802.11g Wireless LAN PCI Card

User Manual

Version: 1.0
(April, 2005)

COPYRIGHT

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

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

FCC Caution

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CONTENTS

1 Introduction

Thank you for purchasing the 802.11g Wireless LAN Adapter. This Adapter is designed to comply with IEEE 802.11g Wireless LAN standard and easy to carry with the Mini size. It is suitable for any Laptop or Desktop computers.

This adapter supports 64/128/152-bit WEP data encryption that protects your wireless network from eavesdropping. It also supports WPA (Wi-Fi Protected Access) feature that combines IEEE 802.1x and TKIP (Temporal Key Integrity Protocol) technologies. Client users are required to authorize before accessing to APs or AP Routers, and the data transmitted in the network is encrypted/decrypted by a dynamically changed secret key.

It supports the SuperG mode feature to enhance the data rate to reach to 108Mbps, it can enhance the data rate when it connect with Super G product.

This adapter is with the versatile features; it is the best solution for you to build your wireless network.

1.1 Features

- Complies with the IEEE 802.11b and IEEE 802.11g 2.4GHz standards.
- Up to 54Mbps high data transfer rate. (108M : Super G mode enabled)
- Support 64/128/152-bit WEP, WPA, IEEE 802.1x high level of security.
- Complies with IEEE 802.11d country roaming standard.
- Support the most popular operating system: Windows 98SE/Me/2000/XP.
- Supports Standard 32bit PCI interface.

1.2 Specifications

- Standard: IEEE 802.11g/b
- Bus Type: 32-bit PCI Interface
- Frequency Band: 2.4000~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: OFDM with BPSK, QPSK, 16QAM, 64QAM (11g)

  BPSK, QPSK, CCK (11b)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback (108Mbps: Super G enabled)
- Security: 64/128/152-bit WEP Data Encryption, WPA , IEEE 802.1x
- Antenna: External detachable dipole antenna
- Drivers: Windows 98SE/Me/2000/XP/2003 Server
- LED: TX/RX, Link
- Transmit Power: 16 ~18 dBm (Typical)
- Power consumption: Tx: 350mA, Rx: 250mA
- Dimension: 19(H) x 127(W) x 121(D) mm
- Temperature: 32~131°F (0 ~55°C)

- Humidity: 0-95% (NonCondensing)
- Certification: FCC, CE

1.3 Package Contents

Before you begin the installation, please check the items of your package. The package should include the following items:

- One PC Card
- One CD (Driver/Utility/User's Manual.)
- One Quick Guide

If any of the above items is missing, contact your supplier as soon as possible.

2 Installation Procedure

Before you proceed with the installation, please notice following descriptions.

Note1: The following installation was operated in Windows XP. (Procedures are similar for Windows 98SE/Me/2000/2003 Server.)

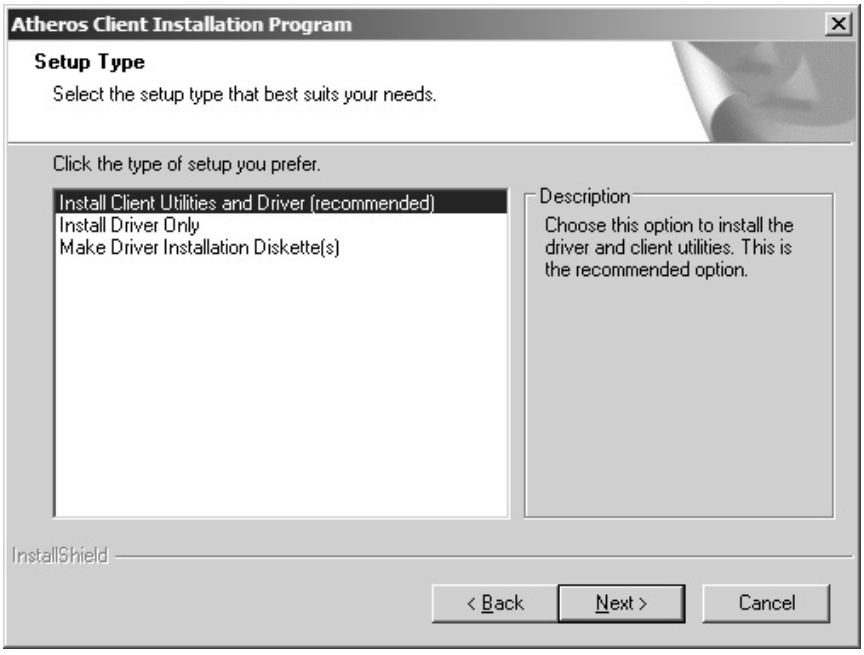
Note2: If you have installed the Wireless PCI Card driver & utility before, please uninstall the old version first.

This chapter describes using the Atheros installer to install the Atheros wireless network adapter driver.

Installation

To install the ACU and device driver:

1. Insert the device into the computer, and insert the installation CD.
2. Open the InstallShield Wizard (**setup.exe**).
3. The Atheros Client Installation installer opens. Click Next.
4. The Atheros license agreement window appears. Read and accept the agreement to continue. Click Next.
5. The Installation Program window appears with three setup options.



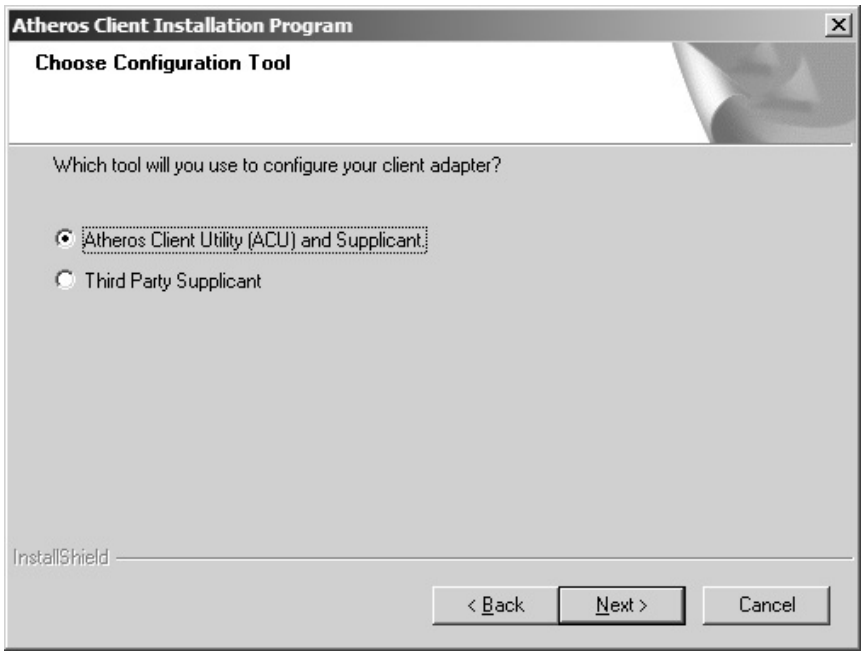
To install the client utilities and driver, select the appropriate installation type (see Table (2-1) and click Next.

Table 2-1. **Installer Installation Selections**

Radio Button	Description
Install Client Utilities and Driver (recommended)	Installs the driver and client utilities. This is the recommends option.

