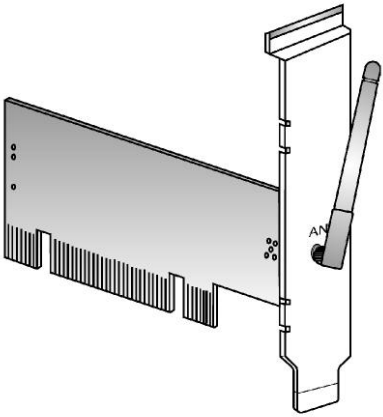
Wireless PCI Network Adapter

networks@work

USER'S MANUAL



COMPEX *iWave*Port SERIES

WLP54G 3C
WLP54AG 3C
WLP54G 3B
WLP54G 6C (RoHS-compliant)
WLP54AG 6C (RoHS-compliant)
WLP54G 6B (RoHS-compliant)

Manual Number: U-0539-V1.6C

Trademark Information

Compex®, ReadyLINK® and MicroHub® are registered trademarks of Compex, Inc. Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. NetWare is the registered trademark of Novell Inc. All other brand and product names are trademarks or registered trademarks of their respective owners.

Manual Revision by Daniel
Manual Number: U-0539-V1.6C Version 1.6, December 2006

Disclaimer

Compex, Inc. provides this manual without warranty of any kind, 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

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-G PCI Network Adapter, Compex WLP54 is a licensed product of Compex Systems Pte Ltd. This document contains instructions for installing, configuring and using Compex WLP54. 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 WLP54.

Drivers & Utilities

This manual is written based on Drivers version 5.0.0.108; Utility version 5.0.0.272

Conventions

In this document, special conventions are used to help and present the information clearly. The Compex Wireless PCI Network Adapter is often referred to as Compex WLP54 in this document. Below is a list of conventions used throughout.

NOTE
This section will consist of important features or instructions

CAUTION
This section concerns risk of injury, system damage or loss of data

WARNING
This section concerns risk of severe injury

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

Thank you for purchasing this Wireless 108Mbps PCI Network Adapter. Data security is facilitated with WPA, IEEE 802.1x Authentication and 64-bit, 128-bit and 152-bit WEP (Wired Equivalent Privacy). They support easy Plug and Play installation and combine simplicity, data privacy, and reliability for your wireless network.

1.2 Features and Benefits

- **Interoperability**
  The PCI adapter is able to inter-operate with other wireless network devices using different standards. In addition, the dynamic rate shifting capability allows automatic selection of optimum connection speed to any wireless LAN devices or access points.

- **Easy Monitoring**
  The client manager (Atheros Wireless Utility) comes with a built-in monitoring & diagnostic software that detects wireless sites or access points, providing valuable information like signal strength and channels used. It also allows testing of your wireless card hardware, software driver and firmware integrity through the card diagnostic option for easier troubleshooting of the network adapter.

- **Profile Management**
  The client manager allows the user to configure different profiles, allowing the wireless card to operate in different wireless networks by simply changing to the relevant profile.

- **Networking Modes**
  The network adapter supports two types of networking modes: infrastructure mode and ad-hoc mode. In infrastructure mode, clients communicate with each other through an access point. Whereas in ad-hoc mode, clients directly communicate with one another without the need for an access point.

Chapter 2 Basic Setup

This chapter outlines the basic requirement for the installation and configuration of the network adapter.

This network adapter is a plug-and-play device. You can plug it into the PCI slot of your PC for auto-detection.

2.1 Hardware Installation

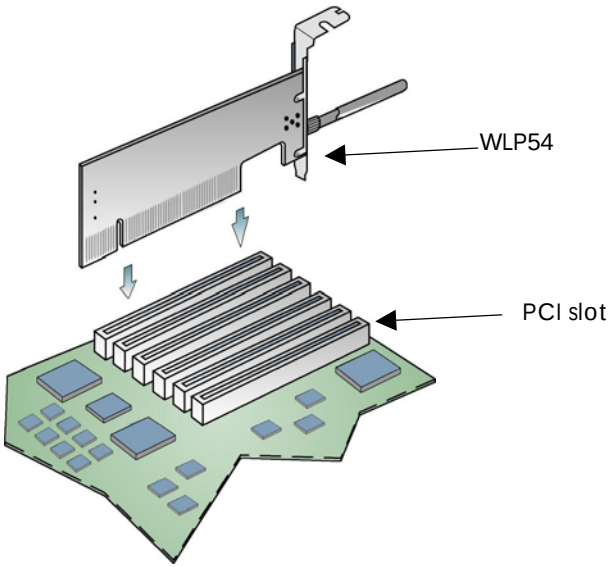
1. Turn off your PC and switch off the power from the main power supply.

2. Remove the back cover of the PC.

3. Then insert the network adapter into your PCI slot as shown below. Ensure that the network adapter is properly seated into the slot.

4. Replace the back cover.

5. Power on your PC.

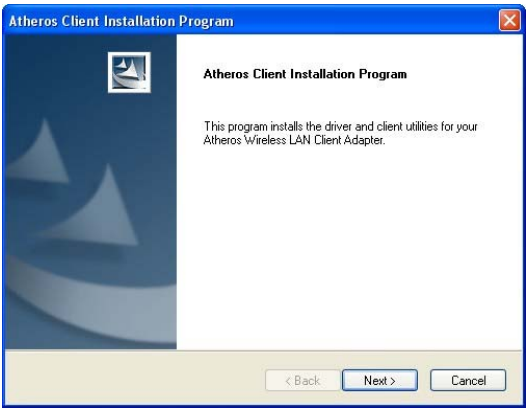


2.2 Driver & Utility Installation

1. Insert the Product CD into your computer CD-ROM drive.

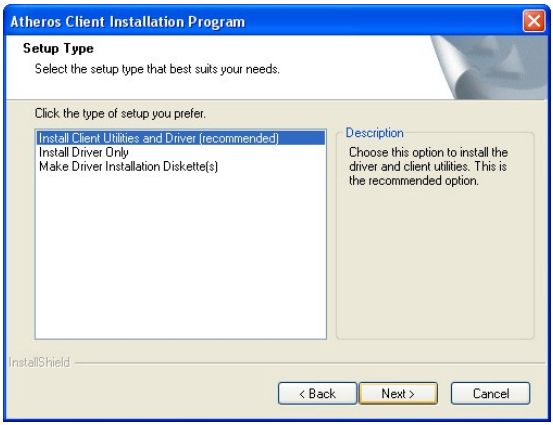
2. Click on **Driver & Utility** section and the system will run the *setup.exe* automatically.

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



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:



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

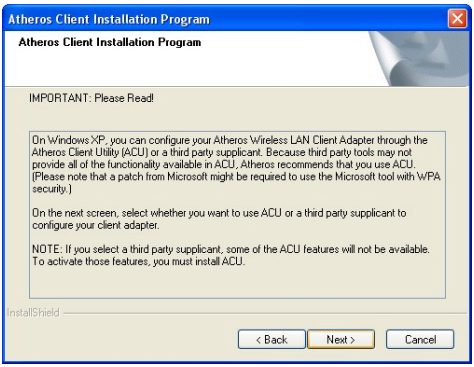
Install Driver Only option (For Windows XP user only)
Select this option if you are going to use the Wireless Zero Configuration Utility to configure your PCI adapter. Note that only Windows XP comes with the Wireless Zero Configuration Utility.

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

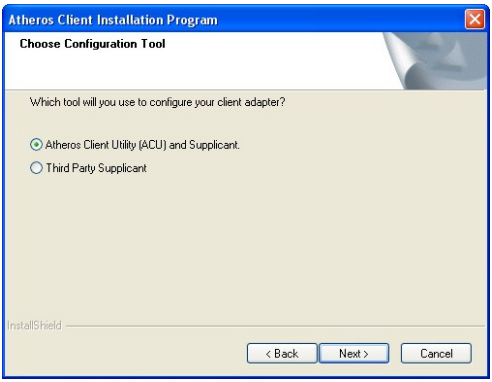
6. Click on the **Next>** button and follow the instructions stated on the screen.

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.



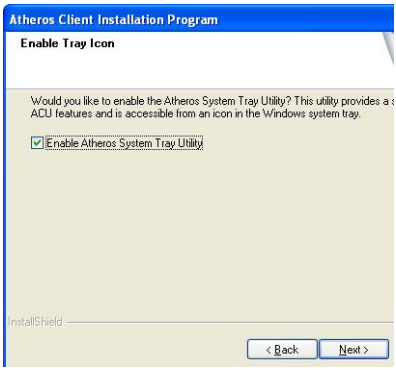
8. Select your choice of tool to assist you in configuring your USB adapter. Click on the **Next>** button to proceed.



Atheros Client Utility (ACU) and Supplicant option
Select this option to install your network adapter. (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 utility; configuration using the utility will not be allowed.
If you have selected **Third Party Supplicant** configuration tool, a screen similar to that below will appear, prompting you to enable/disable the system tray icon.

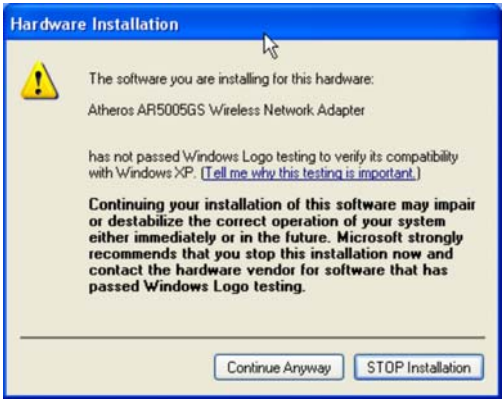
9. Click on the checkbox besides **Enable Atheros System Tray Utility** and click on the **Next>** button to proceed.



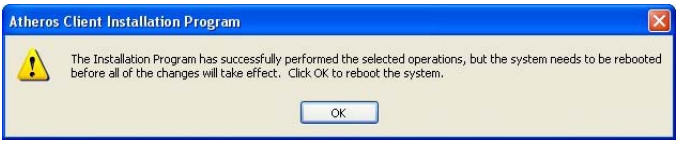
10. The screen below appears to inform you that the driver will be automatically installed if you have already inserted your client adapter into the PCI slot of your computer.

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

11. If a similar screen similar to the one shown below appears, click on the **Continue Anyway** button to continue the installation.



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



Chapter 3 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.

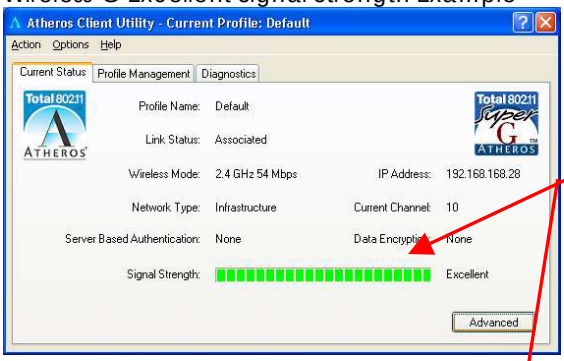
Exit

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

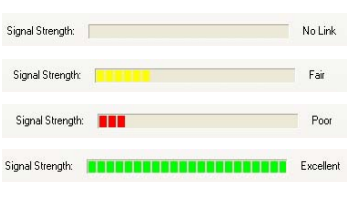
Open Atheros Client Utility…

Launch the Client Utility.

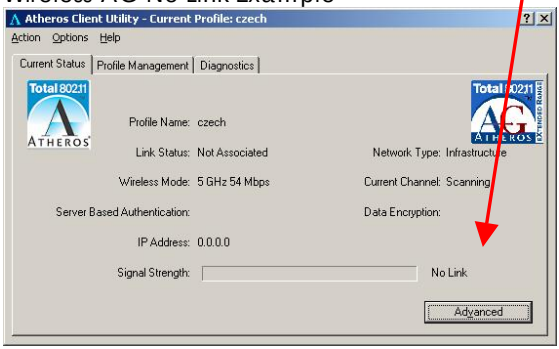
Wireless-G Excellent Signal Strength Example



Different signal strength indications

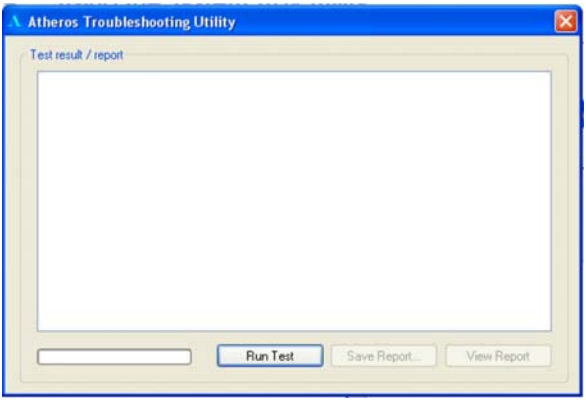


Wireless-AG No Link Example



Troubleshooting

This option allows you to identify and resolve the wireless adapter configuration and association problems only when the network adapter is operating in the infrastructure mode.



Click on **Run Test**. The button display then changes to **Start Test** and at the same time, the test messages are displayed. To stop the incoming test messages, click **Stop Test**.

To save the report to your desired directory on disk, click **Save Report**.

