WLU108AG-MC

User manual

© Copyright 2007 Compex Systems Pte Ltd

Trademark Information

Manual Revision by Daniel
Manual Number: U-0550-V1.4C, Version 1.4, May 2007

Disclaimer

Compex, Inc. provides this manual without warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Compex, Inc. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Compex, Inc will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

Your Feedback

We value your feedback. If you find any errors in this user's manual, or if you have suggestions on improving, we would like to hear from you. Please contact us at:

Fax:	(65) 62809947
Email:	feedback@compex.com.sg

FCC NOTICE

This device 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 device 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 device does cause harmful interference to radio or television reception, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC Compliance Statement: 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.

This device must accept any interference received, including interference that may cause undesired operation.

Caution: Exposure to Radio Frequency Radiation.

RF exposure warning: The equipment complies with FCC RF exposure limits set forth for an uncontrolled environment. The equipment must not be co-located or operating in conjunction with any other antenna or transmitter.

Max. SAR Measurement (1g)
802.11b: 0.542 W/kg
802.11g: 0.540 W/kg
802.11a (5.2GHz): 1.205 W/kg
802.11a (5.8GHz): 1.314 W/kg

Outdoor operations in the 5.15-5.25GHz band is prohibited.
This device has no Ad-hoc capability or peer-to-peer operations for 5250~5350 and 5470~5725 MHz.
IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

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

Note: This device has the same WLAN behavior with all other WLAN devices because we design this device to be compliant to 802.11 specifications.

The fundamental access method of the IEEE802.11 MAC is CSMA/CA, that means when one station desiring to transmit sense the medium, if the medium is busy(i.e. some other station is transmitting) then the station will defer its transmission to a later time. If the medium is sensed free then the station is allowed to transmit. The receiving station will check the CRC of the received packet and send an acknowledgement packet(ACK). Receipt of the ACK will indicate that no collision occurred. If the sender does not receive the ACK then it will retransmit the fragment until it gets acknowledged or thrown away after a given number of retransmissions

When WLAN device is in idle status, it is listening (RX), and it won't send any packets.

In fault condition, or WLAN device is out of control, WLAN device self can not generate any packets, even beacon frames, so that WLAN device won't send out unexpected frames to air and break FCC rules.

DECLARATION OF CONFORMITY

Compex, Inc. declares that the product:
Product Name: Compex Wireless 108Mbps USB 2.0 Adapter
Model No.: WLU108 conforms to the following Product Standards:
This device complies with the Electromagnetic Compatibility Directive (89/336/EEC) issued by the Commission of the European Community.

Compliance with this directive implies conformity to the following European Norms (in brackets are the equivalent international standards.)

Electromagnetic Interference (Conduction and Radiation):

EN 55022 (CISPR 22)

EMC Standards:

FCC Part 15: Subpart B, Subpart C, Subpart E;

Low Voltage Directive:

EN 60 950-1: 2001.

Therefore, this product is in conformity with the following regional standards:

FCC Class B - following the provisions of FCC Part 15 directive;

Technical Support Information

The warranty information and registration form are found in the Quick Install Guide.

For technical support, you may contact Compex or its subsidiaries. For your convenience, you may also seek technical assistance from the local distributor, or from the authorized dealer/reseller that you have purchased this product from. For technical support by email, write to support@compex.com.sg.

Refer to the table below for the nearest Technical Support Centers:

Technical Support Centers	
Contact the technical support center that services your location.	
U.S.A., Canada, Latin America and South America	
✉ Write	**Compex, Inc.** 840 Columbia Street, Suite B, Brea, CA92821, USA
☎ Call 📠Fax	Tel: +1 (714) 482-0333 (8 a.m.-5 p.m. Pacific time) Tel: +1 (800) 279-8891 (Ext.122 Technical Support) Fax: +1 (714) 482-0332
Asia, Australia, New Zealand, Middle East and the rest of the World	
✉ Write	**Compex Systems Pte Ltd** 135, Joo Seng Road #08-01, PM Industrial Building Singapore 368363
☎ Call 📠Fax	Tel: (65) 6286-1805 (8 a.m.-5 p.m. local time) Tel: (65) 6286-2086 (Ext.199 Technical Support) Fax: (65) 6283-8337
Internet access/	E-mail: **support@compex.com.sg** FTPsite: **ftp.compex.com.sg**
Website:	**http://www.cpx.com** *or* **http://www.compex.com.sg**

About This Document

The product described in this document, Compex Wireless 108Mbps USB 2.0 Adapter, Compex WLU108 is a licensed product of Compex Systems Pte Ltd. This document contains instructions for installing, configuring and using Compex WLU108. It also gives an overview of the key applications and the networking concepts with respect to the product.

This documentation is for both Network Administrators and the end user who possesses some basic knowledge in the networking structure and protocols.

It makes a few assumptions that the host computer has already been installed with TCP/IP and already up & running and accessing the Internet. Procedures for Windows 2000/XP operating systems are included in this document.

How to Use this Document

This document may become superseded, in which case you may find its latest version at http://www.compex.com.sg

The document is written in such a way that you as a user will find it convenient to find specific information pertaining to the product. It comprises of chapters that explain in detail the installation and configuration of Compex WLU108.

Drivers & Utilities

This manual is written based on Drivers version 1.5.0.102; Utility version 40.1.2.75

Conventions

In this document, special conventions are used to help and present the information clearly. The Compex Wireless 108Mbps USB 2.0 Adapter is often referred to as Compex WLU108 in this document. Below is a list of conventions used throughout.

NOTE

NOTE
This section will consist of important features or instructions

References on Menu Command, Push Button, Radio Button, LED and Label appear in **Bold**. For example, “Click on **Ok**.”

Chapter 1 Product Overview

1.1 Introduction

The Wireless 108Mbps USB 2.0 Adapter delivers the performance and capabilities that every mobile user is looking for. Embedded with Atheros chipset, it boasts network robustness, stability and wider coverage for long-range connectivity. Despite its small size, the USB adapter is big on features; compatibility with wireless 802.11 networks ensures that you can be connected easily.

Bandwidth needs in the home are increasing rapidly with the introduction of new devices and services. As broadband infrastructure becomes common in homes, the demand for multimedia services such as video streaming or VoIP also increases.

Connecting to a wireless LAN without adequate security measures generally opens up your shared folders to any casual snoopers. To protect your privacy, the USB adapter is armed with many enhanced wireless security features such as WPA, IEEE 802.1x Authentication and 64/128/152-bit WEP (Wired Equivalent Privacy) to ensure privacy for the heterogeneous mix of users within the same wireless LAN while maintaining full access to the establishment's resources.

1.2 Features and Benefits

- **Compact and Mobile**
  The USB adapter is designed especially for the mobile generation. The casing is compact and sleek, and the antenna is built-in to further preserve the miniature footprint. Weighing just 20 grams, the device is light enough to be carried around!

- **Fast and Reliable Transmission**
  The USB adapter can deliver up to 108Mbps wireless throughput. At the same time, the USB adapter provides reliable wireless transmission to all wireless users with its auto rate fallback capability.

- **USB powered and USB 2.0 fast transfer rate**
  Leveraging on the USB standard, the USB adapter is powered through its USB connection and requires no additional power adapter. USB 2.0 standard allows a significant improvement in transfer rate, of up to 40 times that of USB 1.1. You have access to the full 108Mbps transfer rate of Super-AG on USB 2.0. The small form factor of the USB adapter is conveniently designed to fit exactly into a USB port without blocking up neighboring USB ports.

  Designed with a USB2.0 interface, the USB adapter can provide 40 times higher throughput when connected to the USB2.0 slot of your PC/notebook. It is also backwards compatible with USB1.1 though the throughput will then be limited to the 12Mbps of the USB1.1 standard.

- **Easy Set up**
  Using your wireless USB adapter is quick and convenient with USB plug-and –play. The USB adapter is installed externally so you do not have to open up your PC.

- **Highly Secured Traffic**
  The USB adapter supports wireless security features such as 64/128/152-bit WEP and the stronger industry standard WPA and 802.1x authentication to ensure that your data remains secure while in transit.

Chapter 2 Getting Started

This chapter outlines the basic requirement for any installation and configuration on the USB adapter.

2.1 Overall Setup Procedures

Here are some of the basic steps to guide you along:

1. **Hardware Installation**
   Please refer to **Section 3.1 “Hardware Installation”**.

2. **Drivers and Utility Installation**
   Please refer to **Section 3.2 “Drivers and Utility Installation”**.

3. **Configure your USB adapter**
   Please refer to **Chapter 5 “The Atheros Utility Configuration”**.

   For Windows XP user, you can use the built-in utility – Wireless Zero Configuration to configure your USB adapter. Please refer to **Appendix III “Windows XP Wireless Zero Configuration Utility”**.

NOTE
It is advisable to activate EITHER one of the utilities: the Wireless Zero Configuration Utility OR the Atheros Utility.

Chapter 3 Wireless Adapter Installation

The USB adapter is a plug-and-play device. You can plug it into the USB slot of your PC/notebook for auto-detection.

3.1 Hardware Installation

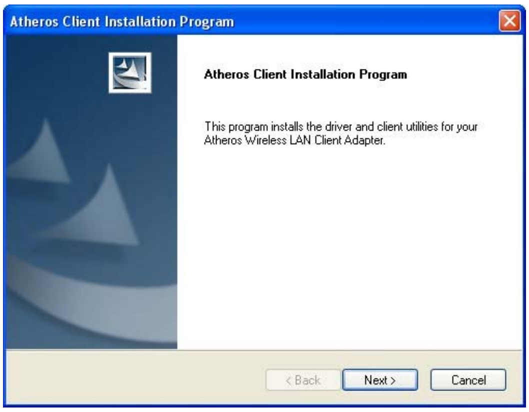
1. Insert the USB adapter directly into the USB slot of your PC/notebook.

3.2 Drivers & Utility Installation

1. Insert the Product CD into your computer CD-ROM drive. Click on **Utilities** and the system will run the *setup.exe* automatically.

2. Click on **Drivers & Utilities** section and the system will run the *setup.exe* automatically. Soon the **Atheros Client Installation Program** screen appears.

3. Next, the **Atheros Client Installation Program** screen appears. Click on the **Next>** button to proceed.

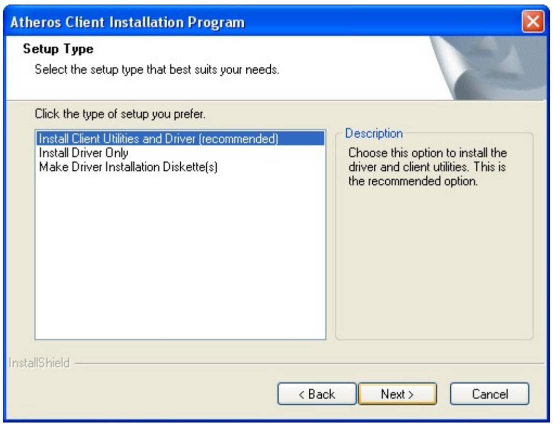


Atheros Client Installation Program

This program installs the driver and client utilities for your Atheros Wireless LAN Client Adapter.

4. When the License Agreement screen appears, you are required to read and accept the agreement to continue. Click on the **Next>** button to proceed.

5. Select your preferred setup:



Setup Type

Select the setup type that best suits your needs.

Click the type of setup you prefer.

Install Client Utilities and Driver (recommended)
Install Driver Only
Make Driver Installation Diskette(s)

Description

Choose this option to install the driver and client utilities. This is the recommended option.

Install Client Utilities and Driver (Recommended) option
You are recommended to select this setup type. This option will install both the drivers and utility that support your USB adapter.

Install Driver Only option (For Windows XP user only)

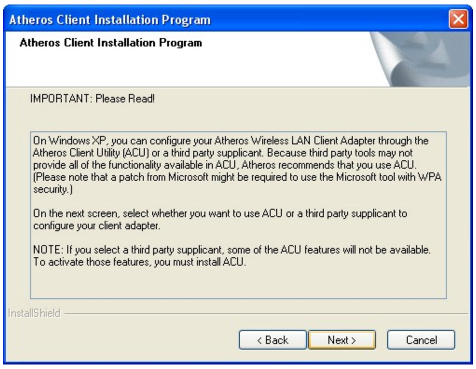
Select this option if you are going to use the Wireless Zero Configuration Utility to configure your USB adapter. Note that only Windows XP comes with the Wireless Zero Configuration Utility.

Make Driver Installation Diskette(s)
Select this option if you wish to make a duplicate copy of the drivers and store in the diskette/s.

6. Click on the **Next>** button and follow the instructions stated on the screen.

For Windows XP users

7. If you are using Windows XP as operating system, the following screen will appear. Read the notice carefully and click on the **Next>** button to proceed.



Atheros Client Installation Program

Atheros Client Installation Program

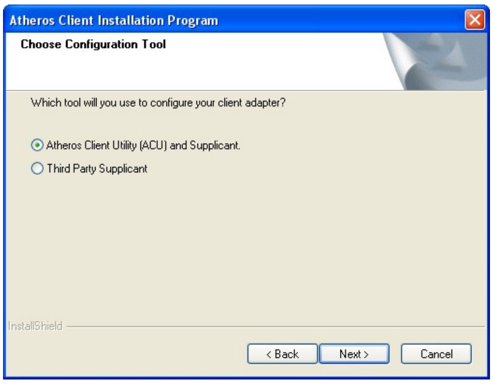
IMPORTANT: Please Read!

On Windows XP, you can configure your Atheros Wireless LAN Client Adapter through the Atheros Client Utility (ACU) or a third party supplicant. Because third party tools may not provide all of the functionality available in ACU, Atheros recommends that you use ACU. (Please note that a patch from Microsoft might be required to use the Microsoft tool with WPA security.)

On the next screen, select whether you want to use ACU or a third party supplicant to configure your client adapter.

NOTE: If you select a third party supplicant, some of the ACU features will not be available. To activate those features, you must install ACU.

8. Select your choice of tool to assist you in configuring your USB adapter. Click on the **Next>** button to proceed.



Atheros Client Installation Program

Choose Configuration Tool

Which tool will you use to configure your client adapter?

● Atheros Client Utility (ACU) and Supplicant.

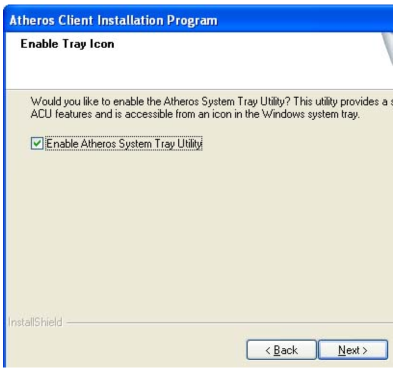
○ Third Party Supplicant

Atheros Client Utility (ACU) and Supplicant option
Select this option to install your USB adapter's utility. (Recommended)

Third Party Supplicant option
Select this option if you decide to use Wireless Zero Configuration Utility to configure your wireless device. Installing this tool will only allow you to view the status of the connected wireless device/s through the USB adapter's utility; configuration using the USB adapter's utility will not be allowed.

Third Party Supplicant option (continued..)
If you have selected **Third Party Supplicant** configuration tool, a screen similar to that on the right will appear, prompting you to enable/disable the system tray icon.

9. Click on the checkbox besides **Enable Atheros System Tray Utility** and click on the **Next>** button to proceed.



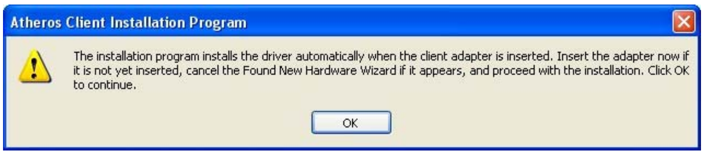
Atheros Client Installation Program

Enable Tray Icon

Would you like to enable the Atheros System Tray Utility? This utility provides a s
ACU features and is accessible from an icon in the Windows system tray.

