

Tx Power >> Auto

Preamble >> Auto

Channel >> 11

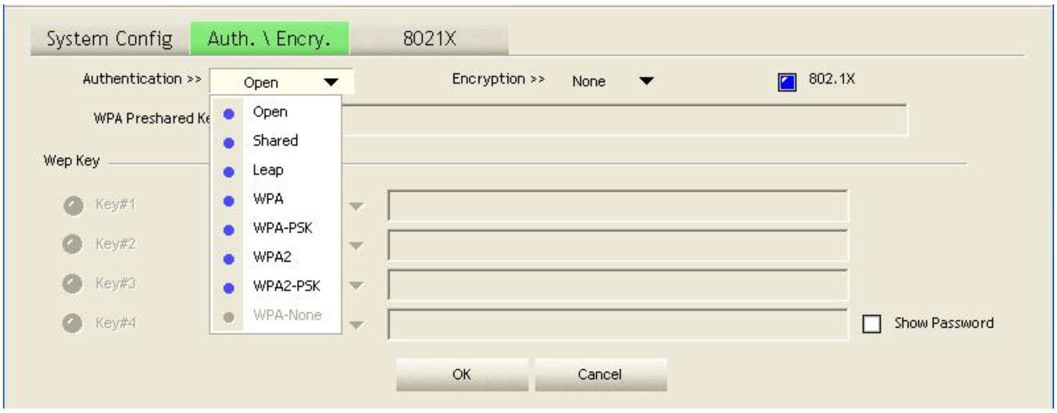
☑ RTS Threshold 0 2347 2347

☑ Fragment Threshold 256 2346 2346

- **Profile:** Enter a name for the profile; this does not need to be the same as the SSID.
- **SSID**: Enter the SSID of the network or select one from the drop-down list. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Network Type:** Select **Ad-hoc** from the drop-down list.
- **TX Power:** Select a transmit power from the drop-down list. If your notebook is connected to external power then select **100**% or **auto**, if not, select one of the lower values for power saving.
- Click on the **OK** button to save the changes.

3.4 Authentication and Security

The **Security** tab allows you to configure the authentication and encryption settings such as: WEP, WPA, WPA-PSK, WPA2, and 802.1x. Each security option is described in detail below.



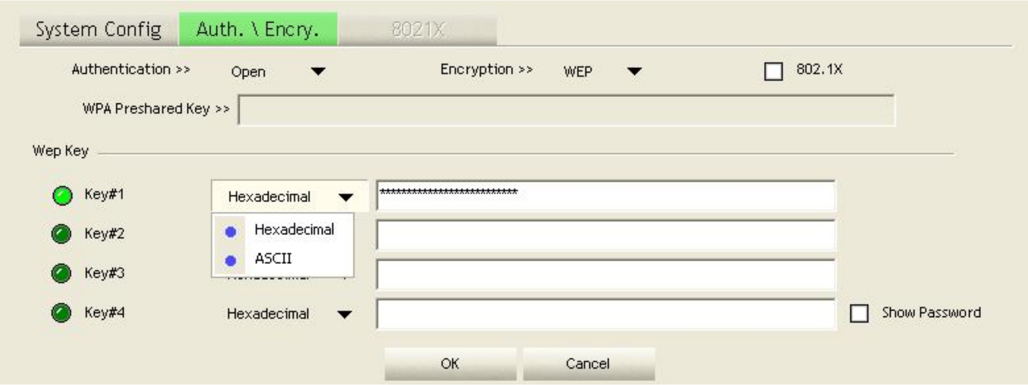
Authentication >> Open

Encryption >> None

☑ 802.1X

3.4.1 WEP Encryption

The **WEP** tab displays the WEP settings. Encryption is designed to make the data transmission more secure. You may select 64 or 128-bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase. The following information is included in this tab, as the image depicts below.



Authentication >> Open

Encryption >> WEP

□ 802.1X

WPA Preshared Key >>

Key#1 Hexadecimal **************************

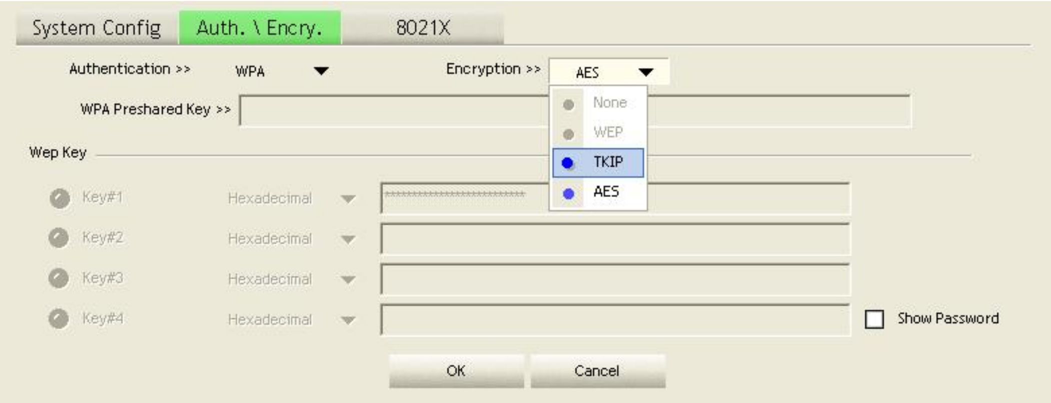
Key#4 Hexadecimal

- **Authentication Type:** Select **Open** or **Shared** from the drop-down list.
- **Encryption:** Select WEP from the drop-down list.
- **WEP Key:** Type a character string into the field. For 64-bit enter 5 alphanumeric or 10 hexadecimal characters. For 128-bit enter 13 alphanumeric or 26 hexadecimal characters.

- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

3.4.2 WPA, WPA2 Authentication & TKIP, AES Encryption

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-checking feature which makes sure that keys haven't been tampered with. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



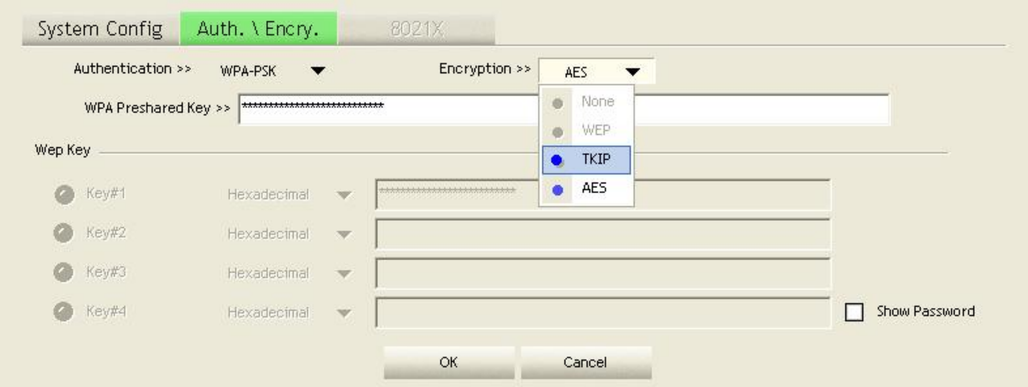
Authentication >> WPA

Encryption >> AES

- **Authentication Type**: Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

3.4.3 WPA-PSK Authentication & TKIP, AES Encryption

WPA – PSK (Pre-shared Key) is used in a Pre Shared Key mode that does not require an authentication server. Access to the Internet and the rest of the wireless network services is allowed only if the pre-shared key of the computer matches that of the Access Point. This approach offers the simplicity of the WEP key, but uses stronger TKIP encryption. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.



Authentication >> WPA-PSK

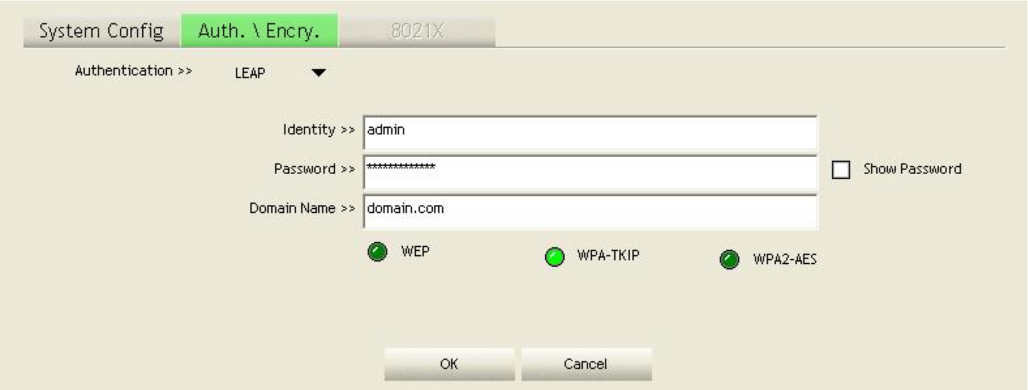
Encryption >> AES

WPA Preshared Key >> ****************************

- **Authentication Type**: Select **WPA** or **WPA2** from the drop-down list.
- **Encryption:** Select **TKIP** or **AES** from the drop-down list.
- **WPA Preshared key:** Enter a pass phrase which is between 8 and 32 characters long.
- Click on the **Apply** button to save the changes.
- **Show Password** check box. If you want to make sure the accuracy of password you type, click the **Show Password** box to check it.

3.4.4 LEAP Authentication

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client



Authentication >> LEAP

Identity >> admin

Password >> *************

Domain Name >> domain.com

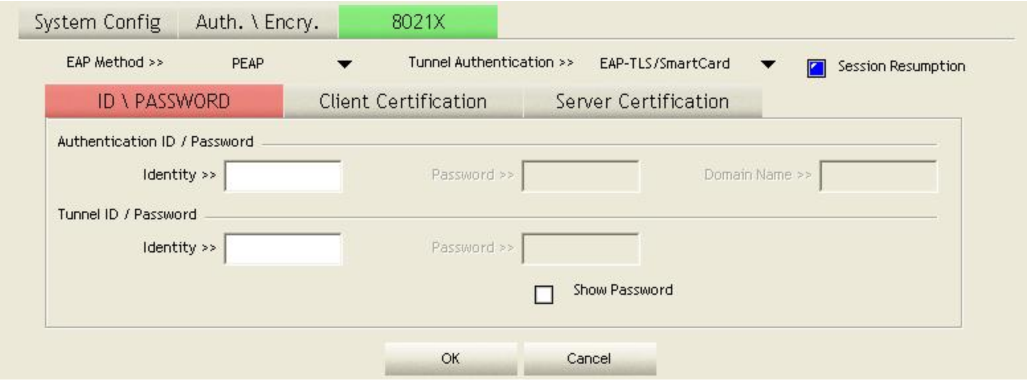
- **Authentication Type**: Select **LEAP** from the drop-down list.
- **Identity:** Enter the user name.
- **Password**: Enter the password.
- **Domain**: Enter a domain name.
- **Encryption**: Select **WEP**, **WPA-TKIP** or **WPA2-AES** encryption.
- Click on the **OK** button to save the changes.

3.4.5 802.1x with PEAP

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

3.4.5.1 PEAP Authentication with EAP/TLS Smartcard

EAP/TLS Smartcard 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.



EAP Method >> PEAP

Tunnel Authentication >> EAP-TLS/SmartCard

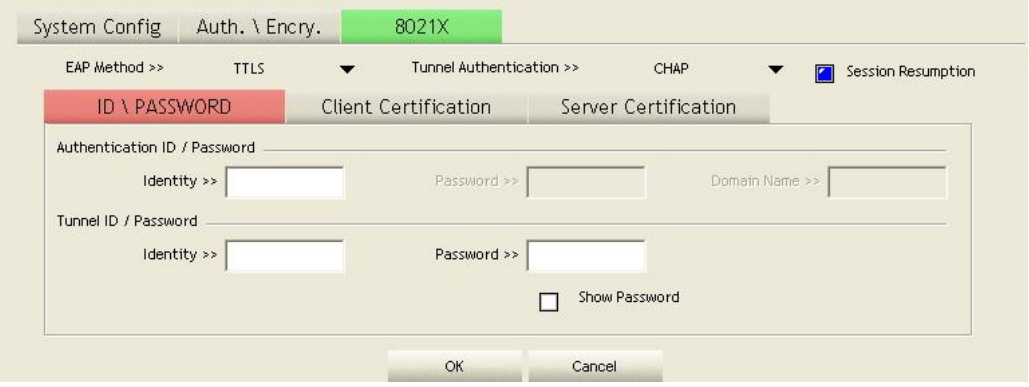
☑ Session Resumption

□ Show Password

- **Authentication Type**: Select **PEAP** from the drop-down list.
- **Protocol**: If your network uses TLS or Smart Card to authenticate its users, select **TLS/Smartcard** from the drop down list. **TLS** (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.
- **Identity**: Enter the user name.
- Click on the **OK** button to save the changes.

