PLANET
Networking & Communication

802.11g Wireless LAN USB Adapter w/SMA connector

WL-U356A

User Manual

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

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

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

FCC Caution

To assure continued compliance. (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

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

Federal Communication Commission (FCC) Radiation Exposure Statement

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

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8,2000.

Safety

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

EU Countries Not Intended for Use

The ETSI version of this device is intended for home and office use in Austria Belgium, Denmark, Finland, France (with Frequency channel restrictions). Germany, Greece, Ireland, Italy, Luxembourg .The Netherlands, Portugal, Spain, Sweden and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

Potential restrictive use

France: Only channels 10,11,12 and 13

Revision

User's Manual for PLANET 802.11g Wireless LAN USB Adapter
Model: WL-U356A
Rev: 1.0 (October, 2004)
Part No. EM-WLU356A

Table of Contents

Chapter 1 Introduction

The PLANET 802.11g Wireless USB 2.0 Adapter, WL-U356A, is a high-efficiency wireless adapter for wireless networking at home, in office, or in public places. This USB adapter connects directly to any USB-ready desktop/notebook computers, so that you can share files, printers, and high-speed access to the Internet over your existing wireless network easily, without disassembling your computer.

The WL-U356A has support data rate up to 54Mbps, and can auto-negotiate to be compatible with any IEEE 802.11b/g device. Support of 64, 128 and 256bit WEP encryption plus WPA (Wi-Fi Protected Access) high-level encryption prevents your wireless communications from unauthorized access and ensures secure data transfer.

The WL-U356A can operate in either Ad-Hoc mode (Point to Point/Point to Multipoint without Access Point) or Infrastructure mode (Point to Point/Point to Multipoint with Access Point). It also supports Software AP function to provide the convenience for users to establish their wireless connection. With the provided external antenna connector, users can change the antenna freely to increase wireless performance.

1.1 Features

- Compliant with the IEEE 802.11g 2.4GHz (OFDM) standard
- High data transfer rate - up to 54Mbps
- Supports WEP 64/128/256 bits, WPA protection
- Supports Infrastructure and Ad-Hoc mode
- Software AP function support
- Data rate automatic fallback increases reliability
- Supports the most popular operating systems: Windows 98SE/Me/2000/XP
- Detachable antenna design
- USB 2.0 interface

1.2 Package Contents

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

1 x WL-U356A
1 x Driver and User's manual CD
1 x Quick Installation Guide
1 x External Antenna
1 x Wall-mount Accessory pack

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

Chapter 2 Installation Procedures

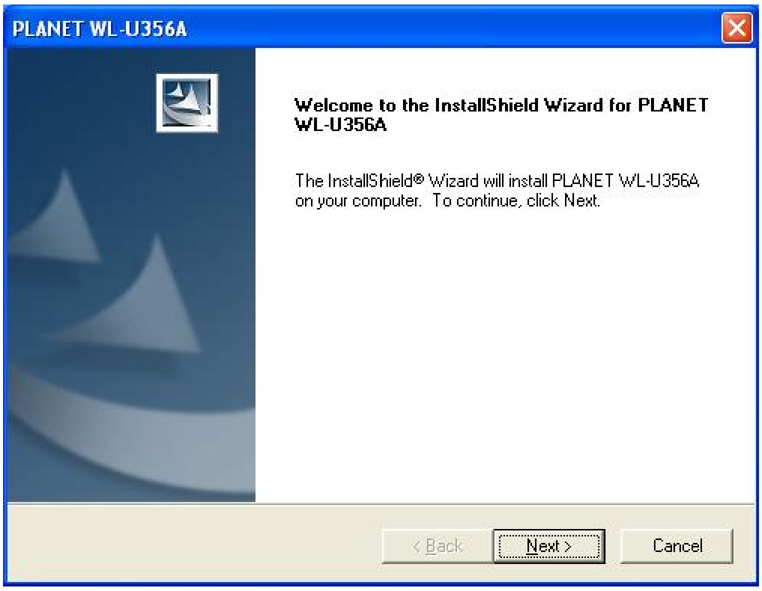
2.1 Install Utility Software

Note!	Before installing the utility software, **DO NOT** insert WL-U356A into your PC. If the WL-U356A is inserted already, Windows will detect the WL-U356A and request for a driver. Click **Cancel** to quit the wizard and remove the adapter from your PC. If you have installed the WL-U356A or other wireless card driver & utility already, please uninstall them firstly.

Step 1: Insert the provided Drivers and User's Manual CD into your CD drive to initiate the autorun program. Once completed a menu screen will appear.

Step 2: Click on "Configuration Utility" hyper link in WL-U356A field to initiate the installation. If the menu screen is not shown, you can click "Start" button and choose "Run". When the dialog box appears, enter "E:\Utility\setup.exe" (Suppose "E" is your CD-ROM drive) and click "OK" to continue.

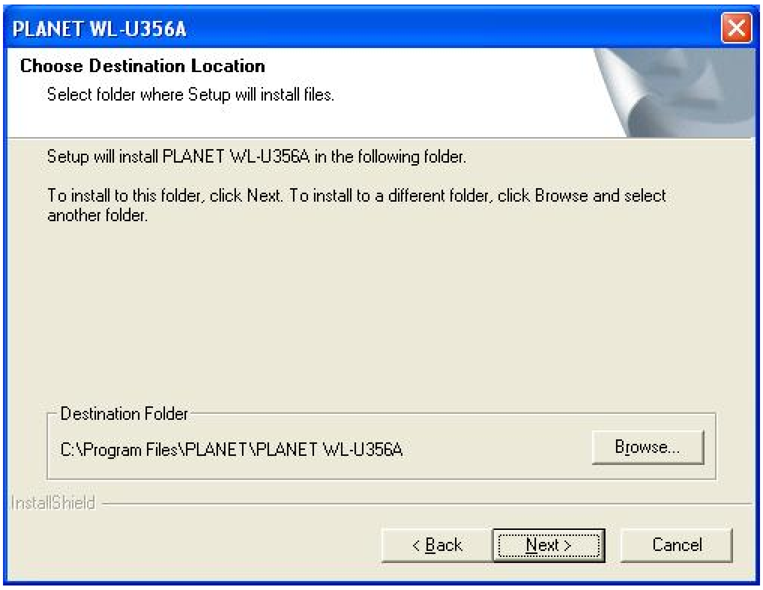
Step 3: When the welcome screen appears, click "Next**".**


PLANET WL-U356A

Welcome to the InstallShield Wizard for PLANET WL-U356A

The InstallShield® Wizard will install PLANET WL-U356A on your computer. To continue, click Next.

Step 4: Click "Next" to accept the default destination folder for the software or click "Browse" to manually select a destination folder.



PLANET WL-U356A

Choose Destination Location

Select folder where Setup will install files.

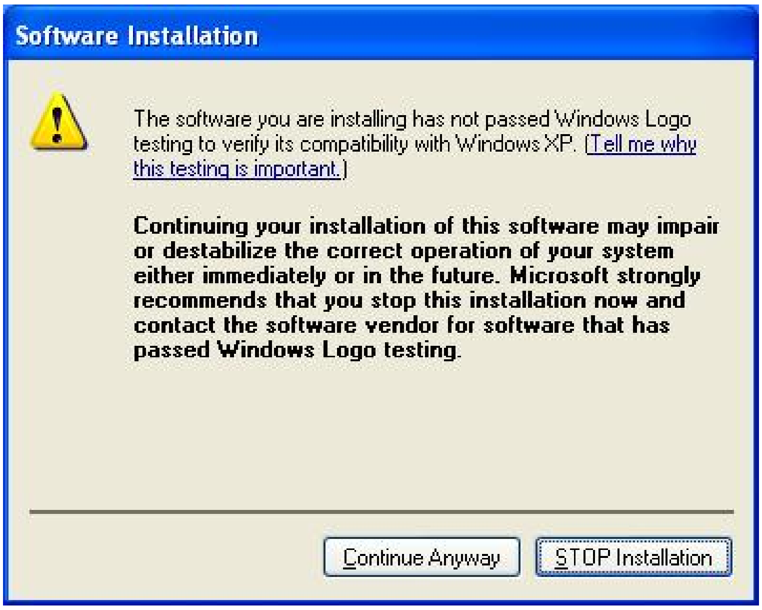
Setup will install PLANET WL-U356A in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\PLANET\PLANET WL-U356A

Step 5: For Windows XP, click "Continue Anyway" at the Windows Logo Compatibility screen.

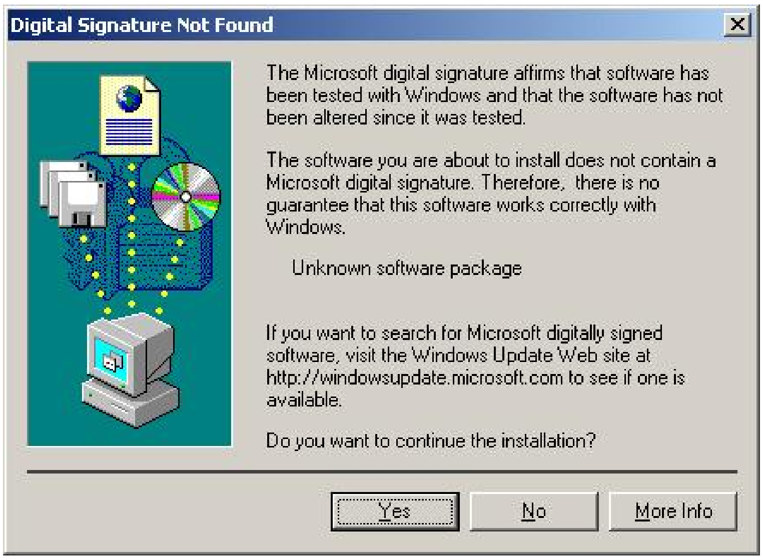


Software Installation

The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the software vendor for software that has passed Windows Logo testing.

For Windows 2000, click “Yes” at the Digital Signature screen.



Digital Signature Not Found

The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

Unknown software package

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

Step 6: Remove the Driver & Utility CD from your CD drive and then restart your PC.