☑ Enable Atheros System Tray Utility

10. The screen below appears to inform you that the driver will be automatically installed if you have already inserted your client adapter into the USB slot of your computer.

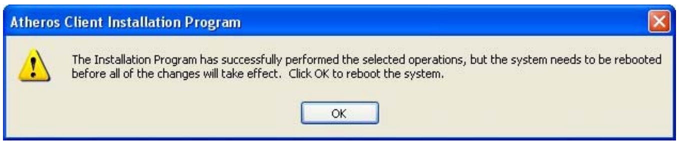


Atheros Client Installation Program

The installation program installs the driver automatically when the client adapter is inserted. Insert the adapter now if it is not yet inserted, cancel the Found New Hardware Wizard if it appears, and proceed with the installation. Click OK to continue.

Cancel the **Found New Hardware** Wizard if it appears and click on the **OK** button to begin the installation.

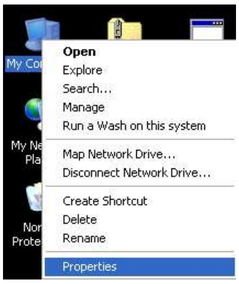
11. Click on the **OK** button to reboot your system and this will complete the installation.



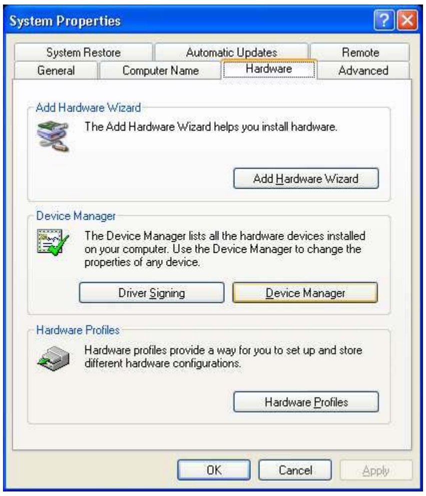
The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Click OK to reboot the system.

To confirm if the driver has been successfully installed on your system,

1. Proceed to your desktop, right click on **My Computer** and select **Properties**.



2. Select the **Hardware** tab and click on **Device Manager**.

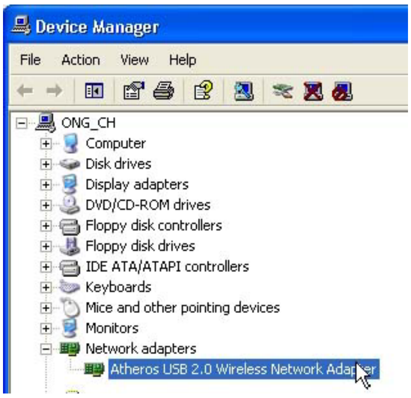


The Add Hardware Wizard helps you install hardware.

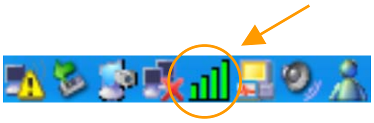
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Hardware profiles provide a way for you to set up and store different hardware configurations.

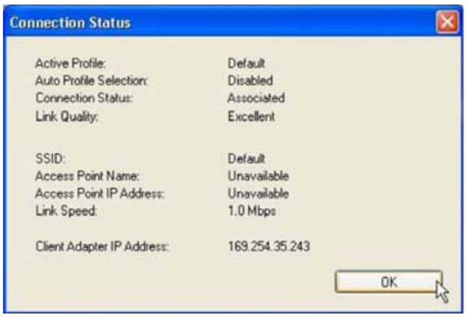
The folder name, **Atheros USB 2.0 Wireless Network Adapter** will appear in the **Network Adapters** section. This indicates that the driver for the USB adapter has been successfully installed on your system!



To activate the utility program, double click on the icon shown in the system tray.

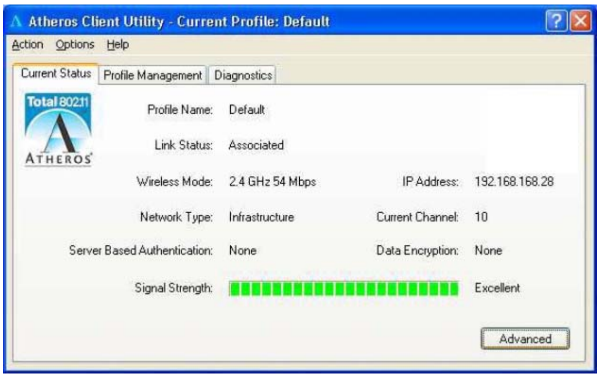


If you have double-click on the utility option, the following screen will appear to give you a glimpse of your connection status. To exit it, click on the **OK** button.



Active Profile:	Default
Auto Profile Selection:	Disabled
Connection Status:	Associated
Link Quality:	Excellent
SSID:	Default
Access Point Name:	Unavailable
Access Point IP Address:	Unavailable
Link Speed:	1.0 Mbps
Client Adapter IP Address:	169.254.35.243

To use the **Atheros Client Utility**, go to the **Start** Menu followed by **Programs**. Then select **Atheros**. From **Atheros**, select **Atheros Client Utility**. You may now start to configure your USB adapter.



Profile Name: Default

Link Status: Associated

Wireless Mode: 2.4 GHz 54 Mbps

IP Address: 192.168.168.28

Network Type: Infrastructure

Current Channel: 10

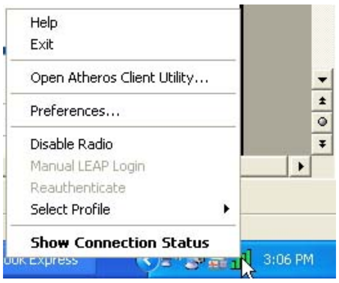
Server Based Authentication: None

Data Encryption: None

Signal Strength: Excellent

Chapter 4 Using the System Tray Utility

This chapter will elaborate on the Atheros system tray utility found at the right bottom corner of your screen. Right click on the utility icon and the menu will appear.

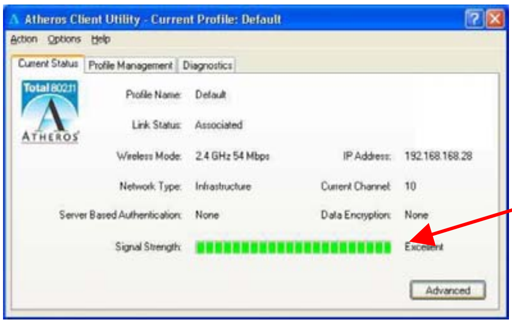


The following explains the different options available on the menu:

Help
Open the online help.

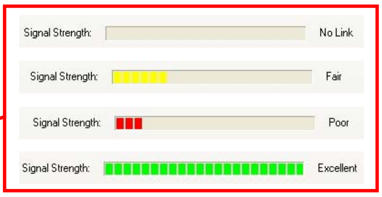
Exit
Exit the Atheros Client Utility application. Once you exit, the icon will disappear from the system tray.

Open Atheros Client Utility…
Launch the Client Utility.



Profile Name: Default
Link Status: Associated
Wireless Mode: 2.4 GHz 54 Mbps
IP Address: 192.168.168.28
Network Type: Infrastructure
Current Channel: 10
Server Based Authentication: None
Data Encryption: None
Signal Strength: Excellent

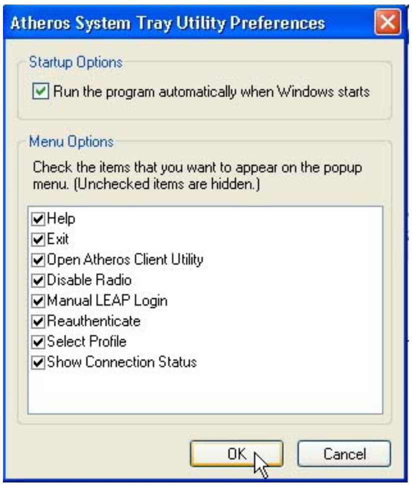
Different signal strength indications



Signal Strength: No Link
Signal Strength: Fair
Signal Strength: Poor
Signal Strength: Excellent

Preferences

This option allows you to set the startup and menu options for the utility. You can decide whether the program should start automatically when Windows starts, and which menu items should appear on the pop up menu.



Atheros System Tray Utility Preferences

Startup Options

☑ Run the program automatically when Windows starts

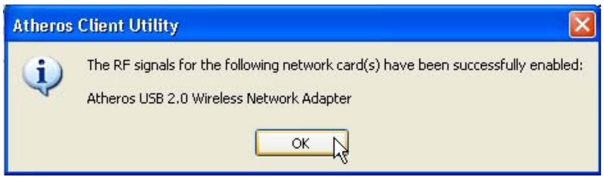
Menu Options

Check the items that you want to appear on the popup menu. (Unchecked items are hidden.)

- ☑ Help
- ☑ Exit
- ☑ Open Atheros Client Utility
- ☑ Disable Radio
- ☑ Manual LEAP Login
- ☑ Reauthenticate
- ☑ Select Profile
- ☑ Show Connection Status

Disable/Enable Radio

If you are unable to detect the RF signal, disable and enable the radio again. Once the radio is enabled, the system will prompt you that the RF signals have been successfully enabled.



Atheros Client Utility

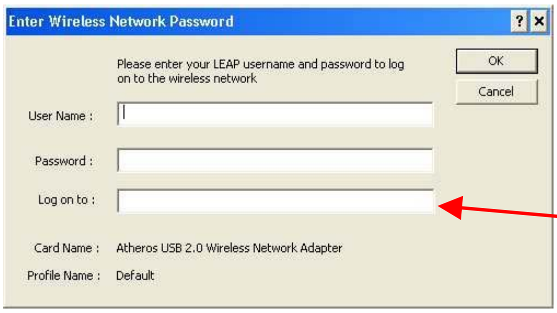
The RF signals for the following network card(s) have been successfully enabled:

Atheros USB 2.0 Wireless Network Adapter

Click on the **OK** button to proceed.

Manual LEAP Login

If you select this option, you will have to manually start the LEAP authentication process to login to the network instead of being prompted for your LEAP username and password during your windows logon.



Please enter your LEAP username and password to log on to the wireless network

User Name :

Password :

Log on to :

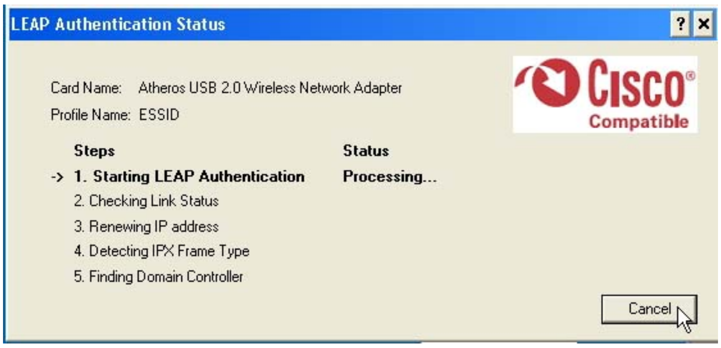
Card Name : Atheros USB 2.0 Wireless Network Adapter

Profile Name : Default

(Optional) Enter the domain name that you wish to logon to.

Reauthenticate

Reauthenticate to a LEAP-configured access point each time you login to a LEAP network.



Card Name: Atheros USB 2.0 Wireless Network Adapter

Profile Name: ESSID

Steps	Status
-> **1. Starting LEAP Authentication**	**Processing...**
2. Checking Link Status	
3. Renewing IP address	
4. Detecting IPX Frame Type	
5. Finding Domain Controller	

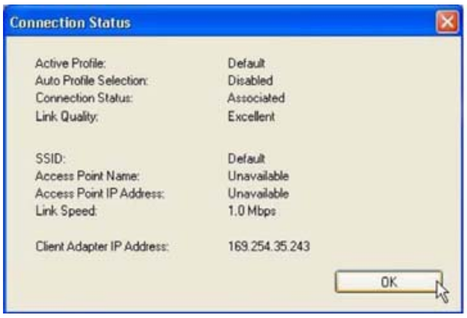
Select Profile

Click on a configuration profile name to switch to a particular wireless network. If no configuration profile exists, you will need to add a profile first.

Connection Status

To view the connection status of your wireless USB adapter.

Alternatively, you may also double click on the utility icon in the system tray.



Active Profile:	Default
Auto Profile Selection:	Disabled
Connection Status:	Associated
Link Quality:	Excellent
SSID:	Default
Access Point Name:	Unavailable
Access Point IP Address:	Unavailable
Link Speed:	1.0 Mbps
Client Adapter IP Address:	169.254.35.243

Active Profile Displays the name of the active configuration profile.

Auto Profile Selection Shows whether auto profile selection is enabled.

Connection Status Displays whether the adapter is connected to a wireless network.

Link Quality States the quality of the link connection.

SSID Displays the SSID of the network to which the wireless adapter is associated.

Access Point Name Shows the name of the access point the wireless adapter is connected to (if any).

Access Point IP Address Shows the IP address of the access point the wireless adapter is connected to (if any).

Link Speed States the speed of the link connection.

Client Adapter IP Address Displays the IP address of the wireless adapter.

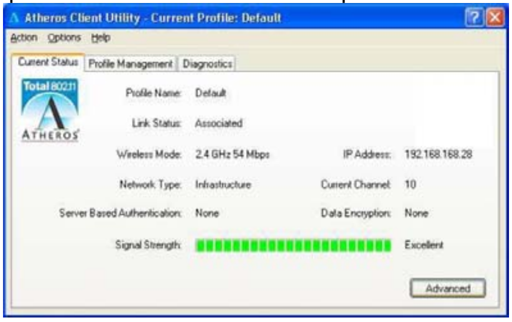
Chapter 5 Wireless Adapter Utility Features

This chapter shows you how to make use of the utility to view the status of your wireless connection; to change your settings and also to monitor your wireless performance via the statistics.

NOTE
It is advisable to activate only one of the utilities: Either the Wireless Zero Configuration Utility OR the Atheros Utility.

5.1 Current Status Tab

Displays the performance of the USB adapter in the wireless network.



Profile Name: Default

Link Status: Associated

Wireless Mode: 2.4 GHz 54 Mbps

IP Address: 192.168.168.28

Network Type: Infrastructure

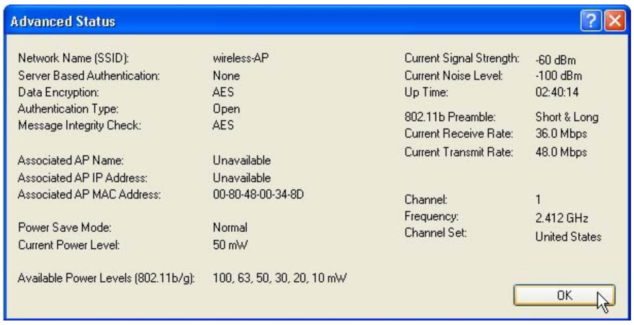
Current Channel: 10

Server Based Authentication: None

Data Encryption: None

Signal Strength: Excellent

Upon clicking on the **Advanced** button, you will be able to view all information on the respective profile, e.g. the types of encryption and authentication, the signal strength, the MAC address of the connected AP (if you are in Infrastructure mode), etc.



