IEEE 802.11a/b/g Atheros Wireless USB 2.0 Adapter



User's Manual Version: 1.0

Table of Contents

1	INTR	ODUCT	ION	4
	1.1 1.2 1.3	PACKAG	ES & BENEFITS E CONTENTS APTER DESCRIPTION	. 5
	1.4	SYSTEM	REQUIREMENTS	. 5
	1.5		TIONS	
	1.6	NETWOR	RK CONFIGURATION	7
2	INST	ALL DR	IVERS & CLIENT UTILITY	9
	2.1	BEFORE	You Begin	. 9
	2.2	INSTALL	ING THE DRIVERS	9
3	USIN			15
	3.1		IT STATUS	
	3.2		MANAGEMENT	
	3.2.1		for available networks	
	3.2.2		te a New Profile	
	3.2.3		rity	
	-		Security Disabled	
	-	-	WPA – TLS, TTLS	
		2.3.3 2.3.4	WPA – PEAP (EAP-GTO)	ר זי
			WPA – LEAP	
			WPA – Passphrase	
			802.1x – TLS, TTLS	
		2.3.8	802.1x – PEAP (EAP-GTC)	
	_		802.1x – PEAP (EAP-MSCHAP-V2)	32
	3.:		802.1x – LEAP	
	3.:	2.3.11	Pre-Shared Key (Static WEP)	36
	3.2.4		nced Settings	
	3.		Infrastructure Settings	
			Ad Hoc Settings	
	3.3		STICS	
	3.4		/ DISABLE RADIO	
	3.5		TRAY ICON	
	3.6		SETTINGS	
4			THE DRIVERS & CLIENT UTILITY	
A	PPENDI	X A – SF	PECIFICATIONS	47
A	PPENDI	X B – FC	C INTERFERENCE STATEMENT	48

Revision History

Version	Date	Notes
1.0	June 20, 2005	Initial Version

1 Introduction

This is a wireless USB 2.0 adapter that supports dual-band 802.11a/b/g (2.4GHz & 5GHz) radio operation. It provides a high-speed wireless connection with data rate up to 108Mbps.

To protect your wireless connectivity, the high-speed wireless USB adapter can encrypt all wireless transmissions through 64/128/152-bit WEP data encryption and also supports WPA. Dynamic Frequency Selection (DFS) puts your network on the cleanest channel in your location. With the high-speed wireless USB adapter, you will experience the best wireless connectivity available.

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

Features	Benefits
High Speed Data Rate up to 108Mbps	Capable of handling heavy data payloads
(Super A/G)	such as MPEG video streaming.
High Output Power up to 23 dBm	More high power can advance the distance.
Standard (AES), Temporal Key Integrity	Powerful data security (802.11i).
Protocol (TKIP) and Wired and	
Equivalent Privacy (WEP)	
IEEE802.1x Client Support	Enhances authentication and security.
Support for 802.11e standard	Quality of Service support (QoS) for wireless
	multimedia enhancements
Advanced Power Management	Low power consumption (up to 98%)in power
	saving mode
Support eXtended Range technology	eXtended Range technology offers Wi-Fi
	products twice the range of existing designs

1.1 Features & Benefits

1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- > One Wireless LAN USB Adapter
- One USB Cable
- > One Quick Installation Guide
- One CD-ROM with User's Manual Included

1.3 USB Adapter Description

The USB adapter is a standard USB adapter that fits into any USB interface. The USB adapter has a LED indicator and an external high-sensitivity dipole antenna.



1.4 System Requirements

The following are the minimum system requirements in order to use the USB adapter.

- > PC/AT compatible computer with a USB interface.
- ➤ Windows 98SE/ME/ /2000/XP operating system.
- 20 MB of free disk space for installing the USB adapter driver and utility program.

1.5 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

a) Difficult-to-wire environments

There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

b) Temporary workgroups

Consider situations in parks, athletic arenas, exhibition centers, disasterrecovery, temporary offices and construction sites where one wants a temporary WLAN established and removed.

c) The ability to access real-time information Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

d) Frequently changed environments Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

e) Small Office and Home Office (SOHO) networks SOHO users need a cost-effective, easy and quick installation of a small network.

f) Wireless extensions to Ethernet networks

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

g) Wired LAN backup

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

h) Training/Educational facilities

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.