3.4.6 802.1x with TTLS with EAP-MD5, MS-CHAP, MS-CHAPv2

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate based authentication of both the client and authentication server.



EAP Method >> TTLS

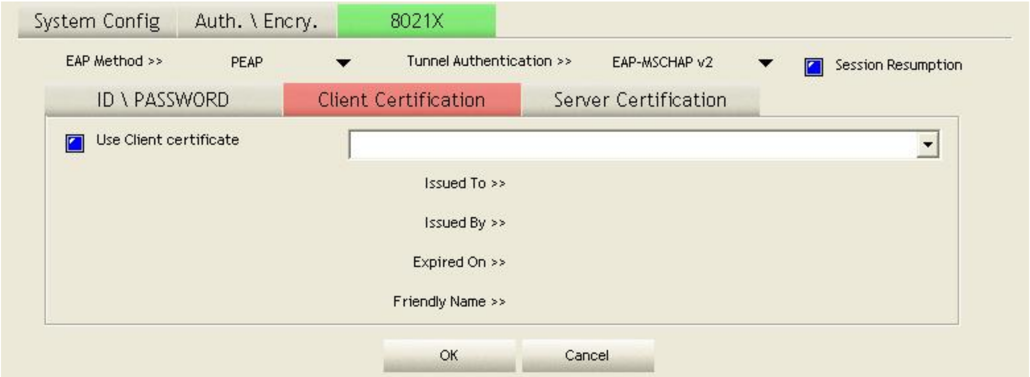
Tunnel Authentication >> CHAP

☑ Session Resumption

- ➤ **Authentication Type**: Select **TTLS** from the drop-down list.
- ➤ **Protocol**: Select EAP-MSCHAP v2, MS-CHAP, or CHAP from the drop-down list.
- ➤ **Identity**: Enter the user name.
- ➤ **Password**: Enter the password.
- ➤ Click on the **OK** button to save the changes.

3.4.7 802.1x 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 Certificate Authority.



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

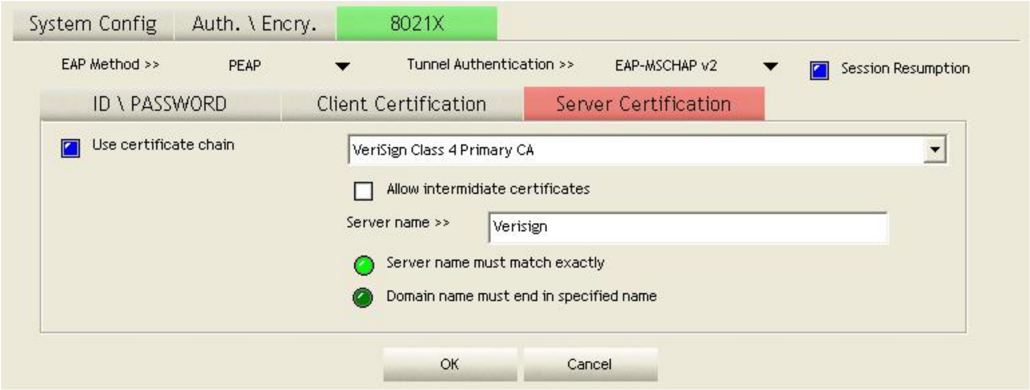
☑ Use Client certificate

Issued To >>

Issued By >>

Expired On >>

Friendly Name >>



EAP Method >> PEAP

Tunnel Authentication >> EAP-MSCHAP v2

☑ Session Resumption

☑ Use certificate chain

VeriSign Class 4 Primary CA

□ Allow intermidiate certificates

Server name >> Verisign

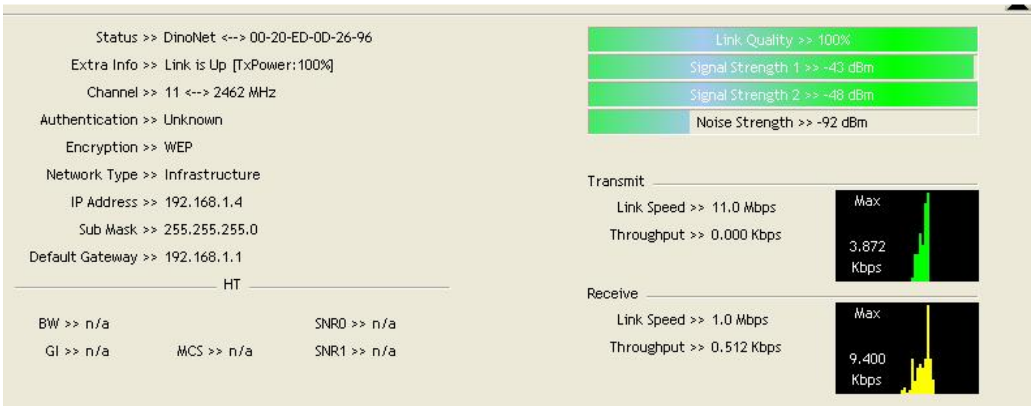
● Server name must match exactly

● Domain name must end in specified name

- **Use certificate chain**: Place a check in this to enable the certificate use.
- **Certificate issuer**: Select the Certification Authority from the drop-down list.
- **Allow intermediate certificates:** During tunnel creation the client must verify the server's certificate. When checking this certificate the signature is verified against a list of trusted certificate authorities. If this parameter is true then the client will also accept a signature from a trusted intermediate certificate authority, otherwise it will not.
- **Server name:** Enter the server name if not selected from the existing drop-down list above.
- Click on the **OK** button to save the changes.

3.5 Network

The **Network** tab displays the current status of the wireless radio. The following information is included in this tab, as the image depicts below.