Network Name (SSID): wireless-AP
Server Based Authentication: None
Data Encryption: AES
Authentication Type: Open
Message Integrity Check: AES

Associated AP Name: Unavailable
Associated AP IP Address: Unavailable
Associated AP MAC Address: 00-80-48-00-34-8D

Power Save Mode: Normal
Current Power Level: 50 mW

Available Power Levels (802.11b/g): 100, 63, 50, 30, 20, 10 mW

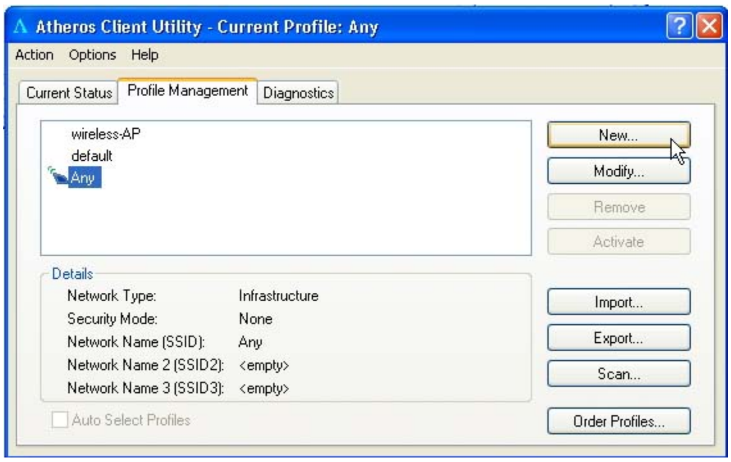
Current Signal Strength: -60 dBm
Current Noise Level: -100 dBm
Up Time: 02:40:14

802.11b Preamble: Short & Long
Current Receive Rate: 36.0 Mbps
Current Transmit Rate: 48.0 Mbps

Channel: 1
Frequency: 2.412 GHz
Channel Set: United States

5.2 Profile Management Tab

This option allows you to manage your profile, set your security options, and scan for other wireless networks.



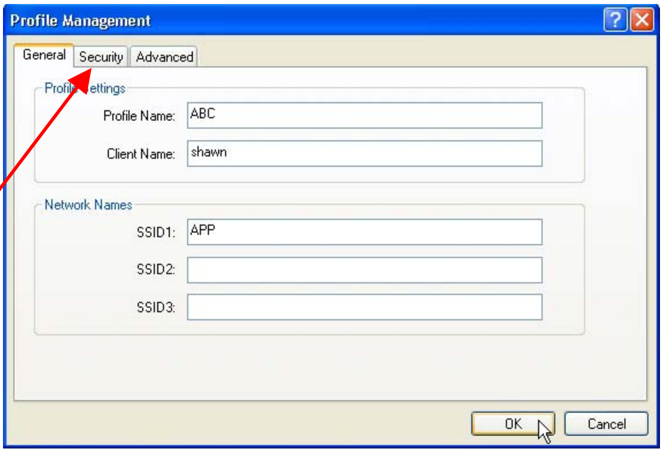
wireless-AP
default
Any

Details

Network Type: Infrastructure
Security Mode: None
Network Name (SSID): Any
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

Click on **New** button to create a new profile. Enter the profile name (a unique name to identify this profile), a client name and the SSID of the wireless network to connect to. Note that the **Client name** refers to the name that is registered to your PC/notebook. You can enter up to 3 different SSIDs in order of preference, per profile. We are using *ABC* as the profile name and *APP* as the SSID1.

For details on how to set the different authentication and encryption types available under the **Security** Tab, kindly refer to **Chapter 7 "Types of Authentication and Encryption mode"**



Profile Name: ABC

Client Name: shawn

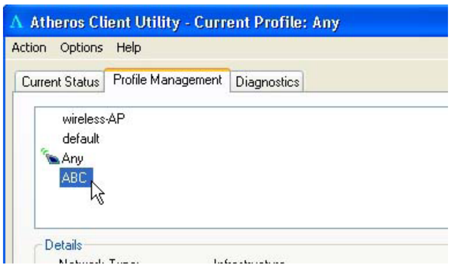
SSID1: APP

SSID2:

SSID3:

Click on the **OK** button to update the changes.

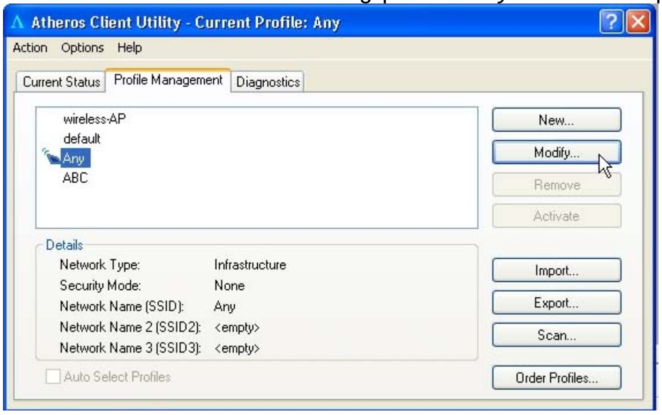
Notice that ABC has been added to the profile list.



wireless-AP
default
Any
ABC

Modify...

To modify an existing profile, select the profile that you wish to modify and click on this button. We are using profile: *Any* as an example.



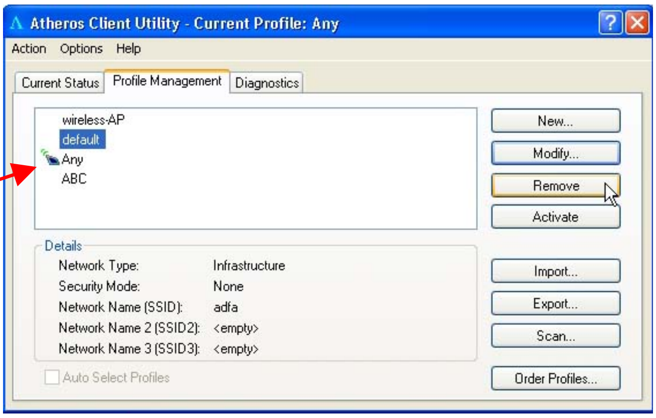
Details

Network Type: Infrastructure
Security Mode: None
Network Name (SSID): Any
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

Remove

To delete an existing profile, select the particular profile that you wish to delete and click on this button. We are using profile: *default* as an example.

Note that the active profile (the profile that you are currently using) cannot be deleted!



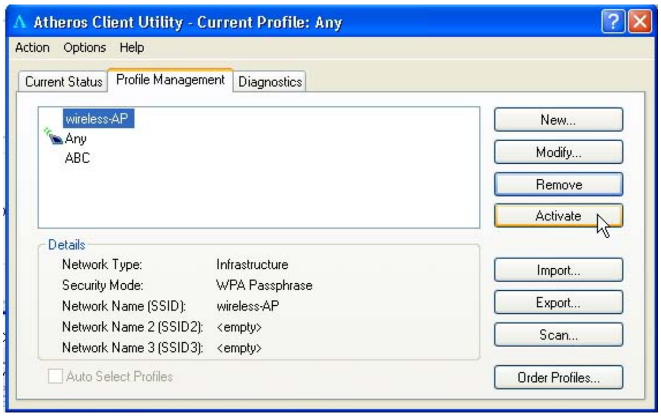
Details

Network Type: Infrastructure
Security Mode: None
Network Name (SSID): adfa
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

Active profile indicated by this icon cannot be deleted!

Activate

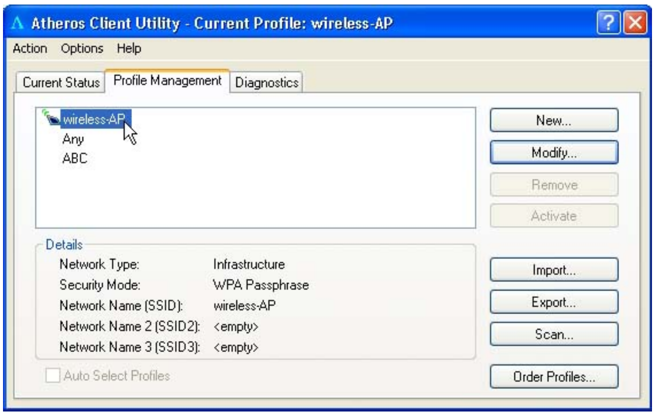
To activate a profile, select the profile and click on this button. We are using profile: *wireless-AP* as an example.



Details

Network Type: Infrastructure
Security Mode: WPA Passphrase
Network Name (SSID): wireless-AP
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

Once a profile is activated, this icon will appear next to the profile name: *wireless-AP*.



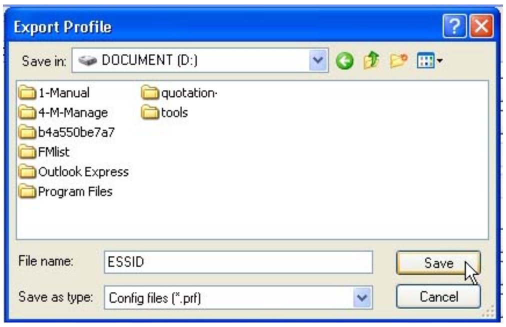
Details

Network Type: Infrastructure
Security Mode: WPA Passphrase
Network Name (SSID): wireless-AP
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

Export...

This function allows you to save the settings of your profile onto disk. Select the profile that you wish to save and click on this button. We are using profile: *ESSID* as an example.

Choose the folder to save to, enter the name under which to save the profile and click on the **Save** button.



Export Profile

Save in: DOCUMENT (D:)

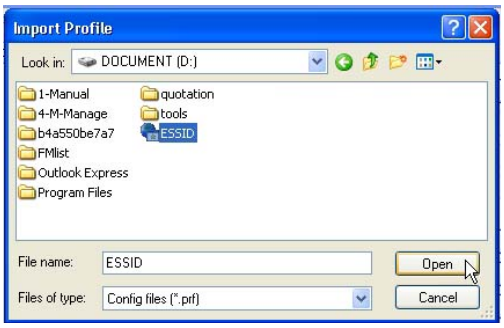
File name: ESSID

Save as type: Config files (*.prf)

Now, your profile is saved to your selected folder.

This function allows you to retrieve a saved profile from disk. We are using profile: *ESSID* as an example.

Go to the folder where you have saved your profile, select *ESSID.prf* and click on the **Open** button.

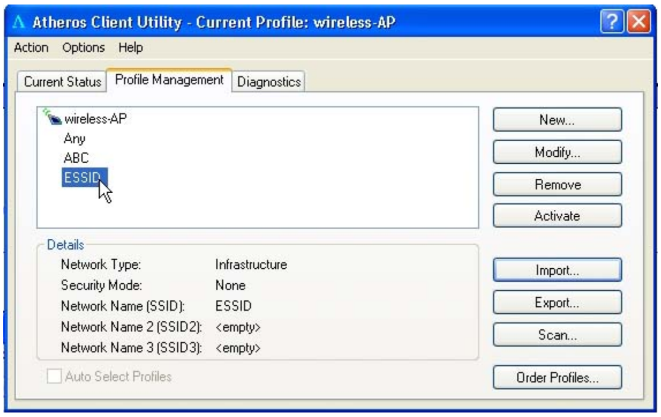


Look in: DOCUMENT (D:)

File name: ESSID

Files of type: Config files (*.prf)

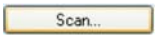
Notice that the profile: *ESSID* has been imported to the list of profiles.



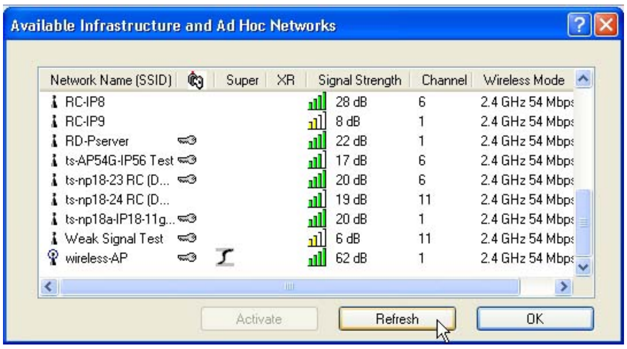
Details

Network Type: Infrastructure
Security Mode: None
Network Name (SSID): ESSID
Network Name 2 (SSID2): <empty>
Network Name 3 (SSID3): <empty>

□ Auto Select Profiles



This function allows you to scan for wireless networks detected by the adapter.



Available Infrastructure and Ad Hoc Networks

Network Name (SSID)	🔑	Super	XR	Signal Strength	Channel	Wireless Mode
RC-IP8				28 dB	6	2.4 GHz 54 Mbps
RC-IP9				8 dB	1	2.4 GHz 54 Mbps
RD-Pserver	🔑			22 dB	1	2.4 GHz 54 Mbps
ts-AP54G-IP56 Test	🔑			17 dB	6	2.4 GHz 54 Mbps
ts-np18-23 RC (D...	🔑			20 dB	6	2.4 GHz 54 Mbps
ts-np18-24 RC (D...				19 dB	11	2.4 GHz 54 Mbps
ts-np18a-IP18-11g...	🔑			20 dB	1	2.4 GHz 54 Mbps
Weak Signal Test	🔑			6 dB	11	2.4 GHz 54 Mbps
wireless-AP	🔑	✓		62 dB	1	2.4 GHz 54 Mbps

The icons shown beside the Network Name (SSID) indicate the type of WLAN detected.

📡 Connected to Infrastructure (AP)

🔑 Encryption Active

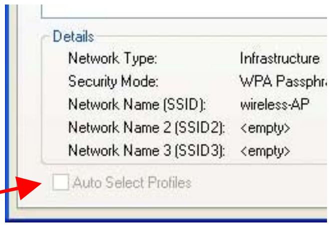
Notice that if there is a ∫ icon appearing in the Super column, this shows that the wireless network supports Super-AG technology (108Mbps).

Click on the **Refresh** button to renew the list of wireless networks detected.

Click on the **OK** button to exit the window.

If you have created several profiles, this function allows you to establish the priority order in which the USB adapter should try to connect to a WLAN. If the USB adapter is unable to connect to the 1st profile, it will then try to connect to the 2nd profile and so on.

Notice that if this function is disabled, this means that you have not added any profile in the **Auto Selected Profiles** list.



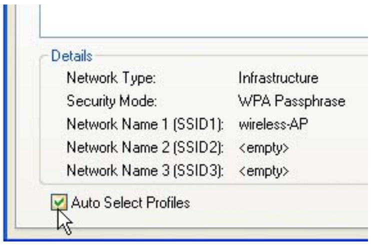
Details

Network Type:	Infrastructure
Security Mode:	WPA Passphr
Network Name (SSID):	wireless-AP
Network Name 2 (SSID2):	<empty>
Network Name 3 (SSID3):	<empty>

□ Auto Select Profiles

When auto profile selection is enabled, the USB adapter scans for available wireless networks and will connect to the highest priority profile that matches the networks detected.

To do so, simply click on the **Add** button from the **Available Profiles** list. Refer to the screen shown below.

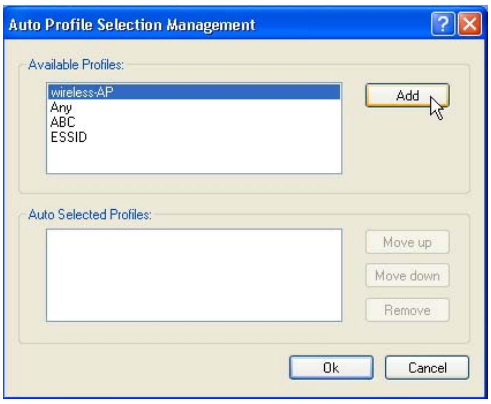


Details

Network Type:	Infrastructure
Security Mode:	WPA Passphrase
Network Name 1 (SSID1):	wireless-AP
Network Name 2 (SSID2):	<empty>
Network Name 3 (SSID3):	<empty>

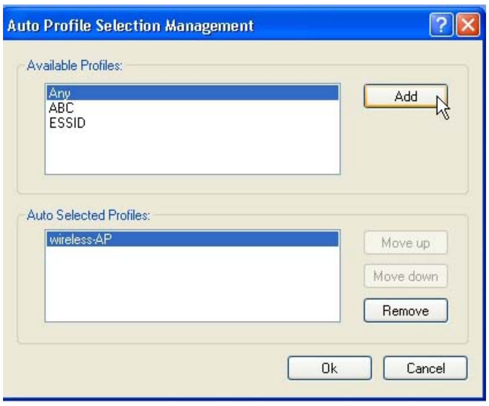
☑ Auto Select Profiles

Please note that you need AT LEAST TWO profiles to activate the **Auto Select Profiles** function; and that each of your profile must connect to at least one **Network Name (SSID)**.



