11g Wireless LAN
USB 2.0 Client Adapter

User's Manual

Version: 1.0

Table of Contents

Revision History

Version	Date	Notes
1.0	July 8, 2004	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 (11Mbps) and the 802.11g (54Mbps) wireless 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 data encryption allowing you to experience the most secure wireless connectivity available.

This chapter describes the features & benefits, package contents, applications, and network configuration.

1.1 Features & Benefits

Features	Benefits
High-speed data rate up to 54 Mbps	Capable of handling heavy data payloads such as MPEG video streaming.
IEEE 802.11 b/g compliant	Fully interoperable with IEEE 802.11b/g compliant products
Wi-Fi Protected Access (WPA)	Powerful data security
IEEE 802.1x client support	Enhances authentication and security
Plug and Play USB interface	Easy installation
Multi-country roaming (802.11d) support	Automatically adjusts regulatory domain to operate in different countries.
Advanced Power Management	Low power consumption in power saving mode.

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 USB Cable
- One Quick Installation Guide
- One CD-ROM with User's Manual Included

1.3 USB Adapter Description

The USB adapter is a standard USB adapter that fits into any USB interface. The USB adapter has a LED indicator and an external flip-up 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 98SE/ME/ /2000/XP operating system.
- 10 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.

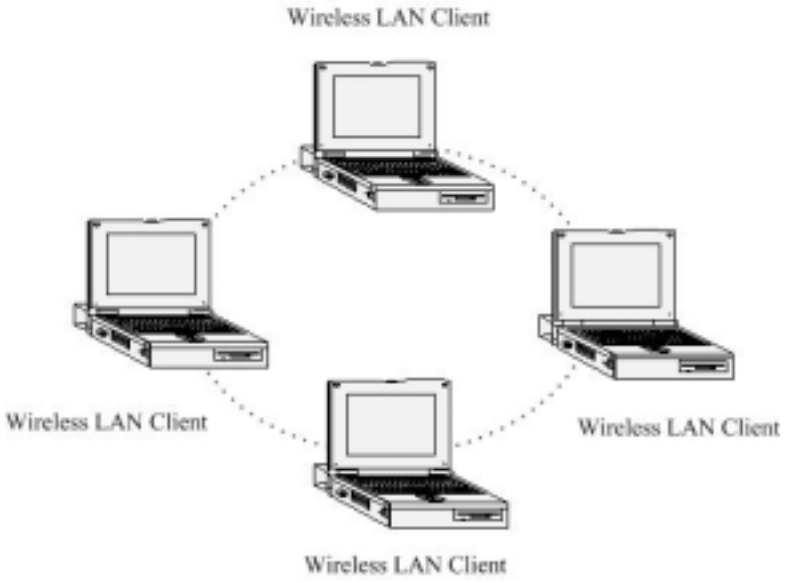
1.6 Network Configuration

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.

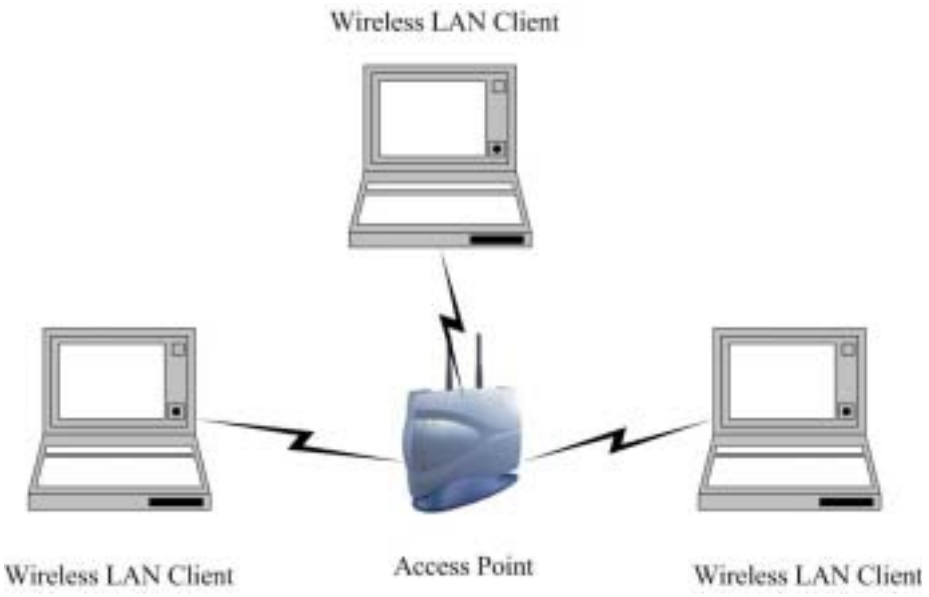
a) Ad-hoc (peer-to-peer) Mode

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 Install Drivers & Client Utility

2.1 Before You Begin

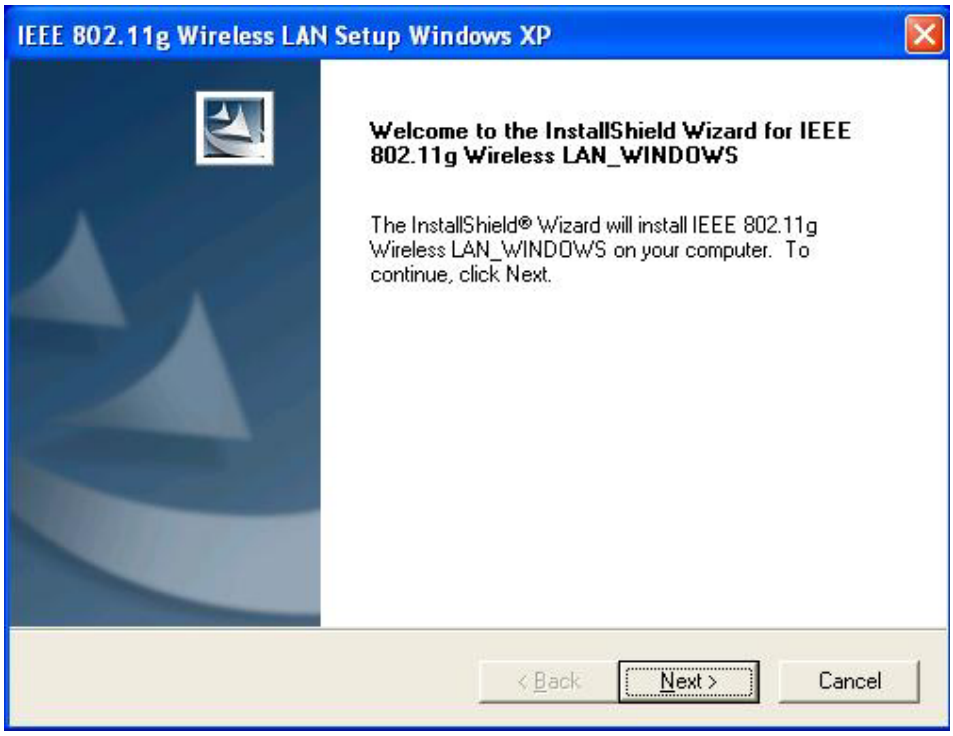
Before installing the new drivers of your USB adapter, you need to disable all of the Wireless LAN USB drivers that you have installed.

During the installation, Windows 98SE/ME/2000/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.