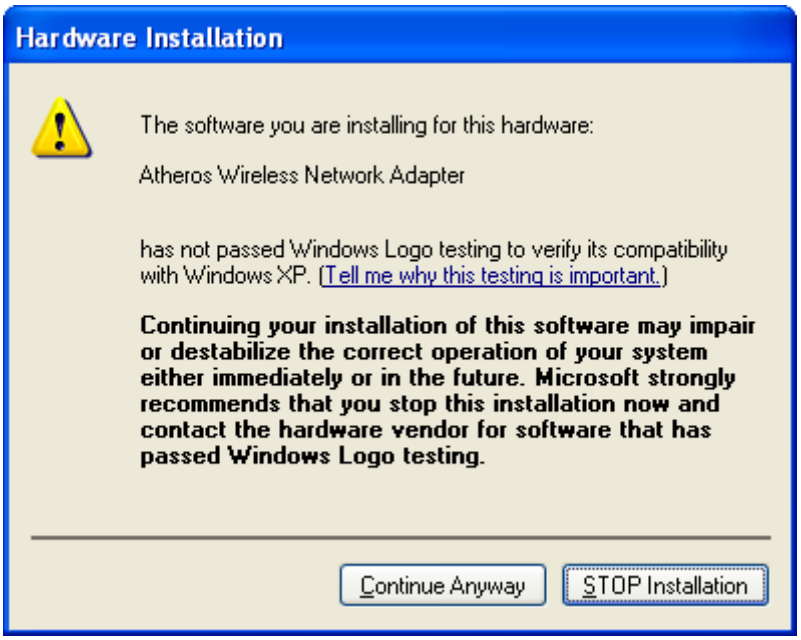
Install Driver Only	Installs only the driver without installing the client utilities.
Make Driver Installation Diskette(s)	Creates driver installation diskettes.

6. A prompt appears warning that the install requires the system to be rebooted at the end of the installation process. Click Yes to continue.
7. Choose the setup directory. The default is **C:\Program Files \ Atheros.** Click Next.
8. Choose the program folder for the start menu. The default is **Atheros.** Click Next.
9. For a windows XP installation, the next screen defines the Windows Zero Configuration. Windows XP Zero Configuration provides functionality to automatically try to connect the station to available wireless networks. For complete information on Windows Zero Configuration, see the Microsoft web site.
10. In this installation, select the Atheros Client Utility and Supplicant.



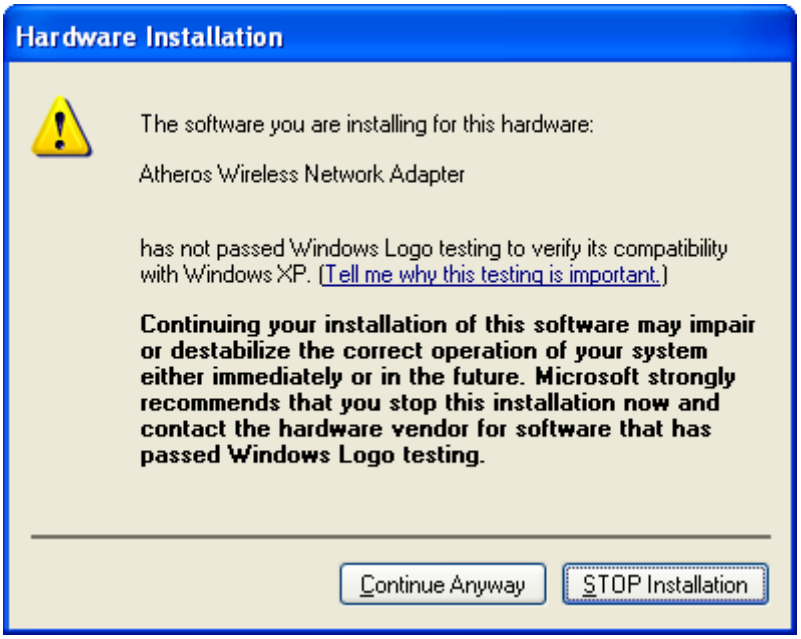
Click Next. The installer automatically installs the driver.

11. Make sure that the device is inserted. If it is not, insert it, then cancel the found New Hardware Wizard if it appears. Proceed with the installation. Click OK.
12. Windows may display a Windows Logo error for the USB bootloader. Click Continue Anyway.



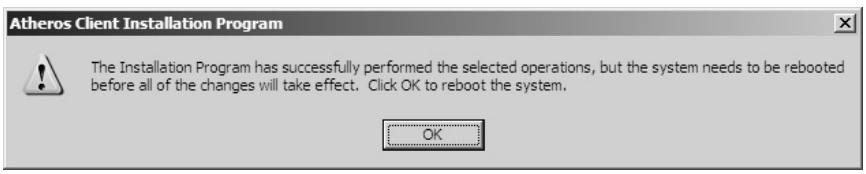
The installer continues installation.

13. Windows may display a Windows Logo error for the WLAN driver. Click Click Continue Anyway.



The installer continues installation.

14. Click OK at the prompt to reboot and complete the installation.



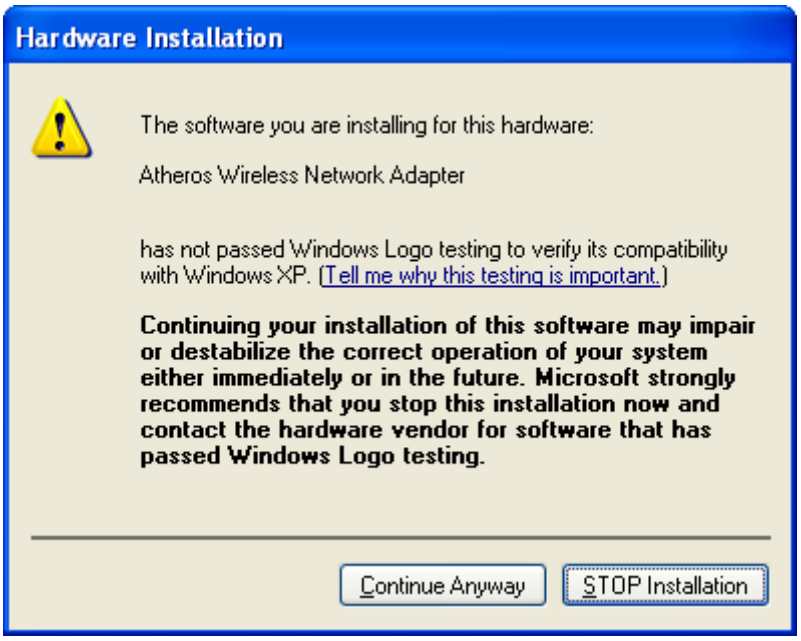
Installing the Atheros Wireless Network Adapter

To install the driver and the Atheros Client Utility, see “To install the ACU and device driver:” on page 2-1.

To install the Device Driver separately:

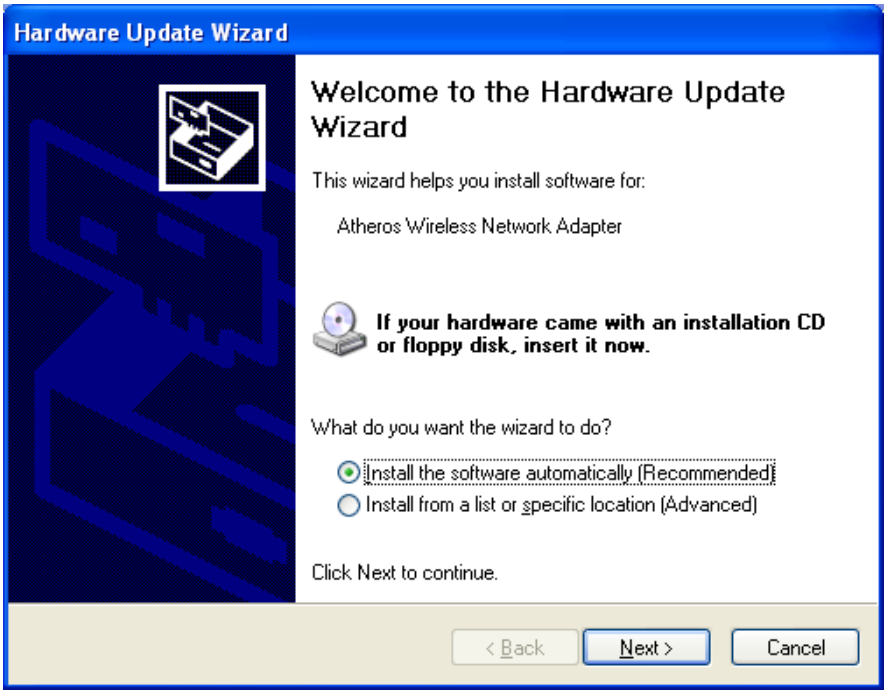
1. Insert the device into the computer: The Found New Hardware Wizard opens. Choose advanced installation and click Next.
2. Choose Search for driver in these locations. The driver is located in the NDIS5x directory.