Notice that when a selected profile has been added, it will be transferred to the **Auto Selected Profiles** list.

Select and click on the **Add** button to transfer another profile.



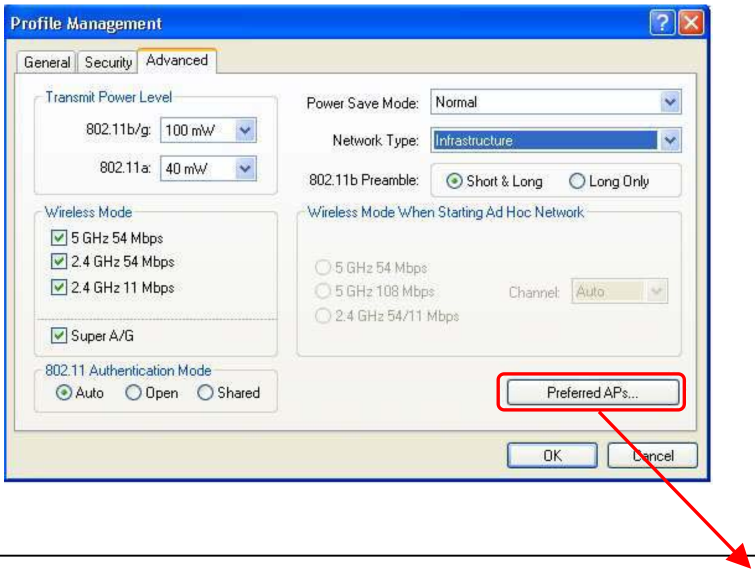
You need to transfer at least two profiles to the **Auto Selected Profiles** list to activate the **Auto Select Profile** function.

5.2.1 Security Tab

Please refer to **Chapter 7 “Types of Authentication and Encryption mode”**

5.2.2 Advanced Tab

This option allows you to configure the more advanced connection settings of your wireless client.



Transmit Power Level

802.11b/g: 100 mW

802.11a: 40 mW

Power Save Mode: Normal

Network Type: Infrastructure

802.11b Preamble: ● Short & Long ○ Long Only

Wireless Mode

☑ 5 GHz 54 Mbps

☑ 2.4 GHz 54 Mbps

☑ 2.4 GHz 11 Mbps

☑ Super A/G

Wireless Mode When Starting Ad Hoc Network

○ 5 GHz 54 Mbps

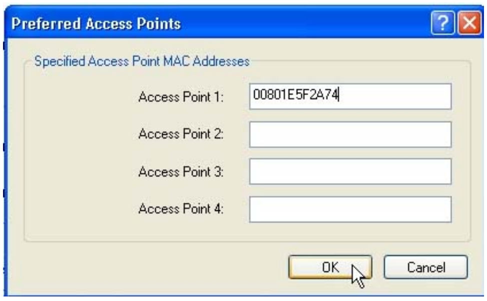
○ 5 GHz 108 Mbps

○ 2.4 GHz 54/11 Mbps

Channel: Auto

802.11 Authentication Mode

● Auto ○ Open ○ Shared



Access Point 1: 00801E5F2A74

Access Point 2:

Access Point 3:

Access Point 4:

Only applicable to Infrastructure mode.
You may key in the MAC address of at most four access points to which you would prefer to connect.

Transmit Power Level
Specifies the wireless transmit power to be used. Reducing the power level lowers the risk of interference with other nearby wireless devices and conserves battery power but decreases radio range.

Power Save Mode (Only applicable to Infrastructure mode)
This feature reduces power consumption by the USB adapter to extend the battery life of your notebook. There are 3 options for this mode:

- **Off**
  The power management is disabled and the card consumes full power from the computer.

- **Normal**
  The driver turns off the power to the adapter for brief periods over briefly spaced time intervals.

- **Maximum**
  The driver turns off power to the adapter for longer periods over more widely spaced time intervals.

The guideline for choosing between the **Normal** and **Maximum** options:
The USB adapter wakes up more often and responds sooner to network requests in **Normal** mode than in **Maximum** mode; and the **Maximum** mode consumes less power than **Normal** mode.

Network Type
Select either Infrastructure if you are connecting to the WLAN using an access point or Ad-hoc if you are connecting directly to another computer equipped with a wireless adapter.

802.11b Preamble
The preamble is part of the IEEE 802.11b physical layer specification. It is mandatory for all 802.11b devices to support the long preamble format, but they may optionally support the short preamble. This USB adapter supports both the short and long preambles.

- **Short & Long**
  This option allows communication with other 802.11b devices that support short preamble to boost the throughput.

- **Long**
  If your device is having trouble to communicate with other 802.11b devices, you may try to select the Long Only option.

Wireless Mode
Specifies 5GHz 54 Mbps, 2.4 GHz 54 Mbps, 2.4 GHz 11 Mbps, or Super A/G operation in a wireless network where there is an access point.

The wireless adapter must match the wireless mode of the access point it associates to.

802.11 Authentication Mode (Only applicable to Infrastructure mode, after you have enabled the encryption mode)
Select which mode the wireless adapter uses to authenticate to an access point:

- **Auto**
  Causes the adapter to attempt authentication using shared authentication. It then switches to open authentication if shared authentication fails.
- **Open**
  Enables an adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if the WEP key of the adapter matches that of the access point.

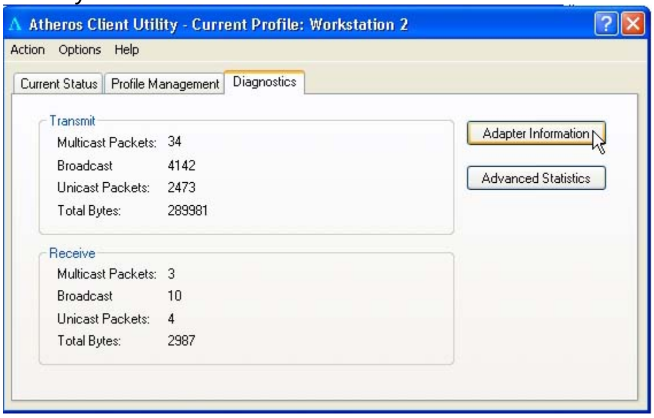
- **Shared only**
  Allows the adapter to authenticate and associate only with access points that have the same WEP key.

Note:
The USB adapter's authentication mode settings must match those of the AP it is trying to connect to for successful communication.

5.3 Diagnostics Tab

The Diagnostics tab lists the following receive and transmit diagnostics for packets received by or transmitted to the USB adapter.

- Multicast packets transmitted and received
- Broadcast packets transmitted and received
- Unicast packets transmitted and received
- Total bytes transmitted and received

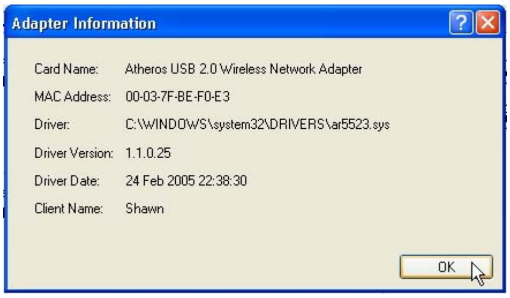


Transmit
Multicast Packets: 34
Broadcast 4142
Unicast Packets: 2473
Total Bytes: 289981

Receive
Multicast Packets: 3
Broadcast 10
Unicast Packets: 4
Total Bytes: 2987

Adapter Information

This button contains general information about the network interface card (the wireless USB adapter) and the network driver interface specification (NDIS).

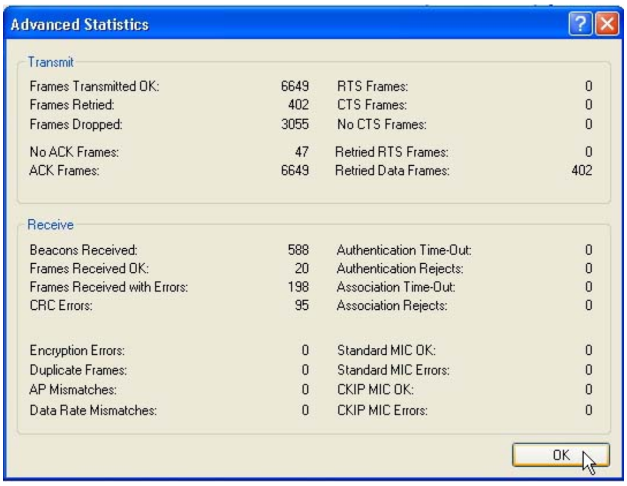


Card Name: Atheros USB 2.0 Wireless Network Adapter
MAC Address: 00-03-7F-BE-F0-E3
Driver: C:\WINDOWS\system32\DRIVERS\ar5523.sys
Driver Version: 1.1.0.25
Driver Date: 24 Feb 2005 22:38:30
Client Name: Shawn

Card Name	The name of the USB adapter
MAC Address	The MAC address of the USB adapter
Driver	The driver name and path of the USB adapter's driver
Driver version	The version of the USB adapter's driver
Driver date	The creation date of the USB adapter's driver
Client Name	The name of the client computer

Advanced Statistics

This button shows more detailed statistical information on frames that are either received by or transmitted to the USB adapter.



Advanced Statistics

Transmit

Frames Transmitted OK:	6649	RTS Frames:	0
Frames Retried:	402	CTS Frames:	0
Frames Dropped:	3055	No CTS Frames:	0
No ACK Frames:	47	Retried RTS Frames:	0
ACK Frames:	6649	Retried Data Frames:	402

Receive

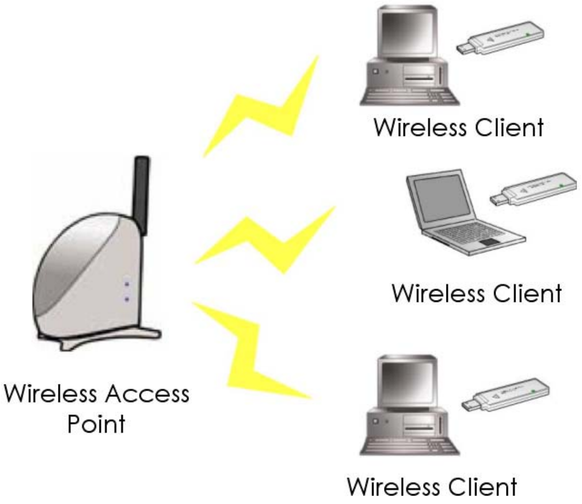
Beacons Received:	588	Authentication Time-Out:	0
Frames Received OK:	20	Authentication Rejects:	0
Frames Received with Errors:	198	Association Time-Out:	0
CRC Errors:	95	Association Rejects:	0
Encryption Errors:	0	Standard MIC OK:	0
Duplicate Frames:	0	Standard MIC Errors:	0
AP Mismatches:	0	CKIP MIC OK:	0
Data Rate Mismatches:	0	CKIP MIC Errors:	0

Chapter 6 Wireless Adapter Utility Configuration

This chapter will elaborate on the Client Manager configuration of the USB adapter using some simple examples.

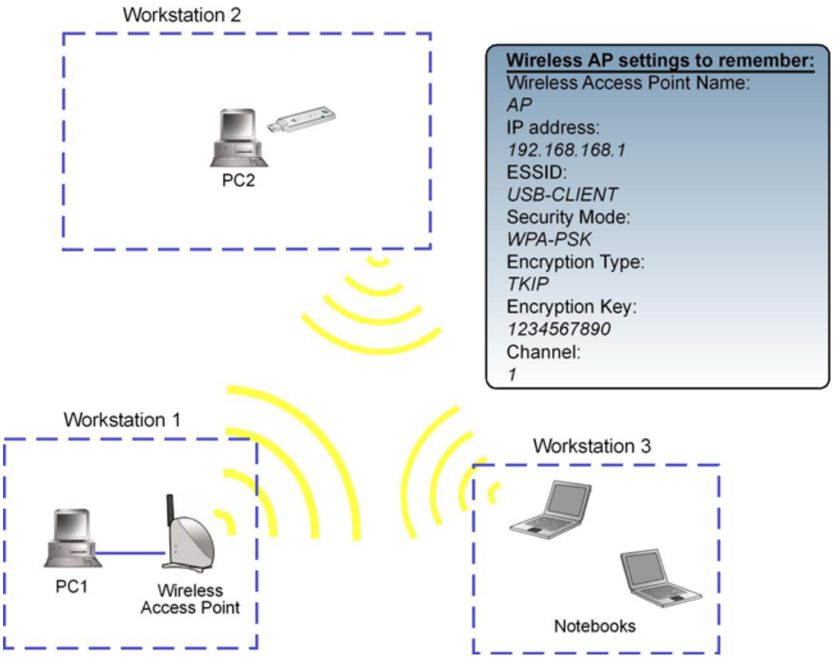
6.1 Infrastructure Mode

In infrastructure architecture, the wireless clients communicate through access points that are devices that act as base station for all wireless communication. Data packets from the wireless clients are transferred to the access points before being transmitted to other hosts on the network. The number of wireless clients supported depends on the access points.



6.1.1 Configuration on Infrastructure Mode

In this example, two notebooks and PC2 act as wireless clients to communicate with the wireless AP. Once all configuration has been done, wireless clients with the same SSID as the AP will be able to access wirelessly to PC1 via the wireless AP.



Wireless AP settings to remember:
Wireless Access Point Name:
AP
IP address:
192.168.168.1
ESSID:
USB-CLIENT
Security Mode:
WPA-PSK
Encryption Type:
TKIP
Encryption Key:
1234567890
Channel:
1

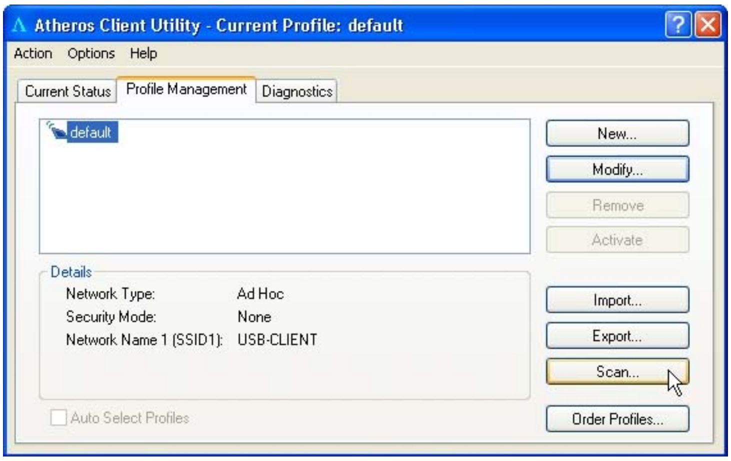
For AP

Ensure that you have enabled the DHCP server in your access point and that your wireless clients are set to receive their IP address dynamically so that the wireless AP can assign an IP address to its wireless clients. Note the wireless configuration settings of your access point as shown in the figure above.