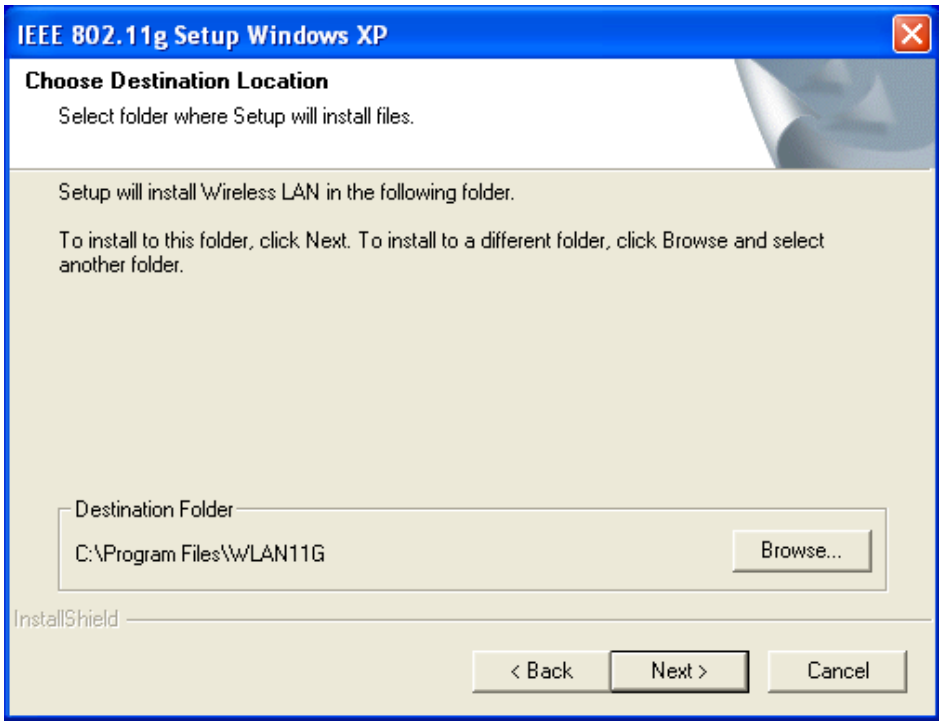
2.2 Installing the Drivers

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

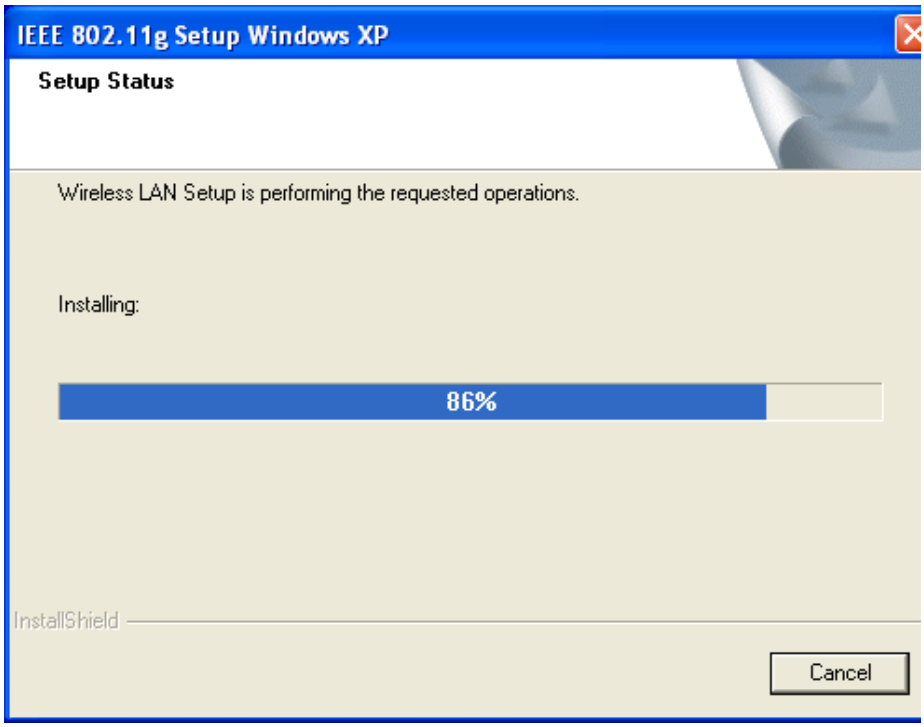
1. Insert the CD-ROM that was provided to you in this package. The setup should run automatically. If the setup does not run automatically, then you must manually select the **setup.exe** file from the CD-ROM drive.
2. Once the setup begins you will see the **Install Shield Wizard**, as the image depicts below.



3. Click on the **Next** button to continue. The Setup Wizard will then let you select a destination folder for the drivers, as the image depicts below.

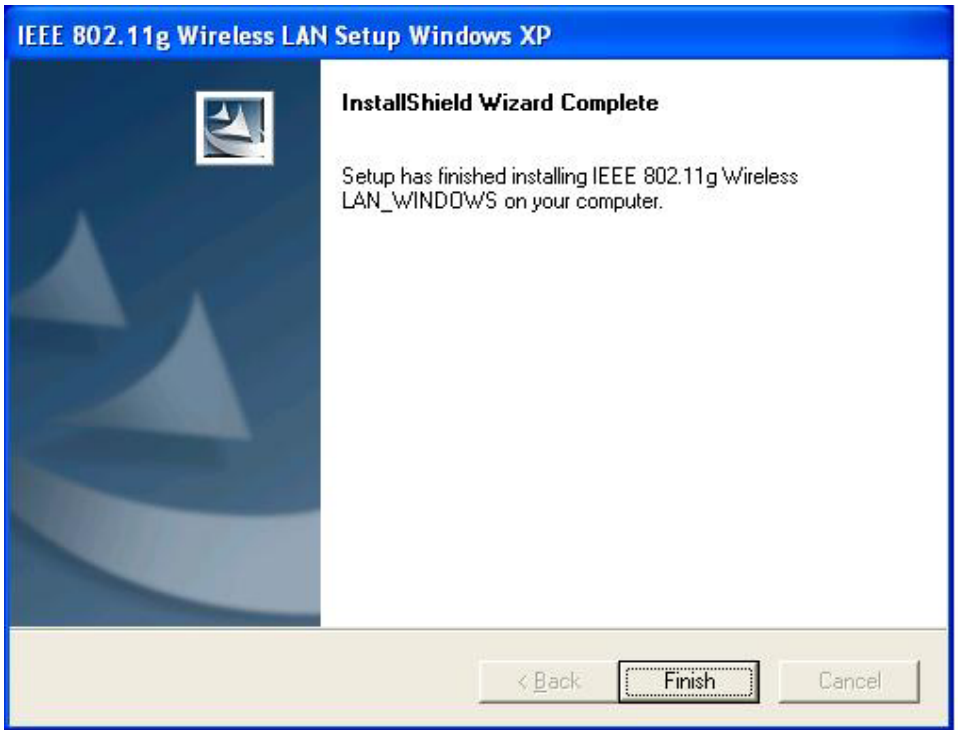


4. Click on the **Browse** button to select another drive or folder to install the drivers, and then click on the **Next** button. If you would like to use the default destination folder, click on the **Next** button. The drivers will then copy to your hard disk drive, as displayed below.



5. The Install Wizard will then remind you to insert the WLAN adapter after the setup is complete. Click on the **OK** button to continue.

6. The first part of the driver installation is complete. Select **Yes, I want to restart my computer now**, radio button and then click on the **Finish** button.



7. After you computer has restarted, plug the USB cable into the USB port of your notebook or PC. Windows will automatically detect the USB adapter and display the **Found New Hardware Wizard**, as the image depicts below.

8. Select the **Install the software automatically (Recommended)** radio button, and then click on the **Next** button to continue.

9. If you are using Windows XP, you will see a message regarding Windows Logo Testing, click on the **Continue Anyway** button to continue.

10. The Setup Wizard will then copy the necessary files. The Driver & Utility installation is now complete, click on the **Finish** button.