1.6 Network Configuration

To better understand how the wireless LAN products work together to create a wireless network, it might be helpful to depict a few of the possible wireless LAN PC card network configurations. The wireless LAN products can be configured as:

- a) Ad-hoc (or peer-to-peer) for departmental or SOHO LANs.
- b) Infrastructure for enterprise LANs.

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



This is the simplest network configuration with several computers equipped with the PC Cards that form a wireless network whenever they are within range of one another. In ad-hoc mode, each client is peer-topeer, would only have access to the resources of the other client and does not require an access point. This is the easiest and least expensive way for the SOHO to set up a wireless network. The image below depicts a network in ad-hoc mode.

b) Infrastructure Mode

The infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between two computers has to be via the AP. It doesn't matter if the AP is stand-alone or wired to an Ethernet network. If used in stand-alone, the AP can extend the range of independent wireless LANs by acting as a repeater, which effectively doubles the distance between wireless stations. The image below depicts a network in infrastructure mode.



Version 1.0

2 Install Drivers & Client Utility

2.1 Before You Begin

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

During the installation, Windows 98SE/ME/2000/XP may need to copy systems files from its installation CD. Therefore, you may need a copy of the Windows installation CD at hand before installing the drivers. On many systems, instead of a CD, the necessary installation files are archived on the hard disk in C:\WINDOWS \OPTIONS\CABS directory.

2.2 Installing the Drivers

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

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



- Click on the **Next** button to continue.
 The Setup Wizard will then allow you to install the driver & utility or just the driver. Select the first option: Install Client Utilities and Driver.

802.11 WLAN Client Installation	on Program	X
Setup Type Select the setup type that best suit		
	Click the type of setup you prefer. Install Client Utilities and Driver (recommended) Choose this option to install the driver Only Choose this option to install the recommended option.	
	< <u>B</u> ack <u>N</u> ext > Cancel	1

- 5. Click on the **Next** button to continue.
- 6. This message informs you that the system must be restarted after the installation is complete.

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

7. Click on the Yes button to continue.

802.11 WLAN Client Installation	n Program	×
Choose Destination Location		
	on program will install the files.	
	The installation program will install the client utilities in the following location:	
	-Destination Folder	
	C:\Program Files\802.11 WLAN Biowse	
	< <u>B</u> ack <u>Next</u> Cancel	

8. Click on the **Browse** button to select another drive or folder to install the drivers, and then click on the **Next** button. If you would like to use the default destination folder, click on the **Next** button.

802.11 WLAN Client Installation	n Program	\mathbf{X}
Select Program Folder Select a program folder.		
	The installation program will add program icons to the Program Folder listed below. You may type a new folder name or select one from the Existing Folders list. Program Folder: WLAN Dual USB Existing Folders: Accessories Acronis Administrative Tools Games NetIQ Chariot SoundMAX Startup WinRAR	
InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel	1

9. Select a program folder for the Start menu, or use the default setting: 802.11

802.11 WLAN Client Installation Progra	am	×
802.11 WLAN Client Installation Program		
IMPORTANT: Please Read!		
On Windows XP, you can configure your 802. 802.11 Client Utility (ACU) or a third party supp provide all of the functionality available in ACU (Please note that a patch from Microsoft might security.) On the next screen, select whether you want t configure your client adapter. NOTE: If you select a third party supplicant, so To activate those features, you must install AC	plicant. Because third party tools may not J, 802.11 recommends that you use ACU. to required to use the Microsoft tool with WPA to use ACU or a third party supplicant to pome of the ACU features will not be available.	
nstallShield		
	<back next=""> Cancel</back>]

WLAN. Click on the Next button to continue.

10. The message depicted above informs you about configuring this device through the 802.11 Client Utility (ACU) or a third party supplicant. If you choose to use a third party supplicant, some of the ACU features will not be available. Click on the **Next** button to continue.

802.11 WLAN Client Installation Program	
Choose Configuration Tool	
Which tool will you use to configure your client adapter?	
802.11 WLAN NIC utility and Supplicant.	
O Third Party Supplicant	
InstallShield	Next > Cancel

 Select one of the options. However, it is recommended to select the first option: 802.11 WLAN Client Utility and 802.1x Supplicant. Click on the Next button to continue.