To view the detailed summary of the configuration tests, click **View Report**.

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.

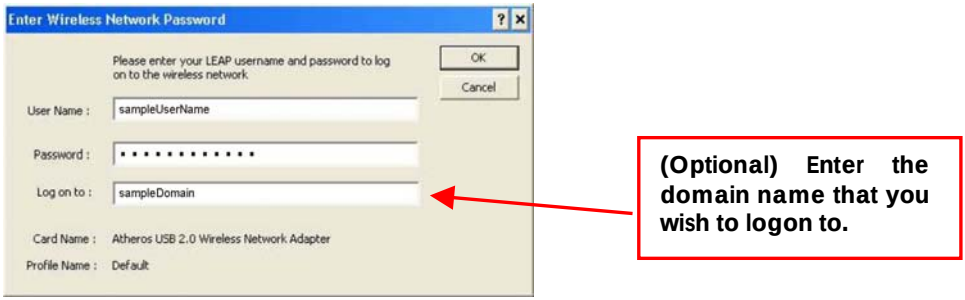
Disable/Enable Radio

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.

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

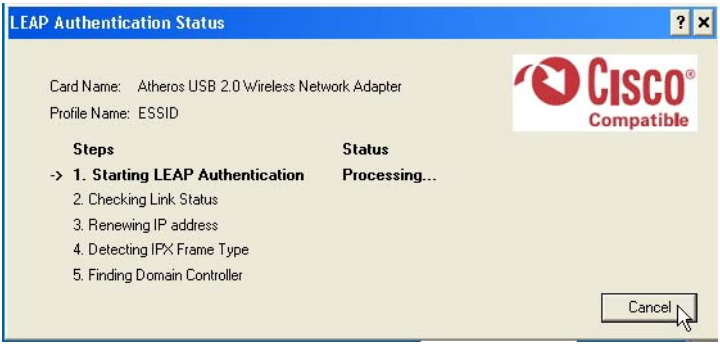
Manual LEAP Login

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.



Reauthenticate

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



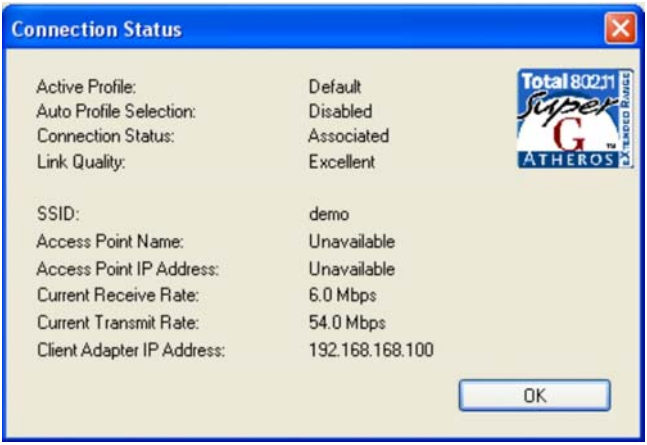
Select Profile

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 PCI adapter.

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



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 network 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).
Current Receive Rate	Displays the data rate at which the wireless adapter is currently receiving from the wireless network.
Current Transmit Rate	Displays the data rate at which the wireless adapter is currently transmitting to the wireless network.
Link Speed	States the speed of the link connection.
Client Adapter IP Address	Displays the IP address of the wireless adapter.

Chapter 4 Utility Features

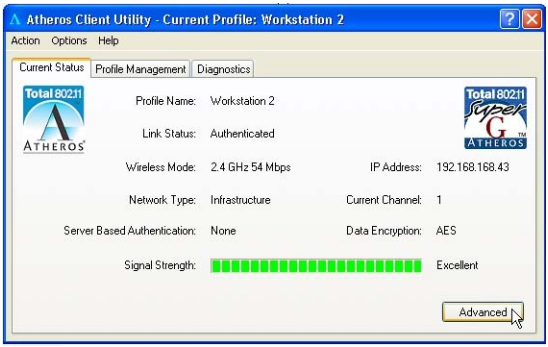
This chapter shows you how to make use of the utility to view the status of your wireless connection, to change your settings and also to monitor your wireless performance via the network statistics.

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

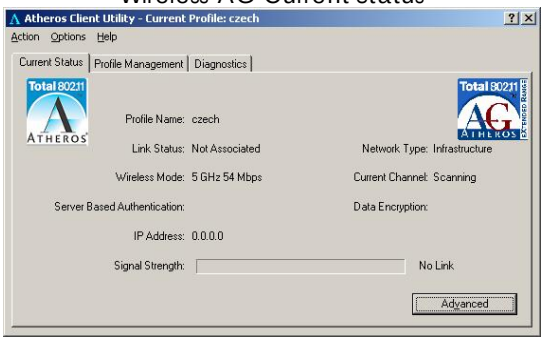
4.1 Current Status Tab

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

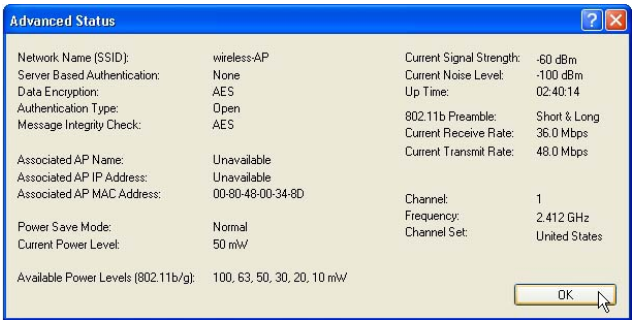
Wireless-G Current Status



Wireless-AG Current Status



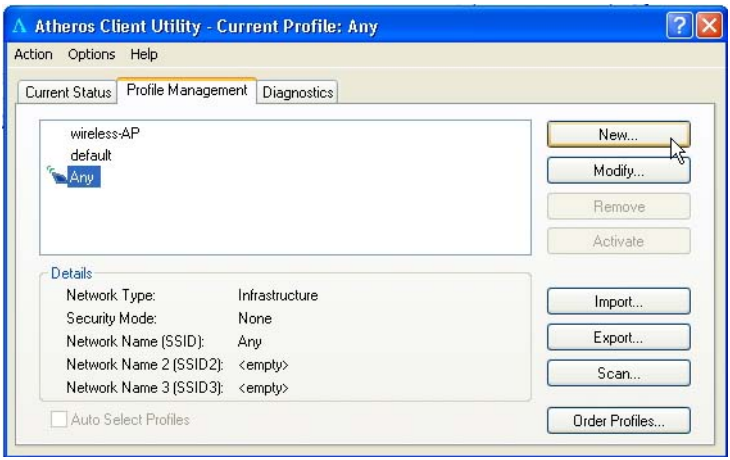
Upon clicking on the **Advanced** button, you will be able to view all information on the respective profile, e.g. the types of encryption and authentication, the signal strength, the MAC address of the connected AP (if you are in Infrastructure mode), etc.



4.2 Profile Management Tab

Selecting this tab displays the profiles and the details.

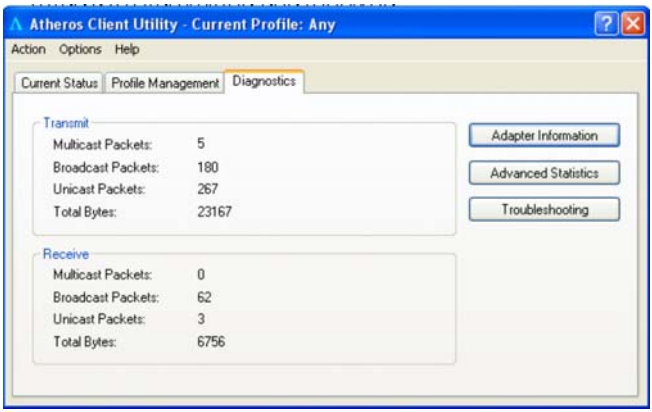
You only need to create a profile if you have more than one wireless connection.



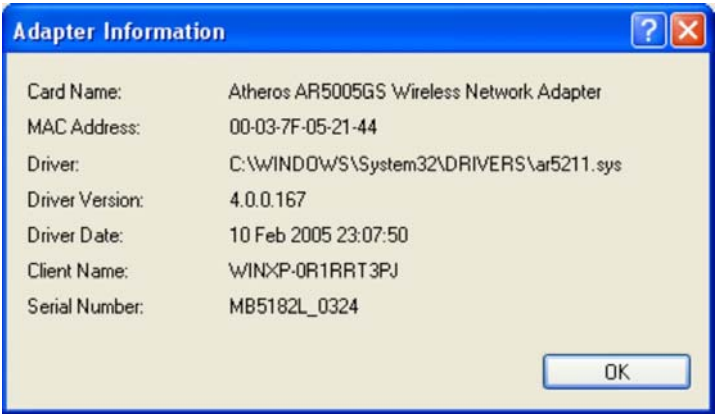
4.3 Diagnostics Tab

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

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



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



Card Name The name of the network adapter

MAC Address The MAC address of the network adapter

Driver The driver name and path

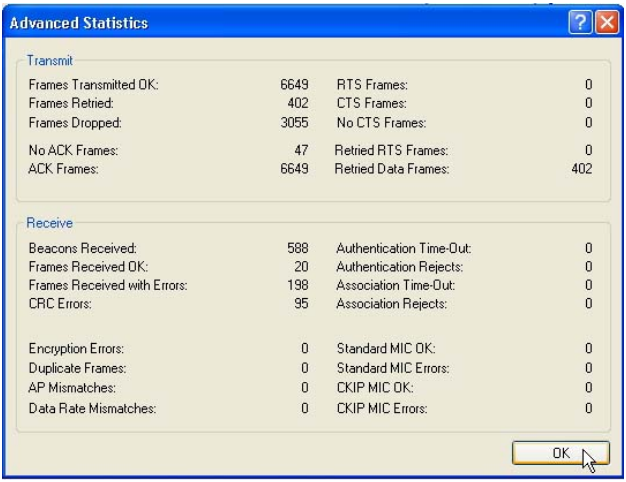
Driver version The version of the driver

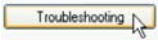
Driver date The creation date of the driver

Client Name The name of the client computer

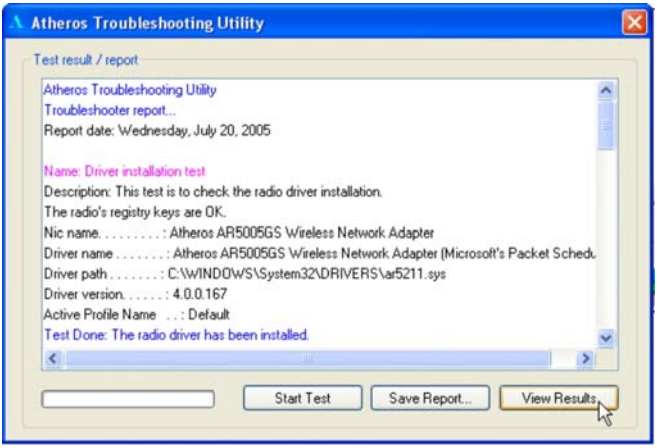
Serial Number The serial number of the network adapter

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





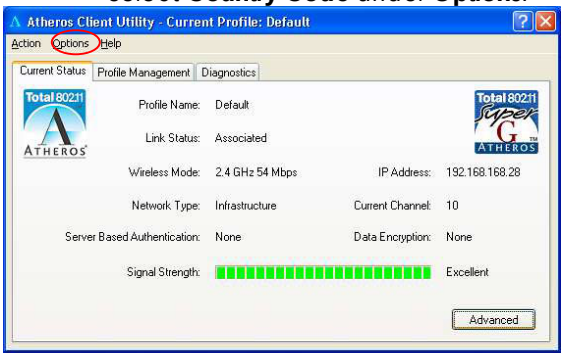
This button allows you to run the diagnostic test, save the test report and view the test results on the wireless adapter configuration and association.



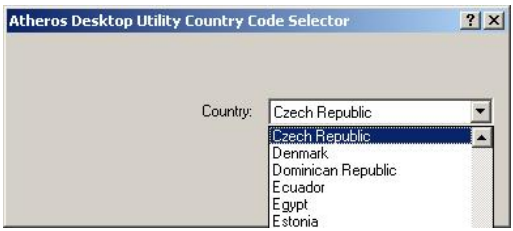
4.4 Country Code Selector

The Country Code Selector sets the wireless configuration certified for the wireless regulatory domain by country. Different wireless regulatory domains have different certifications and this feature ensures that the wireless operation has valid certification.

Select **Country Code** under **Options**.



In **Atheros Desktop Utility Country Code Selector**, select the **Country** (Example: Czech Republic), and click **OK**.