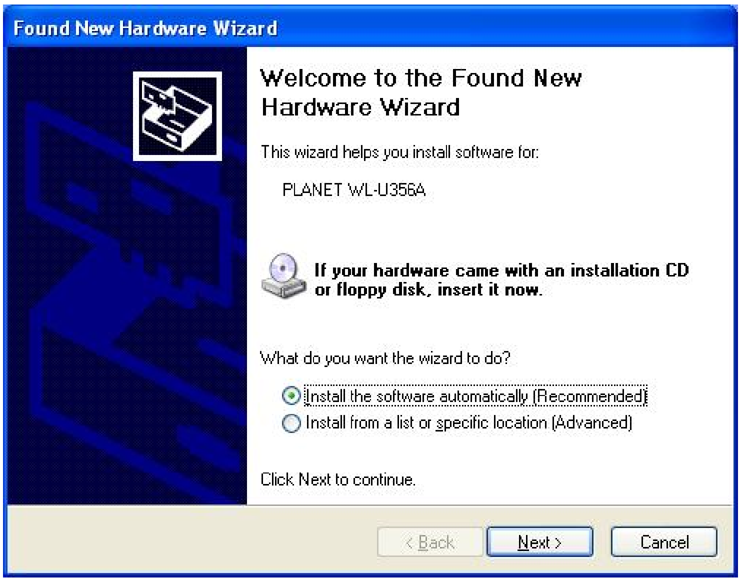
2.2 Install Driver

Note!

In most cases, Windows will automatically install the driver after the PC is restarted. If the Found New Hardware Wizard appears, follow the instructions below. The Found New Hardware Wizard will look different depending on your operating system. Follow the on-screen instructions to complete the installation. For Windows 98SE and Me users, you may be prompted to insert the Windows 98SE or Me CD during the driver installation. Be sure to have your Windows 98SE or Me CD ready.

Step 1: After the PC restart, insert WL-U356A into the USB port of the PC.

Step 2: Select “Install the software automatically” and click “Next”.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

PLANET WL-U356A

If your hardware came with an installation CD or floppy disk, insert it now.

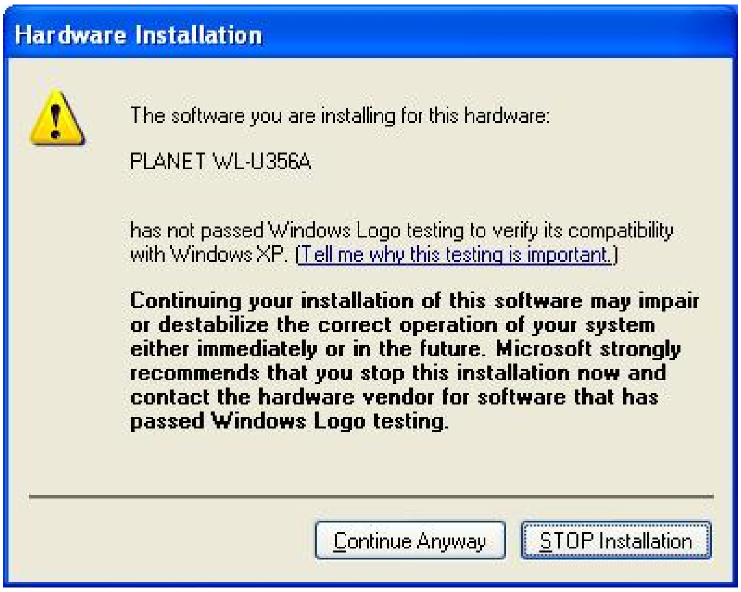
What do you want the wizard to do?

● Install the software automatically (Recommended)

○ Install from a list or specific location (Advanced)

Click Next to continue.

Step 3: For Windows XP, click "Continue Anyway" at the Windows Logo Compatibility screen.



Hardware Installation

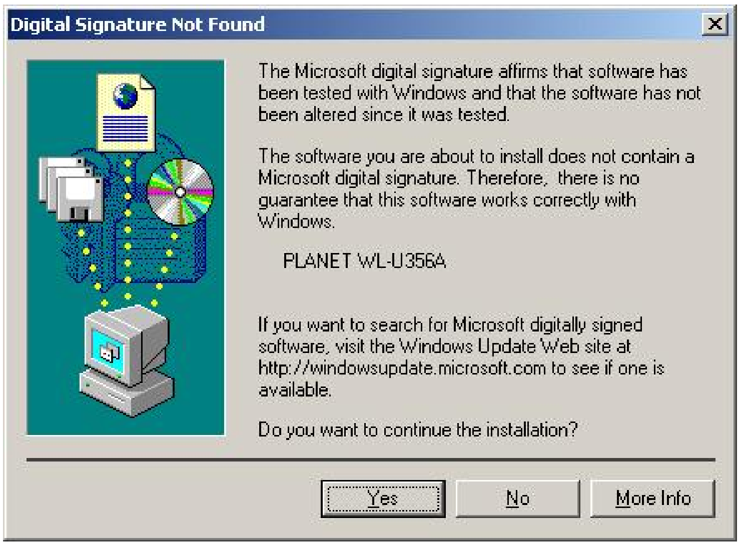
The software you are installing for this hardware:

PLANET WL-U356A

has not passed Windows Logo testing to verify its compatibility with Windows XP. (Tell me why this testing is important.)

Continuing your installation of this software may impair or destabilize the correct operation of your system either immediately or in the future. Microsoft strongly recommends that you stop this installation now and contact the hardware vendor for software that has passed Windows Logo testing.

For Windows 2000, click "Yes" at the Digital Signature screen.



Digital Signature Not Found

The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

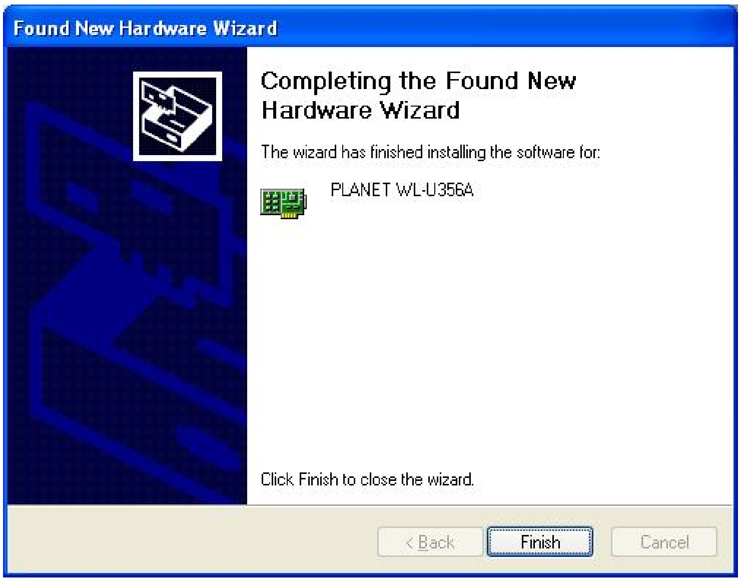
PLANET WL-U356A

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

For Windows 98SE or Me, insert the Windows 98SE or Me CD if prompted to do so and click “OK”.

Step 4: Click “Finish”. Restart the PC if you are prompted to do so.



Found New Hardware Wizard

Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

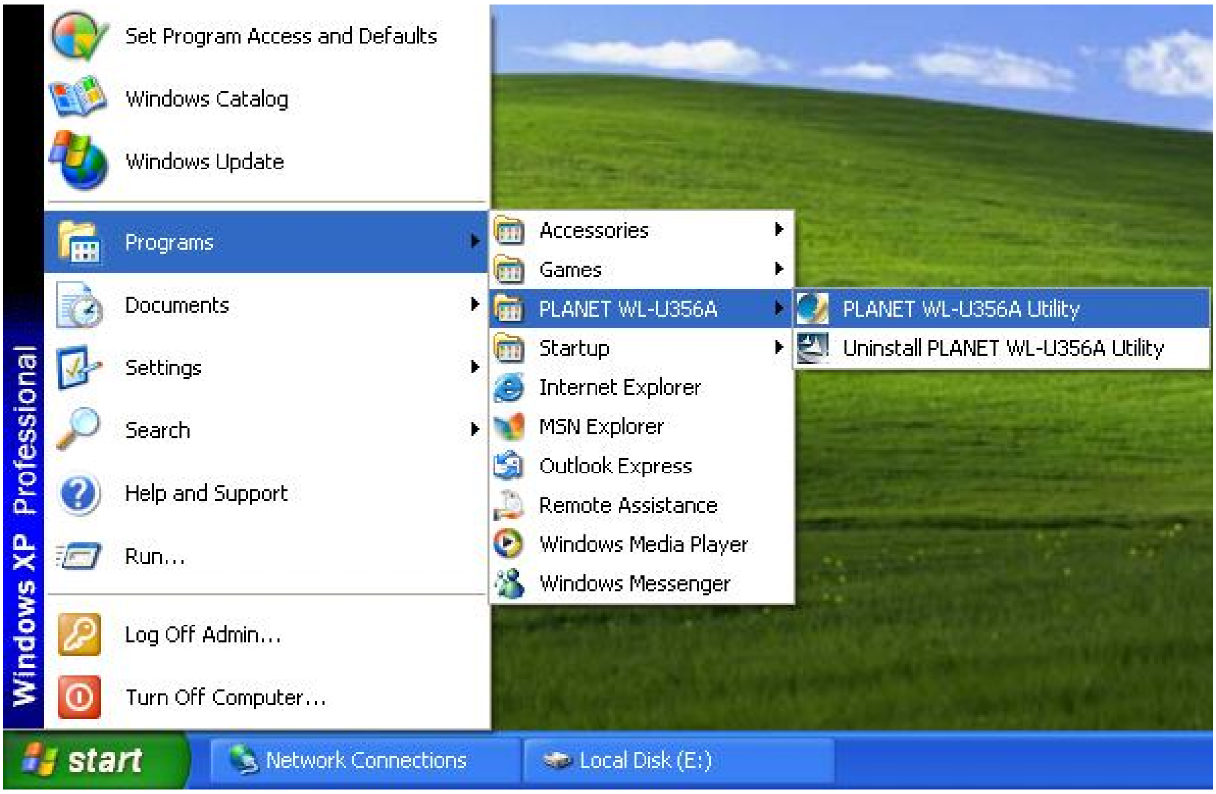
PLANET WL-U356A

Click Finish to close the wizard.