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

- 12. At this point, carefully insert the device into the PCMCIA slot of your computer, and click on the **OK** button.
- 13. Windows will automatically detect the device and display the **Found New Hardware Wizard**, as the image depicts below. It will ask you to connect to the Windows Update website, to search for software. Select **No, not this time**, and click on the **Next** button.

Found New Hardware Wizard		
	Welcome to the Found New Hardware Wizard Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission). <u>Read our privacy policy</u>	
	Can Windows connect to Windows Update to search for software? Yes, this time only Yes, now and every time I connect a device No, not this time	
and the second	Click Next to continue.	
< Back Next > Cancel		

- 14. Once again the **Found New Hardware** Wizard will ask you to install software. Click on the **Cancel** button to continue.
- 15. If you are using Windows XP, you will see a message regarding Windows Logo Testing, click on the **Continue Anyway** button to continue.

Har dwa	re Installation
1	The software you are installing for this hardware: WLAN USB 2.0 Wireless Adapter Bootloader Download has not passed Windows Logo testing to verify its compatibility with Windows XP. (<u>Tell me why this testing is important.</u>) 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.
	Continue Anyway STOP Installation

16. Once again, you will see a message regarding Windows Logo Testing, click on the **Continue Anyway** button to continue.

Hardware	a Installation
	The software you are installing for this hardware: WLAN USB 2.0 Wireless Network Adapter 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.
	Continue Anyway STOP Installation

17. A message will then appear indicating that the installation process is complete Click on the **OK** button to reboot the system.

3 Using the Client Utility

After a successful installation you will see the Cardbus adapter **Client Utility** in the Windows Program group called **802.11 WLAN**.

To run the Client Utility click **Start > Programs > WLAN DUAL USB**. You will then see the Client Utility icon in the system tray of your computer.

To open the Client Utility, right click on the icon in the system tray, and then select **Open 802.11 WLAN Client Utility**.

Exit Qpen 802.11 WLAN Client Utility... Disable Radio Manual LEAP Login Reauthenticate Show Connection Status Select Profile

3.1 Current Status

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

Total 802.11
AG .
Address: 192.168.2.233
Channel: 11
cryption: None
Excellent
Advanced

 Profile Name: Displays the name of this profile. One device can have many profiles, but only one profile can be loaded at a time.

Client Utility -

Note: The profile name and network name (SSID) are not the same.

- State: This indicates the state of the client, associated or not associated.
 Wireless Mode: Displays the 802.11 mode such as: 2.4GHz 11 Mbps,
- 2.4GHz 54 Mbps, 2.4GHz 108Mbps, 5GHz 54Mbps or 5GHz 108Mbps.
 Network Type: Displays the type of network, such as: Infrastructure or
- Ad-hoc.
- Server Based Authentication: Displays information about the authentication method.
- > **IP address**: Displays the IP address of this device.
- Current Channel: Displays the channel at which this device is connected.
- > Current Channel: Displays the type of encryption used.
- Signal Strength: Displays the strength of the signal.

Click on the **Advanced** button to view more details about the current status. This window includes information such as: network name (SSID), AP MAC address, power save mode, power levels, signal strength, noise level, channel, frequency, and channel set (country). Click on the **OK** button to close the window.



3.2 Profile Management

The second tab displayed is the **Profile Management** tab. This tab is used to create a new profile, modify an existing profile, remove an existing profile, and activate an existing profile.

n Options Help rent Status Profile Managemer	t Diagnostics	
Default		New
🐚 wlan		Modify
		Remove
		Activate
r Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name 1 (SSID1):		Export
Network Name 2 (SSID2):		Scan
Network Name 3 (SSID3):	<empty></empty>	
Auto Select Profiles		Order Profiles.

3.2.1 Scan for available networks

Click on the **Scan** button to view a list of available infrastructure and ad-hoc networks. This table lists the network name, encryption key if required, signal strength, channel, and wireless mode.