For PC 2

1. Activate your USB adapter's utility.

2. Go to the **Profile Management** tab, click on the **Scan** button to look for the wireless AP.



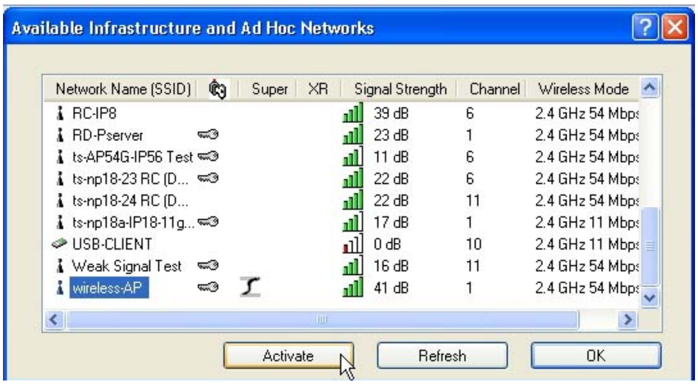
Details

Network Type: Ad Hoc

Security Mode: None

Network Name 1 (SSID1): USB-CLIENT

3. Click on the **Refresh** button if your system is unable to detect your wireless AP. Once found, select the **Network Name (SSID)** used by the AP**:** *Wireless-AP* and click on the **Activate** button to add it to your profile list.



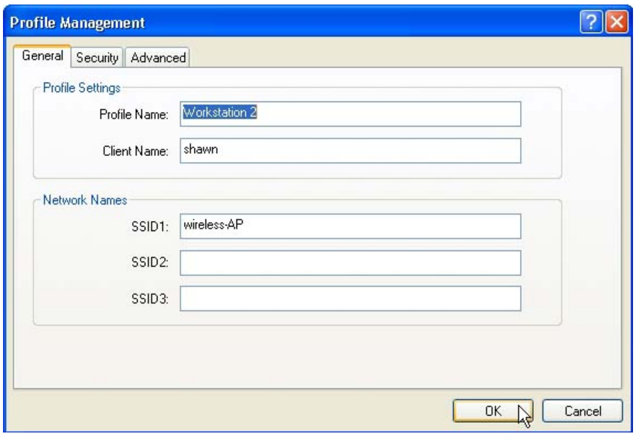
Available Infrastructure and Ad Hoc Networks

Network Name (SSID)	🔑	Super	XR	Signal Strength	Channel	Wireless Mode
RC-IP8				39 dB	6	2.4 GHz 54 Mbps
RD-Pserver	🔑			23 dB	1	2.4 GHz 54 Mbps
ts-AP54G-IP56 Test	🔑			11 dB	6	2.4 GHz 54 Mbps
ts-np18-23 RC (D...	🔑			22 dB	6	2.4 GHz 54 Mbps
ts-np18-24 RC (D...				22 dB	11	2.4 GHz 54 Mbps
ts-np18a-IP18-11g...	🔑			17 dB	1	2.4 GHz 11 Mbps
USB-CLIENT				0 dB	10	2.4 GHz 11 Mbps
Weak Signal Test	🔑			16 dB	11	2.4 GHz 54 Mbps
wireless-AP	🔑	✓		41 dB	1	2.4 GHz 54 Mbps

Notice that the SSID has already been pre-configured in this profile.

The SSID of both the wireless AP and the wireless client must be the same for them to communicate with one another.

4. Enter the **Profile Name**, e.g. *Workstation 2* for easy identification.



Profile Management

Profile Settings

Profile Name: Workstation 2

Client Name: shawn

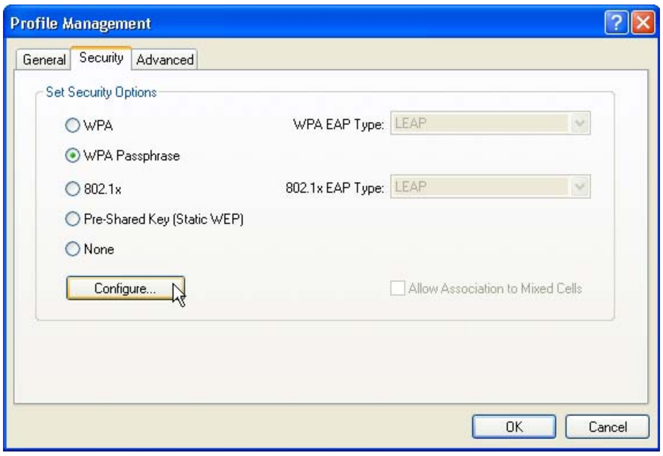
Network Names

SSID1: wireless-AP

SSID2:

SSID3:

5. Next, proceed to the **Security** tab. The wireless client must use the same security mode as the AP. In our example, select **WPA Passphrase** and click on the **Configure…** button.



Profile Management

General | Security | Advanced

Set Security Options

○ WPA WPA EAP Type: LEAP

● WPA Passphrase

○ 802.1x 802.1x EAP Type: LEAP

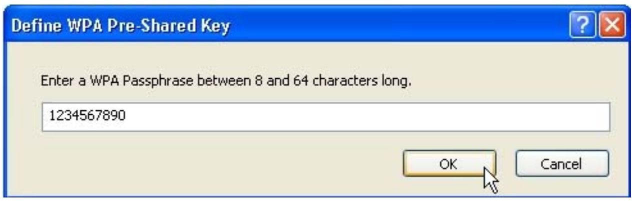
○ Pre-Shared Key (Static WEP)

○ None

Configure... □ Allow Association to Mixed Cells

6. Enter the encryption key in the field provided. Please note that this key must be the same as the one that you had configured for your access point.

7. Click on the **OK** button to update the changes.

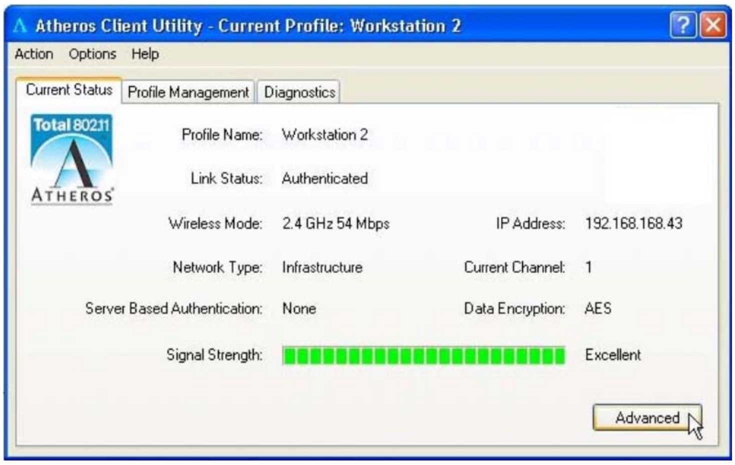


Define WPA Pre-Shared Key

Enter a WPA Passphrase between 8 and 64 characters long.

1234567890

Proceed to your **Current Status** tab to monitor the connection between the access point and the wireless client (PC2).



Profile Name: Workstation 2

Link Status: Authenticated

Wireless Mode: 2.4 GHz 54 Mbps

IP Address: 192.168.168.43

Network Type: Infrastructure

Current Channel: 1

Server Based Authentication: None

Data Encryption: AES

Signal Strength: Excellent

Alternatively, you can also check the connection from the MS-DOS Prompt. From PC2, simply proceed to the **Start** Menu, **Run...** and type in *cmd*. Click on the **OK** button.

In the MS-DOS Prompt window, type *ping 192.168.168.1 –t*, whereby this IP address belongs to your access point.

When the screen appears:

```
Pinging 192.168.168.1: bytes=32 time=2ms TTL=128
Pinging 192.168.168.1: bytes=32 time=2ms TTL=128
Pinging 192.168.168.1: bytes=32 time=2ms TTL=128
…….
```

This indicates that the connection between the access point and the wireless client has been established successfully! You can now access to one another wirelessly!

For the rest of the workstations

Refer to the steps for configuring PC2.

If your other wireless clients are not using the USB adapter, you may refer to the manual of these other adapters for details on Ad-hoc configuration.

For details on other authentication and encryption types, kindly refer to **Chapter 7 "Types of Authentication and Encryption mode"**

Chapter 7 Types of Authentication and Encryption mode

This chapter illustrates the different types of authentication and encryption that can be used in the wireless LAN.

7.1 Infrastructure Network Security

Extensible Authentication Protocol (EAP) is used to authenticate network clients before letting them access the enterprise network. It allows the network administrator to create an arbitrary authentication scheme (such as EAP-TLS, etc) to validate network access.

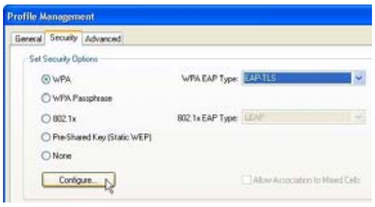
7.1.1 EAP-TLS

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) makes use of client-side and server-side certificates for mutual authentication.

To use EAP-TLS security, access the **Security** tab in the **Profile Management** window.

1. You can select

   WPA radio button



Profile Management

General | Security | Advanced

Set Security Options

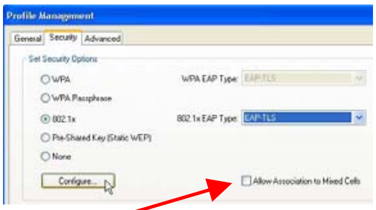
● WPA — WPA EAP Type: EAP-TLS
○ WPA Passphrase
○ 802.1x — 802.1x EAP Type: LEAP
○ Pre-Shared Key (Static WEP)
○ None

Configure...

□ Allow Association to Mixed Cells

   Or

   802.1x radio button
   (802.1x enables 802.1x security.



Profile Management

General | Security | Advanced

Set Security Options

○ WPA — WPA EAP Type: EAP-TLS
○ WPA Passphrase
● 802.1x — 802.1x EAP Type: EAP-TLS
○ Pre-Shared Key (Static WEP)
○ None

Configure...

□ Allow Association to Mixed Cells

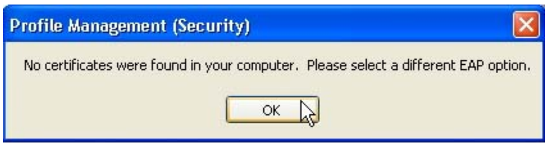
If the access point that the wireless adapter is associating to has WEP set to **Optional** while the wireless adapter has WEP enabled, ensure that **Allow Association to Mixed Cells** is checked to allow association.

Note that this option is available only in **802.1x** and **Pre-Shared Key (Static WEP)**.

2. Choose **EAP-TLS** from the drop-down menu and click on the **Configure…** button.

NOTE
To enable this security, you must ensure that your PC/notebook has already downloaded its EAP-TLS certificates. Check with your system administrator for details.

3. If your system does not support EAP-TLS, the following message will pop up:



Profile Management (Security)

No certificates were found in your computer. Please select a different EAP option.

If EAP-TLS is supported, select the appropriate certificate authority from the list. The server/domain name and the login name are filled in automatically from the certificate information.

4. Click on the **OK** button twice to activate the profile.

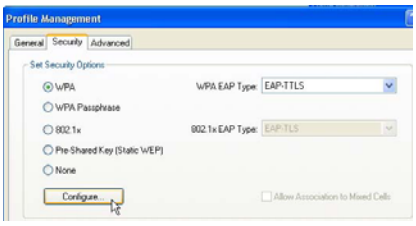
7.1.2 EAP-TTLS

EAP-TTLS (Tunnel **T**ransport **L**ayer Security) authentication is an extension to EAP-TLS. It uses certificates and EAP-TLS to authenticate the server only and establish an encrypted tunnel. Then within that tunnel, the client authenticates to the server using either a username and password or a token card.

To use EAP-TTLS security, access the **Security** tab in the **Profile Management** window.

1. You can select

   WPA radio button



Profile Management

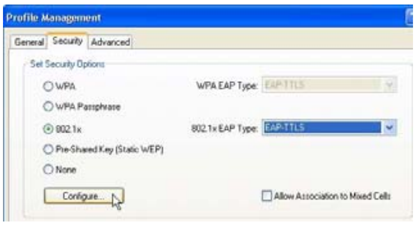
General | Security | Advanced

Set Security Options

● WPA — WPA EAP Type: EAP-TTLS
○ WPA Passphrase
○ 802.1x — 802.1x EAP Type: EAP-TLS
○ Pre-Shared Key (Static WEP)
○ None

   Or

   802.1x radio button



Profile Management

General | Security | Advanced

Set Security Options

○ WPA — WPA EAP Type: EAP-TTLS
○ WPA Passphrase
● 802.1x — 802.1x EAP Type: EAP-TTLS
○ Pre-Shared Key (Static WEP)
○ None

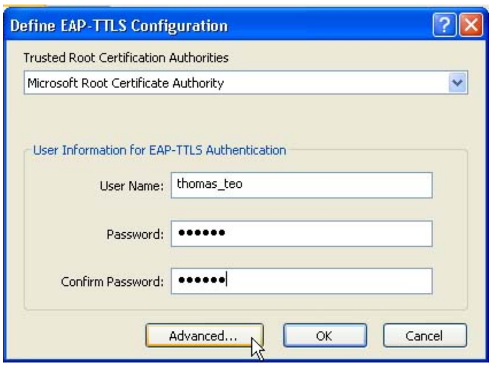
2. Choose **EAP-TTLS** from the drop-down menu and click on the **Configure...** button.

3. Select the appropriate certification authority (CA) from which the server certificate will be downloaded from the **Trusted Root Certification Authorities** drop-down list.

4. The EAP username is pre-defined in the **User Name** field. IF not, specify your username (which is registered with the

server) for EAP authentication. Enter your password in both the **Password** and **Confirm Password** fields.

5. Click on the **Advanced...** button.



Define EAP-TTLS Configuration

Trusted Root Certification Authorities: Microsoft Root Certificate Authority

User Information for EAP-TTLS Authentication

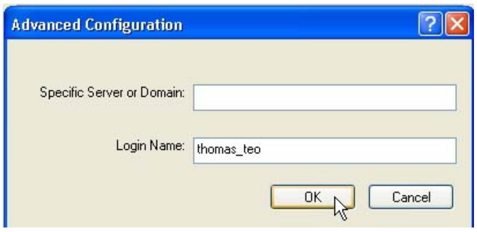
User Name: thomas_teo

Password: ••••••

Confirm Password: ••••••

6. Leave the specification server/domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the CA listed previously. The login name is pre-defined in the **Login name** field.

7. Click the **OK** button.



Advanced Configuration

Specific Server or Domain:

Login Name: thomas_teo

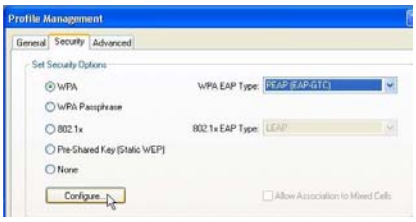
7.1.3 PEAP (EAP-GTC)

The PEAP (EAP-Generic Token Card) method is intended for use with Token Cards supporting challenge/response authentication and MUST NOT be used to provide support for clear text passwords in the absence of a protected tunnel with server authentication.

To use PEAP-GTC security, access the **Security** tab in the **Profile Management** window.

1. You can select

   WPA radio button



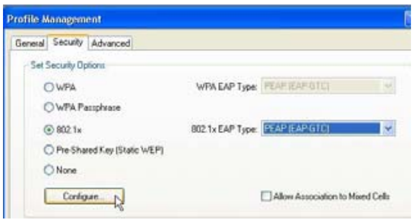
Set Security Options

● WPA WPA EAP Type: PEAP (EAP-GTC)
○ WPA Passphrase
○ 802.1x 802.1x EAP Type: LEAP
○ Pre-Shared Key (Static WEP)
○ None

□ Allow Association to Mixed Cells

   Or

   802.1x radio button



Set Security Options

○ WPA WPA EAP Type: PEAP (EAP-GTC)
○ WPA Passphrase
● 802.1x 802.1x EAP Type: PEAP (EAP-GTC)
○ Pre-Shared Key (Static WEP)
○ None

□ Allow Association to Mixed Cells

2. Choose **PEAP-GTC** from the drop-down menu and click on the **Configure…** button.

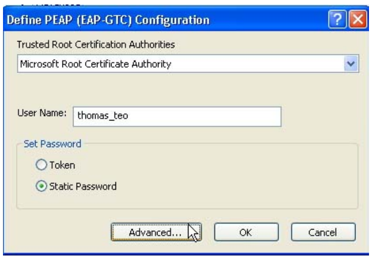
NOTE
To enable this security, you must ensure that your PC/notebook has already downloaded WPA-PEAP certificates; and the server properties must already be set. Check with your system administrator for details.