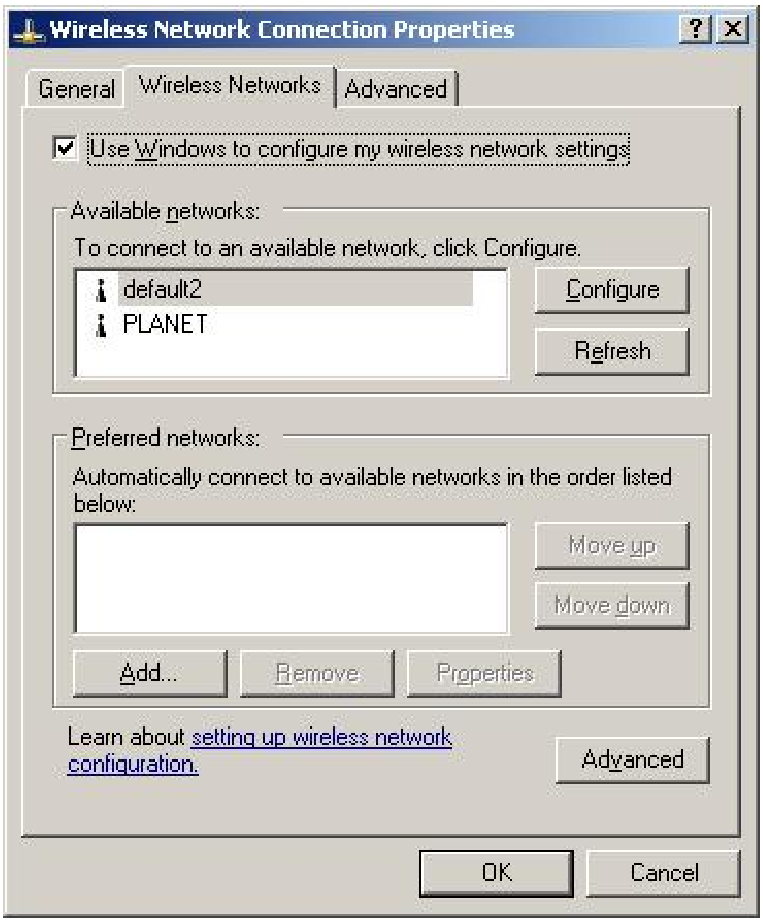
Chapter 3 Wireless Client Mode Configuration

The USB adapter can be set to either **Station** or **Access Point** Mode from the **Mode** drop-down menu. **Station** mode is the default selection and should be selected if you want to connect to a wireless router/access point or conduct peer-to-peer networking.

The configuration utility will be initiated automatically after PC restarts. It is a powerful application that helps you to configure the WL-U356A and monitor the status of the communication process. By double click the icon on the system tray, you can see the configuration utility appear. If configuration utility doesn't start automatically, please go to **Start => Programs =>PLANET WL-U356A=>PLANET WL-U356A Utility** to run the configure utility.



Note!	Windows XP system has a built-in wireless configuration interface. You may use this interface to configure your WL-U356A. You cannot use WL-U356A utility to configure your WL-U356A unless you disable the windows built-in utility first. For disabling windows built-in utility, please clear the checkbox of "Use Windows to configure my wireless settings" in the screen below. Then you can use WL-U356A utility to configure



Wireless Network Connection Properties

General | Wireless Networks | Advanced

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- default2
- PLANET

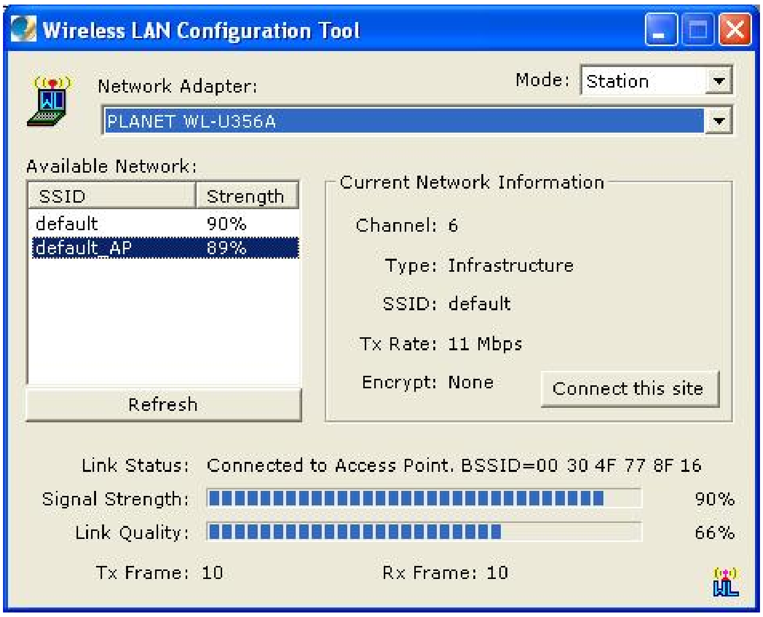
Preferred networks:

Automatically connect to available networks in the order listed below:

Learn about setting up wireless network configuration.

3.1 Wireless Connection Status

When the configuration utility is activated, it will scan all channels to locate available access points. This screen displays all information of current wireless connection.



Wireless LAN Configuration Tool

Network Adapter: PLANET WL-U356A

Mode: Station

Available Network:

SSID	Strength
default	90%
default_AP	89%

Current Network Information

Channel: 6

Type: Infrastructure

SSID: default

Tx Rate: 11 Mbps

Encrypt: None

Link Status: Connected to Access Point. BSSID=00 30 4F 77 8F 16

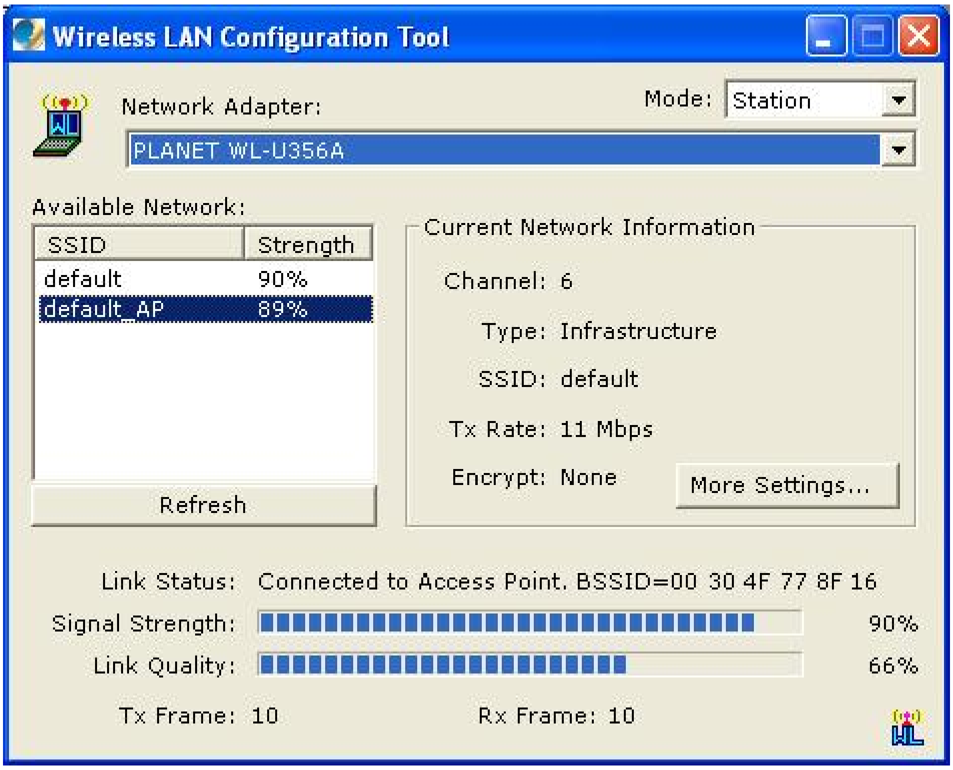
Signal Strength: 90%

Link Quality: 66%

Tx Frame: 10 Rx Frame: 10

Parameters	Description
Mode	Select from "Station" or "Access Point". For more information regarding Access Point Mode configuration, please refer to the Chapter 4.
Network Adapter	Displays the name of the USB adapter.
Available Network	Lists all the available wireless router/access point in your area. You can click on the "Refresh" button to update the list.
Current Network Information	Displays the selected wireless device information of the Available Network option. (An SSID must be highlighted first).
Link Status	Displays the link status.
Signal Strength	Displays the current signal strength.
Link Quality	Displays the current link quality.
Tx Frame	Displays the number of frames transmitted.
Rx Frame	Displays the number of frames received.
Connect this site	Connect to the wireless router/access point you have selected.

After connect to a wireless router/access point, the button name "Connect this site" will become "More settings…". You can click this button and refer to the section below to change the settings.