Network Name (SSIE HotSpot)) 🔞 Supe	er XR Signal Strengtl 11 24 dB		Wireless Mode 2.4 GHz 54 Mbps
i mistest	6	11] 7 dB	1 5	2.4 GHz 54 Mbps 2.4 GHz 54 Mbps
R WLAN		11 dB	11	2.4 GHz 11 Mbps

If you would like to associate with a specific network, select the network name (SSID) and then click on the **Activate** button. You will then get connected to the network if you have the correct permission keys.

3.2.2 Create a New Profile

Multiple profiles can be created for different Network Names (SSIDs). This allows a user to quickly associate with another network, instead of entering the credentials each time.

BO2.11 WLAN Client Utilit on Options <u>H</u> elp urrent Status Profile Managemer		
Default		New
wian		Modify
		Remove
		Activate
🕝 Details		
Network Type:	Infrastructure	Import
Security Mode:	None	
Network Name 1 (SSID1):	WLAN	Export
Network Name 2 (SSID2):	<empty></empty>	Scan
Network Name 3 (SSID3):	<empty></empty>	
Auto Select Profiles		Order Profiles

Click on the **New** button to create a new profile. You will then see the **General** tab of the profile management window.

rofile M	lanagement		2
General	Security Advanced		
	Profile Settings Profile Name: Client Name:	profile1 FAE-9PHBRXC24JH	
	Network Names SSID1:	wireless	
	SSID2:		
	SSID3:		
			OK Cancel

> Profile Name: Enter a name for this profile; this can be any name that

you may associate with your network. This feature comes in handy when you need to work at several locations where there are different network settings. Using this you can configure a different profile for each of your networks.

- > Client Name: Enter any name to describe the profile.
- SSID1: Enter the SSID of the network. The SSID is a unique name shared among all points in your wireless network. The SSID must be identical for all points in the network, and is case-sensitive.
- Click on the **OK** button to continue.

3.2.3 Security

The next tab displayed is the **Security** tab. Here you can configure the authentication and encryption method that is used on your network. There are five types of security methods available: none, WPA, WPA-PSK, 802.1x, Pre-shared WEP key. The configuration steps for each method are described below.

3.2.3.1 Security Disabled

If your network does not require any security methods, then select **None** in the security tab, and then click on the **OK** button.

	Security	Advanced		
Se	et Security	Options		
	0	WPA	WPA EAP Type:	LEAP
	0	WPA Passphrase		
	0	802.1x	802.1x EAP Type:	LEAP
	0	Pre-Shared Key (Stati	ic WEP)	
	۲	None		
		Configure		Allow Association to Mixed Cells

3.2.3.2 WPA – TLS, TTLS

WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity-

checking feature which makes sure that keys haven't been tampered with.

Select the **WPA** radio button, and then select **EAP – TLS** or **EAP – TTLS** from the drop-down list. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.

WPA WPA EAP Type: EAP-TLS EAP-TLS WPA Passphrase EAP-TTLS	~
PEAP (EAP-GTC)	
802.1x 802.1x EAP Type: PEAP (EAP-MSCHAP \ LEAP	(2)
Pre-Shared Key (Static WEP)	
◯ None	
Configure Allow Association to	Mixed Cells

Click on the **Configure** button to configure the TTLS settings.

<any></any>	
User Information for EAF	P-TTLS Authentication
User Name:	james
Password:	
Confirm Password:	

➤ Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.

- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the **Advanced** button.

Advanced Configuration		? 🛛
Specific Server or Domain: Login Name:	james	
	DK Cancel	

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.3 WPA – PEAP (EAP-GTC)

PEAP (EAP-GTC) was standardized along with EAP in RFC 2284. EAP-GTC allows the exchange of clear text authentication credentials across the network. The GTC method does provide a way to move a simple username and password from client to server using an EAP method, so it can be used to provide an authentication method. Naturally, if EAP-GTC is used to transport reusable passwords, it must be used inside a tunnel for protection and server authentication. EAP-GTC can be used with both TTLS and PEAP.

Select the **WPA** radio button, and then select **PEAP (EAP-GTC)** from the dropdown list.

rofile Management		?
General Security Advanced		
⊙ WPA	WPA EAP Type:	EAP-TLS EAP-TTLS
 802.1x Pre-Shared Key (Static WEP) None 	802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP
Configure		Allow Association to Mixed Cells
		OK Cancel

Click on the **Configure** button to configure the PEAP (EAP-GTC) settings.