2.3 Verify the Instillation

Follow the steps below in order to verify that the USB adapter has been installed and is functioning properly:

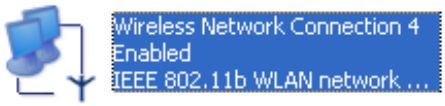
1. Click on **Start > Settings > Control Panel**.
2. Double click on the **System** icon.
3. Click on the **Hardware** tab, and then click on the **Device Manger** button.
4. Select **Network adapters** to view a list of network adapters on your PC. You will then see a window similar to the image below.

5. Make sure that there isn't a yellow (**?**) or a red (**X**) next to the USB adapter (*Local 11g USB*). If you see a (**?**) or (**X**) you would need to uninstall the drivers, and reinstall them again. In order to uninstall the drivers refer to **Chapter 4**.

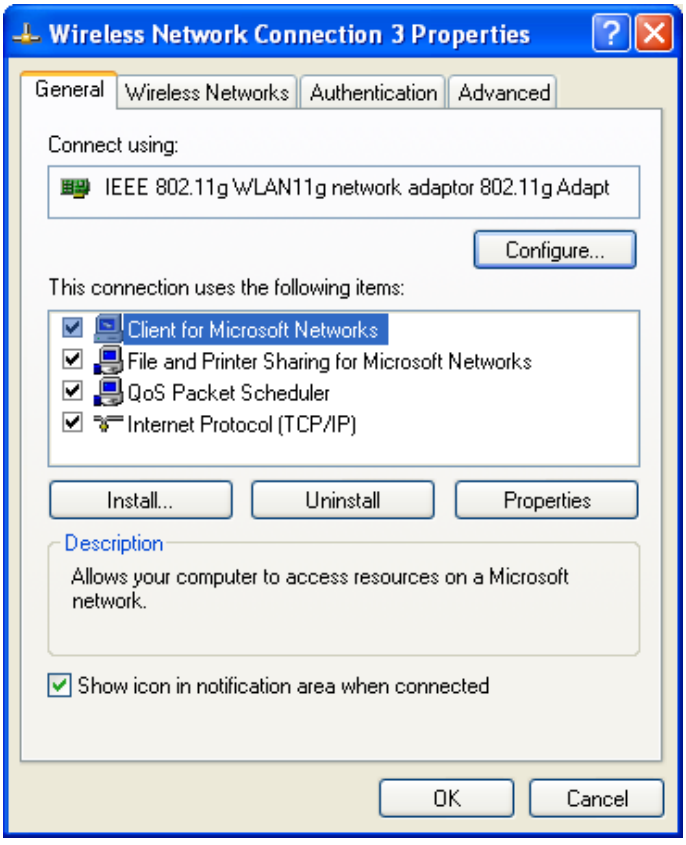
2.4 Disable Windows WEP/SSID Configuration

In order to configure **SSID** and **WEP** settings from the Client Utility, you must first disable the Windows based SSID and WEP configuration from the Network Configuration in the Control Panel. Follow the steps below in order to disable the SSID and WEP on Windows.

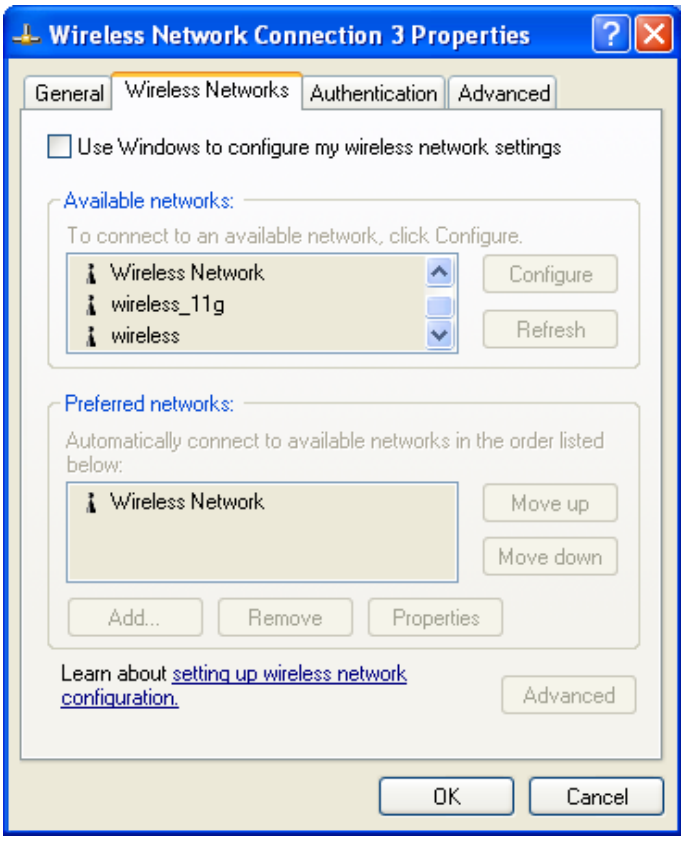
1. Click on **Start > Settings > Control Panel**.
2. Double click on the **Network Connections** icon.
3. Right-click on the wireless network connection for the USB adapter, and then select **Properties**. The icon may look similar to the image below.



After you click on **Properties**, the **Wireless Network Connection Properties** window will appear, as the image depicts below:



4. Click on the **Wireless Networks** tab, you will then see the following screen.



5. Make sure that there isn't any check placed in the **Use Windows to configure my wireless network settings** check box.
6. Click on the **OK** button.

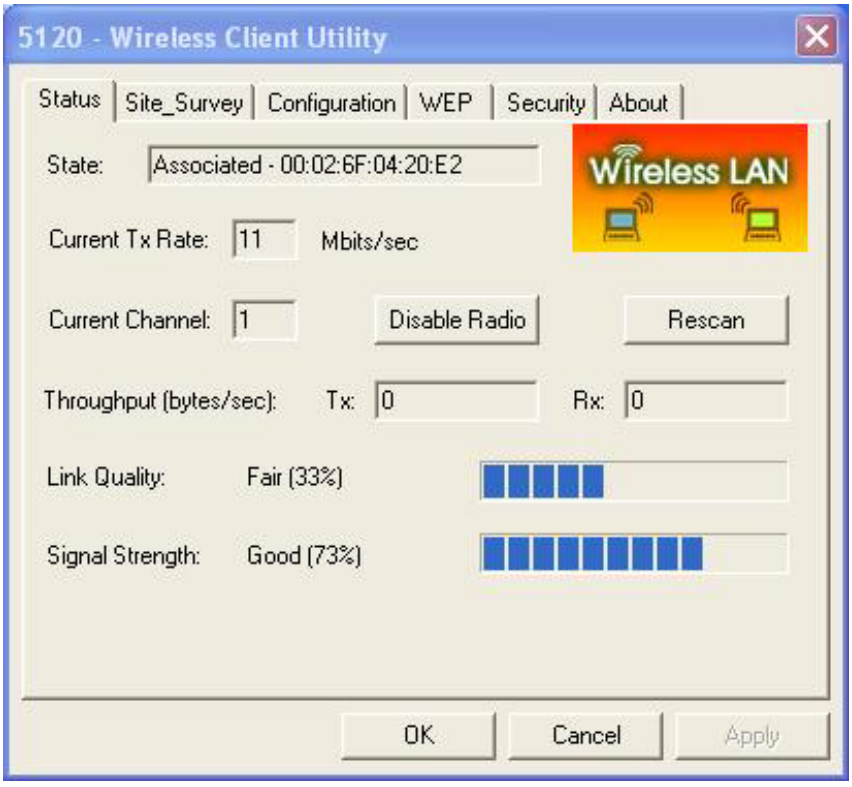
3 Using the Client Utility

After a successful installation you will see the USB adapter **Client Utility** in the Windows Program group called **IEEE 802.11g**.