Wireless LAN Configuration Tool

Network Adapter: PLANET WL-U356A

Mode: Station

Available Network:

SSID	Strength
default	90%
default_AP	89%

Current Network Information

Channel: 6

Type: Infrastructure

SSID: default

Tx Rate: 11 Mbps

Encrypt: None

Link Status: Connected to Access Point. BSSID=00 30 4F 77 8F 16

Signal Strength: 90%

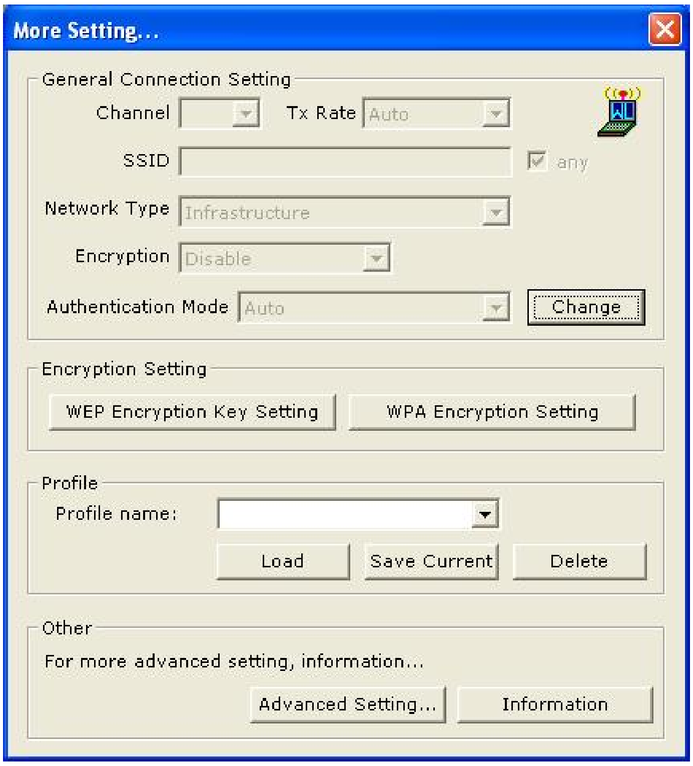
Link Quality: 66%

Tx Frame: 10

Rx Frame: 10

3.2 Configuring General Settings

Click “Change” to configure the adapter’s General Connection Setting.



More Setting...

General Connection Setting

Channel

Tx Rate: Auto

SSID

☑ any

Network Type: Infrastructure

Encryption: Disable

Authentication Mode: Auto

Encryption Setting

Profile

Profile name:

Other

For more advanced setting, information...

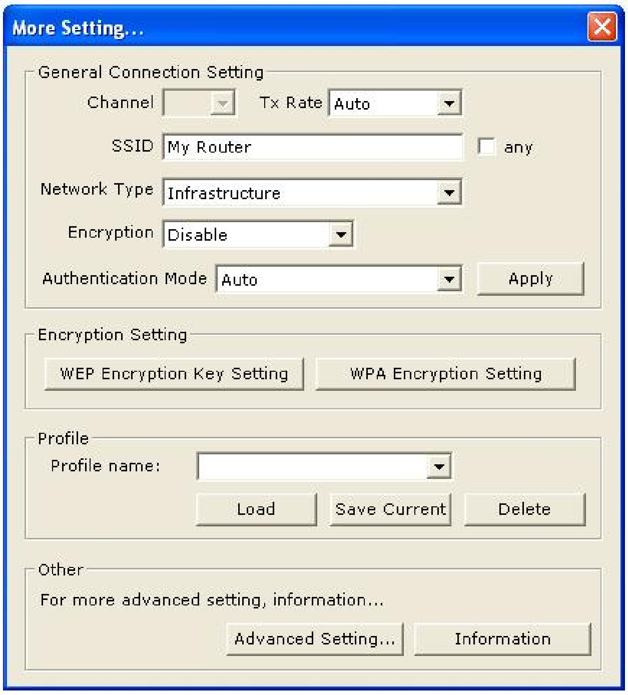
Parameters	Description
Channel	This setting is for **Access Point Mode** only.
Tx Rate	Select the desired transmission rate, or leave the default setting of “Auto” to allow the adapter to automatically select the optimum rate. When WL-U356A connects to an **USB1.1** port, Tx Rate will be fixed to 802.11b standard. The Max. transfer rate will be 11Mbps.
SSID	You can enter the SSID of the wireless router/access point you wish to connect to.
Any	Check this box to allow you connect to any available wireless router/access point. (Check this box if you’re trying to connect to a public hot spot and don’t know the SSID).
Network Type	Choose from “Infrastructure” (for connecting to a wireless router/access point) or “Ad-Hoc” (for computer-to-computer networking, bypassing the wireless router/access point).
Encryption	Choose from “Disable” or “Enable”. When “Enable” selected, you should refer to next section to configure encryption settings.,
Authentication Mode	Choose from “Auto” (recommended), “Open System”, or “Shared Key”. **Open System:** With the same WEP key between the stations, the stations don’t need to be authenticated. This is the default option.

	Shared Key: With the same WEP key between the stations in this Authentication algorithm, this type will use packets with encryption by transferring a challenge text which will be acknowledge by both side of the stations. In order to choose which authentication algorithm will be used, you must know which one the station supports this algorithm first.
Apply	After click “Change” button, the button name will turn into “Apply”. Please click “Apply” to save the configuration.

3.3 Configuring Encryption Security

3.3.1 WEP Configuration

Click “WEP Encryption Key Setting” button to configure the WEP settings.



More Setting...

General Connection Setting

Channel:

Tx Rate: Auto

SSID: My Router

□ any

Network Type: Infrastructure

Encryption: Disable

Authentication Mode: Auto

Encryption Setting

Profile

Profile name:

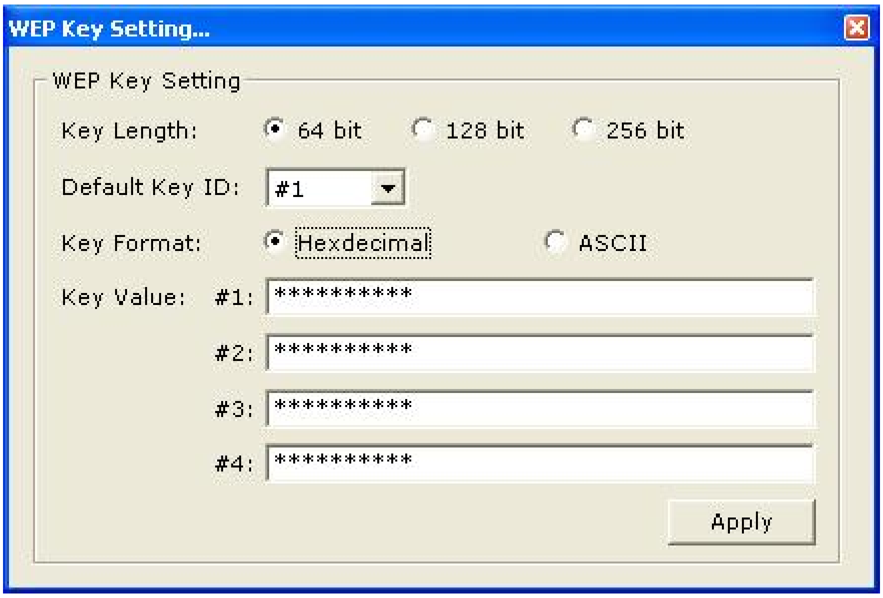
Other

For more advanced setting, information...

Note!

The WEP Key settings must be identical to the WEP settings of the wireless router/access point you wish to connect to.

Please click “Change” button to start configure the WEP Setting. After click, the button name will turn into “Apply’.



WEP Key Setting...

WEP Key Setting

Key Length: ● 64 bit ○ 128 bit ○ 256 bit

Default Key ID: #1

Key Format: ● Hexdecimal ○ ASCII

Key Value: #1: **********

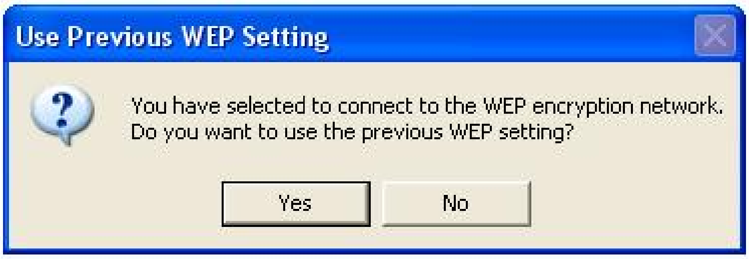
#2: **********

#3: **********

#4: **********

Parameters	Description
Key Length	Select the appropriate encryption key length.
Default Key ID	Select which of the four Key Values you want to use.
Key Format	Select either Hexadecimal (0-9, A-F) or ASCII (any number or letter).
Key Value	Enter the applicable key values. Up to four key values may be entered. Note the following rules when entering Key values: • **64-bit** key length requires **10** Hexadecimal characters (0-9, A-F) or **5** ASCII characters (any number or letter). • **128-bit** key length requires **26** Hexadecimal characters (0-9, A-F) or **13** ASCII characters (any number or letter). • **256-bit** key length requires **58** Hexadecimal characters (0-9, A-F) or **19** ASCII characters (any number of letter).
Apply	Save settings.

After you have applied the changes, return to the utility’s main screen and select the wireless router/access point you wish to connect to. Click “Yes” in below dialog box to connect to the encrypted wireless device.

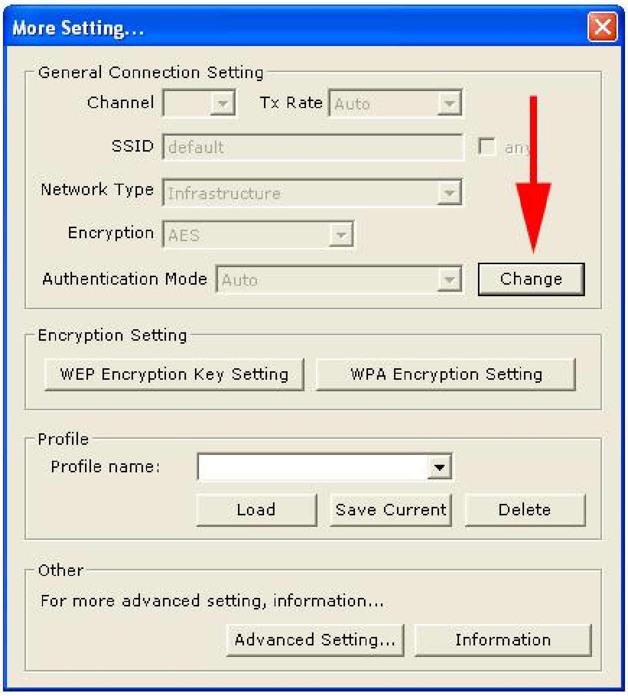


Use Previous WEP Setting

You have selected to connect to the WEP encryption network.
Do you want to use the previous WEP setting?