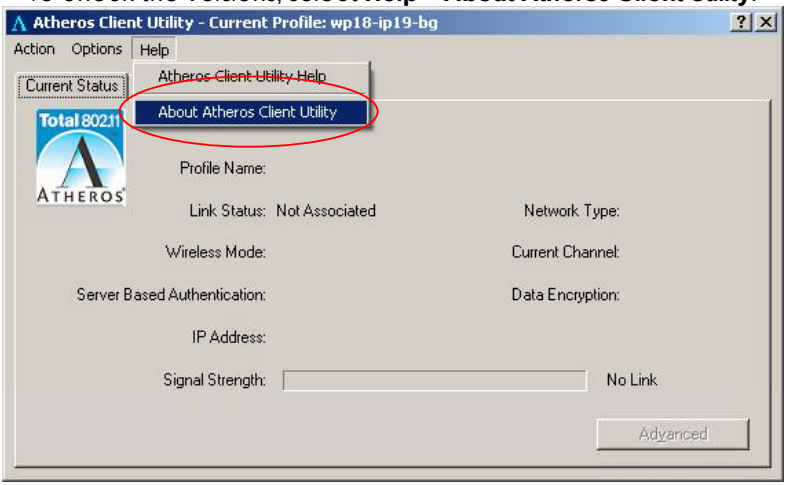


NOTE

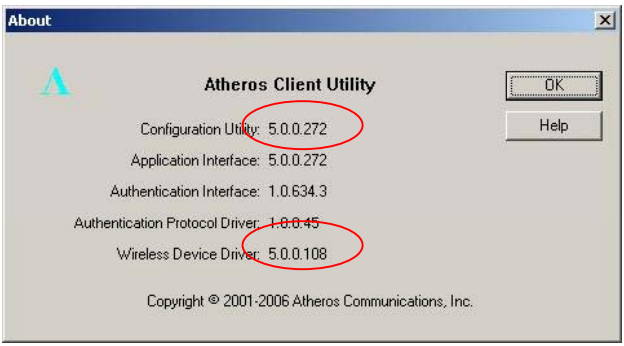
Country Code Selector is only available for Driver Version 5.0.0.108 and Utility Version 5.0.0.272 which is also included on the Product CD.

The default Driver and Utility does not feature the **Country Code Selector**.

To check the versions, select **Help – About Atheros Client Utility**.



About page displays Driver Version and Utility Version.



Chapter 5 Utility Configuration

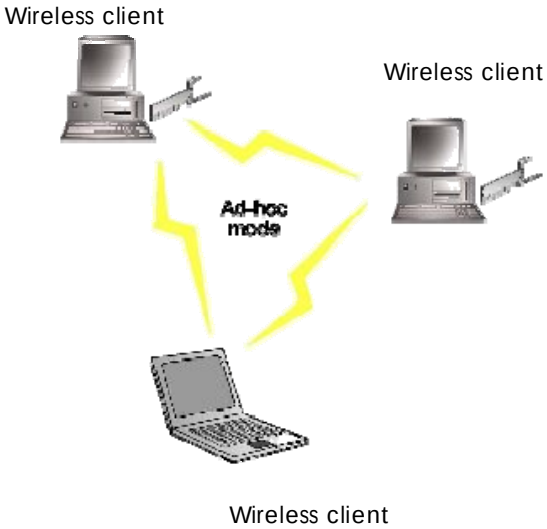
This chapter will elaborate on the Client Manager configuration of the network adapter using some simple examples.

This network adapter can be configured for 2 types of wireless architectures – Ad-hoc and Infrastructure. The different operational modes are shown in the following diagrams to allow you to easily understand how to configure your network adapter.

5.1 Ad-hoc Mode

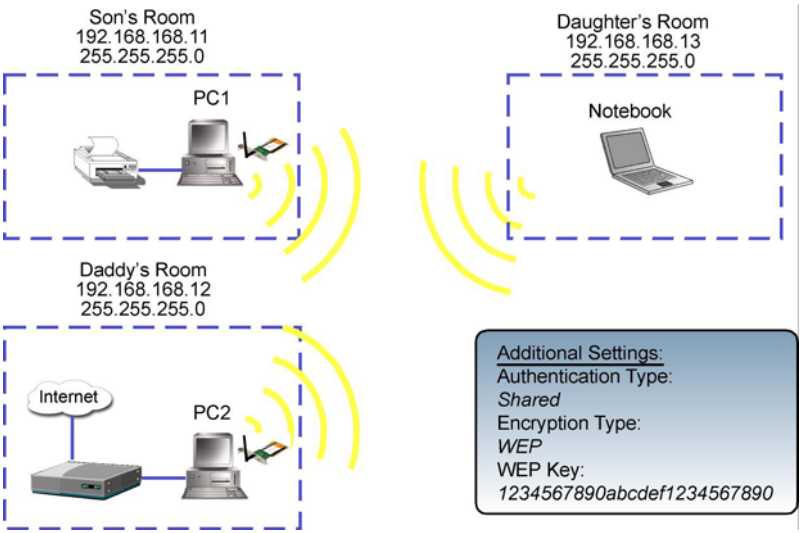
In an Ad-hoc architecture, the wireless clients communicate directly with one another. No access point exists in such a wireless LAN configuration. Each wireless client can directly transfer data packets with each other.

Usually, the operation would be automatically detected and configured between the peers. However, if you wish to, you can also set a common channel for all Ad-hoc clients to use. This will be illustrated in the following section.



5.2 When to set up Ad-hoc Mode

Ad-hoc mode is also referred to as peer-to-peer mode or as Independent Basic Service Set (IBSS). Ad-hoc mode is useful when wireless devices are within range of each other and can discover and communicate among themselves without an AP. The figure below illustrates a family using Ad-hoc mode to share files and devices directly with one another.



For PC1

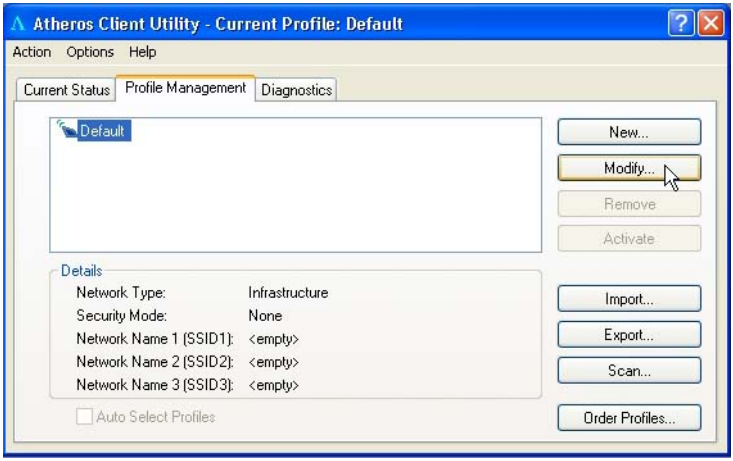
1. Set your PC1's IP address to *192.168.168.11*; subnet mask to *255.255.255.0* and activate your Utility.

NOTE
Ad-hoc mode works best when the network uses static IP addressing. The IP addresses of all the computers in the Ad-hoc network must be in the same subnet (e.g. 192.168.168.xxx); and the subnet mask must also be the same.

2. Proceed to the **Profile Management** tab.

   Once you have installed the utility, the system will automatically create a default profile.

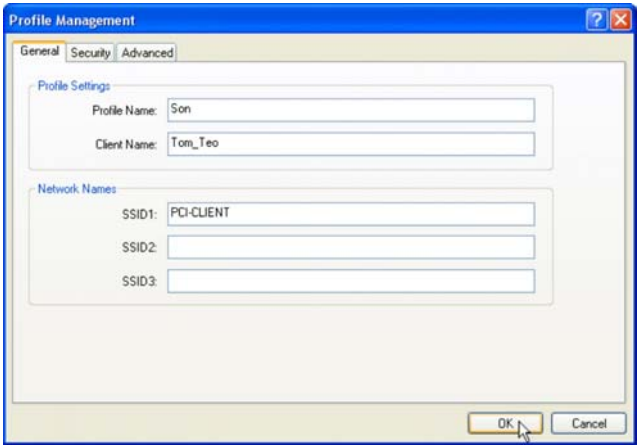
   If you wish to create a new profile, click on **New** button. If not, simply click on **Modify** button to change the default settings.



3. Enter your own profile name, e.g. *son*. The **Client name** refers to the name that is registered to your PC.

4. Set the SSID to *PCI-CLIENT* and click on the **OK** button to update the changes.

   Please ensure that all the clients in your Ad-hoc network use the same SSID, which in our example is set to *PCI-CLIENT*.



5. Next, proceed to **Advanced** tab. Set your **Network Type** to *AdHoc* and **802.11b Preamble** to *Short &Long*.

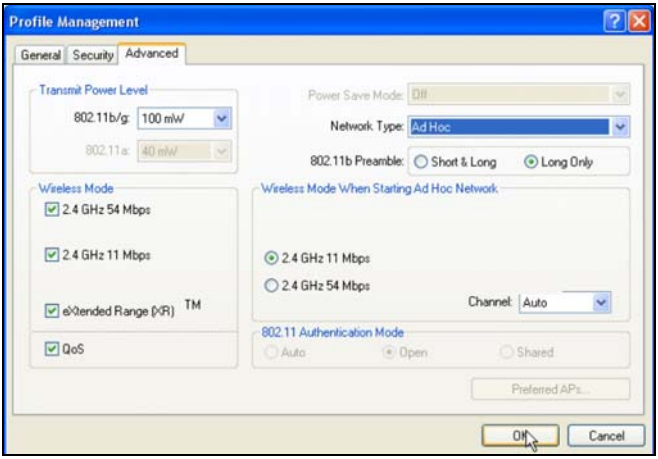
6. You may leave the **Transmit Power Level** at their default values.

7. In the **Wireless Mode** section, check and confirm whether all options are ticked.

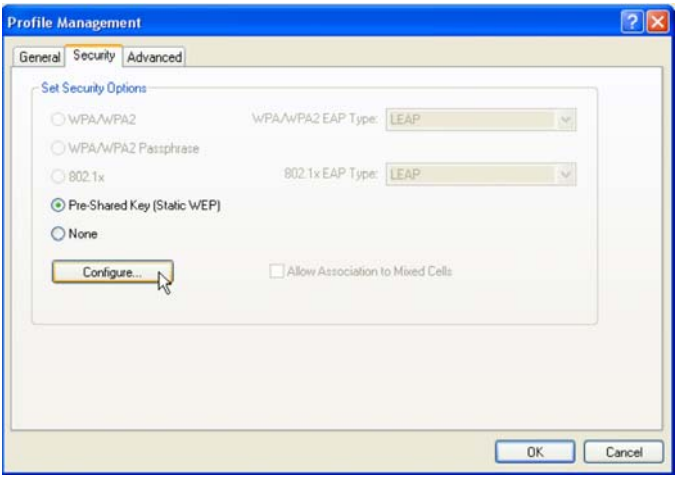
8. Next, proceed to **Wireless Mode when starting Ad-hoc Network** section. The channels available depend on the regulatory domain. If no other wireless adapters are found matching the ad hoc mode, this selection specifies the channel with which the adapter starts a new ad hoc network. Please note that the wireless adapter must match the wireless mode and channel of the other wireless clients it associates to.

9. Set the **Channel** to *Auto* to let the network adapter automatically detect the channel to use.

However, if you wish to set a specific channel, you must ensure that all the wireless clients are in the same channel to enable them to communicate with one another.

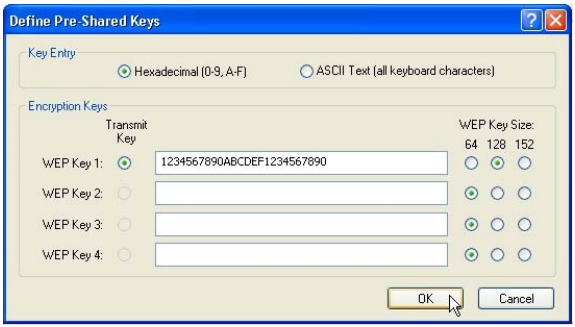


10. Proceed to the **Security** tab. Select **Pre-Shared Key (Static WEP)** option and click on the **Configure...** button.

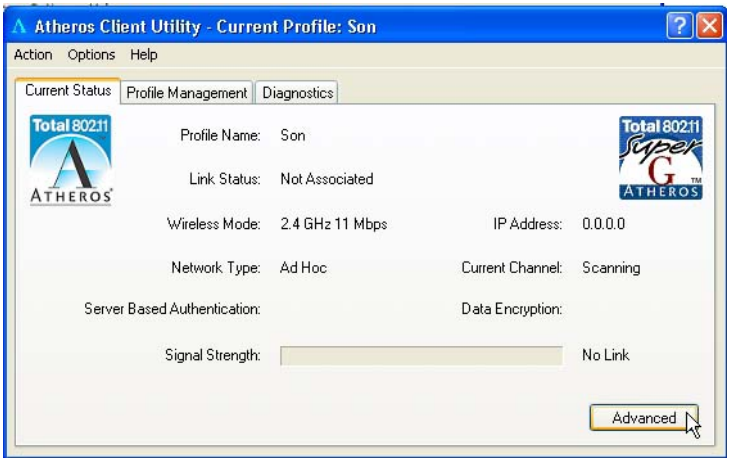


11. Click on the radio button for **WEP Key Size:** *128*, type in, e.g. *1234567890abcdef1234567890* and click on the **OK** button to update the changes.