3. Windows may display a Windows Logo error for the bootloader. Click Continue Anyway.

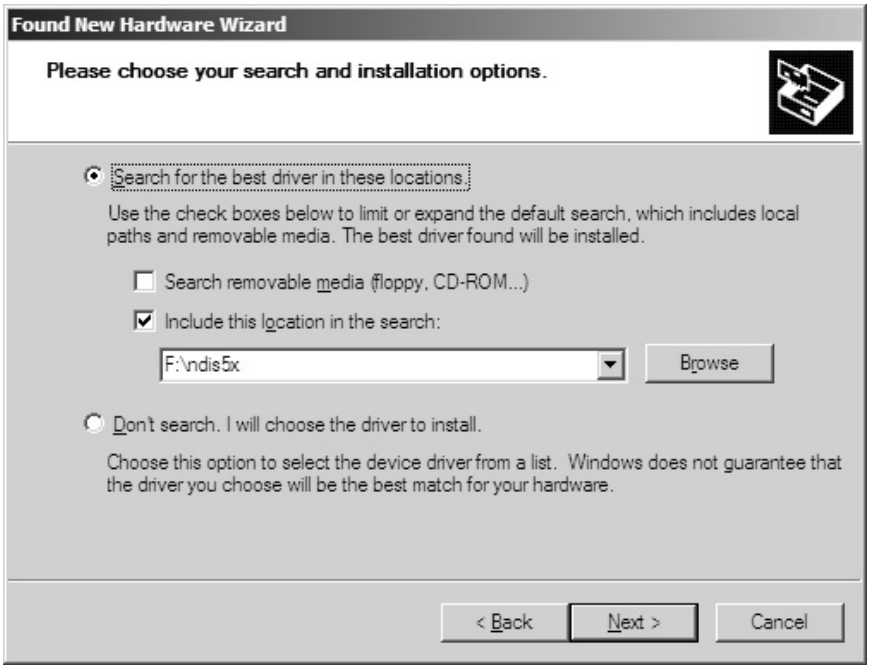


The installer continues installation.

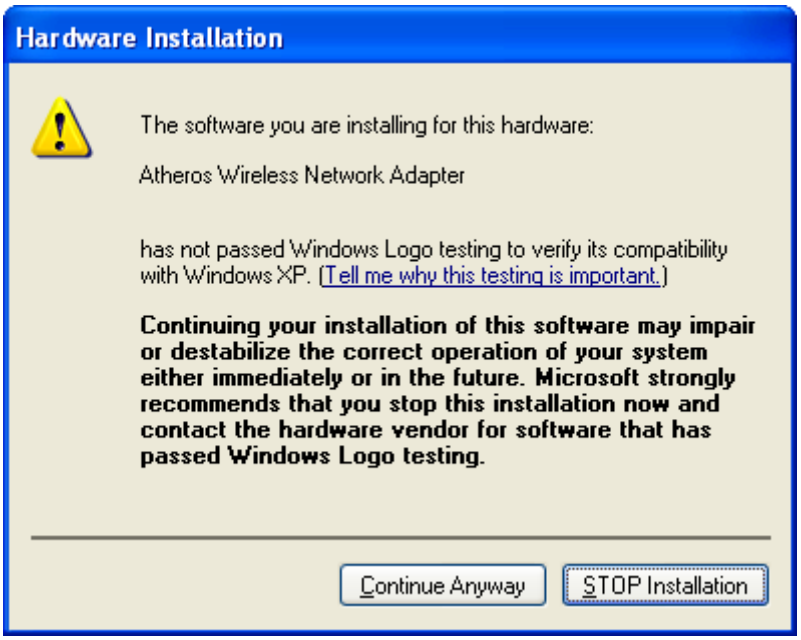
4. Click Finish to close the Found New Hardware Wizard and complete installation of the device bootloader.
5. The Found New Hardware Wizard opens to install software for the device. Click Next to continue.



6. Choose Search for driver in these locations. The driver is located in the NDIS5x directory.

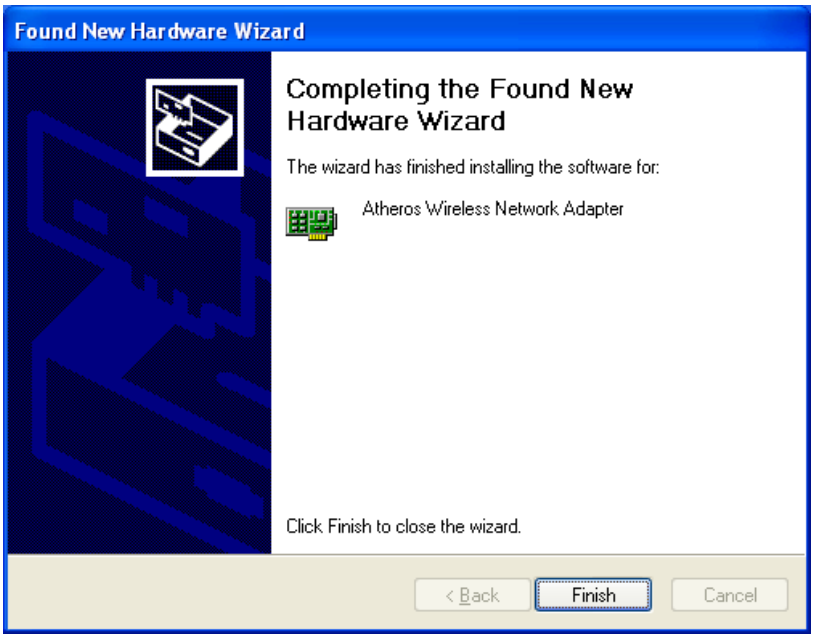


7. Windows may display a Windows Logo error for the WLAN driver. Click Continue Anyway.



The installer continues installation.

8. Click Finish to close the Found New Hardware Wizard and complete installation of the Atheros Network Adapter.



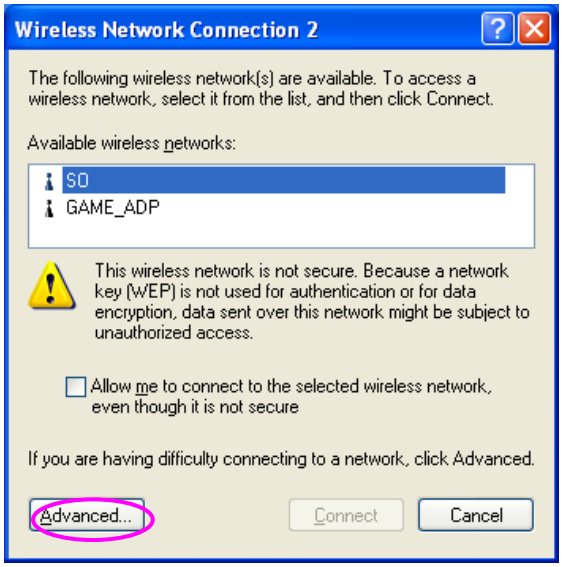
Use the ACU to configure the device driver. The ACU provides extensive online help to aid in configuring the device. Access the ACU by right-clicking the tray icon and choosing Atheros Client Utility.