3.3.2 WPA-PSK Configuration

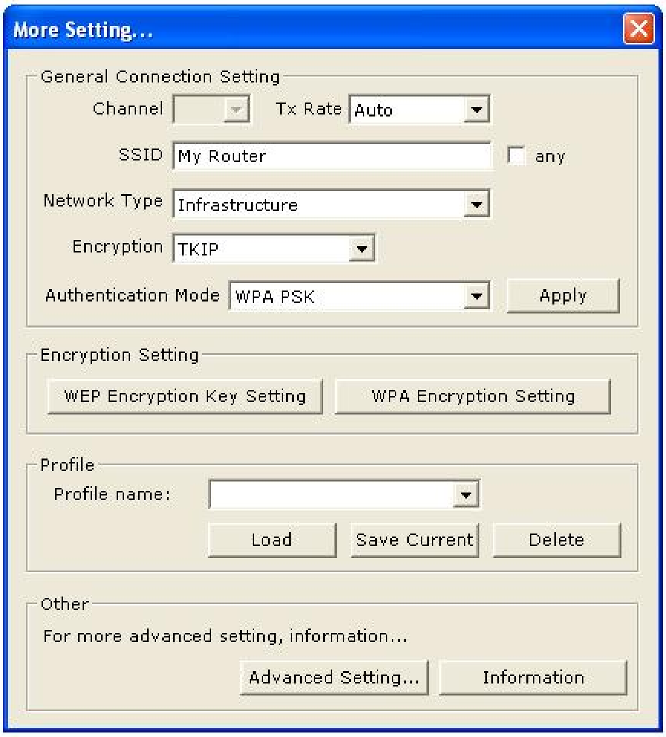
Step1: Please click on “Change” in the General Connection Setting.



Channel:
Tx Rate: Auto
SSID: default
□ any
Network Type: Infrastructure
Encryption: AES
Authentication Mode: Auto
Profile name:
For more advanced setting, information...

Step 2: Select “TKIP” or “AES” for Encryption, “WPA PSK” for Authentication Mode, and click “Apply”.

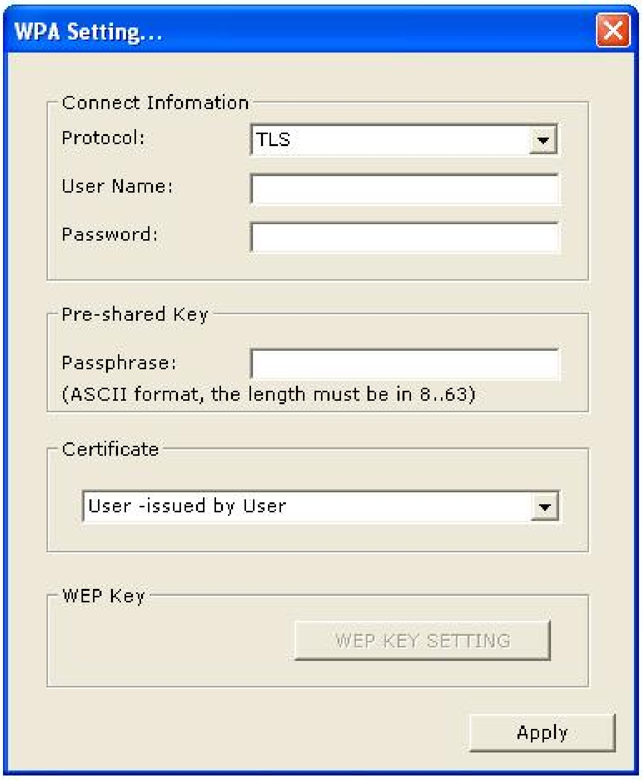
Note! The encryption method and authentication mode must be identical to the settings of the wireless router/access point you wish to connect to.



Channel:
Tx Rate: Auto
SSID: My Router
□ any
Network Type: Infrastructure
Encryption: TKIP
Authentication Mode: WPA PSK
Profile name:
For more advanced setting, information...

Step 3: Click on “WPA Encryption Setting” and click “Change” in the appeared dialog box.

Step 4: Enter the appropriate passphrase in the “Passphrase” field under the “Pre-shared Key” section and click “Apply”. (The passphrase must be identical to the passphrase set on your wireless router/access point and it has to be a string between 8 to 63 ASCII characters long).



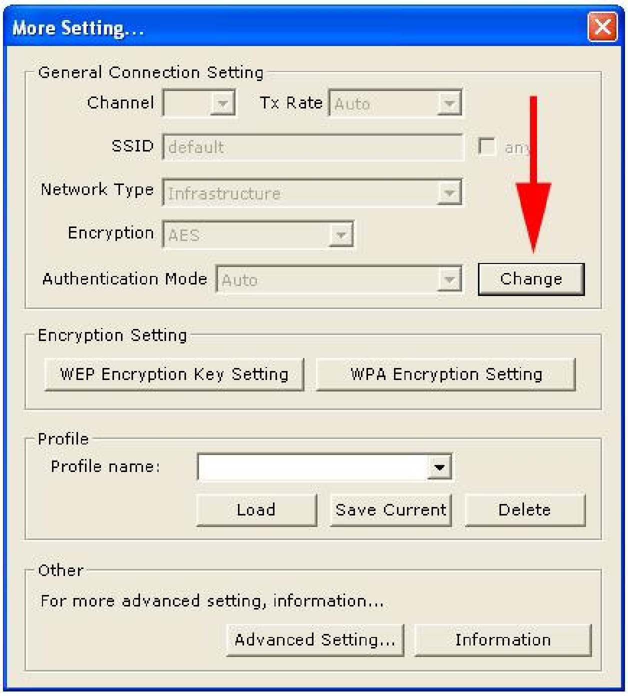
Protocol: TLS

(ASCII format, the length must be in 8..63)

User -issued by User

3.3.3 WPA Configuration

Step1: Please click on “Change” in the General Connection Setting.



More Setting...

General Connection Setting

Channel

Tx Rate Auto

SSID default

□ any

Network Type Infrastructure

Encryption AES

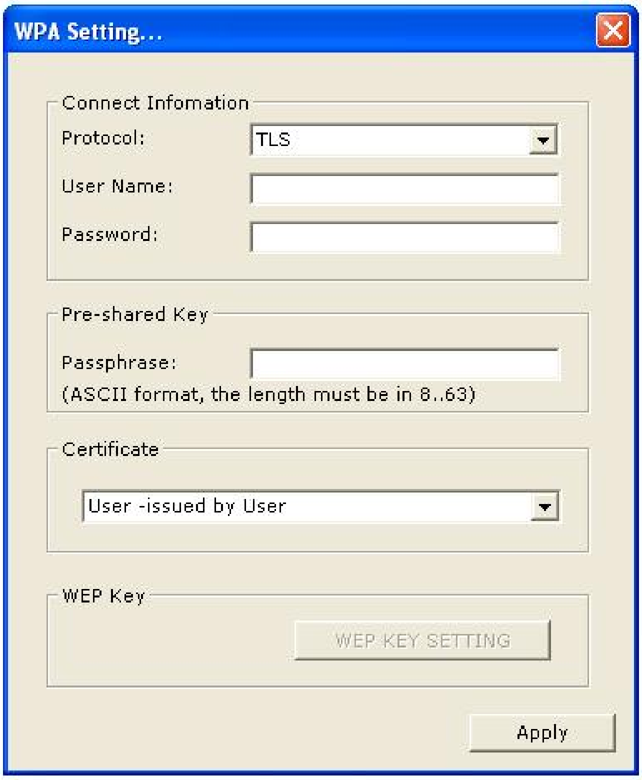
Authentication Mode Auto

Step 2: Select “TKIP” or “AES” for Encryption, “WPA” for Authentication Mode, and click “Apply”.

Note! The encryption method and authentication mode must be identical to the settings of the wireless router/access point you wish to connect to.

Step 3: Click on “WPA Encryption Setting” and click “Change” in the appeared dialog box.

Step 4: Select the appropriate protocol in the “Protocol” field. There are two kinds of protocols for WPA user authentication- TLS and PEAP. TLS and PEAP require a Radius server and the Certificate Authority. The main difference between the 2 protocols is TLS requires both the radius server’s and the client’s certificates, while PEAP requires only the server’s certificate. Moreover, PEAP requires a set of user name of password, which is supposed to be pre-configured by the network administrator. If you are using PEAP protocol, please fill in the following “User Name” and “Password” fields.


WPA Setting...

Connect Infomation

Protocol: TLS

User Name:

Password:

Pre-shared Key

Passphrase:

(ASCII format, the length must be in 8..63)

Certificate

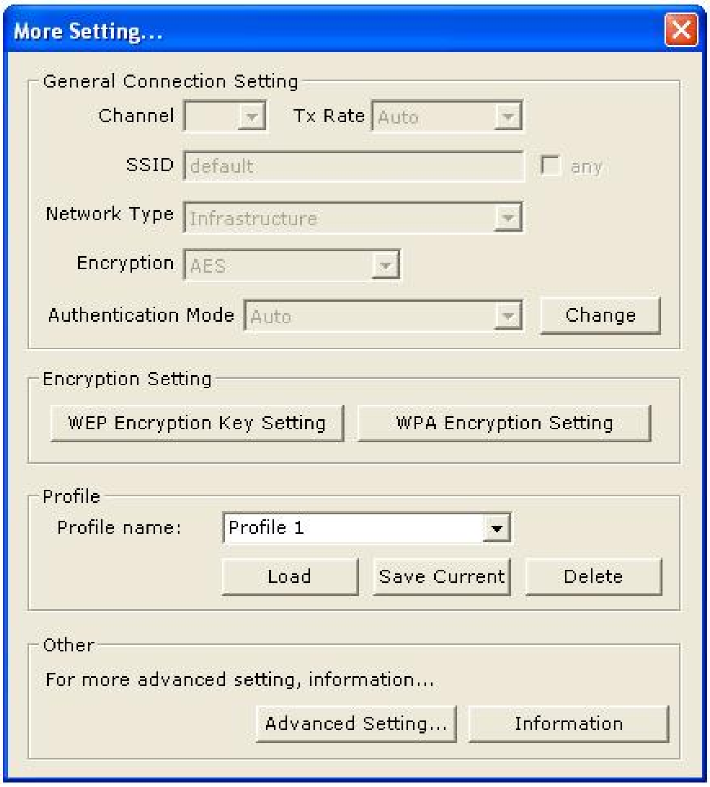
User -issued by User

WEP Key

Step 5: All available certificates for TLS or PEAP will be displayed in the "Certificate" drop-down list. Please select a proper one for user or server authentication.