    Note that the length of the WEP key depends on the type of encryption key that you have selected:
    For 64- bit WEP: 10 hexadecimal or 5 ASCII Text
    For 128-bit WEP: 26 hexadecimal or 13 ASCII Text
    For 152-bit WEP: 13 hexadecimal or 16 ASCII Text



You may now go to the **Current Status** tab to check the status of the connection. Notice that if there is no connection established (Refer to Link Status), this indicates that your WLP54 has not yet detected any other wireless client with SSID set to PCI-CLIENT.



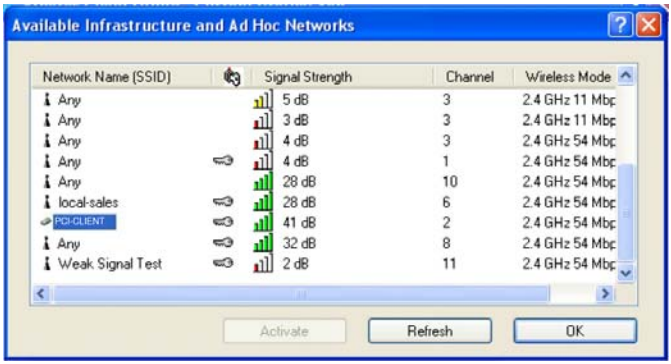
Now, we proceed to configure PC2.

For PC2

1. Set your PC's IP address to *192.168.168.12*; subnet mask to *255.255.255.0*.

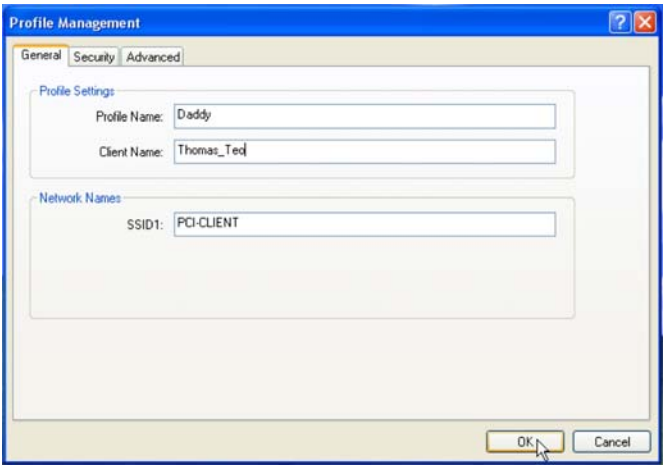
2. Go to the **Profile Management** tab and click on the **Scan** button to look for *PCI-CLIENT* (the SSID that you had previously created in PC1).

3. Once detected, highlight this profile and click on the **Activate** button.



Notice that there is a key beside the Network name (SSID). This shows that you need the encryption key to connect to this network.

Next, you can see that the **SSID** is set to the same SSID as PC1 and that **Client Name** is pre-configured to the name registered to PC2. You need to give a name to your profile, e.g. *Daddy*.

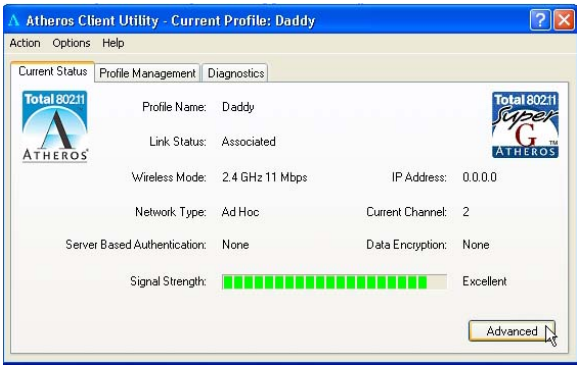


4. Next, proceed to the **Security** tab and set the same security settings as for PC1.

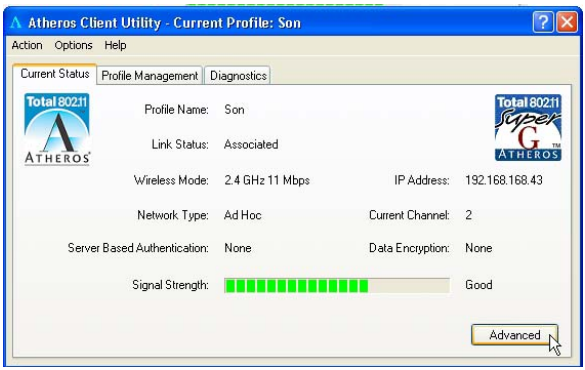
NOTE

The SSID and encryption key for PC1, PC2 and the notebook must be the same in order to communicate with one another. Also, if you are using a specific channel instead of Auto, PC1, PC2 and notebook must be set with the same channel.

5. Click on the **OK** button and go to the **Current Status** tab. Notice that once the connection has been successfully established, the link status will display <associated> and the signal strength will appear as a green bar.



If you go to view the current status from PC1, the status for **Profile:** *Son* will be updated as shown below:



Alternatively, you may also go to the MS-DOS Prompt window of each PC to ping the other PC.

1. From the **Start** menu, go to **Run...**

2. Type in *cmd* and click on the **OK** button.

From the MS-DOS Prompt window of PC2, type *ping 192.168.168.11 –t*, to ping PC1.

When this screen appears:
Pinging 192.168.168.11: bytes=32 time=2ms TTL=128
Pinging 192.168.168.11: bytes=32 time=2ms TTL=128
…….

This indicates that the connection between PC1 and PC2 has been established successfully! You can now access to one another wirelessly!

For notebook

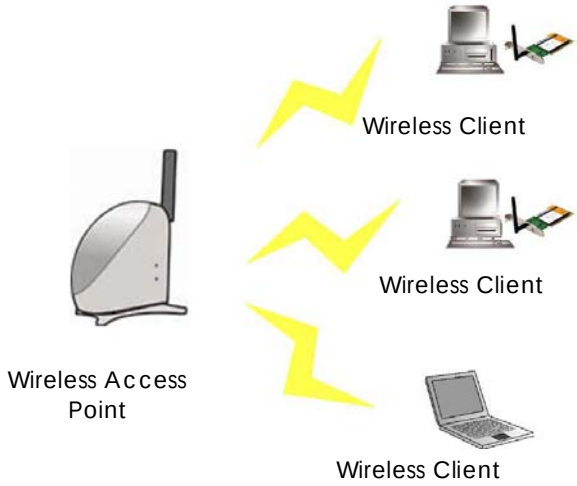
For setting up another wireless client, e.g. the notebook in the daughter's room, you may refer to the steps mentioned for configuring PC2.

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

Note:
All clients need to use the same SSID, channel, security mode and encryption key.

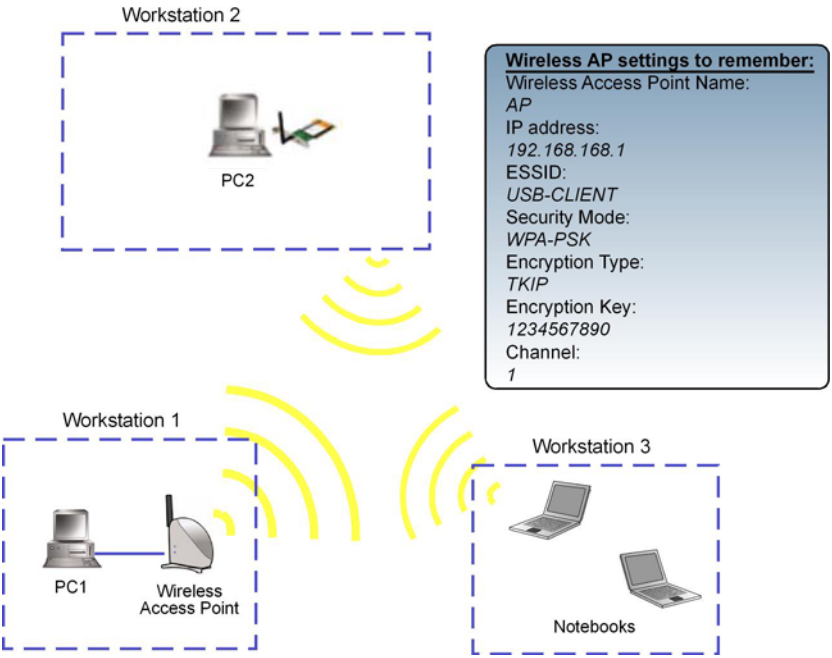
5.3 Infrastructure Mode

In infrastructure architecture, the wireless clients communicate through access points, which 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.



5.4 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.



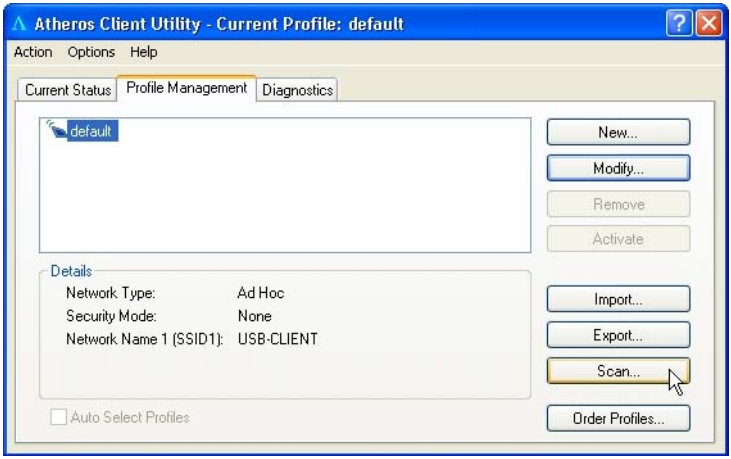
For AP

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 them. Note the wireless configuration settings of your access point as shown in the figure above.

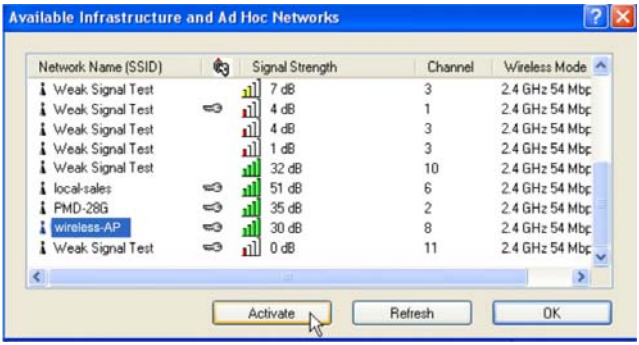
For PC 2

1. Activate your utility.

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



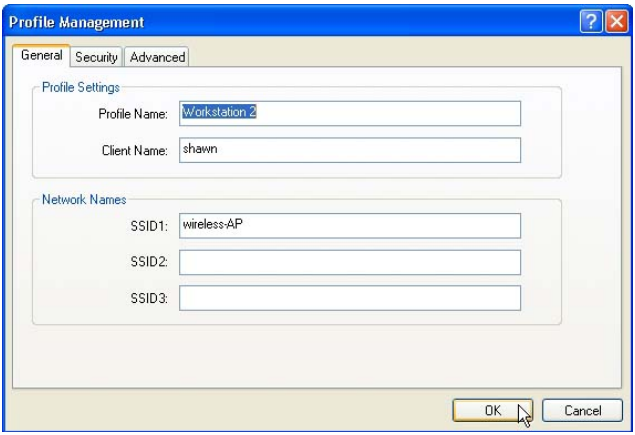
3. Click on the **Refresh** button if your system is unable to detect your wireless AP. Once found, select the **Network Name (SSID)** used by the AP**:** *wireless-AP* and click on the **Activate** button to add it to your profile list.



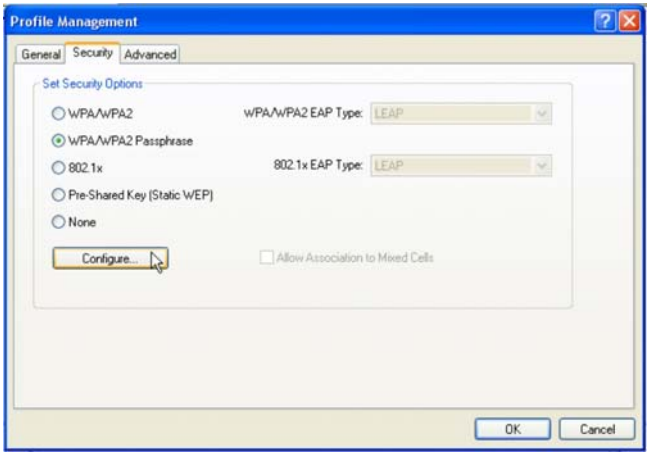
Notice that the SSID has already been pre-configured in this profile.

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.

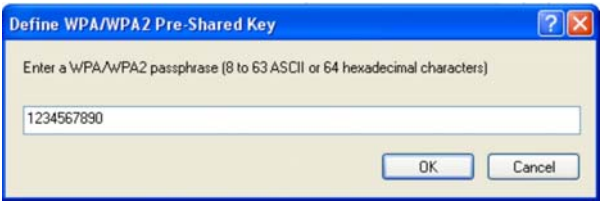


5. Next, proceed to the **Security** tab. The wireless client must use the same security mode as the AP. In our example, select **WPA Passphrase** and click on the **Configure…** button.