Status >> DinoNet <--> 00-20-ED-0D-26-96
Extra Info >> Link is Up [TxPower:100%]
Channel >> 11 <--> 2462 MHz
Authentication >> Unknown
Encryption >> WEP
Network Type >> Infrastructure
IP Address >> 192.168.1.4
Sub Mask >> 255.255.255.0
Default Gateway >> 192.168.1.1

HT

BW >> n/a
SNR0 >> n/a
GI >> n/a
MCS >> n/a
SNR1 >> n/a

Link Quality >> 100%
Signal Strength 1 >> -43 dBm
Signal Strength 2 >> -48 dBm
Noise Strength >> -92 dBm

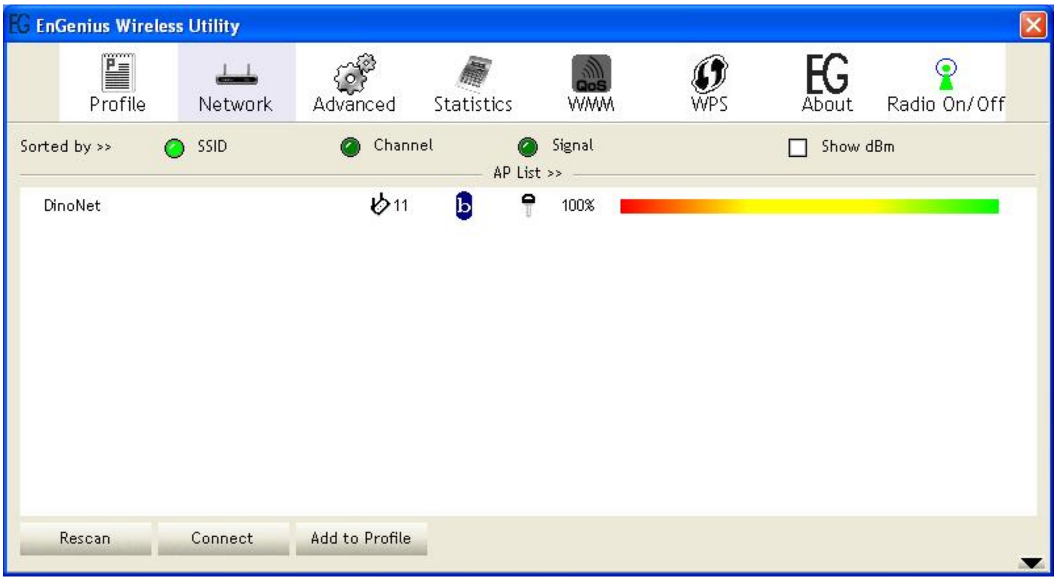
Transmit
Link Speed >> 11.0 Mbps
Throughput >> 0.000 Kbps
Max 3.872 Kbps

Receive
Link Speed >> 1.0 Mbps
Throughput >> 0.512 Kbps
Max 9.400 Kbps

- **Status:** This indicates the state of the client. There are three options:
  - **Associated:** Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of 12 HEX digits, which is the MAC address of the AP.
  - **Scanning:** Indicates that the wireless client is searching for an AP in the area.
  - **Disconnected:** Indicates that there are no APs or clients in the area.
- **Extra Info:** Displayed here are information about the link stats and the percent of output power.
- **Channel:** The operating frequency channel that the client is using (infrastructure mode).
- **Authentication:** Displays the authentication type.
- **Encryption:** Displays the encryption type.
- **Network Type:** Displays the network type; infrastructure or ad-hoc.
- **IP Address:** Displays the IP address.
- **Sub Mask:** Displays the subnet mask IP address.
- **Default Gateway:** Displays the IP address of the default gateway.
- **Link Speed**: The current rate at which the client is transmitting and receiving.
- **Transmit/ReceiveThroughput:** Displays the Tx (transmit) and Rx (receive) kilo-bytes per second.
- **Link Quality:** In infrastructure mode, this bar displays the transmission quality between an AP and a client. In Ad-hoc mode, this bar displays the transmission quality between one client, and another.
- **Signal Strength:** This bar displays the strength of the signal received from an AP or client.
- **Noise Level:** Displays the background noise level; a lower level indicates less interference.
- Click on the **OK** button to close this window.

3.5.1 Site Survey

The **Site Survey** tab displays a list of Access Points and Stations in the area, and allows you to connect to a specific one. The following information is included in this tab, as the image depicts below.



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

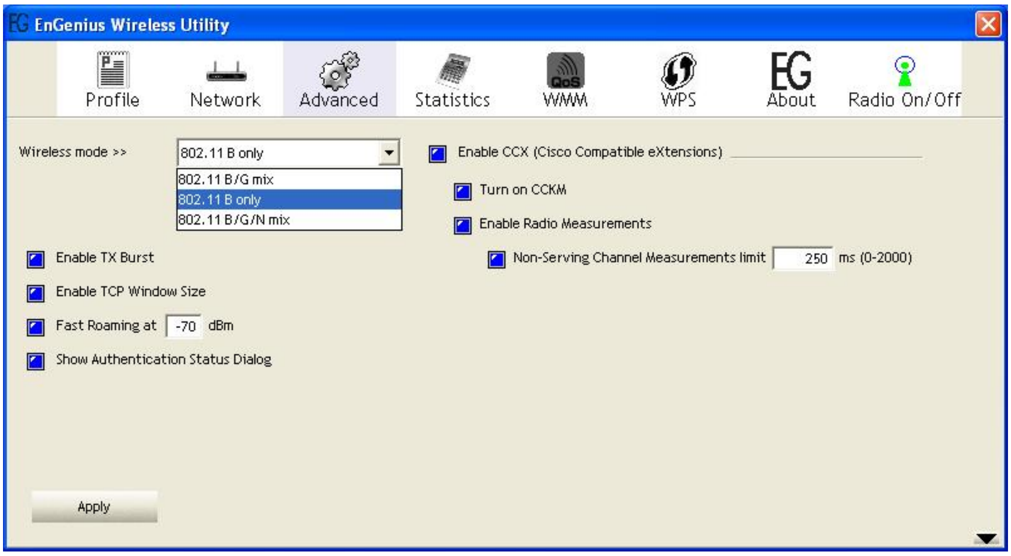
AP List >>

DinoNet 11 b 100%

- **SSID**: Displays the SSID of the Access Point. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- **Channel**: Displays the channel number of the Access Point.
- **Encryption**: Displays the encryption on the Access Point, this includes WEP, TKIP, AES or None.
- **Signal**: Displays the receiving signal strength from the Access Point.
- **Rescan:** Click on this button to view a list of Access Points in the area.
- **Connect**: to connect with a specific Access Point, select the SSID from the list, and then click on the **Connect** button.
- **Add to Profile**: Click on this button to add the SSID and its associated settings into a profile.
- Click on the **OK** button if you have made any changes.