To run the Client Utility click **Start > Programs > IEEE 802.11.g > IEEE 802.11.g WLAN Utility.**

3.1 Status

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



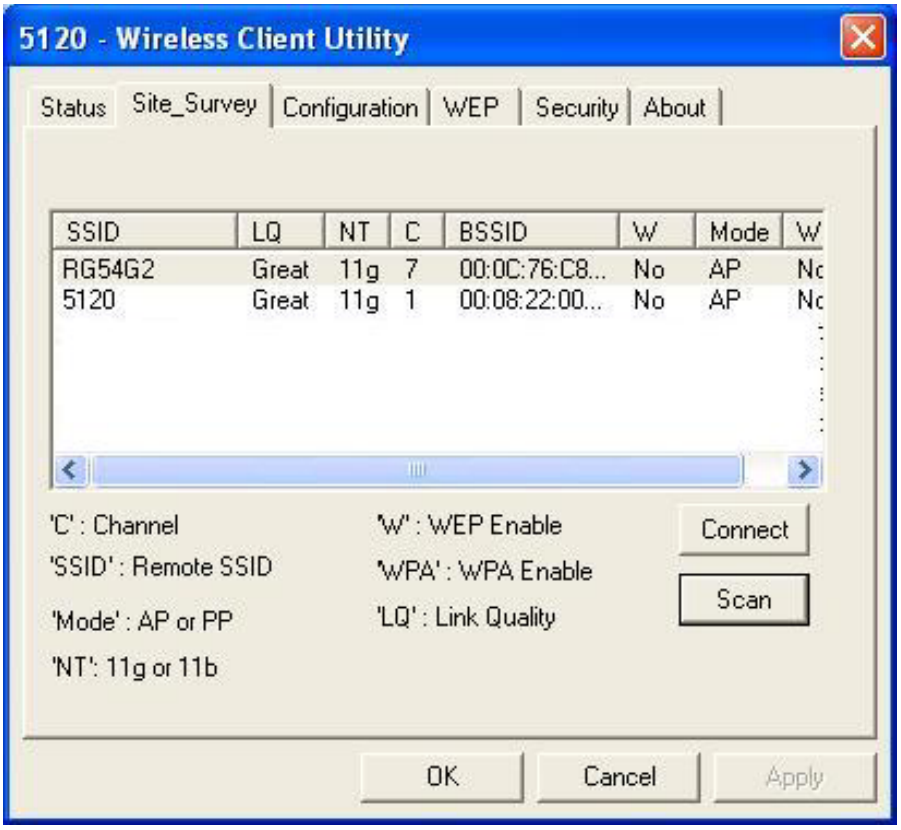
- **State:** This indicates the state of the client. There are three options:
  - **Associated:** Indicates that the wireless client is connected to an Access Point (AP). The BSSID is shown in the form of six HEX digits, which is the MAC address of the AP.
  - **Scanning:** Indicates that the wireless client is searching for an AP in the area.
  - **Disconnected:** Indicates that there are no APs or clients in the area.
- **Current Channel:** The operating frequency channel that the client is using (infrastructure mode).
- **Current Tx Rate**: The current rate at which the client is transmitting.
- **Throughput (bytes/sec):** Displays the Tx (transmit) and Rx (receive)

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.
- **Enable/Disable Radio:** Click on this button to switch on/off the wireless radio.
- **Rescan:** Click on this button to rescan the environment for a better signal/frequency.
- Click on the **Apply** or **OK** button if you have made any changes.

3.2 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.

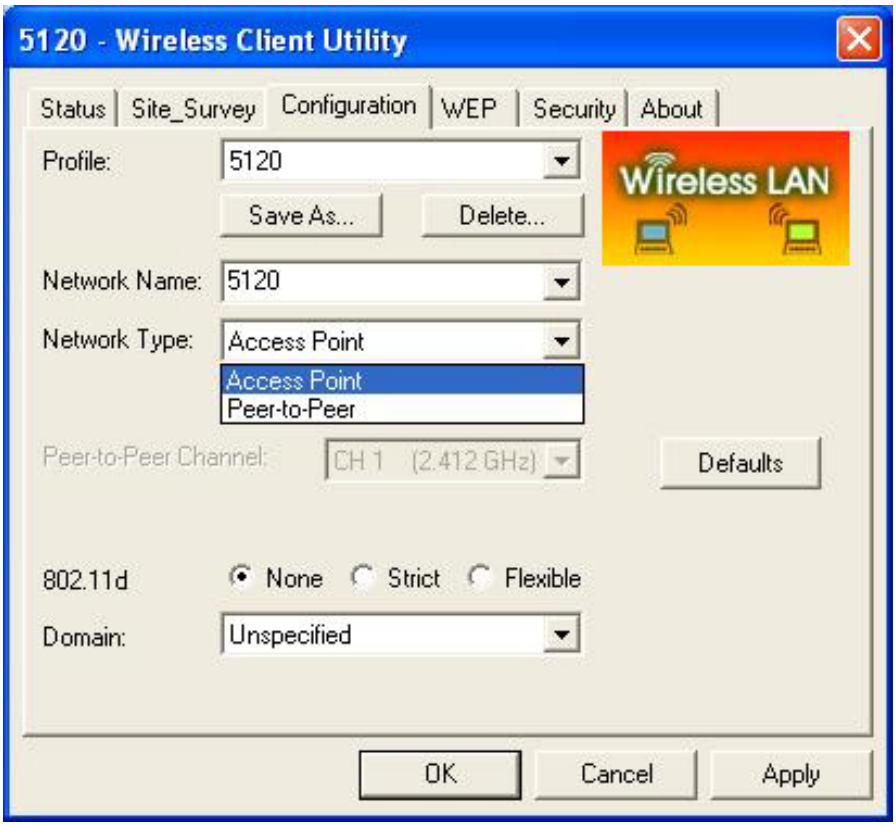


- **SSID**: displays the SSID of the Access Point.
- **LQ**: displays the link quality of the Access Point.
- **NT**: displays the network type, 11g or 11b.
- **C**: displays the channel number of the Access Point.
- **BSSID**: displays the MAC address of the Access Point.
- **W**: indicates whether WEP is enabled.

- **Mode**: indicates whether the SSID is a Station (PP) or Access Point (AP).
- **WPA**: indicates whether WPA (Wi-Fi Protected Access) is enabled.
- **Connect**: to connect with a specific Access Point, select the Access Point from the drop-down list, and then click on the **Connect** button.
- **Scan**: to view a list of Access Points in the area click on the Scan button.
- Click on the **Apply** or **OK** button if you have made any changes.

3.3 Configuration

The **Configuration** tab displays settings such as profile name, network name, network type, and 802.11d country selection. The following information is included in this tab, as the image depicts below.