<any></any>	
User Name:	james
Set Passwo	rd
O Toker	1
💽 Statio	: Password

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Set Password: Select Token or Static Password radio button. The default setting is Static Password.

Click on the Advanced button.

Advanced Configuration		? 🗙
Specific Server or Domain: Login Name:	james	
	OK Cancel	

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.4 WPA – PEAP (EAP-MSCHAP-V2)

The PEAP (EAP-MSCHAP V2) authentication type is based on EAPTLS authentication, but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key, which is derived from the device and RADIUS server, to encrypt data.

Select the WPA radio button, and then select PEAP (EAP-MSCHAP-V2) from the drop-down list.

eneral Security Advanced		
Set Security Options		
⊙ WPA	WPA EAP Type:	PEAP (EAP-MSCHAP V2)
🔘 WPA Passphrase		EAP-TLS EAP-TTLS PEAP (EAP-GTC)
○ 802.1×	802.1x EAP Type:	PEAP (EAP-MSCHAP V2) LEAP
O Pre-Shared Key (Static WEP)		
🔿 None		
Configure		Allow Association to Mixed Cells

Click on the **Configure** button to configure the PEAP (EAP-MSCHAP-V2) settings.

rusted Root Certification	Authorities	
<any></any>		
liser Information for PEA	P (EAP-MSCHAP V2) Authentication	
User Name:	james	ĵ
Password:	••••	
Confirm Password:	••••	16

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the Advanced button.

Advanced Configuration	? 🛛
Specific Server or Domain:	
Login Name:	james
	OK Cancel

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.5 WPA – LEAP

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN.

Select the WPA radio button, and then select LEAP from the drop-down list.

Profile Management		? 🛛
General Security Advanced		
Set Security Options		
⊙ WPA	WPA EAP Type:	
🔿 WPA Passphrase		EAP-TLS EAP-TTLS PEAP (EAP-GTC)
◯ 802.1x	802.1x EAP Type:	PEAP (EAP-MSCHAP V2) LEAP
O Pre-Shared Key (Static WEP)		
◯ None		
Configure		Allow Association to Mixed Cells
		OK Cancel

Click on the **Configure** button to configure the LEAP settings.

LEAP Settings	
LEAP username and passwo	rd settings
OUse Temporary Use	er Name and Password
() Manually	Prompt for LEAP User Name and Password
🕞 Use Saved User Na	me and Password
User Name:	
Password:	
Confirm Password:	
Domain:	
🔽 No Netwo	Vindows Logon Domain with User Name ork Connection Unless User Is Logged In tication Timeout Value (in seconds) OK Cancel

> Use Temporary User Name and Password: Select this radio button for

a temporary user name and password. This will manually prompt for the user name and password.

- Use Saved User Name Password: Select this radio button if the user name and password will be saved in this profile.
- **User Name:** Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- > **Confirm Password:** Re-type the password.

Click on the **OK** button to return to the previous window

3.2.3.6 WPA – Passphrase

neral S	ecurity	Advanced		
Set	Security	Options		
	0	WPA	WPA EAP Type:	LEAP
	۲	WPA Passphrase		
	0	802.1x	802.1x EAP Type:	LEAP
	0	Pre-Shared Key (Stati	o WEP)	
	0	None		
	Г	Configure		Allow Association to Mixed Cells

Select the WPA Passphrase radio button and then click on the Configure button.

Define WPA Pre-Shared Key	? 🔀
Enter a WPA Passphrase between 8 and 64 characters long.	
ОК	Cancel

 Enter a WPA passphrase. For ASCII text, enter 8-63 characters, for hexadecimal enter 64 characters).