3. Select the appropriate certificate authority (CA) from which the server certificate is downloaded from the drop-down list.

4. Enter your PEAP username (which is registered with the server) in the **User Name** field.

5. Specify whether you are using a **Token** or a **Static Password**. Click on the **Advanced** button.

   Note that the Token can take the form of hardware token device or the Secure Computing SofToken Program (version 1.3 or later) to obtain and enter a one-time password for authentication.



Define PEAP (EAP-GTC) Configuration

Trusted Root Certification Authorities: Microsoft Root Certificate Authority

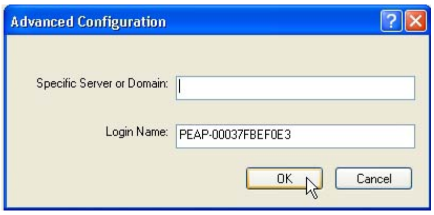
User Name: thomas_teo

Set Password
○ Token
● Static Password

6. Leave the specification server/domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the CA listed previously.

7. The login name will be pre-defined in the field provided. This login name is used for PEAP tunnel authentication. It will be filled in automatically as PEAP-*xxxxxxxxxxxx*, where xxxxxxxxxxxx is the computer's MAC address. You may

change the login name if needed. Click on the **OK** button to save your settings.



Advanced Configuration

Specific Server or Domain:

Login Name: PEAP-00037FBEF0E3

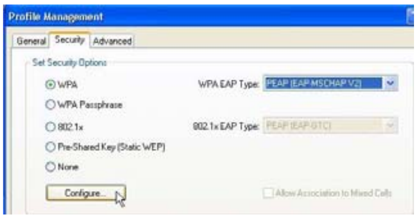
7.1.4 PEAP (EAP-MSCHAP V2)

Microsoft-Challenge Handshake Authentication Protocol V2 (MS-CHAP V2) is a mutual authentication protocol that requires both the client and server's identities to be proven. If your connection is configured to use MS-CHAP V2 as its only authentication method, and the server that you are connecting to does not provide proof of its identity, your connection disconnects.

To use PEAP-MSCHAP V2 security, access the **Security** tab in the **Profile Management** window.

1. You can select

   WPA radio button



Profile Management

Set Security Options

● WPA — WPA EAP Type: PEAP (EAP-MSCHAP V2)

○ WPA Passphrase

○ 802.1x — 802.1x EAP Type: PEAP (EAP-GTC)

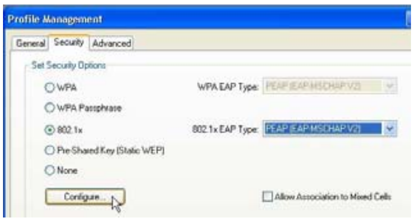
○ Pre-Shared Key (Static WEP)

○ None

□ Allow Association to Mixed Cells

   Or

   802.1x radio button



Profile Management

Set Security Options

○ WPA — WPA EAP Type: PEAP (EAP-MSCHAP V2)

○ WPA Passphrase

● 802.1x — 802.1x EAP Type: PEAP (EAP-MSCHAP V2)

○ Pre-Shared Key (Static WEP)

○ None

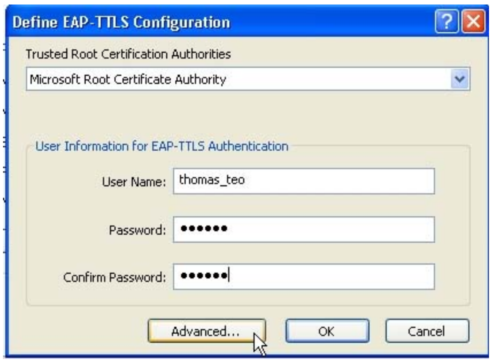
□ Allow Association to Mixed Cells

2. Choose **PEAP (MS-CHAPV2)** from the drop-down menu and click on the **Configure…** button.

NOTE
To enable this security, you must ensure that your PC/notebook has already downloaded WPA-PEAP certificates; and the server properties must already be set. Check with your system administrator for details.

3. Enter your PEAP username and password (which are registered with the server) in the **User Name** and **Password** field respectively. Re-type the password in the **Confirm Password** field.

4. Click on the **Advanced** button.


Define EAP-TTLS Configuration
User Information for EAP-TTLS Authentication
Advanced…
OK
Cancel

Trusted Root Certification Authorities: Microsoft Root Certificate Authority

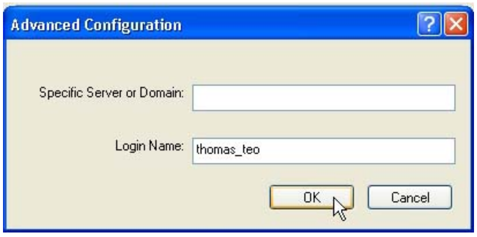
User Name: thomas_teo

Password: ••••••

Confirm Password: ••••••

5. Leave the specification server/domain field blank to allow the client to accept a certificate from any server that supplies a certificate signed by the CA listed previously.

6. Click the **OK** button to enable the profile.



Specific Server or Domain:

Login Name: thomas_teo

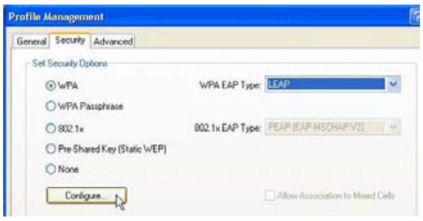
7.1.5 LEAP

Lightweight **E**xtensible **A**uthentication **P**rotocol (LEAP) security requires all infrastructure devices (e.g. access points and servers) to be configured for LEAP authentication.

To use LEAP security, access the **Security** tab in the **Profile Management** window.

1. You can select

   WPA radio button



● WPA

○ WPA Passphrase

○ 802.1x

○ Pre-Shared Key (Static WEP)

○ None

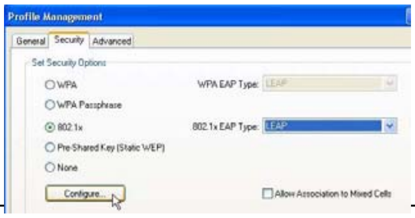
WPA EAP Type: LEAP

802.1x EAP Type: PEAP (EAP-MSCHAP V2)

□ Allow Association to Mixed Cells

   Or

   802.1x radio button



○ WPA

○ WPA Passphrase

● 802.1x

○ Pre-Shared Key (Static WEP)

○ None

WPA EAP Type: LEAP

802.1x EAP Type: LEAP

□ Allow Association to Mixed Cells

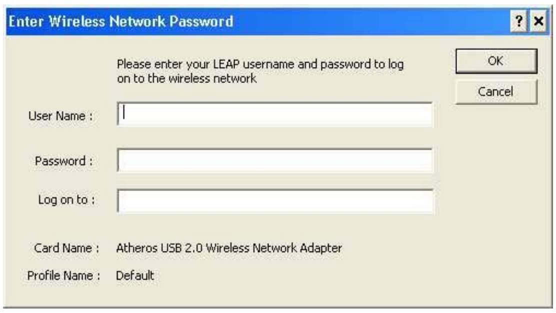
2. Choose **LEAP** from the drop-down menu and click on the **Configure…** button.

3. You may set your username and password to:
   - Use Temporary User Name and Password
   Each time your PC reboots, you will be require to enter your LEAP username and password in order to be authenticated and obtain access to the network.

   - Use Saved User Name and Password.
   Authentication is obtained using a saved username and password (registered with the server) so you will not be require to enter your LEAP username and password each time your PC reboots.

Temporary User Name and Password

1. The login page will pop up as shown below. Fill up the respective fields and click on the **OK** button twice.


Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

User Name :

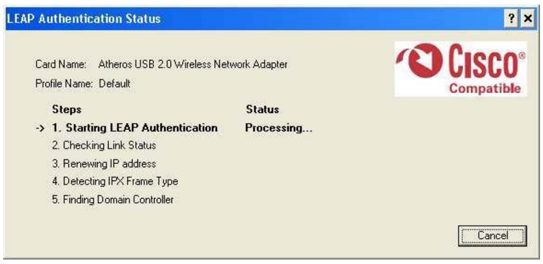
Password :

Log on to :

Card Name : Atheros USB 2.0 Wireless Network Adapter

Profile Name : Default

Next, the system will start the LEAP authentication.



Card Name: Atheros USB 2.0 Wireless Network Adapter
Profile Name: Default

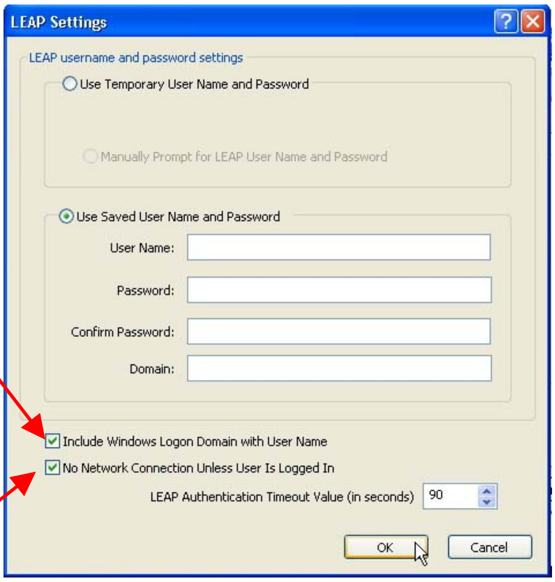
Steps	Status
-> 1. Starting LEAP Authentication	Processing...
2. Checking Link Status	
3. Renewing IP address	
4. Detecting IPX Frame Type	
5. Finding Domain Controller	

Saved User Name and Password

1. Enter the username, password and re-enter password in **Confirm Password** field.
   (Optional) You may enter a specific domain name, which will be passed to the server.

2. Enter the LEAP authentication timeout (between 30 and 500 seconds) to specify how long LEAP should wait before considering an authentication as failed, and sending an error message. The default is 90 seconds.

3. Click on the **OK** button.



LEAP username and password settings

○ Use Temporary User Name and Password

○ Manually Prompt for LEAP User Name and Password

● Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

☑ Include Windows Logon Domain with User Name

☑ No Network Connection Unless User Is Logged In

LEAP Authentication Timeout Value (in seconds) 90

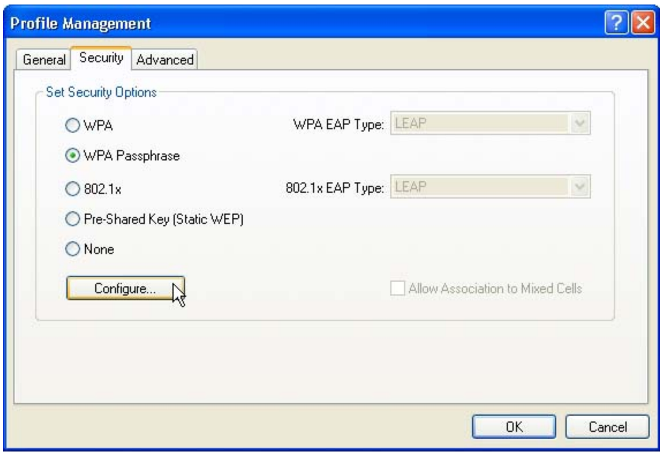
Check the **Include Windows Logon Domain with User Name** option to automatically send your Windows login domain together with your user name to the RADIUS server. (Default)

Check the **No Network Connection Unless User Is Logged In** option to force the wireless adapter to disassociate after you log off.

7.1.6 WPA Passphrase

WPA Passphrase is also known as WPA-PSK (Pre-shared Key). It provides strong encryption protection for home/SOHO users who do not use an enterprise authentication server.

1. Click on the **WPA Passphrase** radio button and click on the **Configure…** button.



Profile Management

General | Security | Advanced

Set Security Options

○ WPA WPA EAP Type: LEAP

● WPA Passphrase

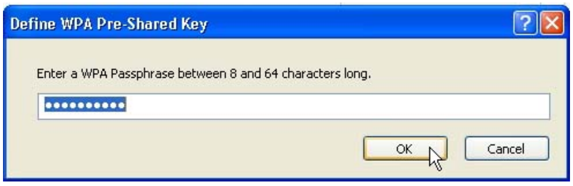
○ 802.1x 802.1x EAP Type: LEAP

○ Pre-Shared Key (Static WEP)

○ None

□ Allow Association to Mixed Cells

2. Enter the password and click on the **OK** button.



Define WPA Pre-Shared Key

Enter a WPA Passphrase between 8 and 64 characters long.

••••••••••

Note:
The WPA Passphrase must match that used by the AP/other wireless clients in the network.

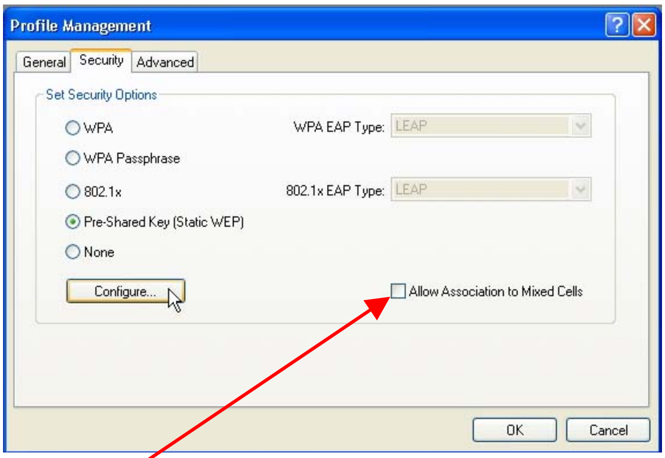
7.1.7 Pre-shared Key (Static WEP)

Wired **E**quivalent **P**rivacy is a security protocol that allows the wireless client adapter to communicate ONLY with access points or other wireless clients that have the same WEP key.

WEP Key is categorized into two types: Hexadecimal and ASCII. Hexadecimal values consist a to f and numbers 0 to 9 whereas ASCII values consist of alphanumeric characters a to z; 0 to 9.

To define pre-shared encryption keys,

1. Choose the **Pre-shared Key (Static WEP)** radio button and click the **Configure…** button to fill in the encryption key.



Set Security Options

○ WPA WPA EAP Type: LEAP

○ WPA Passphrase

○ 802.1x 802.1x EAP Type: LEAP

● Pre-Shared Key (Static WEP)

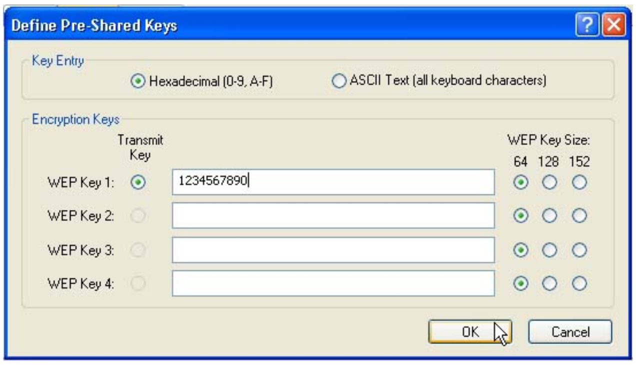
○ None

□ Allow Association to Mixed Cells

If the access point that the wireless adapter is associating to has WEP set to **Optional** while the wireless adapter has WEP enabled, ensure that **Allow Association to Mixed Cells** is checked to allow association.

Note that this option is available only in **802.1x** and **Pre-Shared Key (Static WEP)**.