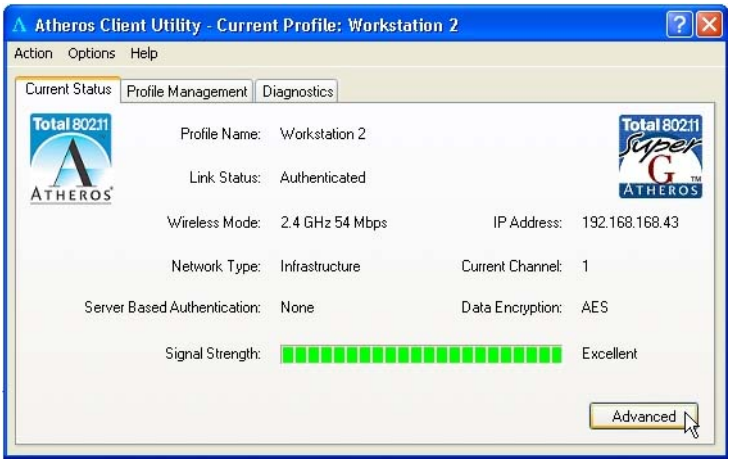


6. Enter the encryption key in the field provided. Please note that this key must be the same as the one that you had configured for your access point.

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



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



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!

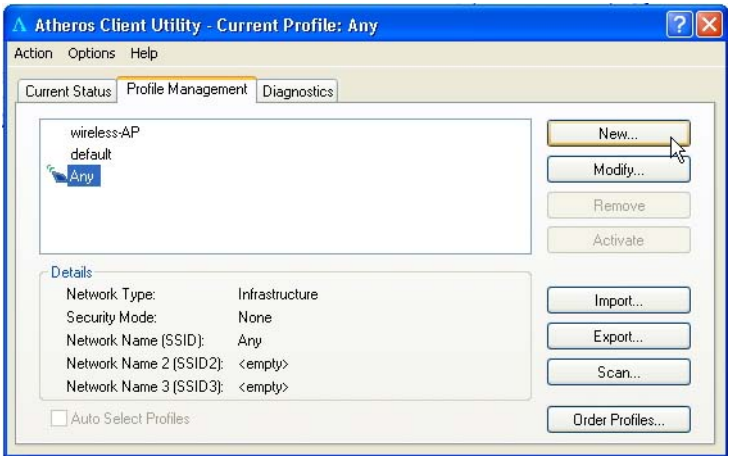
For the rest of the workstations

Refer to the steps for configuring PC2.

If your other wireless clients are not using this network adapter, you may refer to the manual of these other adapters for details on Infrastructure configuration.

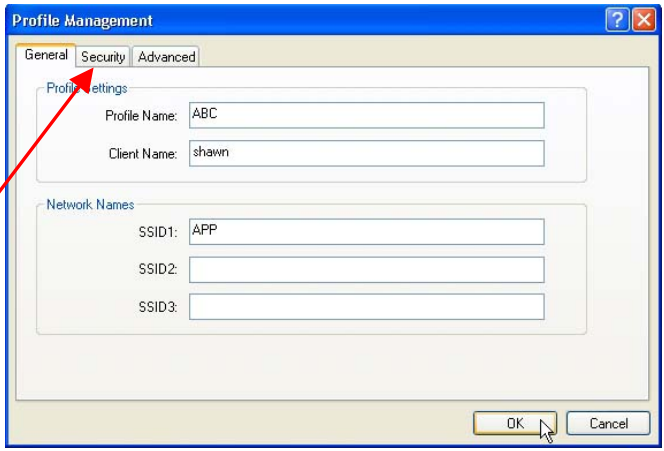
5.5 Profile Management

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



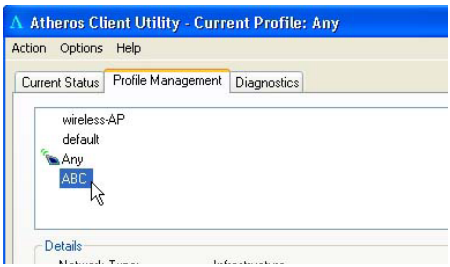
Click on **New** button to create a new profile. Enter the profile name (a unique name to identify this profile), a client name and the SSID of the wireless network to connect to. Note that the **Client name** refers to the name that is registered to your PC. You can enter up to 3 different SSIDs in 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"**

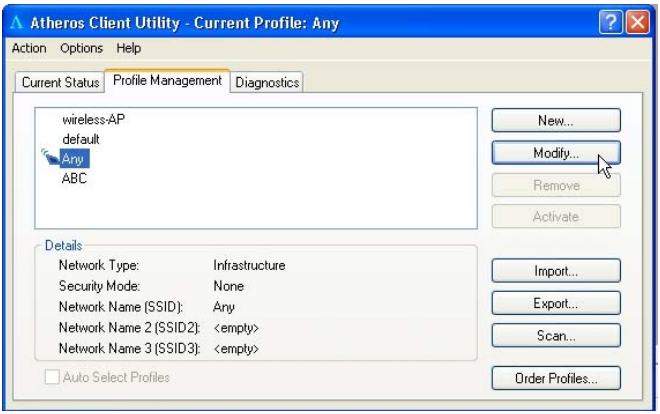


Click on the **OK** button to update the changes.

Notice that ABC has been added to the profile list.

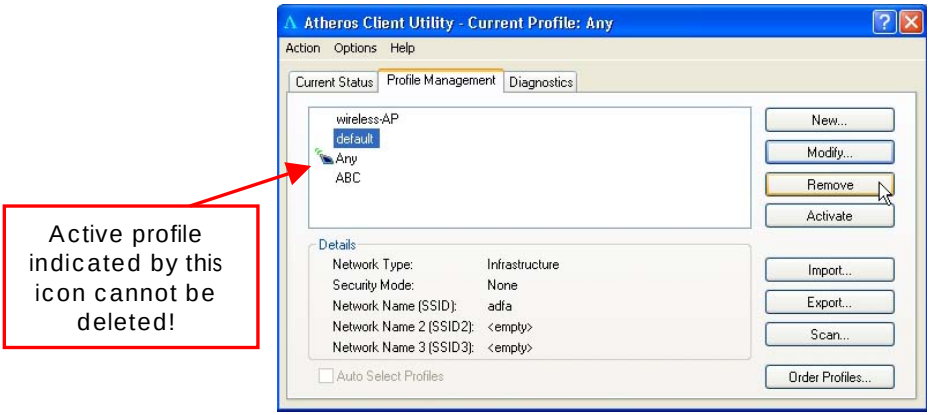


To modify an existing profile, select the profile that you wish to modify and click on this button. We are using profile: *Any* as an example.

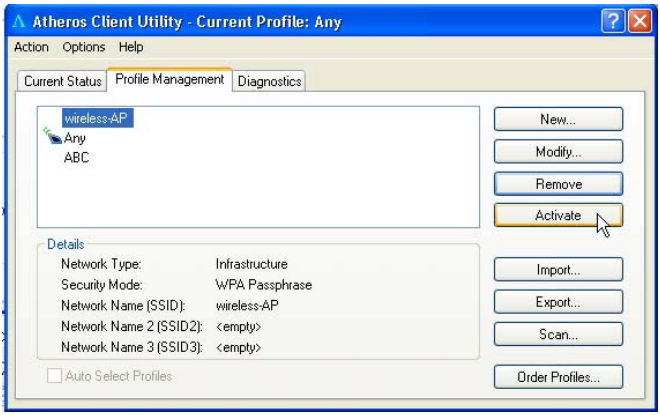


To delete an existing profile, select the particular profile that you wish to delete and click on this button. We are using profile: *default* as an example.

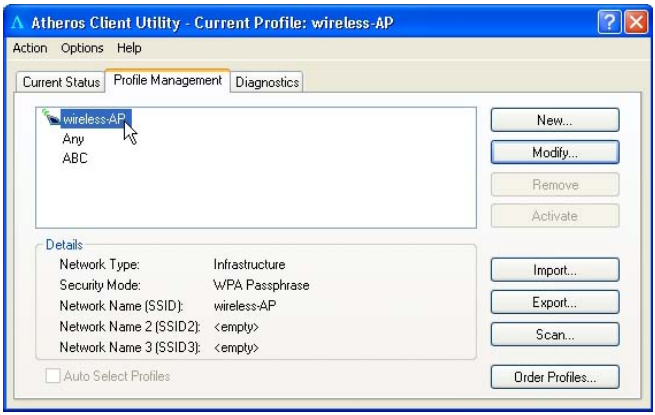
Note that the active profile (the profile that you are currently using) cannot be deleted!



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

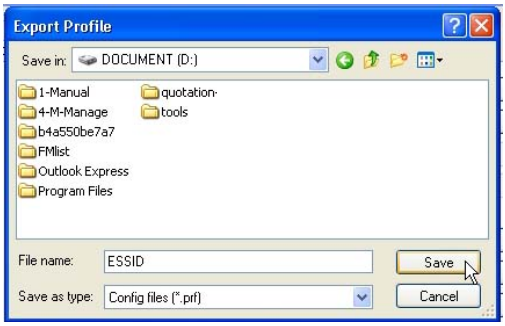


Once a profile is activated, this  icon will appear next to the profile name: *wireless-AP*.



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.

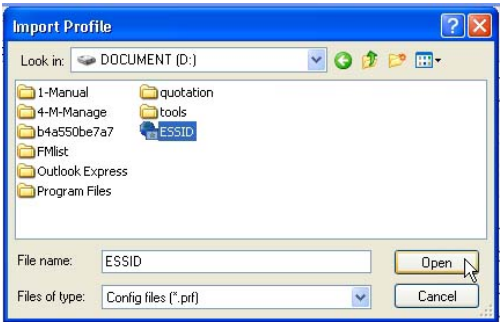
Choose the folder to save to, enter the name under which to save the profile and click on the **Save** button.



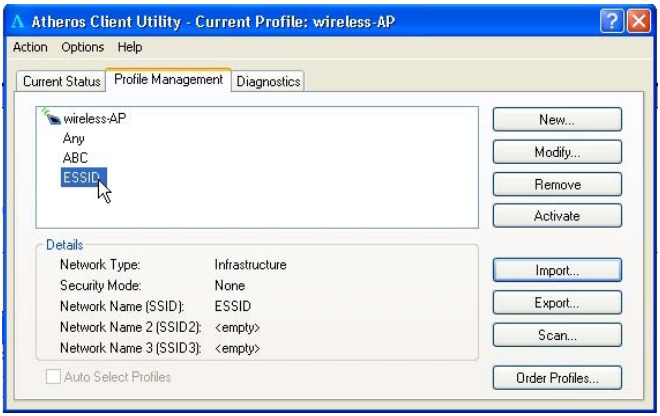
Now, your profile is saved to your selected folder.

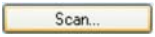
This function allows you to retrieve a saved profile from disk. We are using profile: *ESSID* as an example.

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



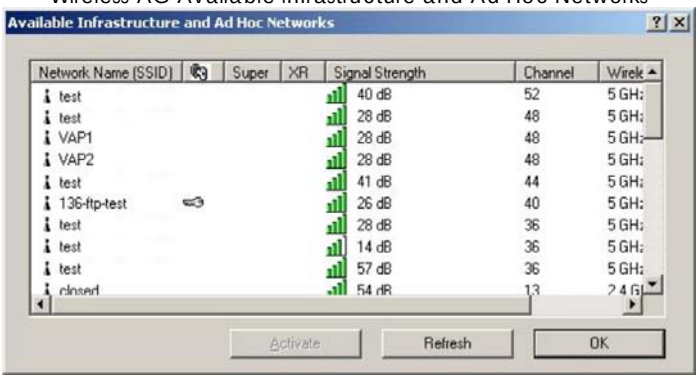
Notice that the profile: *ESSID* has been imported to the list of profiles.



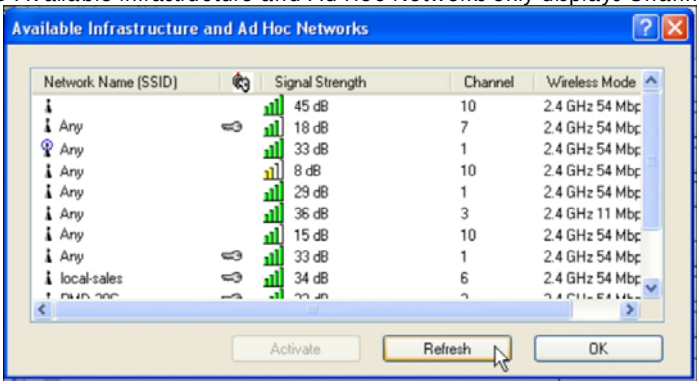


This function allows you to scan for wireless networks detected by the adapter.

Wireless-AG Available Infrastructure and Ad Hoc Networks



Wireless-G Available Infrastructure and Ad Hoc Networks only displays Channel 1 to 13.