3.6 Advanced Configuration

The **Advanced** tab is used to configure the wireless mode (802.11g, 802.11b/g-mixed, or 802.11b/g/n-mixed), and CCX.



Wireless mode >> 802.11 B only
802.11 B/G mix
802.11 B only
802.11 B/G/N mix

☑ Enable TX Burst

☑ Enable TCP Window Size

☑ Fast Roaming at -70 dBm

☑ Show Authentication Status Dialog

☑ Enable CCX (Cisco Compatible eXtensions)

☑ Turn on CCKM

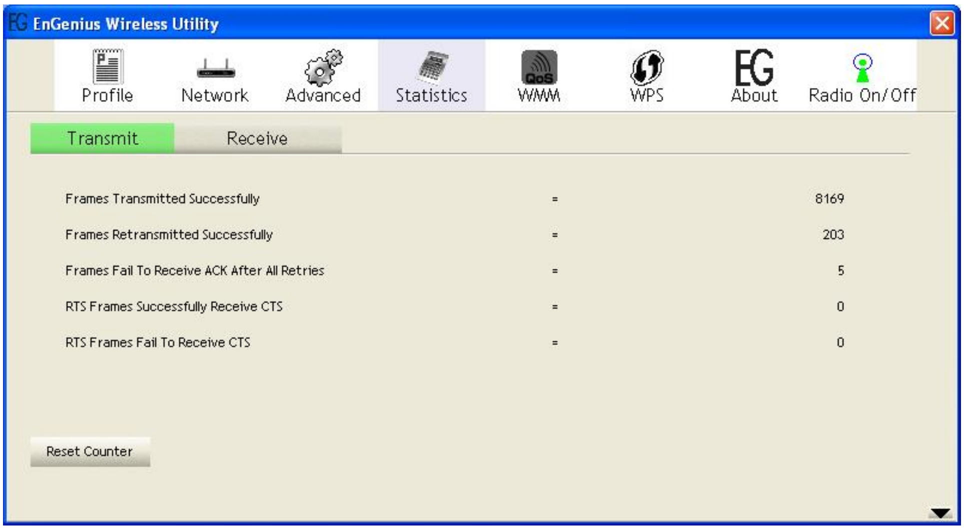
☑ Enable Radio Measurements

☑ Non-Serving Channel Measurements limit 250 ms (0-2000)

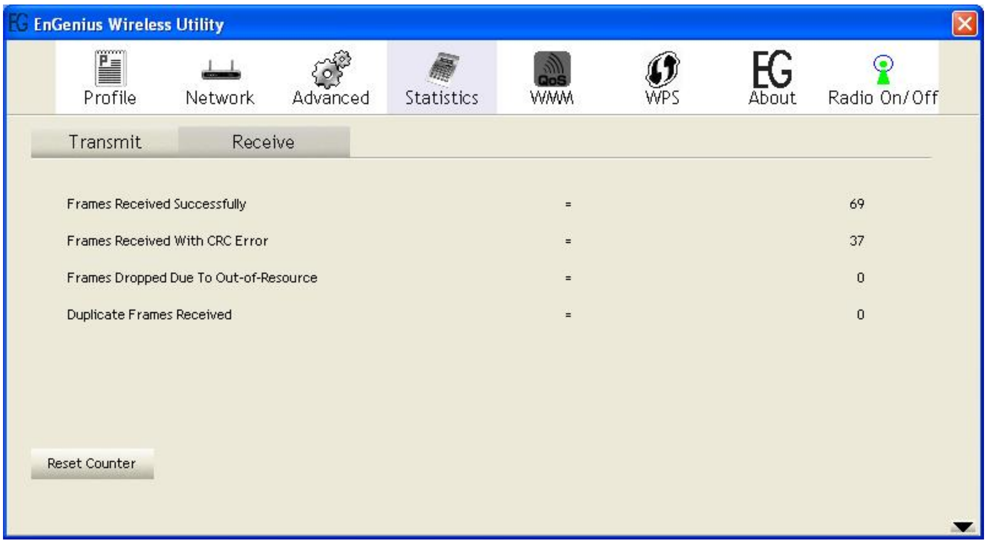
- **Wireless mode**: Select **802.11 b/g/n mix** if the wireless network uses both 11b, 11g, and 11n stations and APs. **B/G Protection**: This is the ERP protection mode of 802.11g. Selecting **auto** will dynamically send frames with and without protection. Select **On** to send a frame without protection, and **Off** to send it with protection.
- **Enable TCP Window Size**: Enhance the throughput if enable this function.
- **CCX**: Enable this option if the network supports Cisco Compatible Extensions.
- Click on the **Apply** button to close this window.

3.7 Statistics

The **Statistics** tab displays transmit and receive packet statistics in real-time. Information included is frames transmitted/received successfully, transmitted successfully without and after retry, received with CRC error, duplicate frames received, etc.



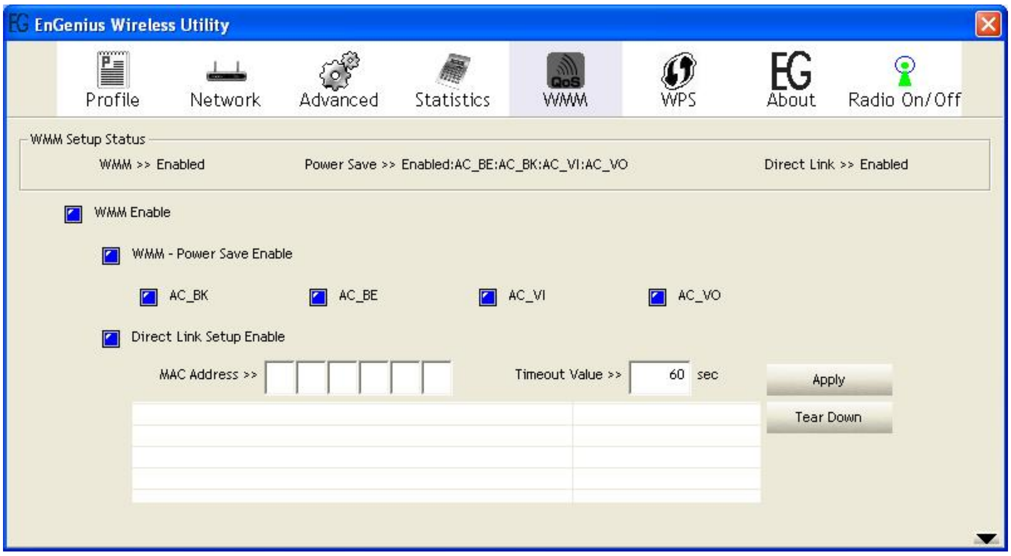
Frames Transmitted Successfully	=	8169
Frames Retransmitted Successfully	=	203
Frames Fail To Receive ACK After All Retries	=	5
RTS Frames Successfully Receive CTS	=	0
RTS Frames Fail To Receive CTS	=	0



Frames Received Successfully	=	69
Frames Received With CRC Error	=	37
Frames Dropped Due To Out-of-Resource	=	0
Duplicate Frames Received	=	0

3.8 WMM (Wireless Multimedia)

Click on the **WMM** tab. Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interpretability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories), however it does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.