2. Enter your WEP key and click on the **OK** button.



Define Pre-Shared Keys

Key Entry

● Hexadecimal (0-9, A-F) ○ ASCII Text (all keyboard characters)

Encryption Keys

	Transmit Key		WEP Key Size: 64	128	152
WEP Key 1:	●	1234567890	●	○	○
WEP Key 2:	○		●	○	○
WEP Key 3:	○		●	○	○
WEP Key 4:	○		●	○	○

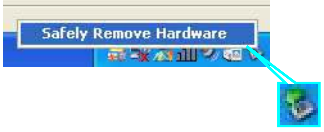
WEP Key size

- 64-bit WEP: 10 hexadecimal or 5 ASCII Text
- 128-bit WEP: 26 hexadecimal or 13 ASCII Text
- 152-bit WEP: 13 hexadecimal or 16 ASCII Text

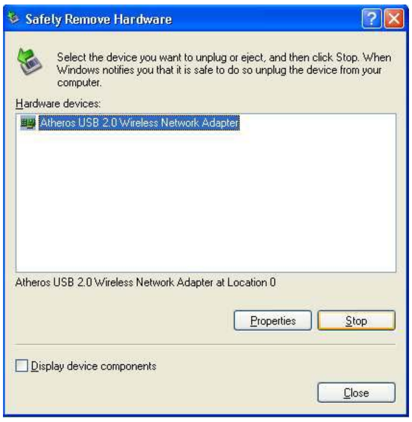
Appendix I Remove USB Adapter from the System

To safely remove your USB adapter from your system,

1. From the system tray, go to **Safely Remove Hardware** icon and click **Safely Remove Hardware**.



2. Select **Atheros USB 2.0 Wireless Network Adapter** and click on the **Stop** button to terminate all activities.



Select the device you want to unplug or eject, and then click Stop. When Windows notifies you that it is safe to do so unplug the device from your computer.

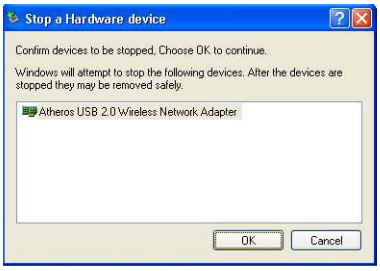
Hardware devices:

Atheros USB 2.0 Wireless Network Adapter

Atheros USB 2.0 Wireless Network Adapter at Location 0

□ Display device components

3. Next, select **Atheros USB 2.0 Wireless Network Adapter** to confirm you will be removing it from the USB port and click on the **OK** button.



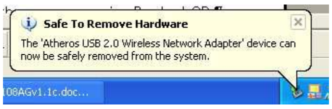
Stop a Hardware device

Confirm devices to be stopped, Choose OK to continue.

Windows will attempt to stop the following devices. After the devices are stopped they may be removed safely.

Atheros USB 2.0 Wireless Network Adapter

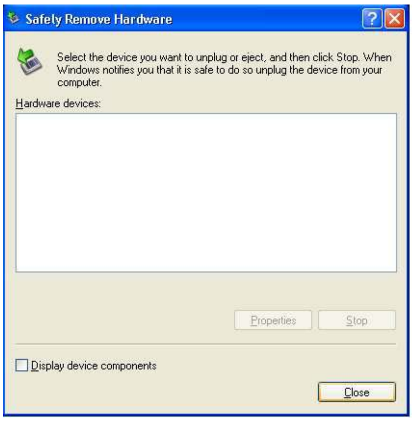
4. The system will then inform you that the device can now be safely removed from the system.



Safe To Remove Hardware

The 'Atheros USB 2.0 Wireless Network Adapter' device can now be safely removed from the system.

5. Click on the **Close** button to exit this window.



Safely Remove Hardware

Select the device you want to unplug or eject, and then click Stop. When Windows notifies you that it is safe to do so unplug the device from your computer.

Hardware devices:

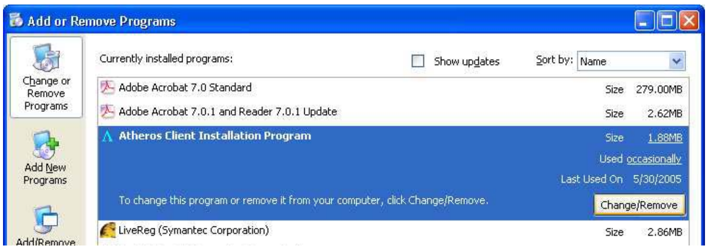
Appendix II Un-install Wireless Adapter

Please note that in case there is a software upgrade for the wireless adapter, you will need to un-install the current software version before installing the new software.

When you un-install the USB adapter's software, any existing profiles will be removed. If you want to re-use your profiles, please refer to **Section 5.2 Profile Management Tab** for further details on how to export a profile to disk. You are advised to close all programs and to leave the USB adapter in the USB slot of your PC/notebook before un-installing your USB adapter.

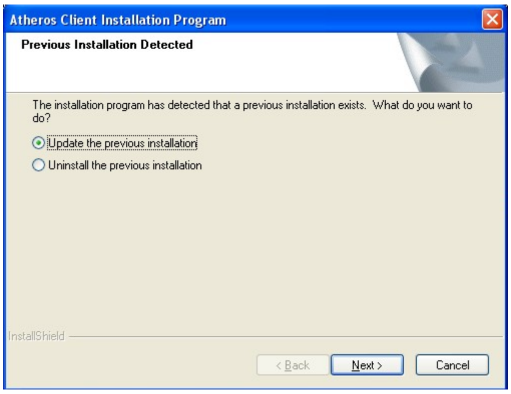
1. From your **Start** menu, go to **Settings, Control Panel** and then click on the **Add or Remove Programs** icon.

2. Highlight the **Atheros Client Installation Program** and click on the **Change/Remove** button.



Adobe Acrobat 7.0 Standard Size 279.00MB
Adobe Acrobat 7.0.1 and Reader 7.0.1 Update Size 2.62MB
Atheros Client Installation Program Size 1.88MB
Used occasionally
Last Used On 5/30/2005
To change this program or remove it from your computer, click Change/Remove.
LiveReg (Symantec Corporation) Size 2.86MB

3. Wait until you see the **Atheros Client Installation Program** screen. Select **Uninstall the previous installation**. Then click on the **Next>** button to proceed.



Atheros Client Installation Program

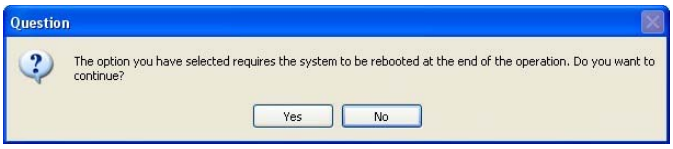
Previous Installation Detected

The installation program has detected that a previous installation exists. What do you want to do?

● Update the previous installation

○ Uninstall the previous installation

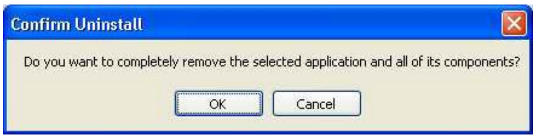
4. The prompt screen appears to notify you that the uninstall option requires the system to be rebooted at the end of the uninstall process. Click on the **Yes** button to proceed.



Question

The option you have selected requires the system to be rebooted at the end of the operation. Do you want to continue?

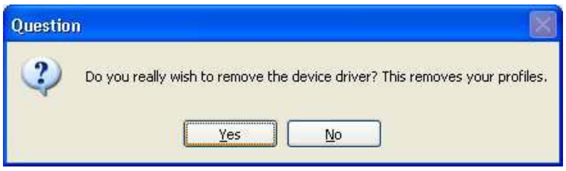
5. Your system will prompt you to confirm whether you want to remove the application completely. Click **OK** to proceed.



Confirm Uninstall

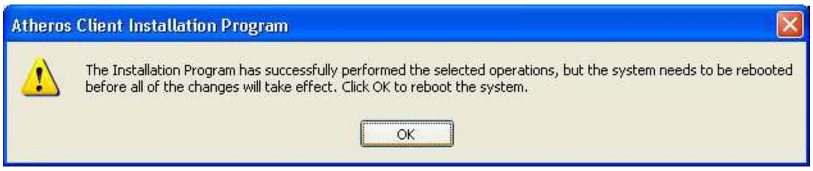
Do you want to completely remove the selected application and all of its components?

6. You will be asked to decide whether to remove the device driver or not. Click on the **Yes** button to accept.



Do you really wish to remove the device driver? This removes your profiles.

7. The uninstall process will then begin. Soon the prompt screen will appear informing you that the uninstall process is successful, and that your system needs to be rebooted.



The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Click OK to reboot the system.

8. Click **OK** to reboot the system.

Appendix III Certificate Application for WPA mode

The USB adapter supports WPA and WPA-PSK mode in Windows 2000/XP.

WPA is a specification of standards-based, interoperable security enhancement that strongly increases the level of data protection (encryption) and access control (authentication) in your wireless network. The technical components of WPA include Temporal Key Integrity Protocol (TKIP) for dynamic key exchange, and 802.1x for authentication.

WPA requires a RADIUS Server to complete the authentication among wireless stations and Access Points. Typically, this mode is used in an enterprise environment. WPA-PSK does not require a RADIUS Server and is very convenient for home/SOHO users. In this chapter, we will explain how to apply for a certificate in order to access to a wireless network using WPA mode.

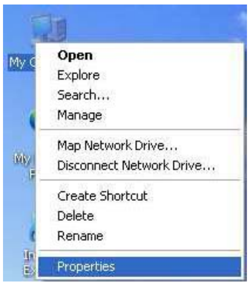
NOTE
For Windows XP users with Service Pack 1 (SP1), you need to upgrade to SP2, available from the Microsoft website or to install the two patch files provided in the Product CD.

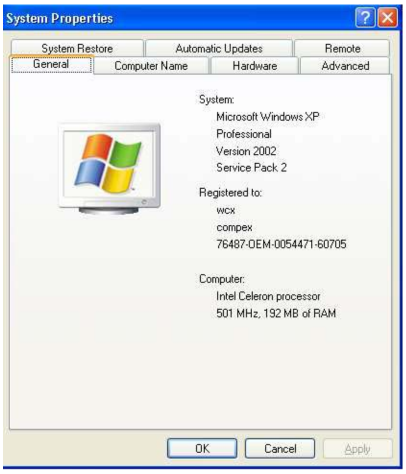
Overall procedures to apply certificate for WPA mode

- Install Windows XP Service Pack 2
- Apply certification via Internet Browser
- Become domain member

AIII.I Installing Window XP Service Pack Patch File (For Windows XP users)

To check whether you have already installed Windows XP SP2, go to **My Computer**, right click and select **Properties**.





System:
Microsoft Windows XP
Professional
Version 2002
Service Pack 2

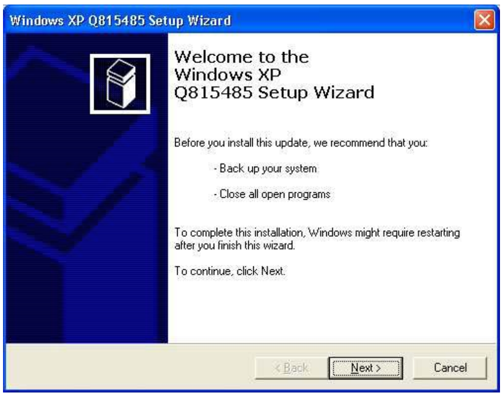
Registered to:
wcx
compex
76487-OEM-0054471-60705

Computer:
Intel Celeron processor
501 MHz, 192 MB of RAM

If you are using the Windows XP SP1 and do not intend to upgrade to SP2, you will need to install the two patch files provided in the Product CD.

1. After ensuring that you have installed Windows XP SP1, insert your Product CD into your CD-ROM drive, go to Drivers & Utilities section, select to install *WindowsXP- Q815485_WXP_SP2_x86_ENU.exe* followed by *WindowsXP-KB826942-x86-ENU.exe.*

   You may need to restart your PC to complete the installation.



Welcome to the Windows XP Q815485 Setup Wizard

Before you install this update, we recommend that you:

- Back up your system
- Close all open programs

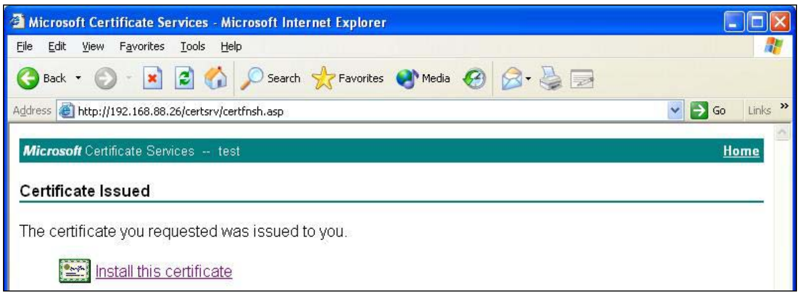
To complete this installation, Windows might require restarting after you finish this wizard.

To continue, click Next.

AIII.2 Installing certificate on your server

If you are using Microsoft Certificates services,

1. Click on the **Install this certificate** link in the window to start the installation.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links

http://192.168.88.26/certsrv/certfnsh.asp

Microsoft Certificate Services -- test

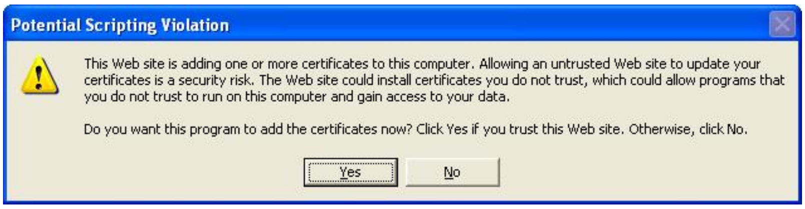
Home

Certificate Issued

The certificate you requested was issued to you.

Install this certificate

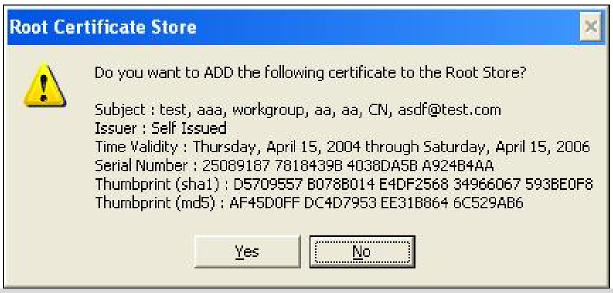
Chapter 8 Click on the Yes button on the pop up window to continue with the installation.



This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data.

Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.

Chapter 9 To add the certificate to the Root Store, click on the Yes button.

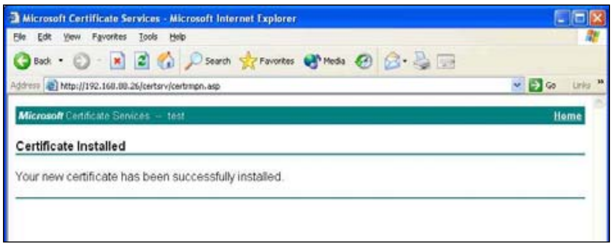


Root Certificate Store

Do you want to ADD the following certificate to the Root Store?

Subject : test, aaa, workgroup, aa, aa, CN, asdf@test.com
Issuer : Self Issued
Time Validity : Thursday, April 15, 2004 through Saturday, April 15, 2006
Serial Number : 25089187 7818439B 4038DA5B A924B4AA
Thumbprint (sha1) : D5709557 B078B014 E4DF2568 34966067 593BE0F8
Thumbprint (md5) : AF45D0FF DC4D7953 EE31B864 6C529AB6

Chapter 10 The following window will appear showing that the certificate has been successfully installed into your PC.