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

 Infrastructure (AP) Network

 Connected to Infrastructure (AP) Network

 Ad-hoc Network

 Connected to Ad-hoc Network

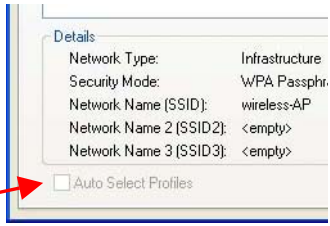
 Encryption Active

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

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

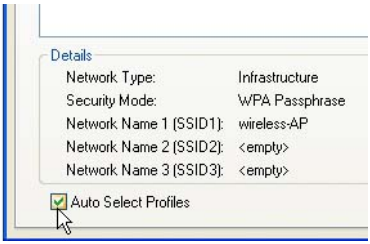
If you have created several profiles, this function allows you to establish the priority order in which the network adapter should try to connect to a WLAN. If the network adapter is unable to connect to a wireless network through the 1st profile, it will then try to connect using the 2nd profile and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

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



When auto profile selection is enabled, the network 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.



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.

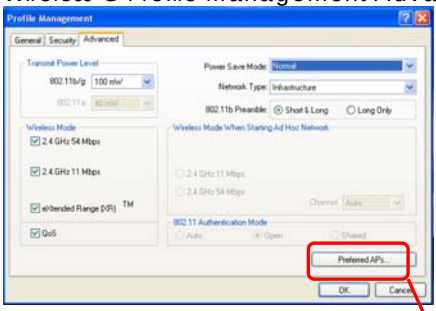
Select and click on the **Add** button to transfer another profile.

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

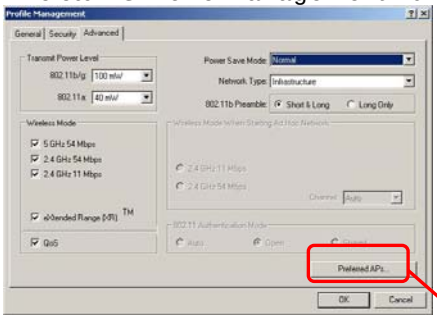
5.5.1 Advanced Tab

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

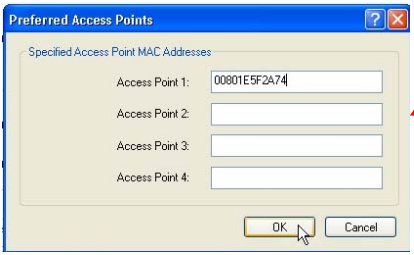
Wireless-G Profile Management Advanced



Wireless-AG Profile Management Advanced



Only applicable to Infrastructure mode.
You may key in the MAC address of at most 4 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 PCI adapter. 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 PCI 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 PCI 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 Only**
  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 54Mbps (Wireless-AG), 2.4 GHz 54 Mbps (Wireless-G), 2.4 GHz 11 Mbps (Wireless-G), Extended Range(XR) or QoS 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.

Wireless Mode when starting Ad-hoc Network (Only applicable to Ad-hoc mode)

Specifies the mode: **5GHz 54Mbps** (Wireless-AG), **2.4GHz 54Mbps** (Wireless-G), or **2.4 GHz 11Mbps** (Wireless-G), in which to start an ad hoc network if no network name is found after scanning for all available networks.

This mode also allows selection of the channel used by the wireless adapters in the Ad-hoc network. The channels available depend on the regulatory domain. If no other wireless adapters are found matching the ad hoc mode, this selection specifies the channel with which the adapter starts a new ad hoc network.

The wireless adapter must match the wireless mode and channel of the other wireless clients 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 PCI adapter to attempt authentication using shared authentication. It then switches to open authentication if shared authentication fails.

- **Open**
  Enables the PCI adapter to attempt authentication regardless of its WEP settings. It will only associate with the access point if its WEP settings match those of the access point.

- **Shared**
  Allows the adapter to authenticate and associate only if it has the same WEP settings as the access point.

Note:

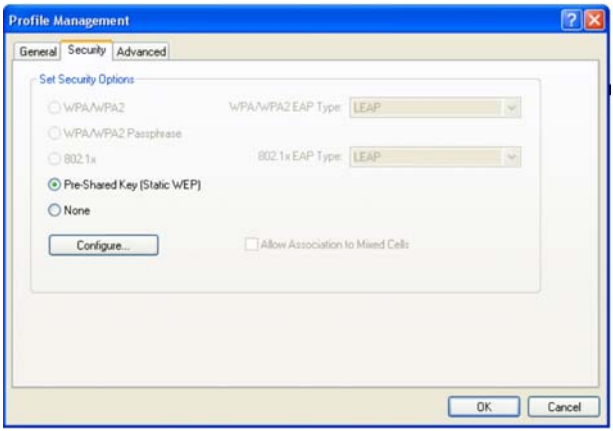
The network adapter authentication mode settings must match those of the AP it is trying to connect to for successful communication.

Chapter 6 Types of Authentication and Encryption mode

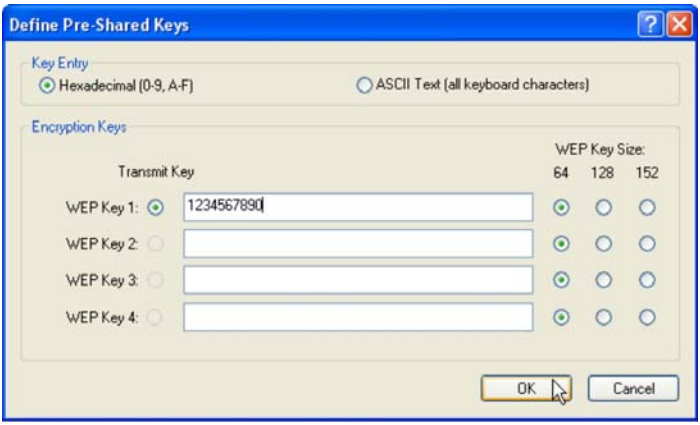
This chapter illustrates the different types of authentication and encryption that can be used in the wireless LAN.

6.1 Ad-hoc Network Security

In a Ad-hoc network, only Pre-shared key (Static WEP) can be configured.



Click on the **Configure**.. button and the following screen will appear:



Key Entry Method

There are 2 types of key entries:

- Hexadecimal: Enter only digits 0 ~ 9 and letters a ~ f/A ~ F.
- ASCII Text: Enter any character that can be found on the keyboard.

WEP Key (1 ~ 4)

Defines a set of shared keys for network security. You must enter at least one WEP key to enable security using a shared key.

If the key that you entered is too long, the utility will truncate it to fit.

WEP Key size

Defines the length of each encryption key.

- 64-bit WEP: 10 hexadecimal or 5 ASCII Text
- 128-bit WEP: 26 hexadecimal or 13 ASCII Text
- 152-bit WEP: 32 hexadecimal or 16 ASCII Text

6.2 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.

6.2.1 EAP-TLS

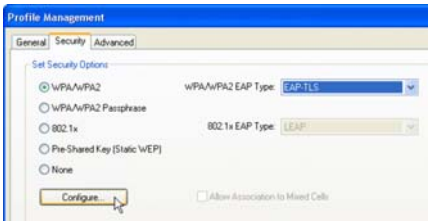
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) makes use of client-side and server-side certificates for mutual authentication.

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

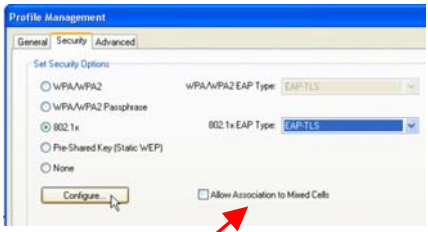
1. You can select

   WPA/WPA2 radio button (WPA stands for Wi-Fi Protected Access)

   Or



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



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 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:

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.

6.2.2 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.

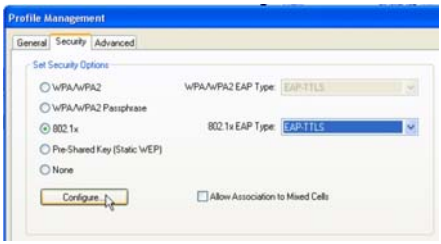
To use EAP-TTLS security, access the **Security** tab in the **Profile Management** window.

1. You can select

   WPA/WPA2 radio button

   Or

   802.1x radio button



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 **Settings...** button.

6. Leave the **Specific Server or 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.

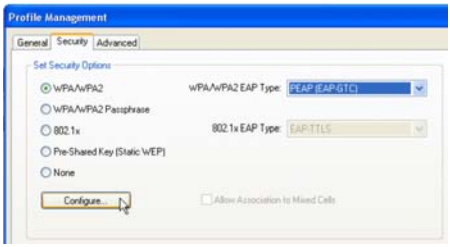
6.2.3 PEAP (EAP-GTC)

Similar to EAP-TTLS, PEAP (Protected EAP) also uses certificates to authenticate the server before creating an encrypted TLS tunnel through which the client can authenticate itself to the server using a challenge response authentication method such as EAP-GTC or EAP-MSCHAPv2.

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

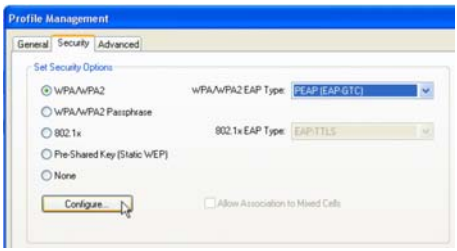
1. You can select

   WPA/WPA2 radio button



   Or

   802.1x radio button



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

3. Select the appropriate certificate authority (CA) from which the server certificate is downloaded from the **Trusted Root Certification Authority** drop-down list.

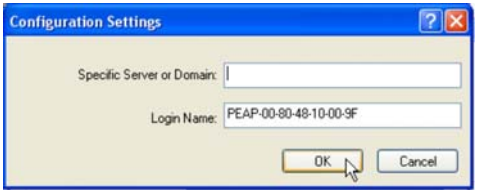
4. Enter your PEAP username (which is registered with the server) in the **User Name** field.

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

6. Leave the **Specific Server or 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.



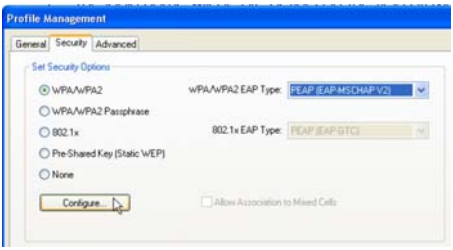
6.2.4 PEAP (EAP-MSCHAP V2)

MS-CHAPv2 uses a one-way cryptographic hash on the password and stores the hash value on the server. An authorized client knows the hash method used and reproduces it, sending the hashed password to the server during the challenge/response authentication. MSCHAPv2 is natively supported in Windows 2000 SP4 and Windows XP.

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

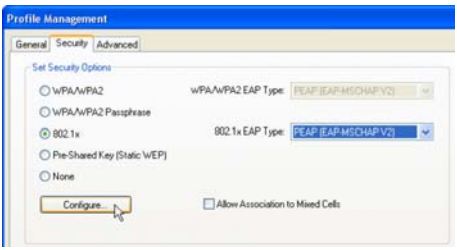
1. You can select

   WPA/WPA2 radio button



   Or

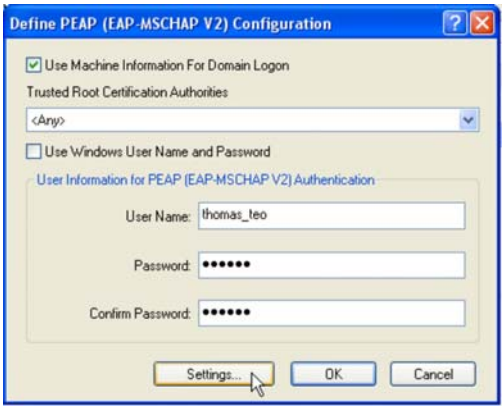
   802.1x radio button



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

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 **Settings....** button.



5. Leave the **Specific Server or 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.

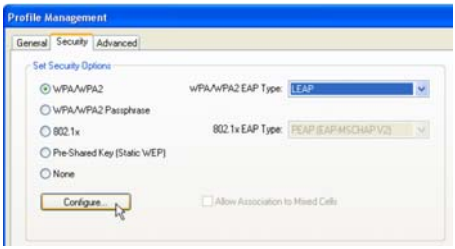
6.2.5 LEAP

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.

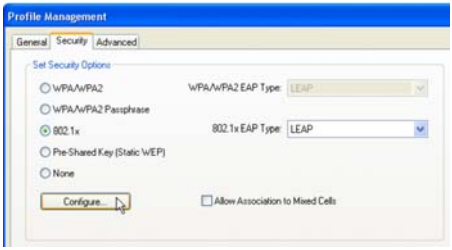
1. You can select

   WPA/WPA2 radio button



   Or

   802.1x radio button



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

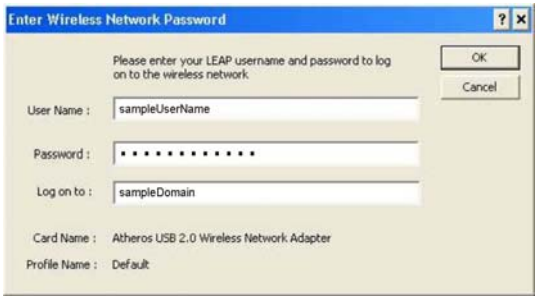
   Each time your PC reboots, you will be required to enter your LEAP username and password in order to be authenticated and obtain access to the network.