WMM Setup Status

WMM >> Enabled Power Save >> Enabled:AC_BE:AC_BK:AC_VI:AC_VO Direct Link >> Enabled

☑ WMM Enable

☑ WMM - Power Save Enable

☑ AC_BK ☑ AC_BE ☑ AC_VI ☑ AC_VO

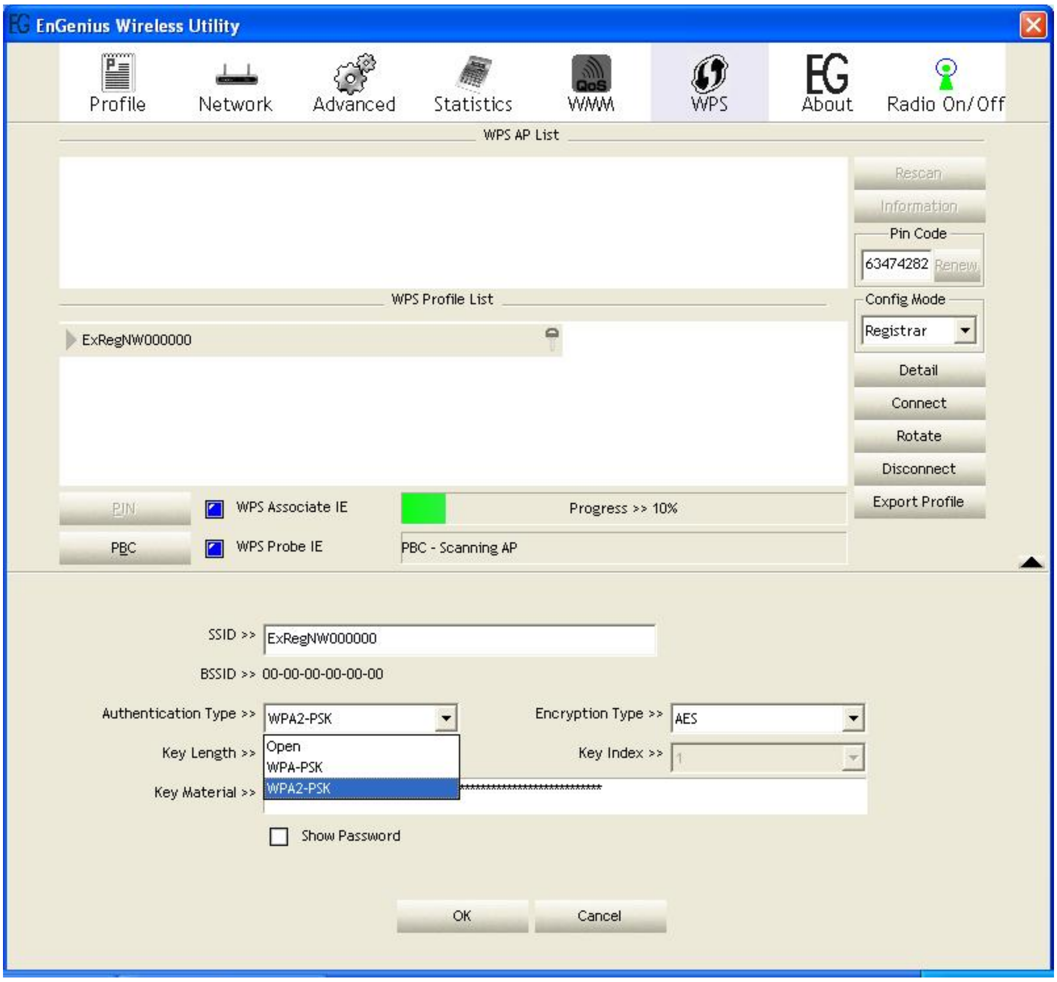
☑ Direct Link Setup Enable

MAC Address >> Timeout Value >> 60 sec

- **WMM Enable**: Choose to enable or disable WMM.
- **WMM Power Save Enable**: Choose to enable or disable power save mode on WMM.
- **Direct Link Setup Enable**: Specify a MAC address and timeout value.
- Click on the **Apply** button to close this window.

3.9 WPS

WPS (Wireless Push Button) is used for WiFi Protected Setup. By pressing this button, the security settings of the device will automatically synchronize with other wireless devices on your network that support Wi-Fi Protected Setup.