Step 6: Click "Apply" to finish the configuration.

3.4 Configuring Profile



More Setting...

General Connection Setting

Channel

Tx Rate: Auto

SSID: default

□ any

Network Type: Infrastructure

Encryption: AES

Authentication Mode: Auto

Encryption Setting

Profile

Profile name: Profile 1

Other

For more advanced setting, information...

After you have configured all the settings, you can save your settings as a profile so you don't have to re-configure them the next time.

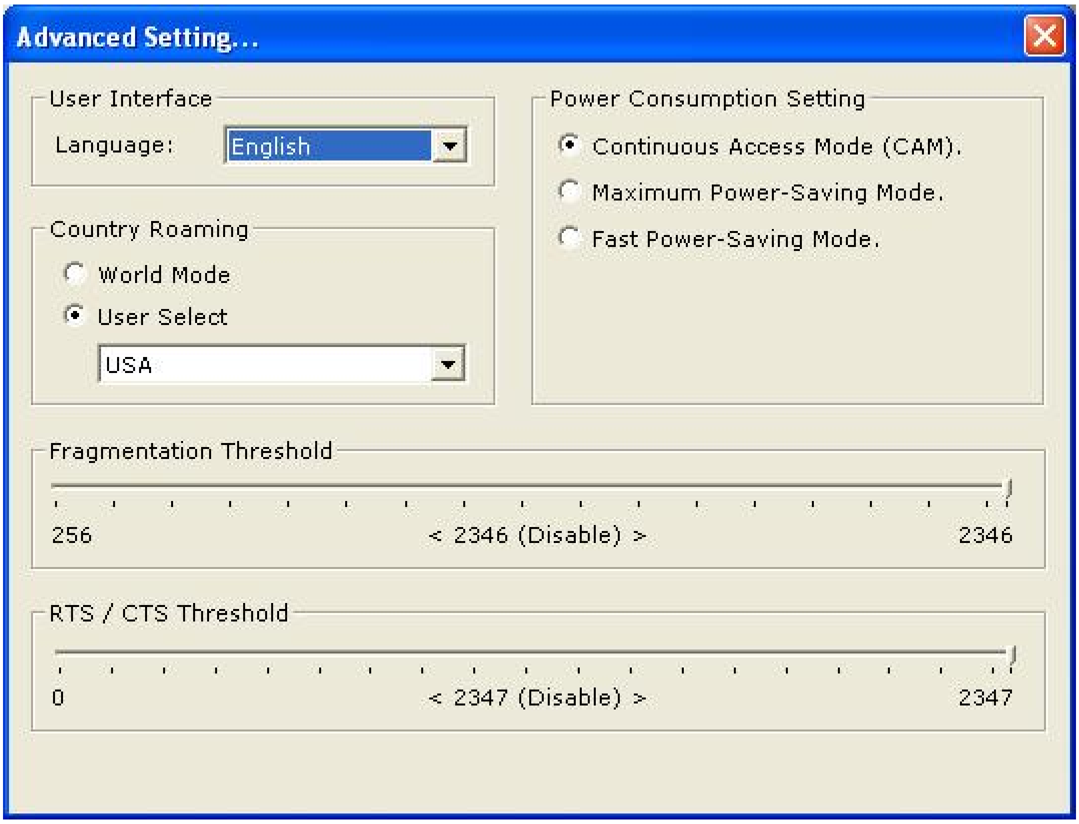
Type in a name for the profile in the "Profile name" field and click "Save Current".

To load a profile, select the profile from the drop-down list and click "Load".

To delete a profile, select the profile from the drop-down list and click "Delete".

3.5 Advanced Settings

Click "Advanced Setting" button in "More Setting" dialog box for configure advanced settings of WL-U356A.



Advanced Setting...

User Interface

Language: English

Country Roaming

○ World Mode

● User Select

USA

Power Consumption Setting

● Continuous Access Mode (CAM).

○ Maximum Power-Saving Mode.

○ Fast Power-Saving Mode.

Fragmentation Threshold

256 < 2346 (Disable) > 2346

RTS / CTS Threshold

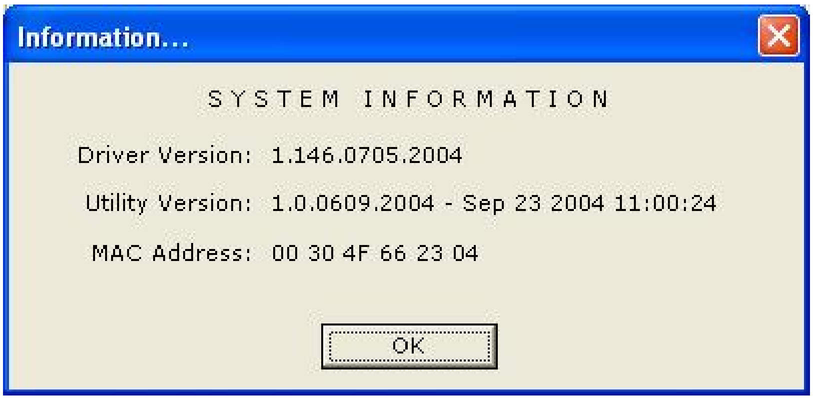
0 < 2347 (Disable) > 2347

Parameters	Description
User Interface	Select the language for the adapter's user interface.
Power Consumption Setting	● **Continuous Access Mode:** The adapter will always stay in active mode. No power-saving function will be activated. ● **Maximum Power-Saving Mode:** Enable the power-saving function when the adapter is idle. This mode applies to PDA best because it saves most power. Its Implementation will cause additional overhead to your wireless network. ● **Fast Power-Saving Mode:** This mode also provides the power-saving function, but the power consumption in this mode is higher than that of the "Maximum Power-Saving Mode". This mode applies to laptops. Its implementation will also cause additional overhead to your wireless network.
Country Roaming	WL-U356A is World Mode supported. You may enable World Mode or select the country that you are stay manually for operate Frequency Domain. ● **World Mode**: The adapter will get its country setting from the access point. ● **User Select**: Choose your country. This is the channel selection of each country regulatory domain, select the country where you are using this wireless device, users are responsible for ensuring that the channel set configuration is in compliance with the regulatory standards of these countries.
Fragmentation Threshold	It is a way of transmitting the packets that will be fragmented. Choose a setting within a range of 256 to 2432 bytes. It is

Threshold	Choose a setting within a range of 256 to 2432 bytes. It is recommended to fragment the packet when the link quality is bad, it is to prevent the wasting time of resending a long packet that is lost.
RTS/CTS Threshold	It is a station initiates the process by sending a RTS frame, the other ends receives the RTS and responds with a CTS frame, the station must receive a CTS frame before sending the data frame. This is to prevent the collisions by each station. Choose a setting within a range of 256 to 2432 bytes. It is recommended limiting a long packet to prevent each station waiting too long to transmit a data.

3.6 Information

Click “Information” button in “More Setting” dialog box to view the driver and utility version and MAC Address of WL-U356A.



SYSTEM INFORMATION

Driver Version: 1.146.0705.2004

Utility Version: 1.0.0609.2004 - Sep 23 2004 11:00:24

MAC Address: 00 30 4F 66 23 04

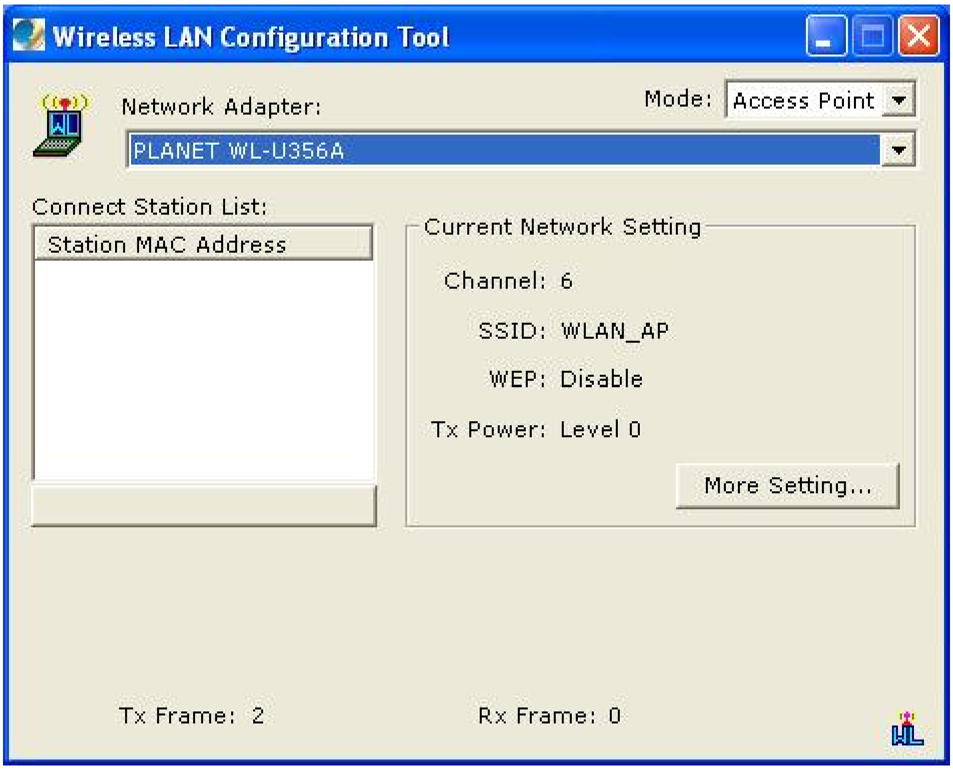
Chapter 4 Access Point Mode Configuration

4.1 Configuring Access Point

You can configure the USB Adapter as an access point for other wireless clients on your network.