   - Use Saved User Name and Password.

   Authentication is obtained using a saved username and password (registered with the server) so you will not be required 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.



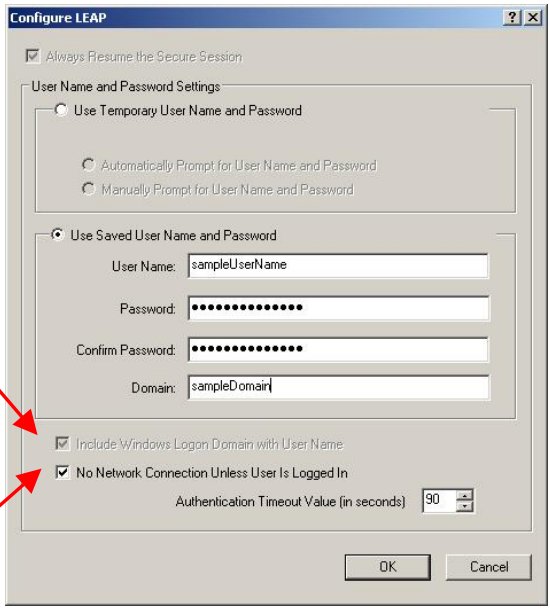
Next, the system will start the LEAP authentication.

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 Value** (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.



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.

6.2.6 EAP-FAST

Extensible **A**uthentication **P**rotocol-**F**ast **A**uthentication via **S**ecure **T**unneling performs the similar authentication methods as EAP-TLS and PEAP. Comparing EAP-TLS and PEAP, EAP-FAST offers a more efficient and better support for security provisioning, and minimizes the number of mechanisms required for asymmetric cryptography and certificate validation. It also provides high-level protection from network attacks such as man-in-the-middle, authentication forging, weak IV attack (AirSnort), packet forgery (replay attack), and dictionary attacks.

EAP-FAST gives support to users who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types and supports password expiration and change.

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

1. You can select

   WPA/WPA2 radio button

   Or

   802.1x radio button

2. Choose **EAP-FAST** 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

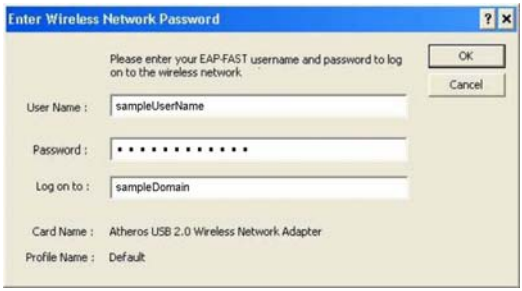
Each time your PC reboots, you will be require to enter your EAP-FAST username and password in order to be authenticated and obtain access to the network.

- 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 EAP-FAST username and password each time your PC reboots.

<u>Temporary User Name and Password</u>

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



Next, the system will start the EAP-FAST authentication.

Saved User Name and Password

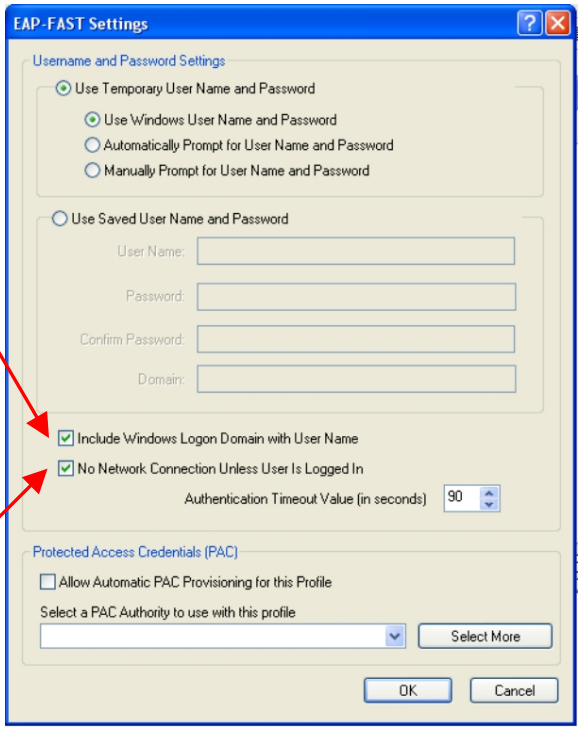
5. Enter the username, password and re-enter password in **Confirm Password** field.
   (Optional) You may enter a specific domain name, which will be passed to the server.

6. Enter the EAP-FAST **Authentication Timeout Value** (between 30 and 500 seconds) to specify how long EAP-FAST should wait before considering an authentication as failed, and sending an error message. The default is 90 seconds.

7. Click on the **OK** button.

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.



Protected Access Credentials (PAC)

The PAC is a unique shared credential used to mutually authenticate client and server. It is associated with a specific client username and a server authority ID.

EAP-FAST provides two ways to supply a client with a new PAC:

- Automatic PAC provisioning

A new PAC will be sent to the client over a secured network connection.

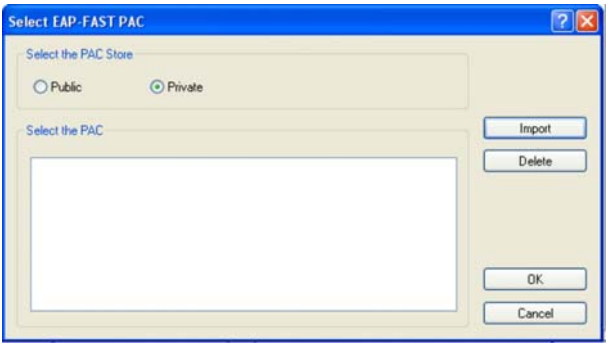
- Manual PAC provisioning

This requires the PAC file to be manually installed onto the client.

8. Tick the **Allow Automatic PAC Provisioning for this Profile** checkbox if you want to allow automatic PAC provisioning for the profile you are using. Otherwise user access will be denied and PAC provisioning must be performed manually.

9. To select a PAC Authority for the profile you are using, click **Select More**. Then you will be asked to decide whether to use a **Public** or **Private** PAC Authority.

10. Next, click **Import** to get the PAC from your own directory to add in the list under the **Select the PAC** section. Click **OK**.



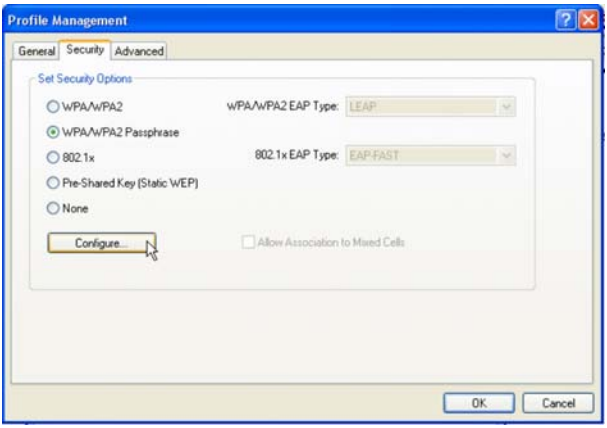
NOTE

After the PAC has been successfully provisioned, EAP-FAST authentication is restarted to gain network access. Therefore, after a successful PAC provisioning, an EAP failure will occur to terminate the previous EAP-FAST session and establish an authenticated wireless connection using a new PAC.

6.2.7 WPA/WPA2 Passphrase

WPA/WPA2 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/WPA2 Passphrase** radio button and click on the **Configure…** button.



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

Note:
The WPA/WPA2 Passphrase must match that used by the AP/other wireless clients in the network.

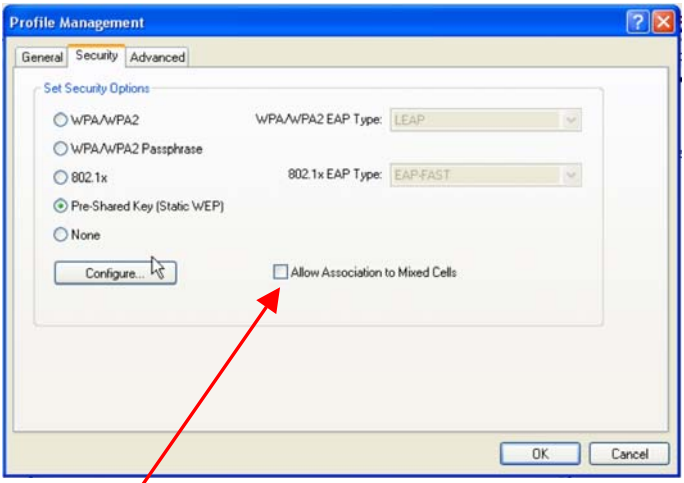
6.2.8 Pre-shared Key (Static WEP)

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,

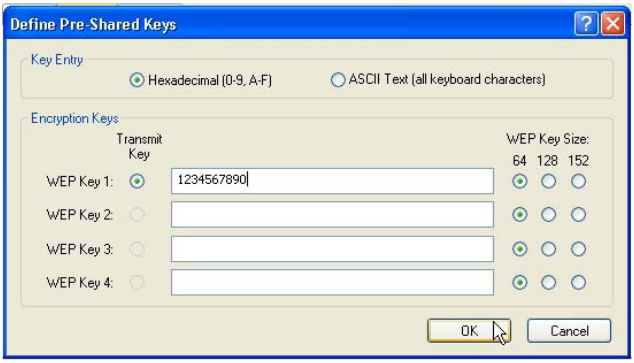
1. Choose the **Pre-shared Key (Static WEP)** radio button and click the **Configure…** button to fill in the encryption key.



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.



WEP Key size

- 64-bit WEP: 10 hexadecimal or 5 ASCII Text
- 128-bit WEP: 26 hexadecimal or 13 ASCII Text
- 152-bit WEP: 32 hexadecimal or 16 ASCII Text

Appendix I Unplug PCI Adapter from the System

To safely remove your PCI adapter from your system,

1. Go to the **Start** menu to select **Shutdown**.

2. Power off your PC and switch off the power from the main power supply.
3. Remove the back cover of the PC.
4. Next, carefully unplug the PCI adapter from the PCI slot of your PC.
5. Replace the back cover and turn on your PC.

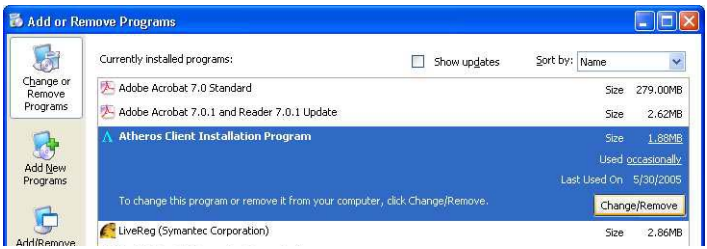
Appendix II Un-install

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

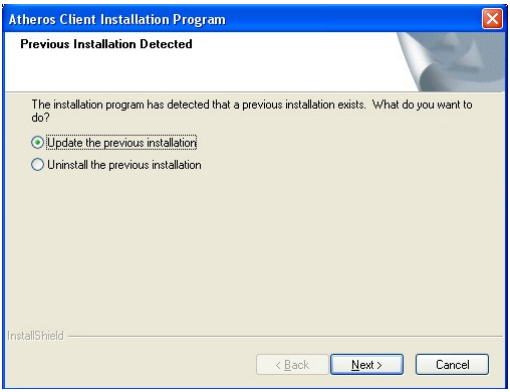
When you un-install the software, any existing profiles will be removed. If you want to re-use your profiles, please refer to **Section 5.2 Profile Management Tab** for further details on how to export a profile to disk. You are advised to close all programs and to leave the network adapter in the PCI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

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

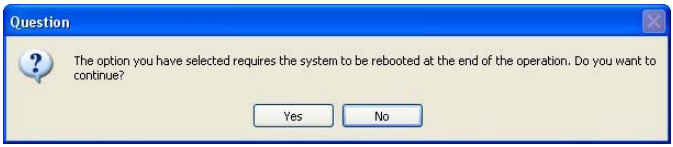
2. Highlight the **Atheros Client Installation Program** and click on the **Change/Remove** button.



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



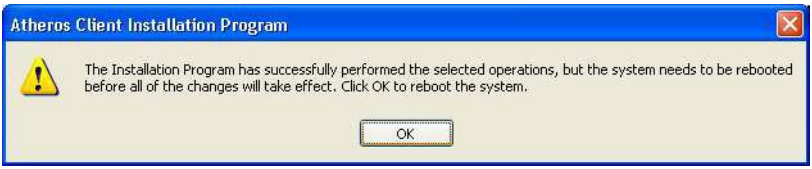
4. The prompt screen appears to notify you that the uninstall option requires the system to be rebooted at the end of the uninstall process. Click on the **Yes** button to proceed.



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

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

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.



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

Appendix III Certificate Application for WPA mode

Wi-Fi Protected Access (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 or patch files for Service Pack 1.
- Apply certification via Internet Browser
- Become domain member

AIII-1 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**.

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.