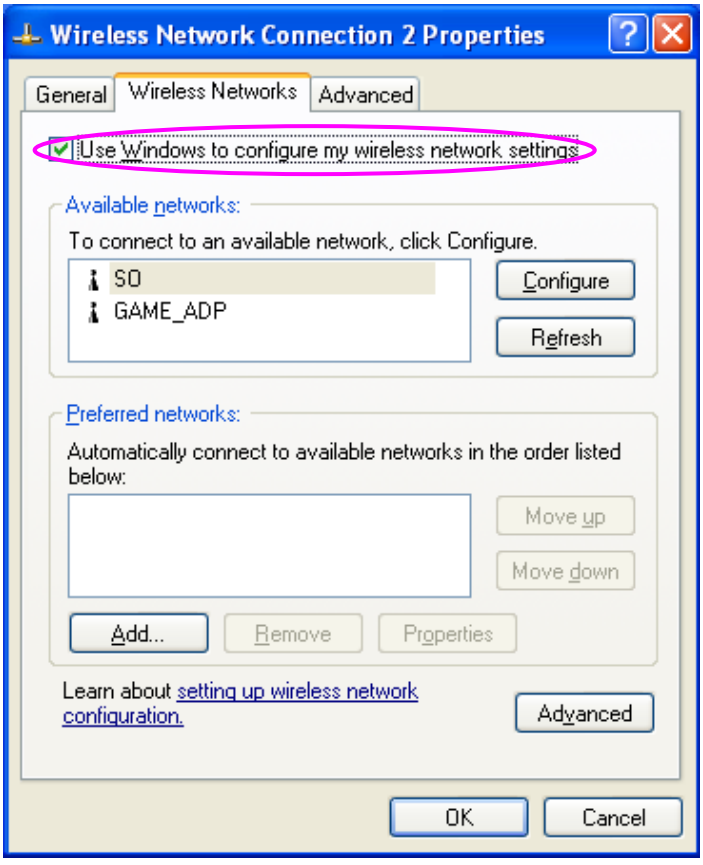
III. Using the Configuration Utility

To setup the adapter, double-click the icon in the system tray.

For Windows XP, there is a “Windows Zero Configuration Tool” by default for you to setup wireless clients. If you want to use the Utility of the adapter, please follow one of the ways as below.

A. Double-click the icon.
B. Click “Advance”.
C. Uncheck “Use Windows to configure my wireless network settings”.



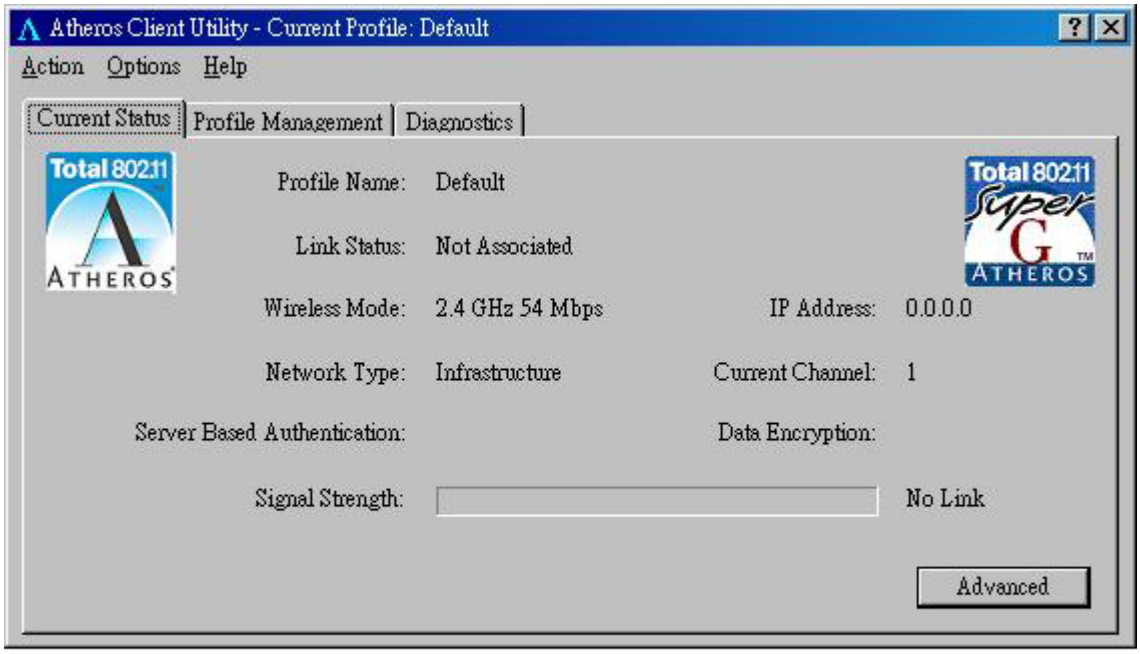


3 Configuration Utility

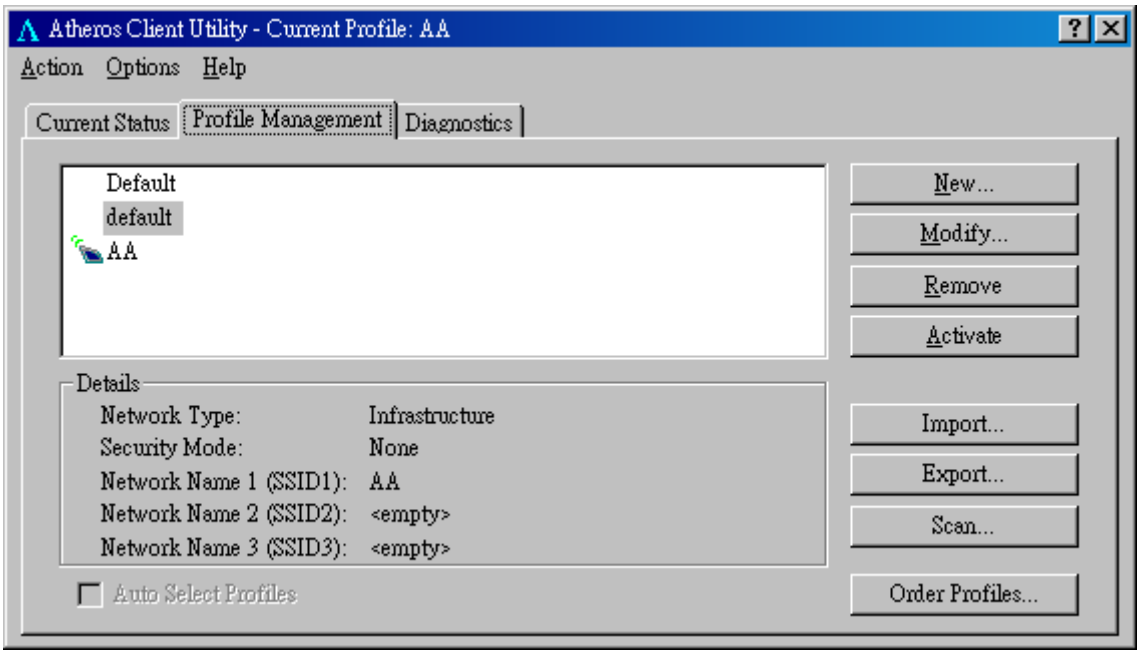
The Client Utility is a user-mode utility designed to edit and add profiles for, as well as display and diagnostics pertaining to a selected wireless adapter.