Pin Code: 63474282

Config Mode: Registrar

WPS Profile List: ExRegNW000000

☑ WPS Associate IE

☑ WPS Probe IE

Progress >> 10%

PBC - Scanning AP

SSID >> ExRegNW000000

BSSID >> 00-00-00-00-00-00

Authentication Type >> WPA2-PSK

Encryption Type >> AES

Key Length >>

Key Index >> 1

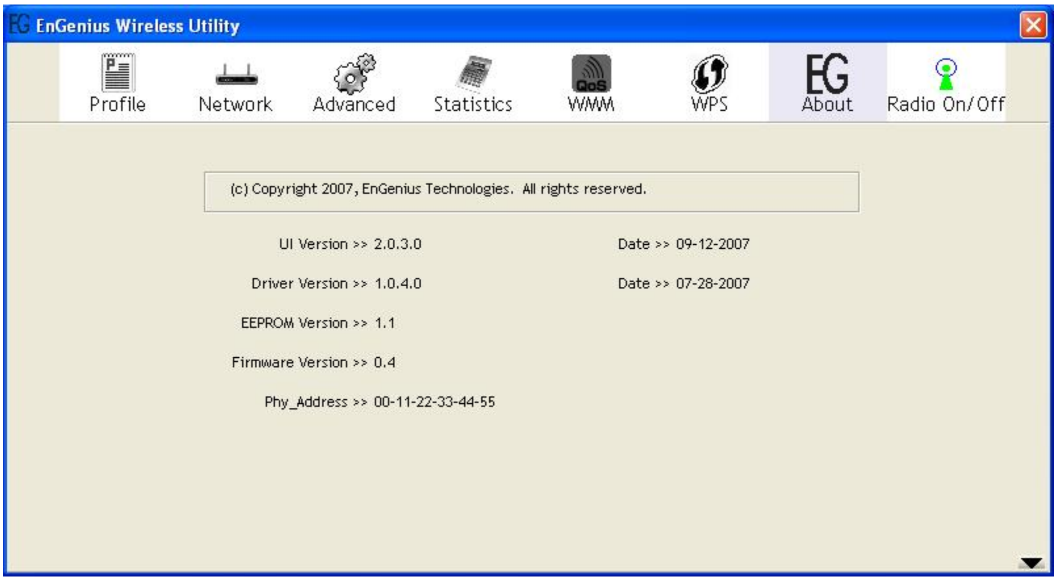
Key Material >> ****************************

□ Show Password

- **Rescan:** Click on this button to view a list of Access Points in the area.
- **WPS Information:**
- **Pin Code:**
- **Config Mode:**
- **Detail:**
- **Connect:**
- **Rotate:**
- **Disconnect:**
- **Import Profile:**
- **PBC:**
- **WPS Associate IE:**
- **WPS Probe IE:**
- Click on the **OK** button if you have made any changes.

3.10 About

The **About** tab displays information about the device, such as: the network driver version and date, configuration utility version and date, and the NIC (Network Interface Card) firmware version and date.



(c) Copyright 2007, EnGenius Technologies. All rights reserved.

UI Version >> 2.0.3.0 Date >> 09-12-2007

Driver Version >> 1.0.4.0 Date >> 07-28-2007

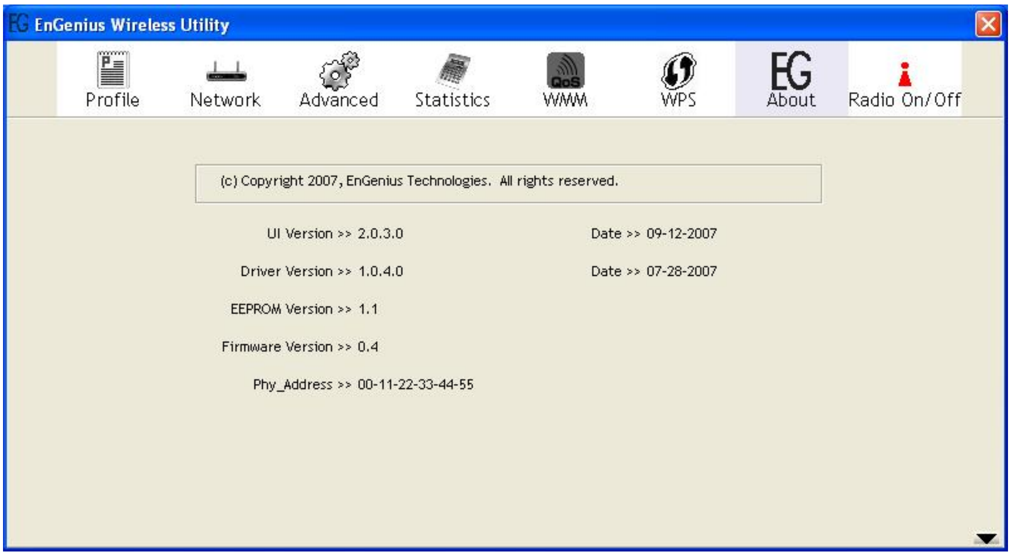
EEPROM Version >> 1.1

Firmware Version >> 0.4

Phy_Address >> 00-11-22-33-44-55

3.11 Radio

The **Radio** tab allows you to enable or disable the radio.



(c) Copyright 2007, EnGenius Technologies. All rights reserved.

UI Version >> 2.0.3.0 Date >> 09-12-2007

Driver Version >> 1.0.4.0 Date >> 07-28-2007

EEPROM Version >> 1.1

Firmware Version >> 0.4

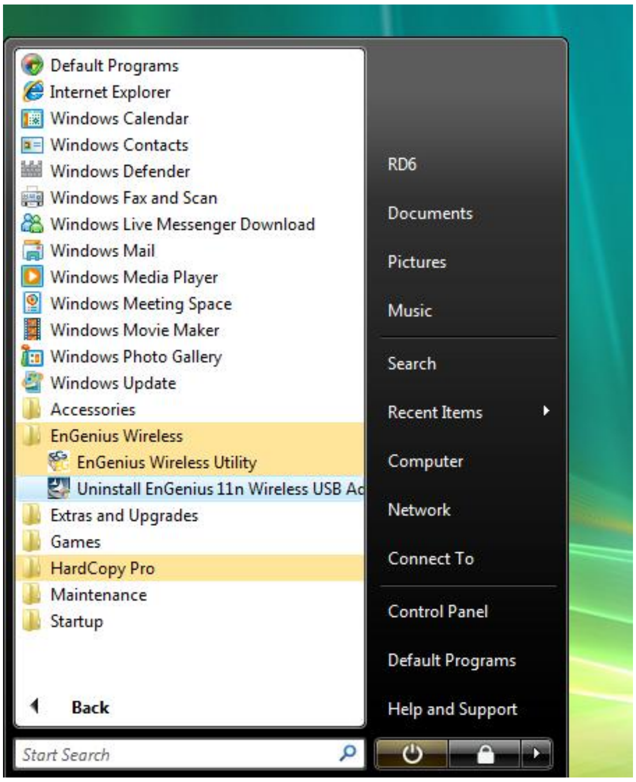
Phy_Address >> 00-11-22-33-44-55

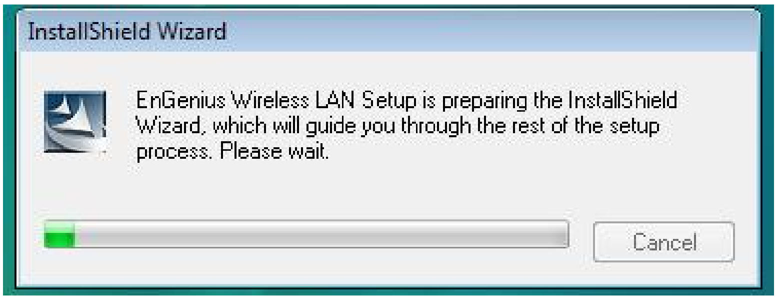
3.12 Uninstall the Drivers & Client Utility