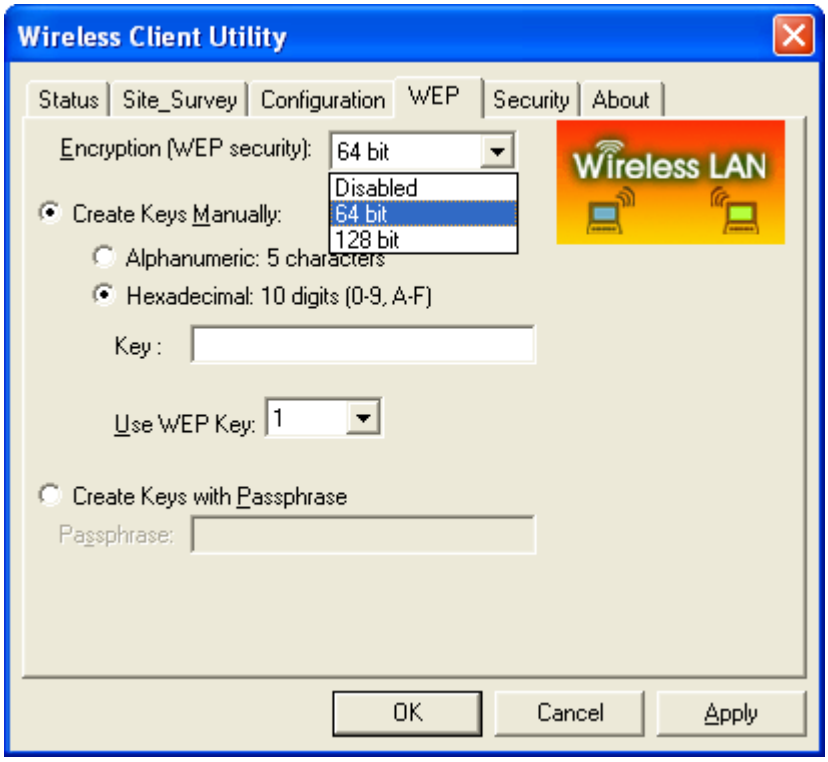


- **Profile:** click on the **Save As** button and enter a name for this profile; this can be any name that you may associate with your network. This feature comes in handy when you need to work at several locations where there are different network settings. Using this you can configure a different profile for each of your networks.
- **Network Name**: enter the SSID of the network. 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 Peer-to-Peer or Access Point from the drop-down list.
  - **Peer-to-Peer**: if two or more stations exchange data directly

without an AP.
  - **Access Point**: if the stations exchange data through an Access Point.
- **Peer-to-Peer Channel:** this option is just for Peer-to-Peer (Ad-Hoc) mode. You need to specify a channel on which the communications are established. Each station in a Peer-to-Peer (Ad-Hoc) network must specify the same channel and network type (SSID).
- **802.11d:** Select **Strict** or **Flexible** if you would like to enable 802.11d. If you select **Flexible**, you must select your country from the **Domain** drop-down list.
- Click on the **Apply** button to save the changes.

3.4 WEP

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.



- **Encryption (WEP security):** Select one of the encryption keys (64-bit, 128-bit, or disable) from the drop-down list. Click either on **Create Keys Manually** radio button or on **Create Keys with Passphrase** radio button.

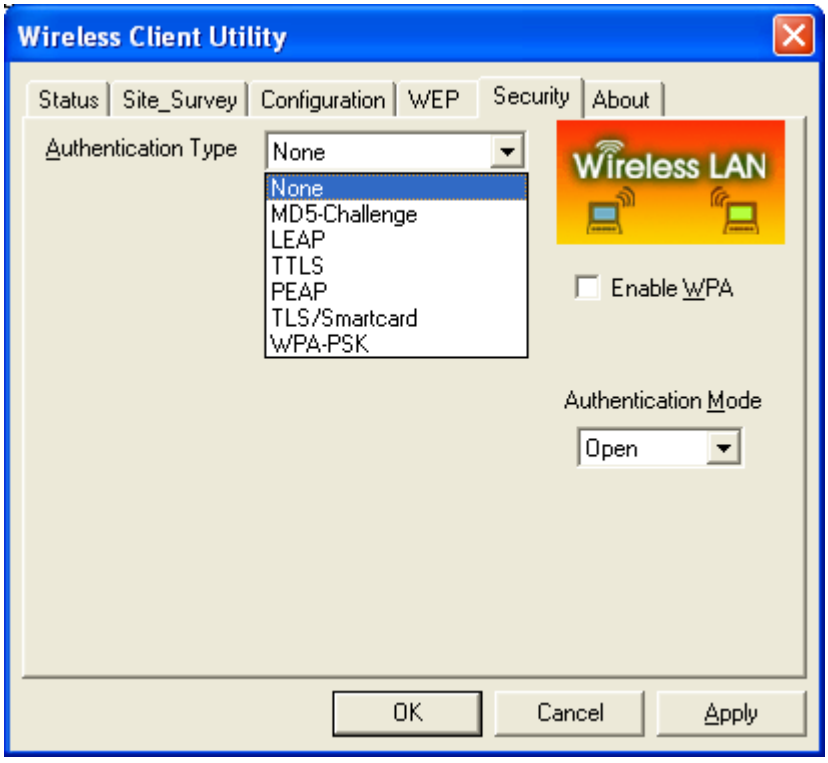
There are two ways, Alphanumeric and Hexadecimal, to set the different characters

- **Create Keys with Pass phrase:** 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.

3.5 Security

The **Security** tab displays the authentication security settings such as MD5, LEAP, TTLS, PEAP, TLS Smart card, and WPA-PSK. Details on how to configure each of these settings are listed in this section.

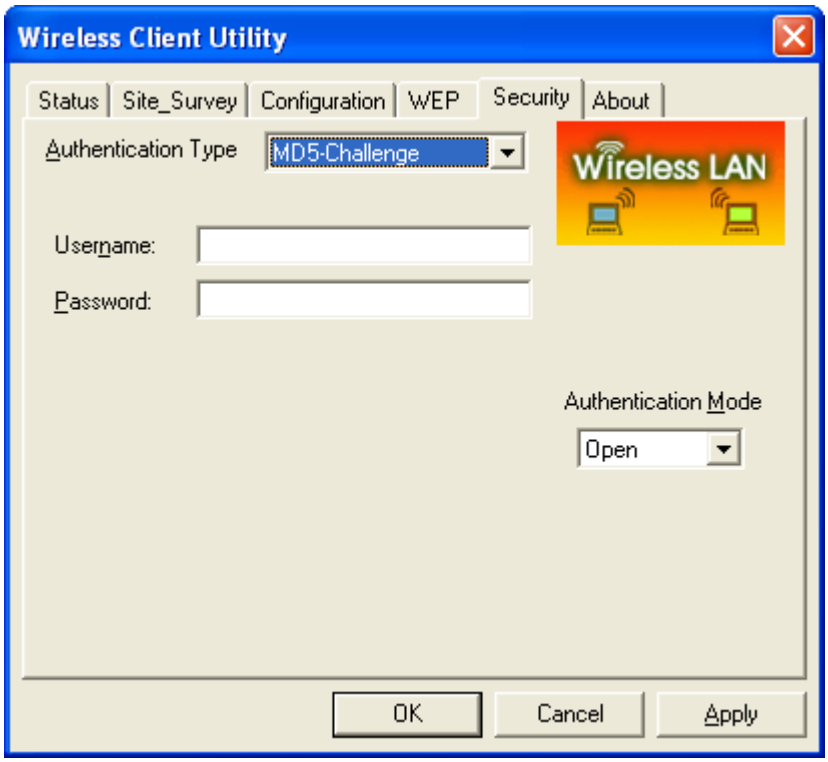
3.5.1 No Authentication



- **Authentication Type**: If your network does not require any authentication, select **None** from the drop down list.
- **Enable WPA:** Place a check in this box if you would like to enable the WPA function. **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.