3.1 Wireless Connection Status

When you open the Configuration Utility, the system will scan all the channels to find all the access points/stations within the accessible range of your card and automatically connect to the wireless device with the highest signal strength. From the screen, you may know all the infomration about the wireless connection.



3.2 Profile Management



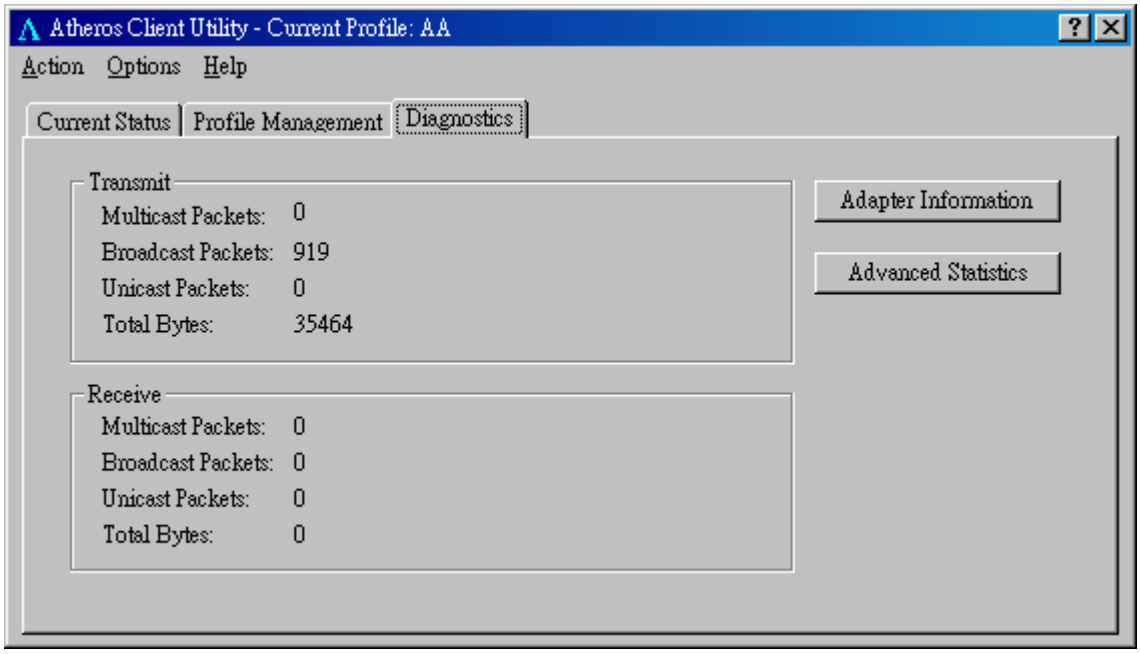
Parameter	Description
New	To add a new configuration profile, click New on the Profile Management tab. To modify a configuration profile, select the configuration from the Profile list and click the Modify button.
Modify	In the Atheros Client Utility, access the General tab by clicking New or Modify on the Profile Management tab. Edit the fields in the General tab to configure the configuration profile. Make sure to also edit the Security and Advanced tabs.
Remove	Select the profile to remove from the list of configuration profiles.
Import	1. From the Profile Management tab, click the Import button. The Import Profile window appears. 2. Browse to the directory where the profile is located. 3. Highlight the profile name. 4. Click Open. The imported profile appears in the profiles list.
Export	1. From the Profile Management tab, highlight the profile to export. 2. Click the Export button. The Export Profile window appears. 3. Browse to the directory to export the profile to. 4. Click Save. The profile is exported to the specified

location.

Order Profiles	Including a profile in the auto selection feature allows the wireless adapter to automatically select that profile from the list of profiles and use it to connect to the network.

3.3 Diagnostics

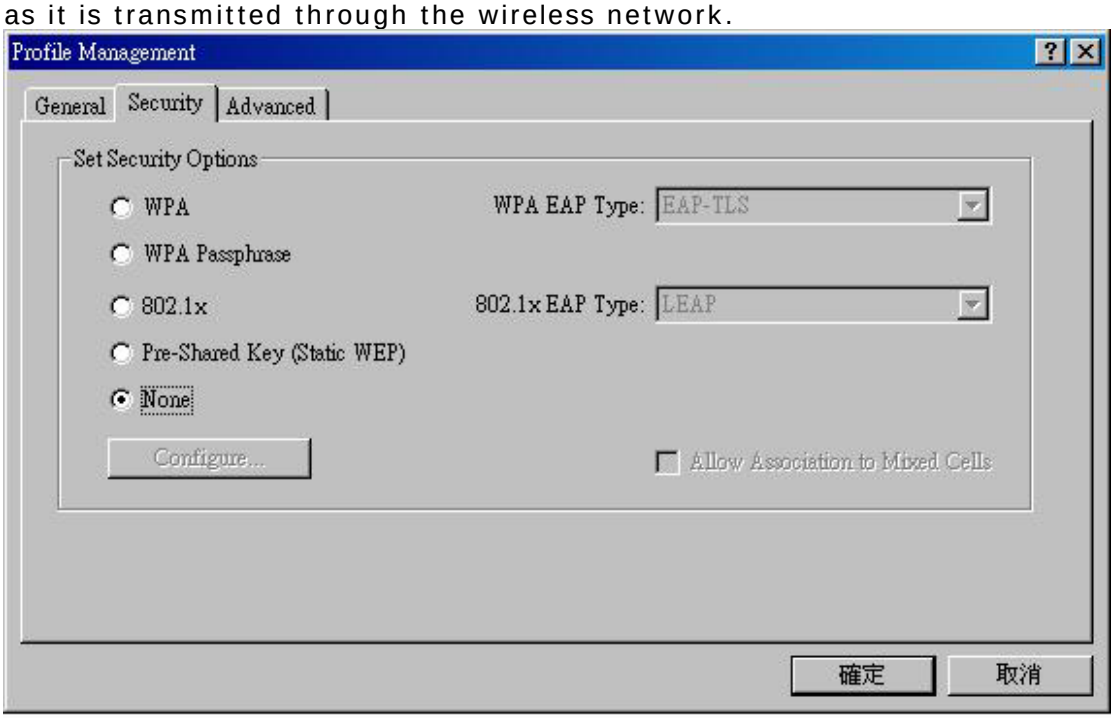
The client utility includes a number of tools to display current diagnostics and status information.



Parameter	Description
Adapter Information	The Adapter Information button contains general information about the network interface card (the wireless network adapter) and the network driver interface specification (NDIS) driver.
Advanced Statistics	The Diagnostics tab of the Atheros Client Utility provides buttons used to retrieve receive and transmit statistics. The Diagnostics tab does not require any configuration

3.4 Security

This Chapter describes setting up security using the Atheros Client Utility(ACU). While using the Atheros wireless network adapter, encryption data can protect its as it is transmitted through the wireless network.