Note: You will not be able to access the Internet if you configure WL-U356A as an access point. To allow other wireless clients to access the Internet, you will need to configure your computer as a router and a DHCP server.

Select **Access Point** from the Mode drop-down list.



Mode: Access Point

PLANET WL-U356A

Channel: 6

SSID: WLAN_AP

WEP: Disable

Tx Power: Level 0

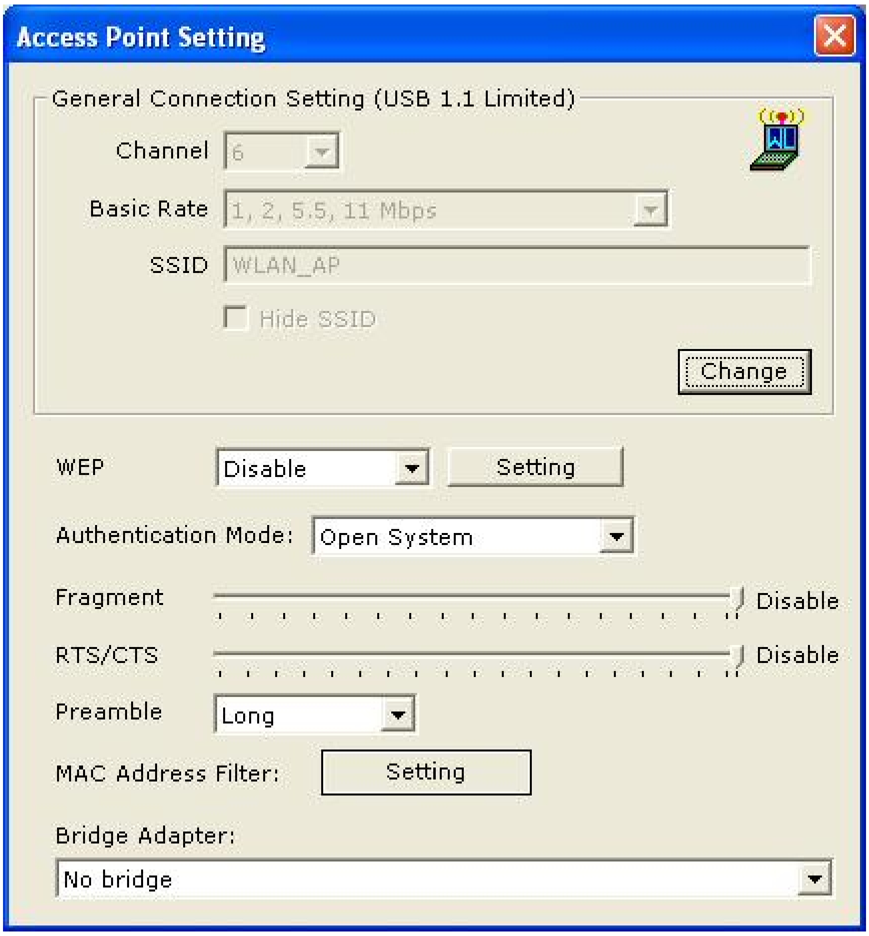
Tx Frame: 2

Rx Frame: 0

The default settings for the access point are as follows:

Channel: 6
SSID: WLAN_AP
WEP: Disable
Tx Power: Level 0

If you want to change the Access Point mode settings, please click “More Setting” button. When below dialog box appear, you may see “USB1.1 Limited” in first option. That is mean you connect WL-U356A to a USB1.1 port. When WL-U356A connects to USB1.1 port, the Basic Rate will limit to 802.11b standard. When WL-U356A connects to USB2.0 port, the message won’t appear and it can fully work with 802.11g/b standard.



Channel: 6
Basic Rate: 1, 2, 5.5, 11 Mbps
SSID: WLAN_AP
□ Hide SSID
WEP: Disable
Authentication Mode: Open System
Fragment: Disable
RTS/CTS: Disable
Preamble: Long
MAC Address Filter:
Bridge Adapter: No bridge

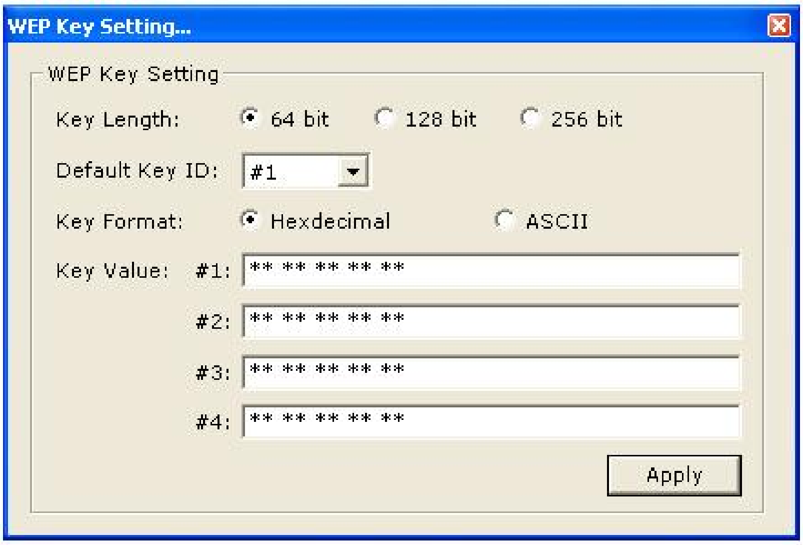
Click “Change” to configure the Access Point mode settings.

Parameters	**Description**
Channel	Select the channel you want to use.
Basic Rate	Select the applicable transfer rate.
SSID	Enter the desired SSID for the access point.
Hide SSID	Check to disable ESSID broadcast function.
Apply	After click “Change” button, the name of this button will become “Apply”. Please click “Apply” to submit the changes.
WEP	You may select “Enable” and refer to section 4.2 to configure the settings after click “Setting” button.
Authentication Mode	**Open System:** With the same WEP key between the stations, the stations don’t need to be authenticated, and this algorithm was set to default. **Shared Key:** With the same WEP key between the stations in this Authentication algorithm, this type will use packets with encryption by transferring a challenge text which will be acknowledge by both side of the stations. In order to choose which authentication algorithm will be used, you must

	know which one the station supports this algorithm first.
Fragmentation Threshold	It is a way of transmitting the packets that will be fragmented. Choose a setting within a range of 256 to 2432 bytes. It is recommended to fragment the packet when the link quality is bad, it is to prevent the wasting time of resending a long packet that is lost.
RTS/CTS Threshold	It is a station initiates the process by sending a RTS frame, the other ends receives the RTS and responds with a CTS frame, the station must receive a CTS frame before sending the data frame. This is to prevent the collisions by each station. Choose a setting within a range of 256 to 2432 bytes. It is recommended limiting a long packet to prevent each station waiting too long to transmit a data.
Preamble	The usage of the preamble is to limit the packet size of the data to transmit. The Default is long preamble.
MAC Address Filter	Please refer to section 4.3.
Bridge Adapter	If you have another Ethernet card installed in your computer, you can select the other Ethernet card as the bridge adapter. This will allow any wireless client that is connected to the access point to be bridged to the wired network that the other Ethernet card is connected to.

4.2 Configuring Encryption Security

Select “Enable” from the WEP drop-down list and click “Setting”.



WEP Key Setting...

WEP Key Setting

Key Length: ● 64 bit ○ 128 bit ○ 256 bit

Default Key ID: #1

Key Format: ● Hexdecimal ○ ASCII

Key Value: #1: ** ** ** ** **

#2: ** ** ** ** **

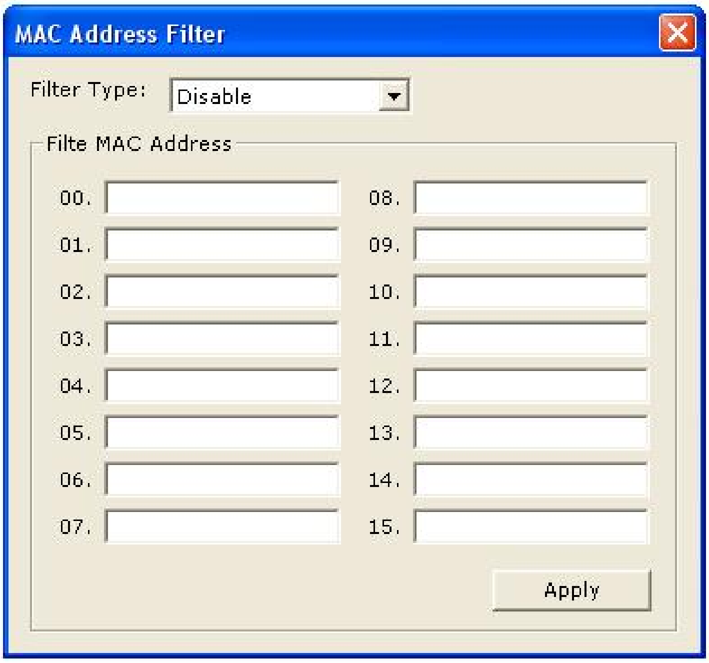
#3: ** ** ** ** **

#4: ** ** ** ** **

Parameters	**Description**
Key Length	Select the appropriate encryption key length.

Default Key ID	Select which of the four Key Values you want to use.
Key Format	Select either Hexadecimal (0-9, A-F) or ASCII (any number or letter).
Key Value	Enter the applicable key values. Up to four key values may be entered. Note the following rules when entering Key values: • **64-bit** key length requires **10** Hexadecimal characters (0-9, A-F) or **5** ASCII characters (any number or letter). • **128-bit** key length requires **26** Hexadecimal characters (0-9, A-F) or **13** ASCII characters (any number or letter). • **256-bit** key length requires **58** Hexadecimal characters (0-9, A-F) or **19** ASCII characters (any number of letter).
Apply	Save current settings.