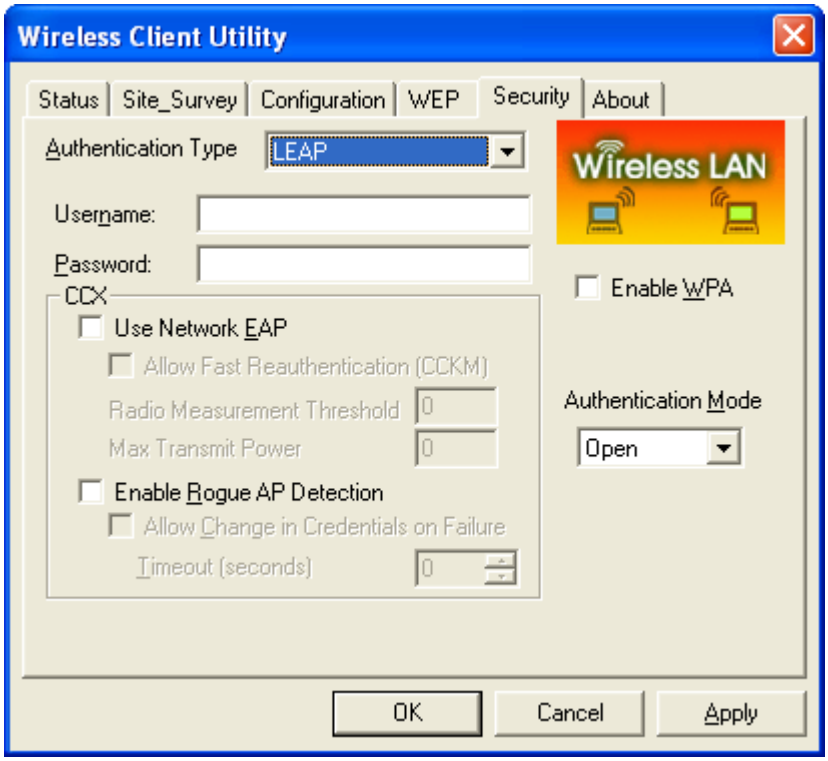
- **Authentication Mode**: select an authentication mode from the drop-down list. Options available are **Open**, **Shared**, or **AutoSwitch**. Select **AutoSwitch** if you would like the device to automatically switch between Open and Shared authentication mode.
- Click on the **Apply** button to save the changes.

3.5.2 MD5-Challenge



- **Authentication Type**: If your network uses MD5 to authenticate its users, select **MD5-Challenge** from the drop down list.
- **Username**: Enter the user name.
- **Password**: Enter the password.
- **Authentication Mode**: select an authentication mode from the drop-down list. Options available are **Open**, **Shared**, or **AutoSwitch**. Select **AutoSwitch** if you would like the device to automatically switch between Open and Shared authentication mode.
- Click on the **Apply** button to save the changes.

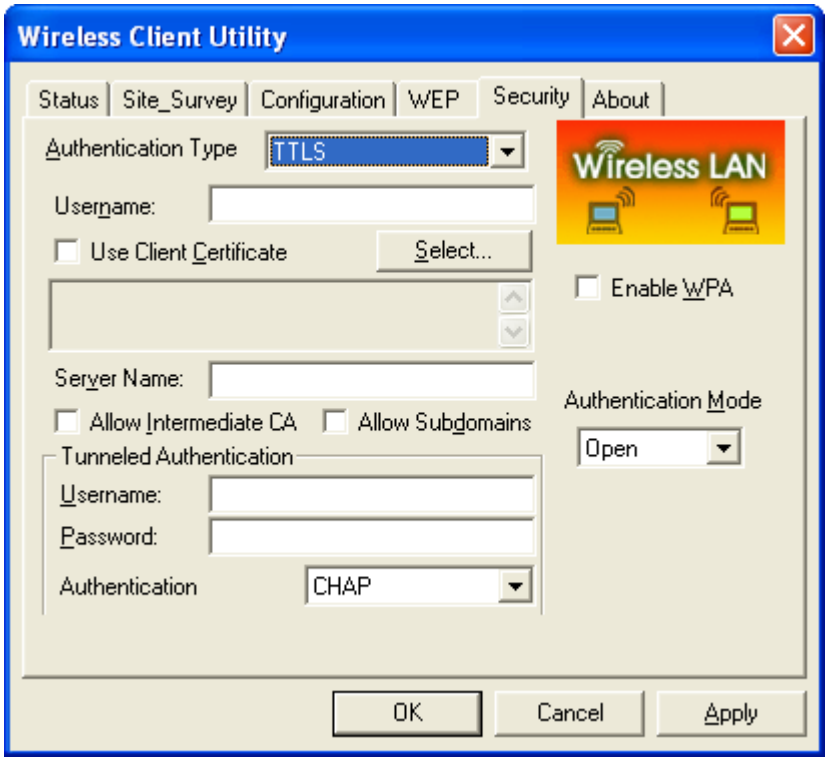
3.5.3 LEAP



- **Authentication Type**: If your network uses LEAP to authenticate its users, select **LEAP** from the drop down list. **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.
- **Username**: Enter the user name.
- **Password**: Enter the password.
- **Enable WPA:** Place a check in this box if you would like to enable the WPA function. **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.
- **Authentication Mode**: select an authentication mode from the drop-down list. Options available are **Open**, **Shared**, or **AutoSwitch**. Select **AutoSwitch** if you would like the device to automatically switch between Open and Shared authentication mode.

- **Use Network EAP:** Place a check in box if you would like to use 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
- Click on the **Apply** button to save the changes.

3.5.4 TTLS

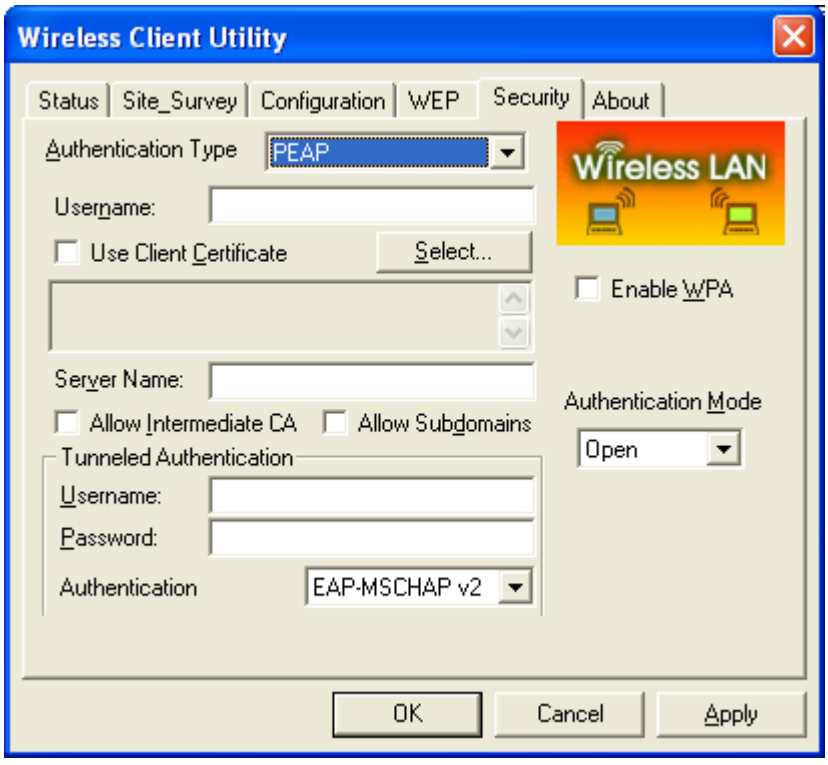


- **Authentication Type**: If your network uses TTLS to authenticate its users, select **TTLS** from the drop down list. **TLS** (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.
- **Username**: Enter the user name.
- **Use Client Certificate**: Place a check in this box if you would like to use a client certificate and then click on the **Select** button.
- **Server Name**: Enter the name of the server.
- **Allow Intermediate CA:** 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 we will not.
- **Allow Subdomains**: During tunnel creation the Client must verify the Server's certificate. This parameter indicates whether the Server's name

must match the **Server Name** parameter exactly or if only the sub domain must match.

- **Tunneled Authentication / Username**: Enter the user name.
- **Tunneled Authentication / Password**: Enter the password.
- **Authentication**: Select an authentication method from the drop-down list.
- **Enable WPA:** Place a check in this box if you would like to enable the WPA function. **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.
- **Authentication Mode**: select an authentication mode from the drop-down list. Options available are **Open**, **Shared**, or **AutoSwitch**. Select **AutoSwitch** if you would like the device to automatically switch between Open and Shared authentication mode.
- Click on the **Apply** button to save the changes.