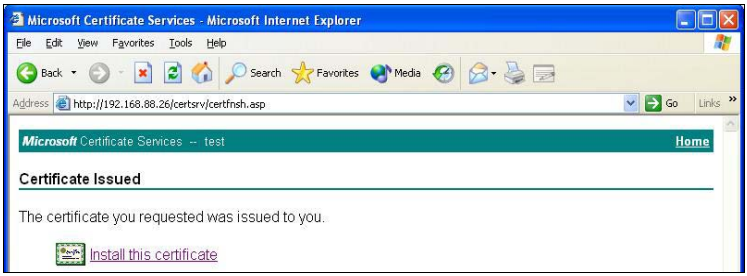
After ensuring that you have installed Windows XP SP1, insert the Product CD into your CD-ROM drive. Go to Windows Explorer and click on your CD-ROM drive icon. From your software folder, select the **WPA_Patch** folder and install both files: *WindowsXP- Q815485_WXP_SP2_x86_ENU.exe* followed by *WindowsXP-KB826942-x86-ENU.exe*.

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

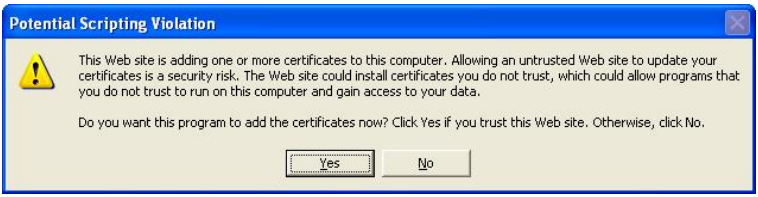
AIII-2 Installing certificate on your server

If you are using Microsoft Certificates services,

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

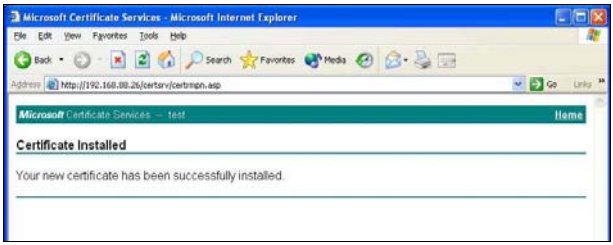


2. Click on the **Yes** button on the pop up window to continue with the installation.



3. To add the certificate to the Root Store, click on the **Yes** button.

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



AIII-3 Applying for Client Certifications

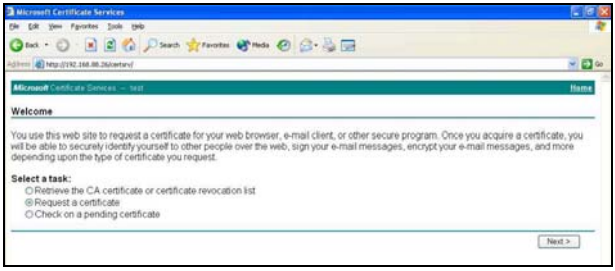
If you have installed Microsoft SP2 or Microsoft XP SP1 with the 2 patch files provided on the Product CD, you are now ready to apply for a certificate for your wireless client.

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

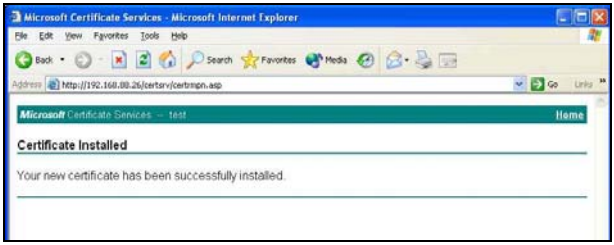
1. Open your Internet browser; enter e.g. *http://192.168.88.26/certsrv* where 192.168.88.26 is the server's IP address.

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

3. 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.

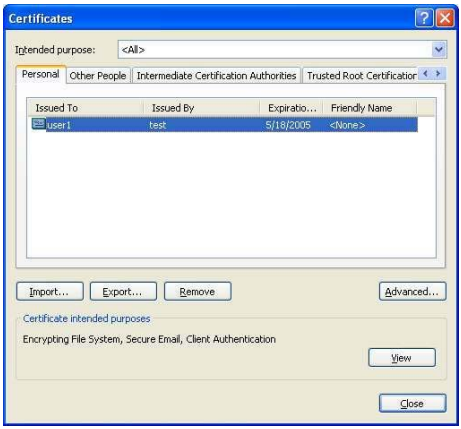


The screen below will appear to indicate that a certificate has been successfully issued to your PC.



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

5. 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.

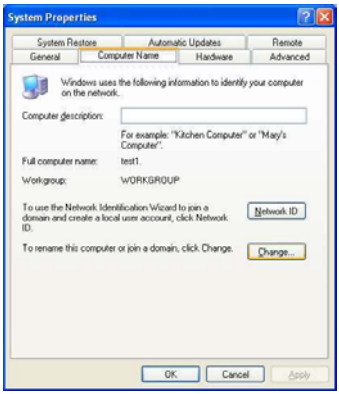


AIII-4 Becoming a domain member

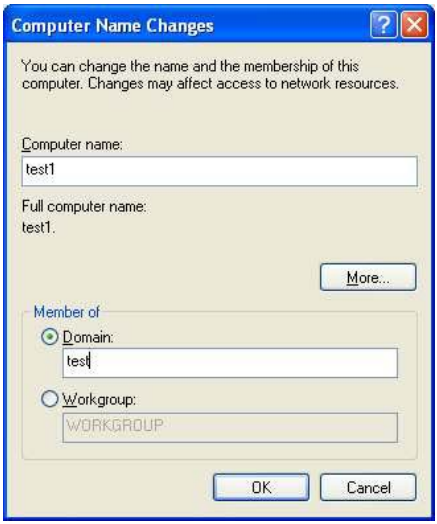
Next, you need to join the correct network domain so that you can communicate with the access point connected to your server.

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

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



3. 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.



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

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

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

Appendix IV Wireless Zero Configuration Utility

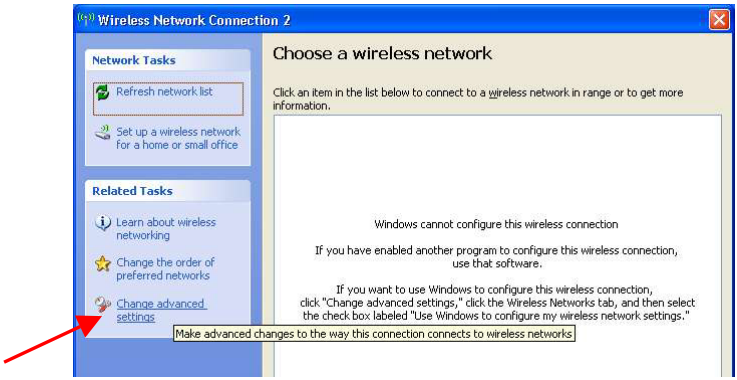
If your computer is running under the Windows XP operating system, you can opt to configure the **Wireless Network Connection** from your Windows XP operating system, instead of the Atheros Utility. You need to exit from the Atheros Utility before accessing to Windows XP's Wireless Zero Configuration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

AIV-1Enable Wireless Zero Configuration Utility

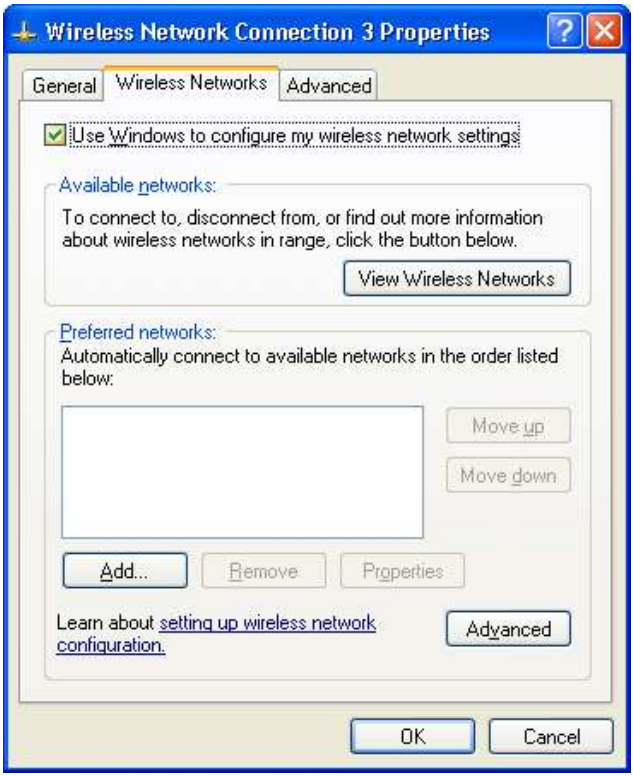
To set Wireless Zero Configuration on Windows XP, take the following steps:

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.



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



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 Atheros utility.

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-2Disable Wireless Zero Configuration Utility

To turn Wireless Zero Configuration Utility off on Windows XP,

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

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

3. When this check box is cleared, all profile settings will be controlled by the utility.

Appendix V Technical Specifications

Network Protocol, Standards and Electrical Emissions	
Industry Standards (WLP54G)	• **IEEE 802.11g** • **IEEE 802.11b**
Industry Standards (WLP54AG)	• **IEEE 802.11g** • **IEEE 802.11b** • **IEEE 802.11a**
Performance	
Frequency Band (WLP54G) **IEEE 802.11g:** **IEEE 802.11b:**	 2.312 ~ 2.484GHz 2.312 ~ 2.472GHz
Frequency Band (WLP54AG) **IEEE 802.11g:** **IEEE 802.11b:** **IEEE 802.11a:**	 2.312 ~ 2.484GHz 2.312 ~ 2.472GHz 5 ~ 5.850GHz
Modulation	• Binary Phase Shift Keying (BPSK) • Quadrature Phase Shift Keying (QPSK) • Complementary Code Keying (CCK) • 16 QAM • 64 QAM • DBPSK • DQPSK
Antenna Type	External 2dBi antenna and an SMA-type connector
Network Interface	PCI 2.3 compatible

Operating Channel (WLP54G)	802.11g • 11 Channels (US & Canada) • 13 Channels (Europe, Asia) • 14 Channels (Japan)
Operating Channel (WLP54AG)	802.11g • 11 Channels (US & Canada) • 13 Channels (Europe, Asia) • 14 Channels (Japan) 802.11a • 13 Channels (US & Canada) • 19 Channels (Europe, Asia) • 10 Channels (Japan)
Drivers/Operating system Supported	Windows XP/2000
Wireless Transmission Power (WLP54G 3CA1100, 3CA1300, 3CA1100S, 3CA1300S, 3BA1100, 3BA1300) **IEEE 802.11b:** **IEEE 802.11g:**	 20 dBm typical 19 dBm typical
Wireless Transmission Power (WLP54G 3CA1100P23, 3CA1300P23) **IEEE 802.11b:** **IEEE 802.11g:**	 23 dBm typical 19 dBm typical
Wireless Transmission Power (WLP54AG 3CA1100, 3CA1300, 3CA1100S, 3CA1300S) **IEEE 802.11b:** **IEEE 802.11g:** **IEEE 802.11a:**	 20 dBm typical 19 dBm typical 17 dBm typical

Receive Sensitivity	Up to –90dBm
Wireless Security	• 64-bit/128-bit/152-bit WEP • IEEE 802.1x support – EAP-TLS, EAP-TTLS, PEAP-GTC, PEAP-MSCHAPv2, LEAP, EAP-FAST • WPA/WPA2, WPA-PSK
Wireless Operating Range (WLP54G 3CA1100, 3CA1300, 3CA1100P23, 3CA1300P23, 3BA1100, 3BA1300) **IEEE 802.11g:** **IEEE 802.11b:**	80m (54Mbps outdoor), 20m(54Mbps indoor) 300m (11Mbps outdoor), 100m (11Mbps indoor)
Wireless Operating Range (WLP54AG 3CA1100, 3CA1300) **IEEE 802.11g:** **IEEE 802.11b:** **IEEE 802.11a:**	80m (54Mbps outdoor), 20m(54Mbps indoor) 300m (11Mbps outdoor), 100m (11Mbps indoor) 85m (54Mbps outdoor), 20m(54Mbps indoor)
Wireless Operating Range (WLP54G 3CA1100S, 3CA1300S) **IEEE 802.11g:** **IEEE 802.11b:**	80m (108Mbps outdoor), 20m(108Mbps indoor) 300m (11Mbps outdoor), 100m (11Mbps indoor)
Wireless Operating Range (WLP54AG 3CA1100S, 3CA1300S) **IEEE 802.11g:** **IEEE 802.11b:** **IEEE 802.11a:**	80m (108Mbps outdoor), 20m(108Mbps indoor) 300m (11Mbps outdoor), 100m (11Mbps indoor) 85m (54Mbps outdoor), 20m(54Mbps indoor)

Physical and Environment	
Environmental Requirements **Operating temperature:** **Storage temperature:** **Operating humidity:** **Non-operating humidity:**	 0°C to 50°C -20°C to 70°C 10% to 70% RH 5% to 90% RH
Power Consumption	3.3V DC, 500mA 350mA Tx 250mA Rx
Physical Dimension	120mm x 64.5 mm x 1.6 mm (LxWxD)