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.7 802.1x – TLS, TTLS

802.1X provides an authentication framework for wireless LANs allowing a user to be authenticated by a central authority. 802.1X uses an existing protocol called EAP. EAP (Extensible Authentication Protocol) is an extension to the PPP protocol that enables a variety of authentication protocols to be used. It passes through the exchange of authentication messages, allowing the authentication software stored in a server to interact with its counterpart in the client.

ofile M	anagem	ent			?
General	Security	Advanced			
S	et Security	Options			
	0	WPA	WPA EAP Type:	LEAP	~
	0	WPA Passphrase			
	۲	802.1x	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)	~
	0	Pre-Shared Key (Static WEP)		EAP-TLS EAP-TTLS	
	0	None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
		Configure		LEAP Allow Association to Mixed C	Cells
				ОК	Cancel

Select the **802.1x** radio button, and then select **EAP – TLS** or **EAP – TTLS** from the drop-down list. TLS (Transport Layer Security) is an IETF standardized authentication protocol that uses PKI (Public Key Infrastructure) certificate-based authentication of both the client and authentication server.

Click on the **Configure** button to configure the TTLS settings.

<any></any>		2
User Information for EA	P-TTLS Authentication	
User Name:	james	
Password:		
Confirm Password:		

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- **User Name:** Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the **Advanced** button.

Advanced Configuration		? 🔀
Specific Server or Domain: Login Name:	james	
	OK Cancel	

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the OK button to return to the previous window. Once again, click on

the **OK** button to return to the Profile Management window.

3.2.3.8 802.1x – PEAP (EAP-GTC)

PEAP (EAP-GTC) was standardized along with EAP in RFC 2284. EAP-GTC allows the exchange of clear text authentication credentials across the network. The GTC method does provide a way to move a simple username and password from client to server using an EAP method, so it can be used to provide an authentication method. Naturally, if EAP-GTC is used to transport reusable passwords, it must be used inside a tunnel for protection and server authentication. EAP-GTC can be used with both TTLS and PEAP.

Select the **802.1x** radio button, and then select **PEAP (EAP-GTC)** from the dropdown list.

Profile M	anagem	ent			? 🔀
General	Security	Advanced			
S	et Security	Options			_
	0	WPA	WPA EAP Type:	LEAP	
	0	WPA Passphrase			
	۲	802.1×	802.1x EAP Type:	PEAP (EAP-GTC)	
	0	Pre-Shared Key (Static WEP)		EAP-TLS EAP-TTLS	
	0	None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
		Configure		LEAP Allow Association to Mixed Cells	
				ОК	Cancel

Click on the **Configure** button to configure the PEAP (EAP-GTC) settings.

Define PEAP (EAP-GT	C) Configuration	? 🛛
Trusted Root Certifi	cation Authorities	
<any></any>		~
User Name: james Set Password O Token O Static Passw		Cancel

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- **User Name:** Enter the user name for the certificate authority.
- Set Password: Select Token or Static Password radio button. The default setting is Static Password.

Click on the **Advanced** button.

Advanced Configuration		? 🔀
Specific Server or Domain: Login Name:	james]
	OK Cancel	

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.9 802.1x – PEAP (EAP-MSCHAP-V2)

The PEAP (EAP-MSCHAP V2) authentication type is based on EAPTLS authentication, but uses a password instead of a client certificate for authentication. PEAP (EAP-MSCHAP V2) uses a dynamic session-based WEP key, which is derived from the device and RADIUS server, to encrypt data.

Select the **802.1x** radio button, and then select **PEAP (EAP-MSCHAP-V2)** from the drop-down list.

Profile M	anagem	ent			? 🗙
General	Security	Advanced			
S	et Security	Options			
	0	WPA	WPA EAP Type:	LEAP	
	0	WPA Passphrase			
	۲	802.1x	802.1x EAP Type:		
	0	Pre-Shared Key (Static WEP)		EAP-TLS EAP-TTLS	
	0	None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP	
		Configure		Allow Association to Mixed Cells	
					Cancel

Click on the **Configure** button to configure the PEAP (EAP-MSCHAP-V2) settings.

<any></any>		~
User Information for PEA	P (EAP-MSCHAP V2) Authentication	
User Name:	james	
Password:	•••••	
Confirm Password:	•••••	

- Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the Advanced button.

Advanced Configuration		? 🔀
Specific Server or Domain: Login Name:		
Lugin Name.	james	
	OK Cancel	

- Specific Server or Domain: Leave the server name blank for the client to accept a certificate from any server with a certificate signed by the authority listed in the Network Certificate Authority drop-down list. (Recommended). You can also enter the domain name of the server from which the client will accept a certificate.
- **Login Name:** Enter the login name if required.