3.5.5 PEAP

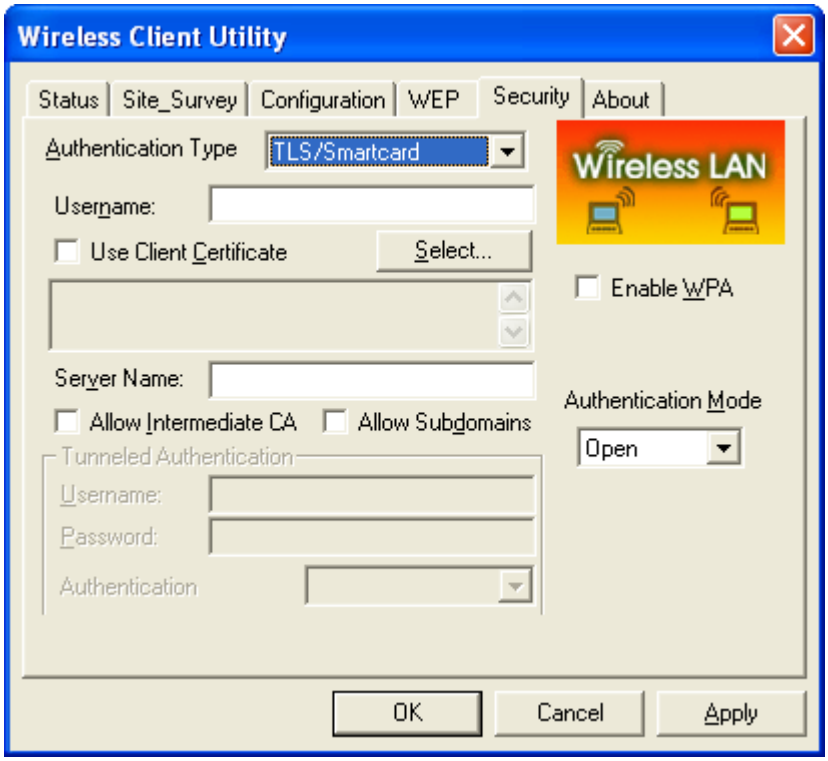


- **Authentication Type**: If your network uses PEAP to authenticate its users, select **PEAP** from the drop down list. **PEAP** (Protected Extensible Authentication Protocol) is a protocol developed jointly by Microsoft, RSA Security, and Cisco for transmitting authentication data, including passwords over an 802.11 wireless network. PEAP authenticates wireless LAN clients using only server-side digital certificates by creating an SSL/TLS tunnel

between the client and the authentication server. The tunnel then protects the subsequent user authentication exchange.

- **Username**: Enter the user name.
- **Use Client Certificate**: Place a check in this box if you would like to use a client certificate and then click on the **Select** button.
- **Server Name**: Enter the name of the server.
- **Allow Intermediate CA:** 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 we will not.
- **Allow Subdomains**: During tunnel creation the Client must verify the Server's certificate. This parameter indicates whether the Server's name must match the **Server Name** parameter exactly or if only the sub domain must match.
- **Tunneled Authentication / Username**: Enter the user name.
- **Tunneled Authentication / Password**: Enter the password.
- **Authentication**: Select an authentication method from the drop-down list.
- **Enable WPA:** Place a check in this box if you would like to enable the WPA function. **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.
- **Authentication Mode**: select an authentication mode from the drop-down list. Options available are **Open**, **Shared**, or **AutoSwitch**. Select **AutoSwitch** if you would like the device to automatically switch between Open and Shared authentication mode.
- Click on the **Apply** button to save the changes.

3.5.6 TLS / Smart Card

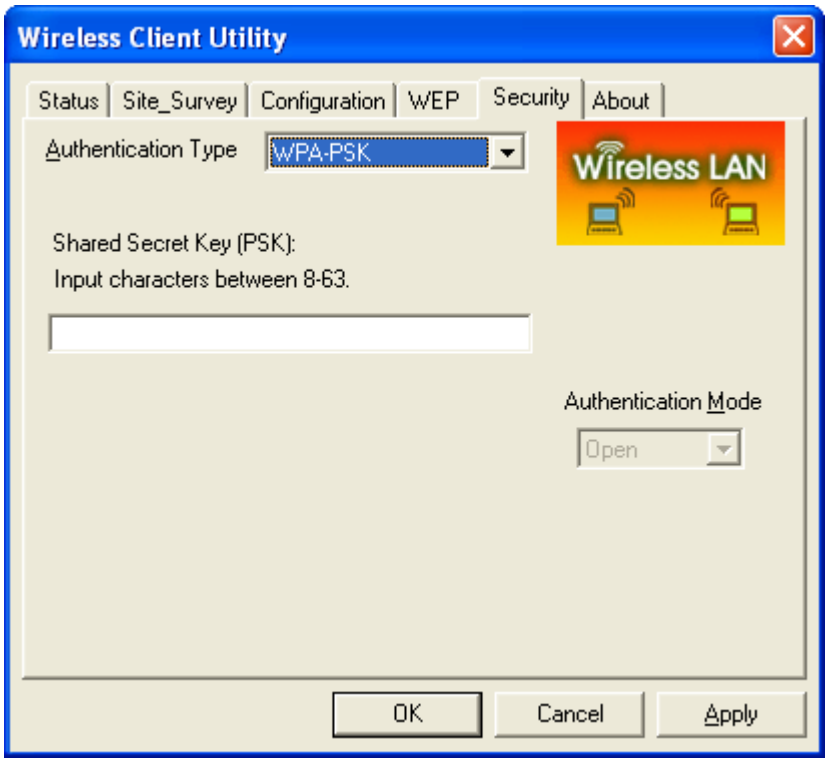


- **Authentication Type**: If your network uses TLS or Smart Card to authenticate its users, select **TLS/Smartcard** from the drop down list. **TLS** (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.
- **Username**: Enter the user name.
- **Use Client Certificate**: Place a check in this box if you would like to use a client certificate and then click on the **Select** button.
- **Server Name**: Enter the name of the server.
- **Allow Intermediate CA:** 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 we will not.
- **Allow Subdomains**: During tunnel creation the Client must verify the Server's certificate. This parameter indicates whether the Server's name must match the **Server Name** parameter exactly or if only the sub domain must match.
- **Tunneled Authentication / Username**: Enter the user name.
- **Tunneled Authentication / Password**: Enter the password.
- **Authentication**: Select an authentication method from the drop-down list.
- **Enable WPA:** Place a check in this box if you would like to enable the WPA function. **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.

- **Authentication Mode**: select an authentication mode from the drop-down list. Options available are **Open**, **Shared**, or **AutoSwitch**. Select **AutoSwitch** if you would like the device to automatically switch between Open and Shared authentication mode.
- Click on the **Apply** button to save the changes.