Radio Button	Description
WPA	Enables the use of Wi-Fi Protected Access (WPA). Choosing WPA opens the WPA EAP drop-down menu. The options include: • EAP-TLS • EAP-TTLS • PEAP (EAP-GTC) • PEAP (EAP-MSCHAP V2) • LEAP
WPA Passphrase	Enables WPA Passphrase security. Click on the Configure button and fill in the WPA Passphrase.
802.1x	Enables 802.1x security. This option requires IT administration. Choosing 802.1x opens the 802.1x EAP type drop-down menu. The options include: • EAP-TLS • EAP-TTLS • PEAP (EAP-GTC)

- PEAP (EAP-MSCHAP V2)
- LEAP

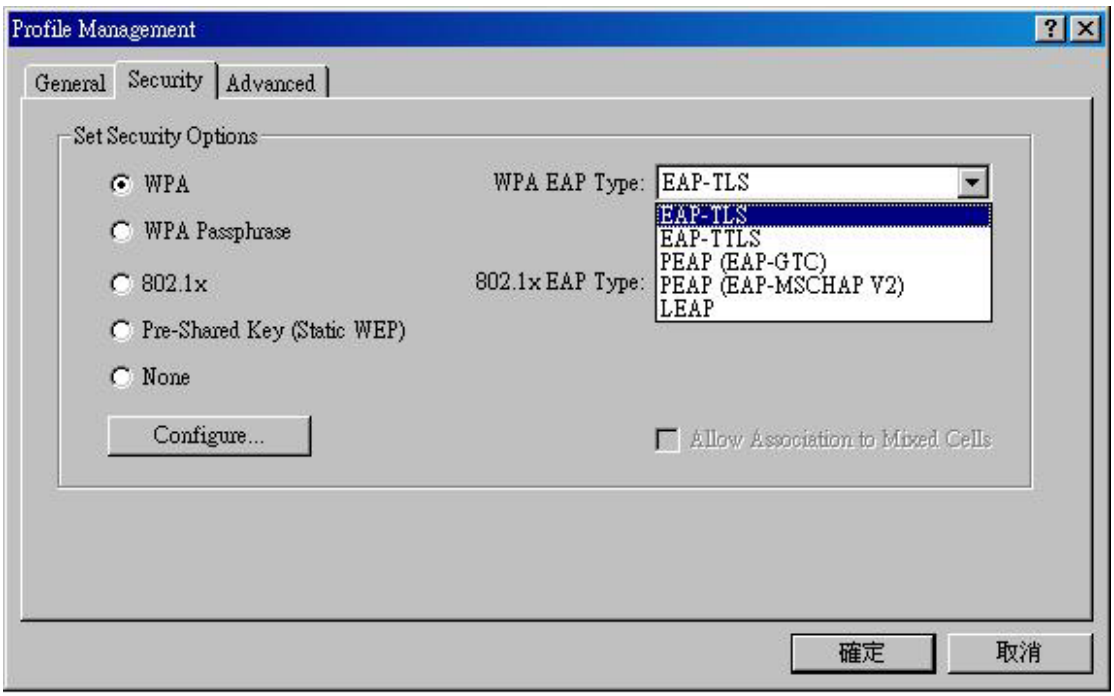
If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.

Pre-Shared Key(Static WEP)	Enables the use of pre-shared keys that are defined on both the access point and the station. To define pre-shared encryption keys, choose the Pre-Shared Key radio button and click the Configure button to fill in the Define Pre-Shared Keys window. If the access point that the wireless adapter is associating to has WEP set to Optional and the client has WEP enabled, make sure that Allow Association to Mixed Cells is checked on the Security Tab to allow association.
None	No security (not recommended).

3.4.1 WPA Setting

Using EAP-TLS Security

To use EAP-TLS security In the Atheros Client Utility, access the Security tab in the Profile Management window.



1. On the Security tab, choose the WPA radio button.
   OR: On the Security tab, choose the 802.1x radio button.
2. Choose EAP-TLS from the drop-down menu.

Enabling EAP-TLS security:

To use EAP-TLS security, the machine must already have the EAP-TLS certificates downloaded onto it. Check with the IT manager.

1. If EAP-TLS is supported, choose EAP-TLS from the drop-down menu on the right, then click the Configure button.
2. Select the appropriate certificate authority from the list. The server/domain name and the login name are filled in automatically from the certificate information. Click OK.
3. Click OK.
4. Activate the profile.

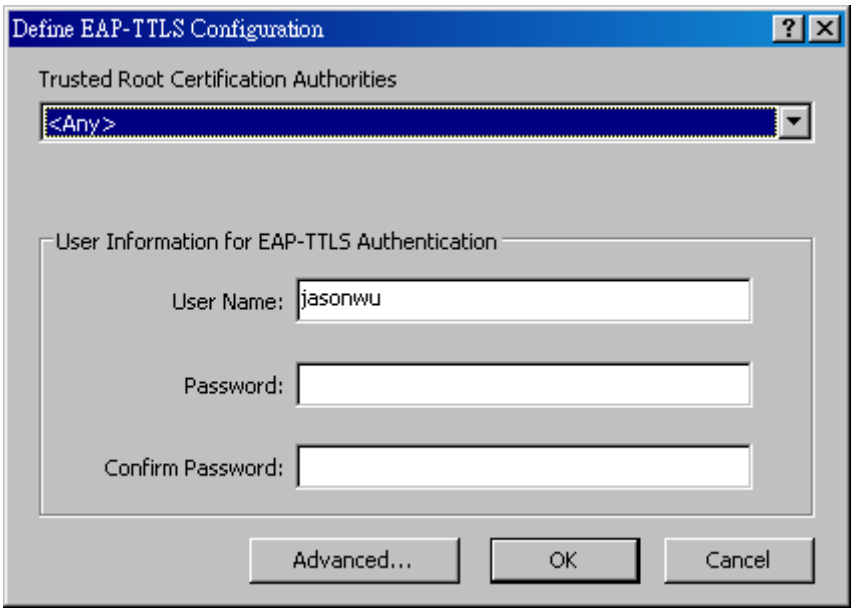
Using EAP-TTLS Security

To use EAP security In the Atheros Client Utility, access the Security tab in the Profile Management window.

1. On the Security tab, choose the WPA radio button.
   OR: On the Security tab, choose the 802.1x radio button.
2. Choose EAP-TTLS from the drop-down menu.

Enabling EAP-TTLS security:

To use EAP-TTLS security, the machine must already have the EAP-TTLS certificates downloaded onto it. Check with the IT manager.



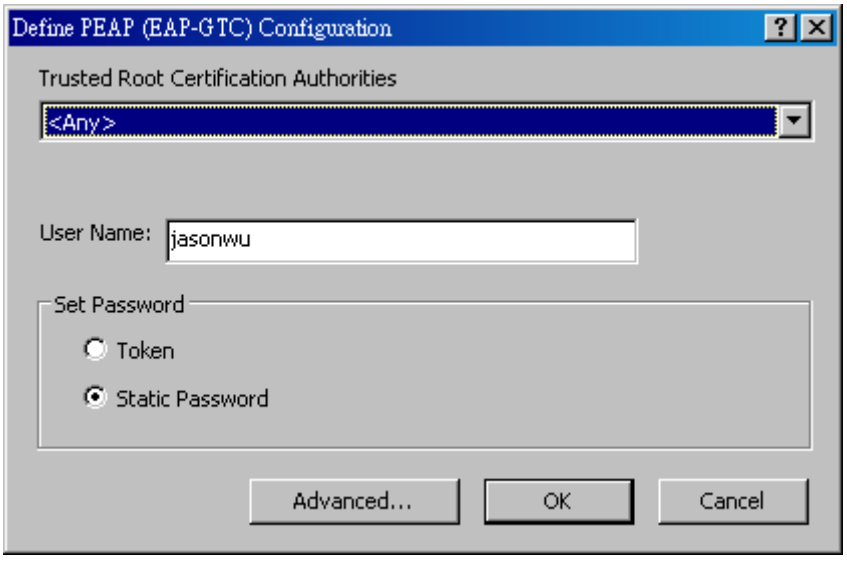
1. If EAP-TTLS is supported, choose EAP-TTLS from the drop-down menu on the right, then click the Configure button.
2. Select the appropriate certificate from the drop-down list and click OK.
3. Specify a user name for EAP authentication:
    - Check Use Windows User Name to use the Windows user name as the EAP user name.
    - OR: Enter a EAP user name in the User Name field to use a separate user name and password and start the EAP authentication process.
4. Click Advanced and:
    - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
    - Enter the domain name of the server from which the client will accept a certificate.
    - Change the login name if needed.
5. Click OK.
6. Enable the profile.