Microsoft Certificate Services - Microsoft Internet Explorer

Address http://192.168.88.26/certsrv/certrmpn.asp

Microsoft Certificate Services -- test

Certificate Installed

Your new certificate has been successfully installed.

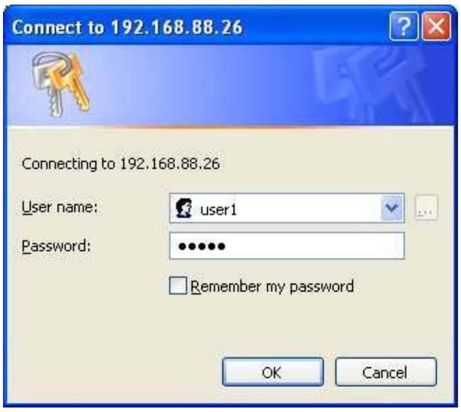
AIII.3 Applying for Client Certifications

If you have installed Microsoft SP2 or Microsoft XP SP1 with the 2 patch files provided on the Product CD, you are now ready to apply for a certificate for your wireless client.

At this stage, ensure that your wireless client has connectivity to the CA server. You should disable your key encryption.

1. Open your Internet browser; enter e.g. *http://192.168.88.26/certsrv* where 192.168.88.26 is the server's IP address.

Chapter 11 **Next, you need to connect to your server in order to get a certification. Enter the** username **and** password **that are provided by your system administrator.**



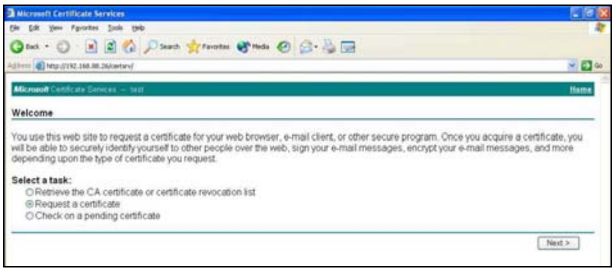
Connecting to 192.168.88.26

User name: user1

Password: ●●●●●

☐ Remember my password

Chapter 12 **Once you get connected to your server, the following screen shot will appear. Select the** Request a certificate **radio button and click on the** Next> **button. Follow the instructions shown on the screen.**


Microsoft Certificate Services
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Home
Next >

http://192.168.88.26/certsrv/

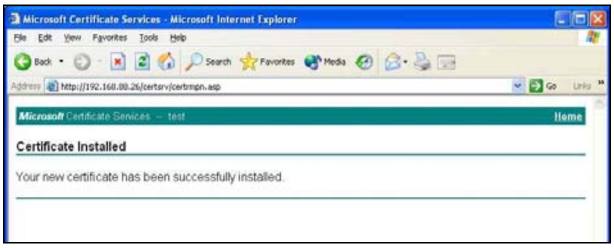
Microsoft Certificate Services -- test

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:
○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

The screen below will appear to indicate that a certificate has been successfully issued to your PC.

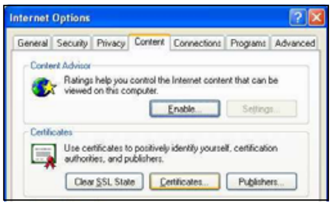

Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Microsoft Certificate Services -- test
Home

http://192.168.88.26/certsrv/certrmpn.asp

Certificate Installed

Your new certificate has been successfully installed.

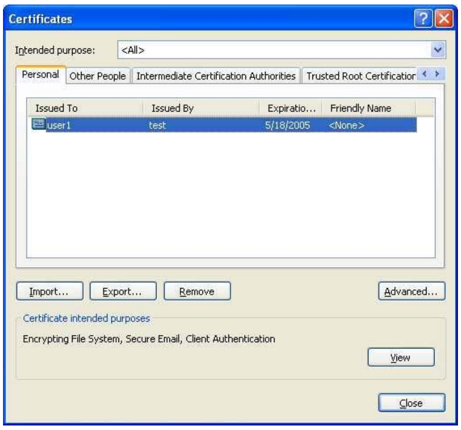
Chapter 13 **To confirm whether you have received your certificate, go to your web browser and select** Internet Options... **from your** Tools **pull down menu.**



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

Chapter 14 **Go to the** Content **tab and click on the** Certificates... **button. Notice that your username is in the listing. This shows that the certificate has been issued to you.**



Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
user1	test	5/18/2005	<None>

Certificate intended purposes

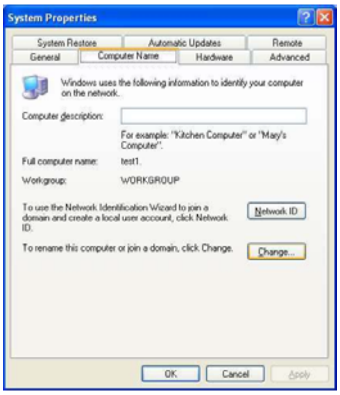
Encrypting File System, Secure Email, Client Authentication

AIII.4 Becoming a domain member

Next, you need to add your username in the domain so that you can communicate with the access point connected to your server.

1. From the **My Computer** icon on your desktop, right click and go to **Properties**.

Chapter 15 Go to the Computer Name **tab and select** Change… **button as shown in the screen on the right.**



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: test1.

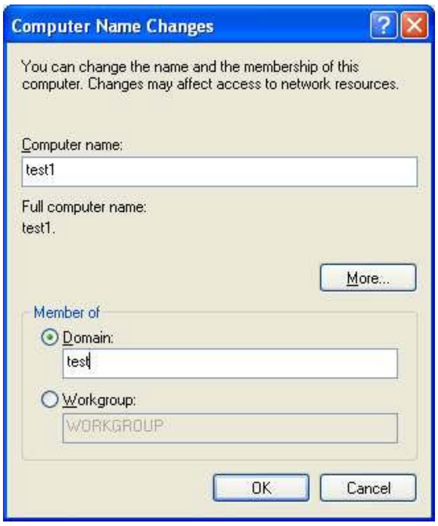
Workgroup: WORKGROUP

To use the Network Identification Wizard to join a domain and create a local user account, click Network ID.

To rename this computer or join a domain, click Change.

Chapter 16 From the Member of **section, select the** Domain: **radio button and enter the name of your domain. In**

this example, we are using *test* as the domain name.



Computer Name Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: test1

Full computer name:
test1.

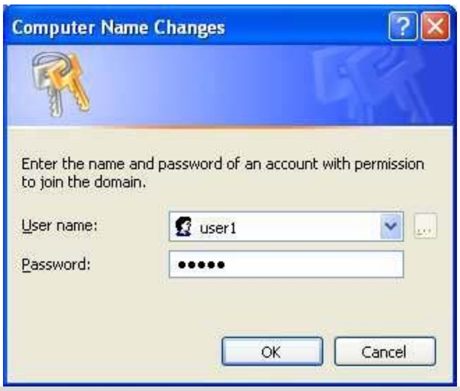
Member of

● Domain: test

○ Workgroup: WORKGROUP

Chapter 17 **Next, you need to enter your username and password again for verification. Please note that your system administrator provides this information.**

Chapter 18 **Click on the** OK **button to proceed.**



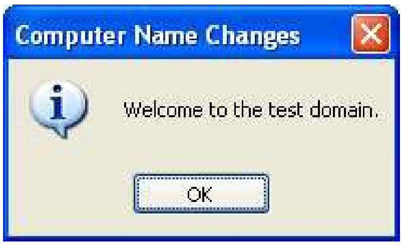
Computer Name Changes

Enter the name and password of an account with permission to join the domain.

User name: user1

Password: •••••

Chapter 19 When done, a message will appear as shown below. You may need to restart your computer for the changes to take effect.



Computer Name Changes

Welcome to the test domain.

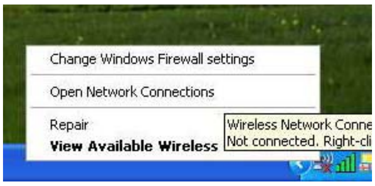
Appendix IV Wireless Zero Configuration Utility

If your computer is running under the Windows XP operating system, you can opt to configure the **Wireless Network Connection** from your Windows XP operating system, instead of the Atheros Utility. You need to exit from the Atheros Utility before accessing to Windows XP's Wireless Zero Configuration Utility.

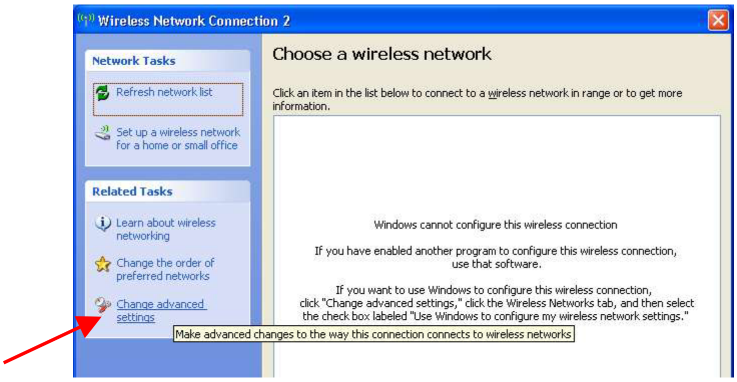
AIV.1 Enable Wireless Zero Configuration Utility

To set Wireless Zero Configuration on Windows XP, take the following steps:

1. From the system tray, right click on the Wireless Network icon and select **View Available Wireless Networks** option.



2. Click on the **Change advanced settings** option on the left-hand column.


Wireless Network Connection 2
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

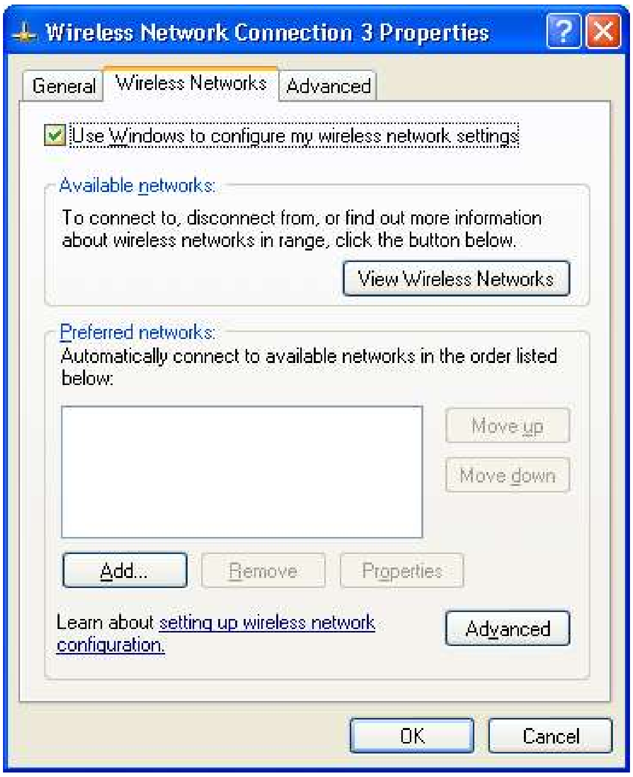
Windows cannot configure this wireless connection

If you have enabled another program to configure this wireless connection, use that software.

If you want to use Windows to configure this wireless connection, click "Change advanced settings," click the Wireless Networks tab, and then select the check box labeled "Use Windows to configure my wireless network settings."

Make advanced changes to the way this connection connects to wireless networks

Chapter 20 Select the check box Use Windows to configure my wireless network settings **to activate Wireless Zero Configuration Utility.**



Wireless Network Connection 3 Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to, disconnect from, or find out more information about wireless networks in range, click the button below.

Preferred networks:

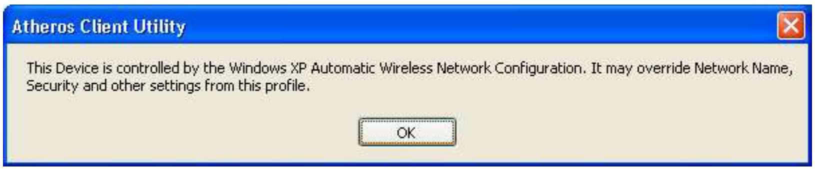
Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

When this check box is selected, Windows XP takes control of these settings for all configuration profiles:

- SSID
- Security Keys
- Ad-hoc settings

When the Wireless Zero Configuration Utility is in use, a pop-up message is displayed on the Utility when you attempt to create or edit a configuration profile from the **Profile Management** tab of the utility.



Atheros Client Utility

This Device is controlled by the Windows XP Automatic Wireless Network Configuration. It may override Network Name, Security and other settings from this profile.

CAUTION
If you activate BOTH (not recommended) the Wireless Zero Configuration Utility and the Atheros Utility simultaneously, the Profile setting configured by the Atheros Utility will be overridden by those of the Wireless Zero Configuration Utility.

AIV.2 Disable Wireless Zero Configuration Utility

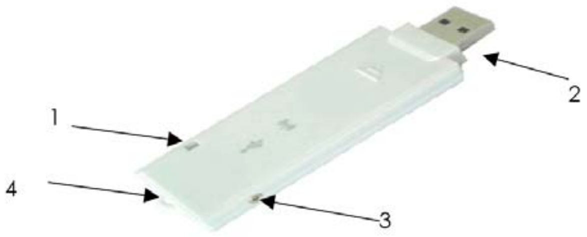
To turn Wireless Zero Configuration Utility off on Windows XP,

1. Open the **Wireless Zero Configuration** Properties dialog box.

Chapter 21 **Clear the check box** Use Windows to configure my wireless network **settings.**

Chapter 22 When this check box is cleared, all profile settings will be controlled by the USB adapter's utility.

Appendix V Panel Views and Descriptions



	Components	Indications & Descriptions	
1	Power	Green	Indicates that power is being supplied to the USB adapter.
2	USB Connector	Connect this end to the USB port of your PC/notebook.	
3	MC Connector (Version MC)	Connect the testing line to the MC connector.	
4	Hook	As a strap holder to prevent the USB adapter form being lost or carelessly dropped.	

Appendix VI Technical Specifications

Network Protocol, Standards and Electrica Emissions	
Industry Standards	• IEEE 802.11b/g • IEEE 802.11b/g/A (Version AG) • USB 2.0
Performance	
Frequency Band **IEEE 802.11g:** **IEEE 802.11b:** **IEEE 802.11a (Version AG):**	2.400 ~ 2.4835GHz (US, Canada) 5.15-5.35GHz;5.725-5.85GHz
Data Rates (with automatic fallback)	108Mbps, 54Mbps, 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 11Mbps, 9Mbps, 6Mbps, 5.5Mbps, 2Mbps, 1Mbps
Modulation	• BPSK (Binary Phase Shift Keying) • QPSK (Quadrature Phase Shift Keying) • CCK (Complementary Code Keying) • 16 QAM, 64 QAM (Quadrature Amplitude Modulation)
Radio Technology	• DSSS (Direct Sequence Spread Spectrum) • OFDM(Orthogonal Frequency Division Multiplexing)
Drivers Operating system Supported	Windows XP/2000
Media Access Protocol	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
RF Output Power	15 dBm (typical)

Receiver Sensitivity	-95 dBm at 1Mbps (typical) -92 dBm at 6Mbps (typical) -90 dBm at 11Mbps (typical) -73 dBm at 54Mbps (typical)
Host Interface	USB 2.0
Security	• 64/128/152-bit WEP encryption • IEEE 802.1x supports – EAP-TLS,EAP- TTLS, PEAP-GTC, PEAP_MSCHAP V2, LEAP • WPA, WPA-PSK

Physical and Environment	
Environmental Requirements **Operating temperature:** **Storage temperature:** **Operating humidity:** **Non-operating humidity:**	 0°C to 55°C -20°C to 70°C 10% to 70% RH 5% to 90% RH
Power Consumption	5V DC, 500mA max
Physical Dimensions	87mm x 26.6mm x 7.7mm