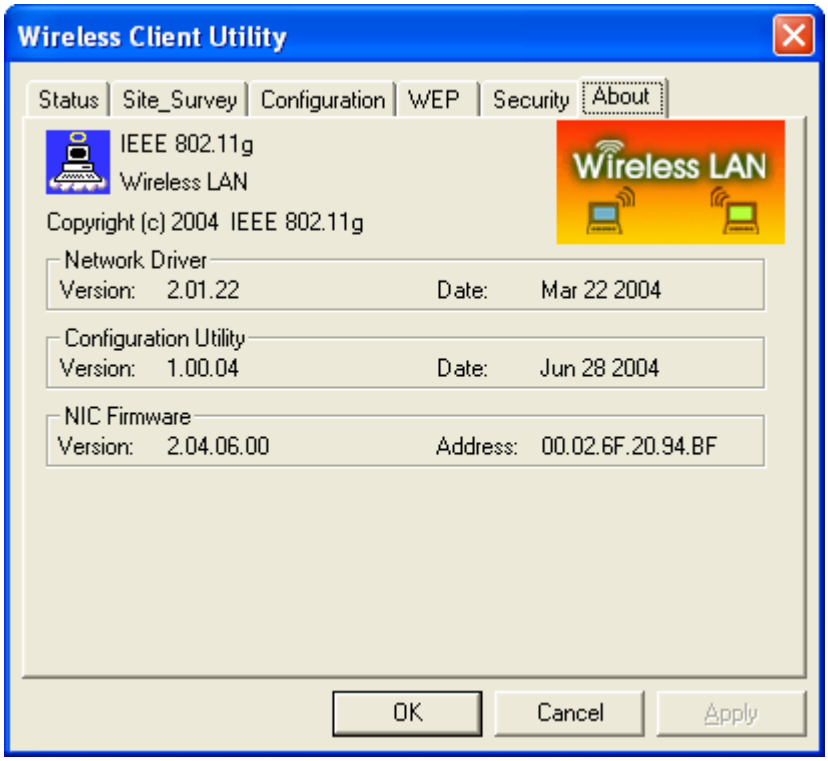
3.5.7 WPA – PSK



- **Authentication Type**: If your network uses WPA-PSK (Pre-shared key) to authenticate its users, select **WPA-PSK** from the drop down list. **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.
- **Shared Secret Key (PSK)**: Enter the shared secret key.
- Click on the **Apply** button to save the changes.

3.6 About

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

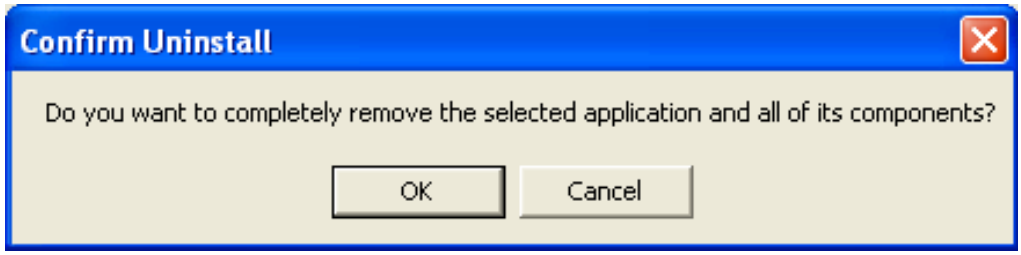


4 Uninstall the Drivers & Client Utility

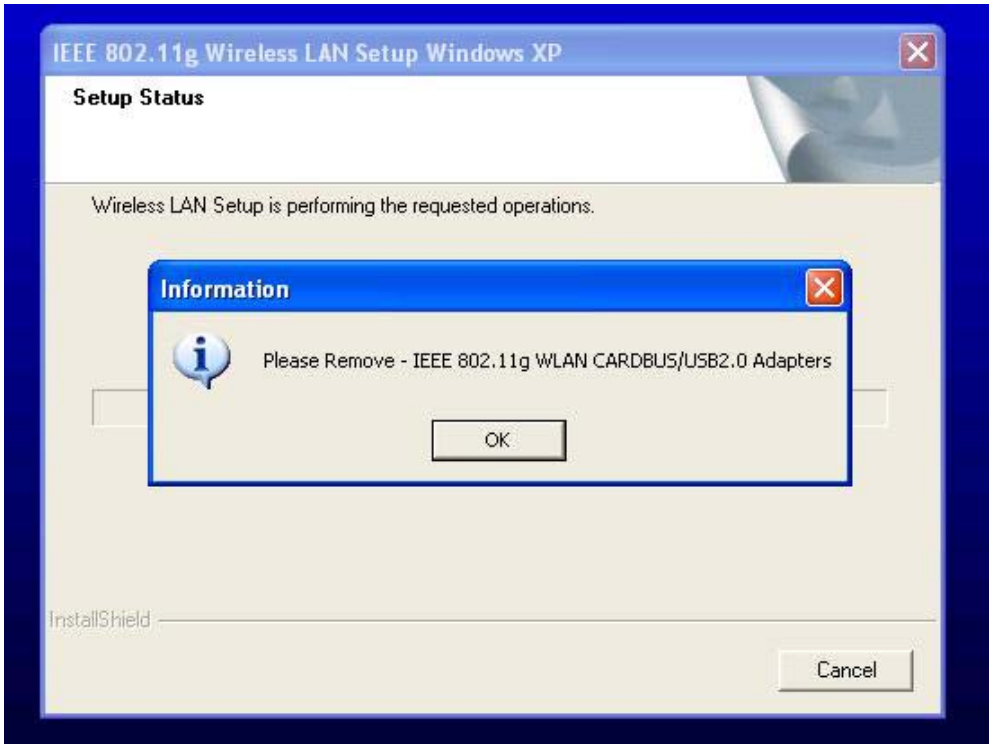
If the USB Client Adapter installation is unsuccessful for any reason, the best way to solve the problem may be to completely uninstall the USB adapter and its utility and repeat the installation procedure again.

Follow the steps below in order to uninstall the Client Utility:

1. Click on **Start > Programs > IEEE 802.11.g > Uninstall WLAN Utility.**
2. You will then see the following message, click on the **OK** button to continue.



3. At this you must remove the device from your notebook or PC, and then click on the **OK** button. The Utility & Drivers will then be removed from your system.



4. The Uninstallation is complete. Select the **Yes, I want to restart my computer now** radio button, and then click on the **Finish** button.

Appendix A – Specifications

General	
Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
Network Standards	IEEE 802.11b, IEEE 802.11g
Compliance	FCC Part 15, ETSI 300/328/CE
USB Interface	● Operational Voltage: 5V ● Current Limited: 500mA ● USB Data Rate: 12Mbps(USB1.1), 480Mbps(USB2.0)
Physical	
Form Factor	USB2.0
Interface	USB Mini A Type
LED	Action: Blinking
Antenna	Omni-directional Integrated Antenna
Dimension	115(L) mm x 100(W) mm x 25.5(H) mm
RF Information	
Frequency Band	2412 – 2483.5 MHz
Channels	11 for North America, 14 for Japan, 13 for Europe, 2 for Spain, 4 for France
Media Access Protocol	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) Orthogonal Frequency Division Multiplexing (OFDM)
Modulation Technology	DBPSK @ 1Mbps DQPSK @2Mbps CCK @ 5.5 & 11Mbps BPSK @ 6 and 9 Mbps QPSK @ 12 and 18 Mbps 16-QAM @ 24 and 36 Mbps 64-QAM @ 48 and 54 Mbps
Receive Sensitivity (typical)	-89dBm @ 1Mbps -87dBm @ 6Mbps -79dBm @ 24Mbps -86dBm @ 2Mbps -87dBm @ 9Mbps -75dBm @ 36Mbps -85dBm @ 5.5Mbps -84dBm @ 12Mbps -68dBm @ 48Mbps -82dBm @ 11Mbps -82dBm @ 18Mbps -68dBm @ 54Mbps
Available transmit power	18dBm @1, 2, 5.5 and 11Mbps 18dBm @6Mbps 14dBm @24Mbps

	18dBm @9Mbps 14dBm @36Mbps 16dBm @12Mbps 12.5dBm @48Mbps 16dBm @18Mbps 12.5dBm @54Mbps
Software	
Drivers	Windows98SE/ME/2000/XP
Security	WEP—64/128bit Encryption WPA— Wi-Fi Protected Access ● PSK (Pre share key) with 64/ 128-bit WEP Key ● IEEE802.1x (TLS/TTLS supplicant) Support ● TKIP
Compliance	WIFI and WHQL compatible
Environmental	
Temperature Range	-0°C to 50°C - Operating -20°Cto 70°C - Storage
Humidity (non-condensing)	5%~95% Typical

Appendix B – FCC Interference Statement

Federal Communication Commission Interference Statement

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

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

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
Senao declared that WUB-3014 is limited in CH1~11 by specified firmware controlled in USA.