Using PEAP-GTC Security

To use PEAP-GTC security In the Atheros Client Utility, access the Security tab in the Profile Management window.

1. On the Security tab, choose the WPA radio button.
   OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-GTC) from the drop-down menu.

To use PEAP (EAP-GTC) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.



1. Click the Configure button.

2. Select the appropriate network certificate authority from the drop-down list.
3. Specify a user name for inner PEAP tunnel authentication:
    - Check Use Windows User Name to use the Windows user name as the PEAP user name.
    - OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
4. Choose Token or Static Password, depending on the user database.

    Note that Token uses a hardware token device or the Secure Computing SofToken program (version 1.3 or later) to obtain and enter a one-time password during authentication.
5. Click Advanced and:
    - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
    - Enter the domain name of the server from which the client will accept a certificate.

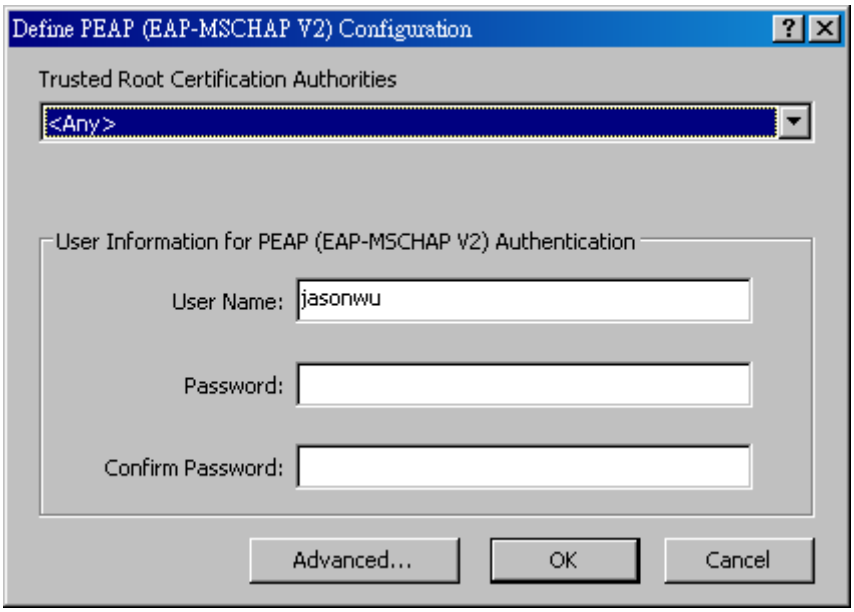
    The login name used for PEAP tunnel authentication, fills in automatically as PEAP-*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the computer's MAC address. Change the login name if needed.
6. Click OK.
7. Enable the profile.

Using PEAP-MSCHAP V2 Security

To use PEAP-MSCHAP V2 security In the Atheros Client Utility, access the Security tab in the Profile Management window.

1. On the Security tab, choose the WPA radio button.
   OR: On the Security tab, choose the 802.1x radio button.
2. Choose PEAP (EAP-MSCHAP V2) from the drop-down menu.

To use PEAP (EAP-MSCHAP V2) security, the server must have WPA-PEAP certificates, and the server properties must already be set. Check with the IT manager.



1. Click the Configure button.
2. Select the appropriate certificate from the drop-down list.
3. Specify a user name for inner PEAP tunnel authentication:
    - Check Use Windows User Name to use the Windows user name as the PEAP user name.
    - OR: Enter a PEAP user name in the User Name field to use a separate user name and start the PEAP authentication process.
4. Click Advanced and:
    - Leave the server name field blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. **(recommended)**
    - Enter the domain name of the server from which the client will accept a certificate.
    - The login name used for PEAP tunnel authentication, fills in automatically as PEAP-*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the computer's MAC address. Change the login name if needed.
5. Click OK.
6. Enable the profile.

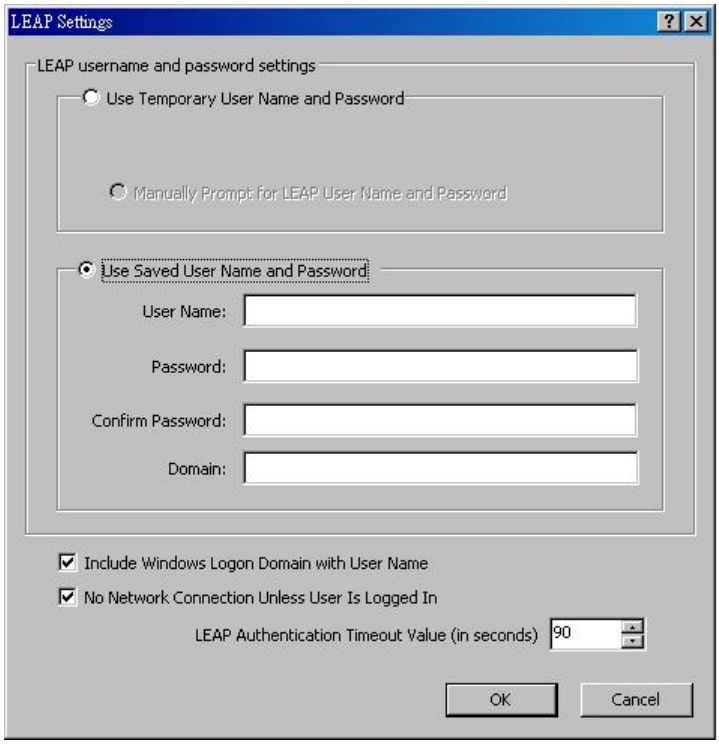
Using LEAP Security

To use security In the Atheros Client Utility, access the Security tab in the Profile Management window.

LEAP security requires that all infrastructure devices (e.g. access points and servers) are configured for LEAP authentication. Check with the IT manager.

Configuring LEAP:

- On the Security tab, choose the WPA radio button. Choose WPA-LEAP from the drop-down menu.
- OR: On the Security tab, choose the 802.1x radio button. Choose LEAP from the drop-down menu.



1. Click the Configure button.
2. Specify a user name and password:

   Select to Use Temporary User Name and Password by choosing the radio button:

   - Check Use Windows User Name to use the Windows user name as the LEAP user name.
   - OR: Check Manually Prompt for LEAP User Name and Password to manually login and start the LEAP authentication process.

   Select to Use Saved User Name and Password by choosing the radio button:

   - Specify the LEAP user name, password, and domain to save and use.
3. Enter the user name and password.
4. Confirm the password.
5. Specify a domain name:

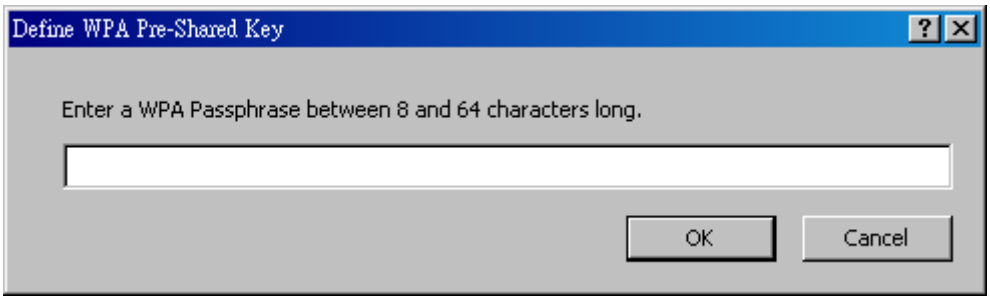
   - Check the Include Windows Logon Domain with User Name setting to pass the Windows login domain and user name to the RADIUS server. **(default)**
   - OR: Enter a specific domain name.
6. If desired, check No Network Connection Unless User Is Logged In to force the wireless adapter to disassociate after logging off.
7. Enter the LEAP authentication timeout time (between 30 and 500 seconds) to specify how long LEAP should wait before declaring authentication failed, and sending an error message. The default is 90 seconds.