4.3 Configuring MAC Address Filter



MAC Address Filter

Filter Type: Disable

Parameters	**Description**
Filter Type	**Disable**: disables MAC address filter. **Accept**: only accepts connection from the MAC address listed. (Connection attempts from MAC address not in the list will be rejected). **Reject**: only rejects connection from the MAC address listed. (Connection attempts from MAC address not in the list will be accepted, provided the client matches the encryption settings as well).
Apply	Click to save the changes.

Specification

Interface	Complaint with USB 2.0 / 1.1 standard	
Standards Conformance	Compliant with 802.11b / 802.11g	
Data Transfer Rate	IEEE802.11b：1 / 2 / 5.5 / 11Mbps (auto sensing) IEEE802.11g：6 / 9 / 12 / 18 / 24 / 36 / 48 / 54Mbps (auto sensing)	
Operating Mode	Infrastructure Mode, Ad-Hoc Mode and Access Point Mode.	
Security	WEP 64/128/256bit, WPA, WPA-PSK	
RF Modulation	OFDM with BPSK, QPSK, 16-QAM, 64QAM	
Media Access Protocol	CSMA / CA	
Operating Frequency / Channel	2.412~2.462GHz (FCC, Canada) / 11 Channels 2.412~2.472GHz (Euro ETSI) / 13 Channels 2.412~2.4835GHz (Japan, TELEC) / 14 Channels	
Output Power	15dBm (Typical)	
Operating Range	Up to 100 meters (328 feet) transmit and receive	
Receiver Sensitivity	802.11b 1 Mbps：-93dBm 2 Mbps：-91dBm 5.5 Mbps：-88dBm 11 Mbps：-85dBm	802.11g 6 Mbps : -90dBm 12 Mbps：-88dBm 18 Mbps : -85dBm 24 Mbps：-83dBm 36 Mbps：-79dBm 48 Mbps : -75dBm 54 Mbps：-72dBm
LED Indicators	ACT	
Power Consumption	Power Save mode = 103mA Standby mode = 2mA Transmit mode = 450mA Receive Mode = 180mA	
Operating systems	Windows XP, Windows2000, Windows Me, 98SE	
Environmental & Mechanical Characteristics		
Temperature	Operating: 32 °F ~ 131 °F (0 °C ~ 55 °C) Storage: -13 °F ~ 158 °F (-20 °C ~ 70 °C)	
Operating Humidity	Operating: 10% to 80% Non-Condensing Storage: 5% to 90% Non-Condensing	
Dimensions	109mm X 74mm X 40mm (L x W x H)	
Weight	195g	
Certifications	FCC, CE	

Appendix

This section provides some technology document of IEEE802.11g. Read the description below to know the standards about IEEE802.11g

✓ **What is the IEEE 802.11g standard?**
The IEEE 802.11g Wireless LAN standard subcommittee that formulates the standard for the industry. The objective is to enable wireless LAN hardware from different manufactures to communicate.

✓ **What IEEE 802.11 features are supported?**
The product supports the following IEEE 802.11 functions:

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

✓ **What is Ad-hoc?**
An Ad-hoc integrated wireless LAN is a group of computers, each with a WLAN adapter, Connected as an independent wireless LAN. Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

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

✓ **Can Wireless products support printer sharing?**
Wireless products perform the same function as LAN products. Therefore, Wireless products can work with Netware, Windows 2000/XP/Server 2003, or other LAN operating systems to support printer or file sharing.

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

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

✓ **What is Spread Spectrum?**

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

Glossary

Access Point: An internetworking device that seamlessly connects wired and wireless networks.

Ad-Hoc: An independent wireless LAN network formed by a group of computers, each with a network adapter.

ASCII: American Standard Code for Information Interchange, ASCII, is one of the two formats that you can use for entering the values for WEP key. It represents English letters as numbers from 0 to 127.

Authentication Type: Indication of an authentication algorithm which can be supported by the Access Point:
1. Open System: Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any station that requests authentication with this algorithm may become authenticated if 802.11 Authentication Type at the recipient station is set to Open System authentication.
2. Shared Key: Shared Key authentication supports authentication of stations as either a member of those who knows a shared secret key or a member of those who does not.

Backbone: The core infrastructure of a network, which transports information from one central location to another where the information is unloaded into a local system.

Bandwidth: The transmission capacity of a device, which is calculated by how much data the device can transmit in a fixed amount of time expressed in bits per second (bps).

Beacon: A beacon is a packet broadcast by the Access Point to keep the network synchronized. Included in a beacon are information such as wireless LAN service area, the AP address, the Broadcast destination addresses, time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

Bit: A binary digit, which is either -0 or -1 for value, is the smallest unit for data.

Browser: An application program that enables one to read the content and

interact in the World Wide Web or Intranet.

BSS: BSS stands for “Basic Service Set”. It is an Access Point and all the LAN PCs that associated with it.

Channel: The bandwidth which wireless Radio operates is divided into several segments, which we call them “Channels”. AP and the client stations that it associated work in one of the channels.

CSMA/CA: In local area networking, this is the CSMA technique that combines slotted time -division multiplexing with carrier sense multiple access/collision detection

(CSMA/CD) to avoid having collisions occur a second time. This works best if the time allocated is short compared to packet length and if the number of situations is small.

CSMA/CD: Carrier Sense Multiple Access/Collision Detection, which is a LAN access method used in Ethernet. When a device wants to gain access to the network, it checks to see if the network is quiet (senses the carrier). If it is not, it waits a random amount of time before retrying. If the network is quiet and two devices access the line at exactly the same time, their signals collide. When the collision is detected, they both back off and wait a random amount of time before retrying.

DHCP: Dynamic Host Configuration Protocol, which is a protocol that lets network administrators manage and allocate Internet Protocol (IP) addresses in a network. Every computer has to have an IP address in order to communicate with each other in a TCP/IP based infrastructure network. Without DHCP, each computer must be entered in manually the IP address. DHCP enables the network administrators to assign the IP from a central location and each computer receives an IP address upon plugged with the Ethernet cable everywhere on the network.

DSSS: Direct Sequence Spread Spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Dynamic IP Address: An IP address that is assigned automatically to a client station in a TCP/IP network by a DHCP server.

Encryption: A security method that uses a specific algorithm to alter the data transmitted, thus prevent others from knowing the information transmitted.

ESS: ESS stands for “Extended Service Set”. More than one BSS is configured to become Extended Service Set. LAN mobile users can roam between different BSSs in an ESS.

ESSID: The unique identifier that identifies the ESS. In infrastructure association, the stations use the same ESSID as AP’s to get connected.

Ethernet: A popular local area data communications network, originally developed by Xerox Corp., that accepts transmission from computers and terminals. Ethernet operates on a 10/100 Mbps base transmission rate, using a shielded coaxial cable or over shielded twisted pair telephone wire.

Fragmentation: When transmitting a packet over a network medium, sometimes the packet is broken into several segments, if the size of packet exceeds that allowed by the network medium.

Fragmentation Threshold: The Fragmentation Threshold defines the number of bytes used for the fragmentation boundary for directed messages. The purpose of "Fragmentation Threshold" is to increase the transfer reliability thru cutting a MAC

Service Data Unit (MSDU) into several MAC Protocol Data Units (MPDU) in smaller size. The RF transmission can not allow to transmit too big frame size due to the heavy interference caused by the big size of transmission frame. But if the frame size is too small, it will create the overhead during the transmission.

Gateway: a device that interconnects networks with different, incompatible communication protocols.

HEX: Hexadecimal, HEX, consists of numbers from 0 – 9 and letters from A – F.

IEEE: The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers, which is the largest technical professional society that promotes the development and application of electro-technology and allied sciences for the benefit of humanity, the advancement of the profession. The IEEE fosters the development of standards that often become national and international standards.

Infrastructure: An infrastructure network is a wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point which connects them to the rest of the network.

ISM Band: The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4GHz, in particular, is being made available worldwide.

MAC Address: Media Access Control Address is a unique hex number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Multicasting: Sending data to a group of nodes instead of a single destination.

Node: A network junction or connection point, typically a computer or workstation.

Packet: A unit of data routed between an origin and a destination in a network.

PLCP: Physical layer convergence protocol

PPDU: PLCP protocol data unit

Preamble Type: During transmission, the PSDU shall be appended to a PLCP preamble and header to create the PPDU. Two different preambles and headers are defined as the mandatory supported long preamble and header which interoperates with the current 1 and 2 Mbps DSSS specification as described in IEEE Std 802.11-1999, and an optional short preamble and header. At the receiver, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The optional short preamble and header is intended for application where maximum throughput is desired and interoperability with legacy and non-short-preamble capable equipment is not consideration. That is, it is expected to be used only in networks of like equipment that can all handle the optional mode. (IEEE 802.11b standard)

PSDU: PLCP service data unit

Roaming: A LAN mobile user moves around an ESS and enjoys a continuous connection to an Infrastructure network.

RTS: Request **T**o **S**end. An RS-232 signal sent from the transmitting station to the receiving station requesting permission to transmit.

RTS Threshold: Transmitters contending for the medium may not be aware of each other. RTS/CTS mechanism can solve this “Hidden Node Problem”. If the packet size is smaller than the preset RTS Threshold size, the RTS/CTS mechanism will NOT be enabled.

SSID: Service Set Identifier, which is a unique name shared among all clients and nodes in a wireless network. The SSID must be identical for each clients and nodes in the wireless network.

Subnet Mask: The method used for splitting IP networks into a series of sub-groups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

TCP/IP: Transmission Control Protocol/ Internet Protocol. The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network, i.e. intranet or internet. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

Throughput: The amount of data transferred successfully from one point to another in a given period of time.

WEP: Wired Equivalent Privacy (WEP) is an encryption scheme used to protect wireless data communication. To enable the icon will prevent other stations without the same WEP key from linking with the AP.