Click on the **OK** button to return to the previous window. Once again, click on the **OK** button to return to the Profile Management window.

3.2.3.10 802.1x – LEAP

LEAP (Lightweight Extensible Authentication Protocol) also known as Cisco-Wireless EAP provides username/password-based authentication between a wireless client and a RADIUS server. LEAP is one of several protocols used with the IEEE 802.1X standard for LAN port access control. LEAP also delivers a session key to the authenticated station, so that future frames can be encrypted with a key that is different than keys used by others sessions. Dynamic key delivery eliminates one big vulnerability; static encryption keys that are shared by all stations in the WLAN.

Select the **802.1x** radio button, and then select **LEAP** from the drop-down list.

rofile M	ofile Management			? ×	
General	Security	Advanced			
S	et Security	Options			-
	0	WPA	WPA EAP Type:	LEAP	
	0	WPA Passphrase			
	۲	802.1x	802.1x EAP Type:	LEAP	
	0	Pre-Shared Key (Static WEP)	EAP-TLS EAP-TTLS	
	0	None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
		Configure		LEAP Allow Association to Mixed Cells	
				ОК С	ancel

Click on the **Configure** button to configure the LEAP settings.

LEAP Settings		? 🔀
LEAP username and passwor	rd settings	
Use Temporary Use	r Name and Password	
O Manually F	Prompt for LEAP User Name and Password	
💿 Use Saved User Nar	ne and Password	-
User Name:		
Password:		
Confirm Password:		
Domain:		
🗹 No Netwo	indows Logon Domain with User Name rk Connection Unless User Is Logged In tication Timeout Value (in seconds) OK Cancel	

- Use Temporary User Name and Password: Select this radio button for a temporary user name and password. This will manually prompt for the user name and password.
- Use Saved User Name Password: Select this radio button if the user name and password will be saved in this profile.
- > User Name: Enter the user name for the certificate authority.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- **Confirm Password:** Re-type the password.

Click on the **OK** button to return to the previous window

3.2.3.11 Pre-Shared Key (Static WEP)

You may select 64, 128 or 152 bit WEP (Wired Equivalent Privacy) key to encrypt data (Default setting is Disable). WEP encrypts each frame transmitted from the radio using one of the Keys from a panel. When you use WEP to communicate with the other wireless clients, all the wireless devices in this network must have the same encryption key or pass phrase.

Set Security				
	WPA	WPA EAP Type:	PEAP (EAP-GTC)	×
0	WPA Passphrase			
0	802.1x	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)	~
۲	Pre-Shared Key (Static Wi	EP)		
0	None			
	Configure		Allow Association to Mixed	Cells

Select the **Pre-Shared Key (Static WEP)** radio button and click on the **Configure** button.

Key Entry	Hexadecimal (0-9, A-F)	ASCII Text (all keyboard characters)
Encryption Ke	ws.	
	Transmit Key	WEP Key Size:
WEP Key		64 128 152
WEP Key	2. ()	
WEP Key	3. ()	
WEP Key	4: 0	000
- Key Entry: Select Hexadecimal or ASCII depending on the WEP key that is used.
- **WEP Key Size:** Select **64**, **128**, or **152** bit WEP key size.
- > Transmit Key: Enter the WEP key in the four WEP key text boxes.

Click on the **OK** button to return to the previous window

3.2.4 Advanced Settings

Click on the **Advanced** tab in the Profile Management section. Here you can configure the transmit power level, wireless mode, power save mode, and network type.

3.2.4.1 Infrastructure Settings

Transmit Power Level	Power Save Mode:	Off	~
802.11b/g: 100 mW 💌	Network Type:	Infrastructure	~
802.11a: 100 mW 💌	802.11b Preamble:	Short & Long	🔘 Long Only
 Wireless Mode ✓ 5 GHz 54 Mbps ✓ 2.4 GHz 54 Mbps ✓ 2.4 GHz 11 Mbps ✓ Super A/G 	Wireless Mode Whe 5 GHz 54 Mb 5 GHz 108 Mi 2.4 GHz 54/1	bps Channel	
802.11 Authentication Mode		P	referred APs