8. Click OK.
9. Enable the profile.

3.4.2 Using WPA Passphrase Security

To use WPA Passphrase security In the Atheros Client Utility, access the Security tab in the Profile Management window.

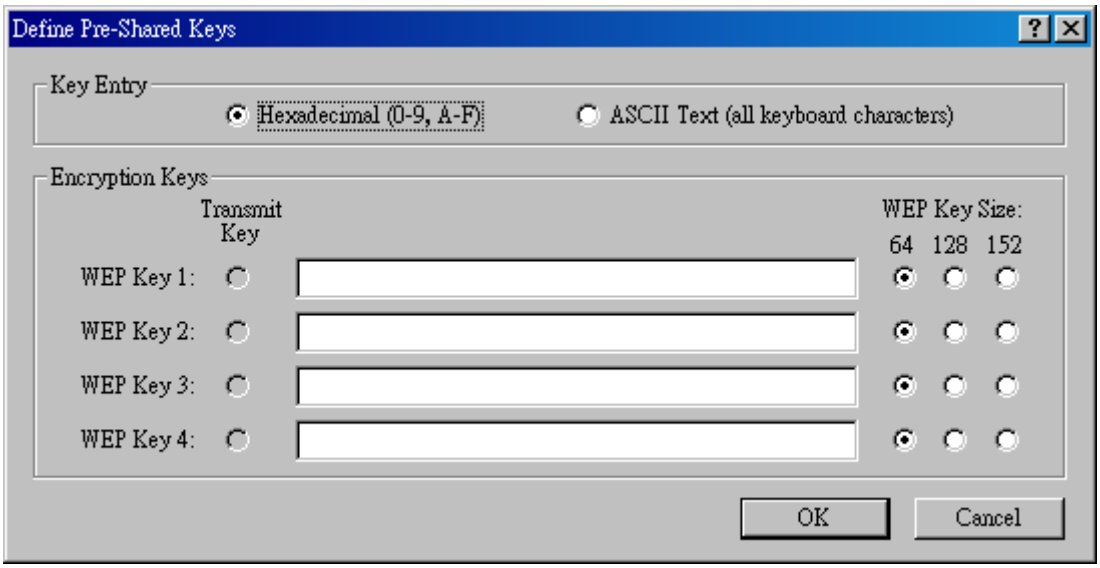
1. On the Security tab, choose the WPA Passphrase radio button.
2. Click on the Configure button.
3. Fill in the WPA Passphrase.
4. Click OK.



3.4.3 Pre-Shared Encryption Keys

Defining pre-shared encryption keys:

1. Click the Define Pre-Shared Keys radio button on the Security tab.
2. Click on Configure.
3. Fill in the fields in the Define Pre-Shared Keys dialog box:



Key Button	Description
Key Entry	Determines the entry method for an encryption key: hexadecimal (0-9, A-F), or ASCII text (all keyboard characters except spaces).
Encryption Keys	Selects the default encryption keys used. Only allows the selection for a shared First, Second, Third, or Fourth key whose corresponding field has been completed.
WEP Keys (1-4)	Defines a set of shared encryption keys for network configuration security. At least one Shared Key field must be populated to enable security using a shared key. Click on the radio button to set the key as the default encryption key.
WEP Key Size	Defines the size for each encryption key. The options include: o 64- bit (enter 10 digits for hexadecimal, 5 ASCII characters) o 128- bit (enter 26 digits for hexadecimal, 13 digits for ASCII) 152-bit (enter 32 digits hexadecimal, 16 digits for ASCII)

4. Click OK for the changes to take effect.

Overwriting an Existing Static WEP Key

1. Click the Define Pre-Shared Keys radio button on the Security tab.
2. Click on Configure.
3. In the window, all existing static WEP keys are displayed as asterisks for security reasons. Click in the field of the existing static WEP key to overwrite.
4. Delete the asterisks in that field.

5. Enter a new key.
6. Make sure to select the Transmit Key button to the left of this key is selected for the key to transmit packets.
7. Click OK.

Disabling Static WEP

- To disable static WEP for a particular profile, choose None on the Profile Management tab and click OK.
- OR: Select any other security option on the Profile Management tab to automatically disable static WEP.

4 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the adapter.

1. What is the IEEE 802.11g standard?

802.11g is the new IEEE standard for high-speed wireless LAN communications that provides for up to 54 Mbps data rate in the 2.4 GHz band. 802.11g is quickly becoming the next mainstream wireless LAN technology for the home, office and public networks. 802.11g defines the use of the same OFDM modulation technique specified in IEEE 802.11a for the 5 GHz frequency band and applies it in the same 2.4 GHz frequency band as IEEE 802.11b. The 802.11g standard requires backward compatibility with 802.11b.

The standard specifically calls for:

A. A new physical layer for the 802.11 Medium Access Control (MAC) in the 2.4 GHz frequency band, known as the extended rate PHY (ERP). The ERP adds OFDM as a mandatory new coding scheme for 6, 12 and 24 Mbps (mandatory speeds), and 18, 36, 48 and 54 Mbps (optional speeds). The ERP includes the modulation schemes found in 802.11b including CCK for 11 and 5.5 Mbps and Barker code modulation for 2 and 1 Mbps.

B. A protection mechanism called RTS/CTS that governs how 802.11g devices and 802.11b devices interoperate.

2. What is the IEEE 802.11b standard？

The IEEE 802.11b Wireless LAN standard subcommittee, which formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

3. What does IEEE 802.11 feature support？

The product supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge Protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS Feature
- Fragmentation
- Power Management

4. What is Ad-hoc？

An Ad-hoc integrated wireless LAN is a group of computers, each has a Wireless LAN adapter, Connected as an independent wireless LAN. Ad hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

5. What is Infrastructure？

An integrated wireless and wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to central database, or wireless application for mobile workers.

6. What is BSS ID？

A specific Ad hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

7. What is WEP？

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40 bit shared key algorithm, as described in the IEEE 802 .11 standard.

8. What is TKIP?

TKIP is a quick-fix method to quickly overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP is involved in the IEEE 802.11i WLAN security standard, and the specification might be officially released by early 2003.

9. What is AES?

AES (Advanced Encryption Standard), a chip-based security, has been developed to ensure the highest degree of security and authenticity for digital information, wherever and however communicated or stored, while making more efficient use of hardware and/or software than previous encryption standards. It is also included in IEEE 802.11i standard. Compare with AES, TKIP is a temporary protocol for replacing WEP security until manufacturers implement AES at the hardware level.

10. Can Wireless products support printer sharing？

Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000, or other LAN operating systems to support printer or file sharing.

11. Would the information be intercepted while transmitting on air？

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, WLAN series offer the encryption function (WEP) to enhance security and Access Control. Users can set it up depending upon their needs.

12. What is DSSS？What is FHSS？And what are their differences？

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip is, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without-the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

13. What is Spread Spectrum？

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communication systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread –spectrum signal looks like background noise. There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).