If the USB client adapter installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the USB adapter and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the client utility:

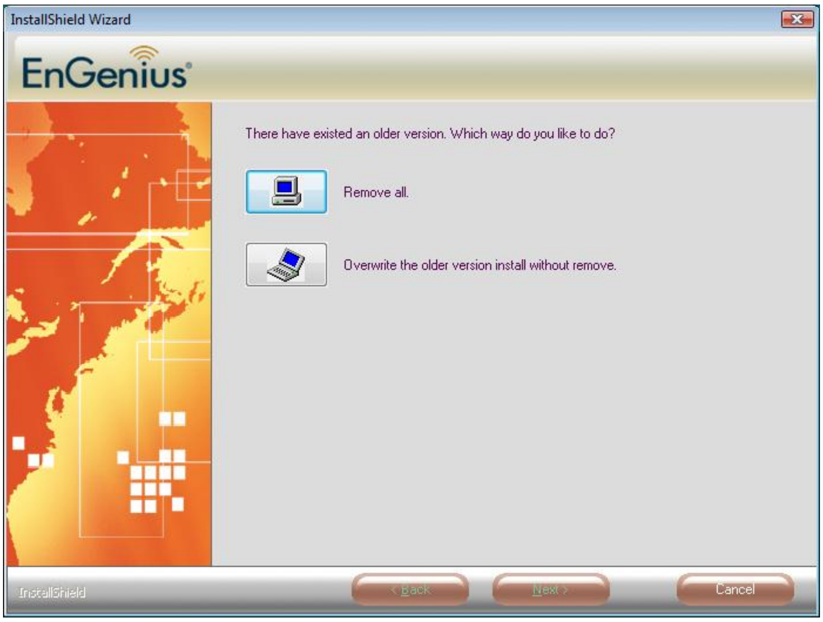
1. Click on **Start > EnGenius Wireless > Uninstall EnGenius Wireless USB Adapter**




InstallShield Wizard

EnGenius Wireless LAN Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

2. The un-installation process will then begin.



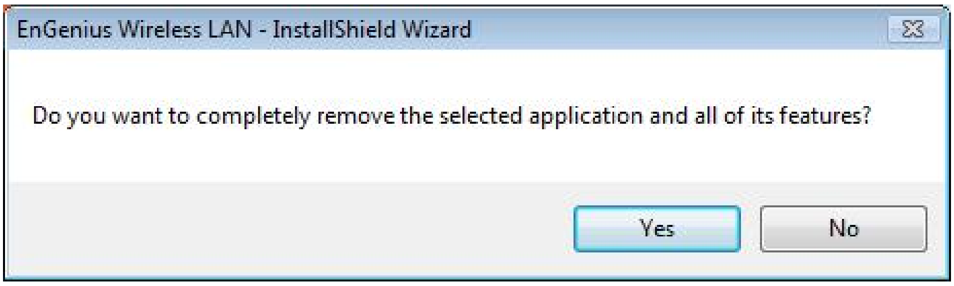
InstallShield Wizard

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

Remove all.

Overwrite the older version install without remove.

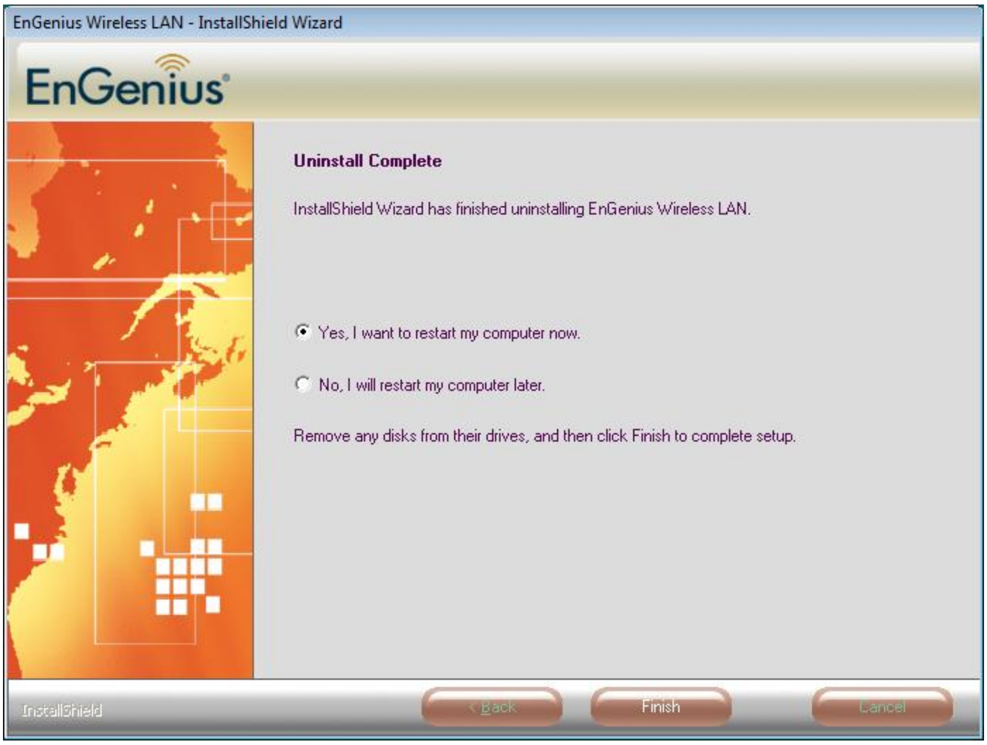
3. Select the **Remove all** button and then click on the **Next** button.



EnGenius Wireless LAN - InstallShield Wizard

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

4. Click on the **Yes** button to confirm the un-installation process.



EnGenius Wireless LAN - InstallShield Wizard

Uninstall Complete

InstallShield Wizard has finished uninstalling EnGenius Wireless LAN.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

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

5. The un-installation process is complete. Select **Yes, I want to restart my computer now** radio button and then click on the Finish button. Then remove the USB adapter.