- ➤ Transmit Power level: Select a transmit power level from the dropdown list for the 802.11 a/b/g radio.
- > Wireless Mode: Place a check in the preferred frequency and data rates.
- Power Save Mode: Select Maximum, Normal, or Off from the dropdown list. Selecting Maximum will save the most power; this is recommended if using a laptop running on battery. For other instances, use the Normal of Off setting.
- > Network Type: Select Infrastructure from the drop-down list.
- ➤ 802.11 Preamble: This setting should be the same as the access point. If you are not sure of that setting, select Short & Long.
- Preferred APs: Click on this button to add specific access points to this profile. Then enter the MAC addresses of the specific access points and then click on the OK button to return to the previous window.

Preferred Access Points	? 🛛
Specified Access Point MAC Addresses]
Access Point 1:	
Access Point 2:	
Access Point 3:	
Access Point 4:	
	OK Cancel

3.2.4.2 Ad Hoc Settings

- Transmit Power Level	Power Save Mode:	Off	
802.11b/g: 100 mW 💌	Network Type:	Ad Hoc	~
802.11a: 100 mW 💉	802.11b Preamble:	Short & Long	Eong Only
Wireless Mode	Wireless Mode Whe	n Starting Ad Hoc Net	work
2.4 GHz 54 Mbps 2.4 GHz 11 Mbps	○ 5 GHz 54 Mb ○ 5 GHz 108 M	bps Channel:	Auto 💌
Super A/G	⊙ 2.4 GHz 54/1	I Mbps	
802.11 Authentication Mode		P	referred APs

- Transmit Power level: Select a transmit power level from the dropdown list for both the 802.11 b/g and 802.11a radios.
- Wireless Mode: Place a check in the preferred frequency and data rates.
- > Network Type: Select Ad hoc from the drop-down list.
- 802.11 Preamble: This setting should be the same as the access point. If you are not sure of that setting, select Short & Long.

Click on the **OK** button to return to the previous window

3.3 Diagnostics

The third tab displayed is the **Diagnostics** tab. This tab displays the number of transmitted and received packets.

tion Options Help	ity - Current Profile: wlan	
Current Status Profile Managem	ent Diagnostics	
- Transmit	·	Adapter Information
Multicast Packets		
Broadcast Packet	s: 345	Advanced Statistics
Unicast Packets:	3885	Advanced Statistics
Total Bytes:	147357	
Receive		
Multicast Packets	49	
Broadcast Packet	s: 66429	
Unicast Packets:	45	
Total Bytes:	8134792	

Click on the **Adapter Information** button to view information about the Cardbus adapter such as: card name, MAC address, driver name, driver version, and driver date.

Adapter Information	1.	? 🛛
Card Name: MAC Address:	WLAN USB 2.0 Wireless Network Adapter 00-03-7F-BE-F0-E3	
Driver:	C:\WINDOWS\system32\DRIVERS\ar5523.sys	
Driver Version:	1.0.0.114	
Driver Date:	06 Oct 2004 16:52:28	
Client Name:	FAE-9PHBRXC24JH	
	OK	

Click on the \mathbf{OK} button to return to the previous window

Click on the **Advanced Statistics** button to view detailed statistics about transmit and receive frames.

Transmit			
Frames Transmitted OK:	4299	RTS Frames:	0
Frames Retried:	231	CTS Frames:	0
Frames Dropped:	1931	No CTS Frames:	0
No ACK Frames:	0	Retried RTS Frames:	0
ACK Frames:	4299	Retried Data Frames:	231
Receive			
Beacons Received:	0	Authentication Time-Out:	0
Frames Received OK:	92993	Authentication Rejects:	0
Frames Received with Errors:	0	Association Time-Out:	0
CRC Errors:	1449	Association Rejects:	0
Encryption Errors:	0	Standard MIC OK:	0
Duplicate Frames:	7	Standard MIC Errors:	0
AP Mismatches:	0	CKIP MIC OK:	0
Data Rate Mismatches:	0	CKIP MIC Errors:	0

Click on the OK button to return to the previous window

Version 1.0

3.4 Enable / Disable Radio

To **disable** the radio, click on **Action** in the menu bar, and then click on **Disable Radio**.

)isable <u>R</u> adio	anagement [Diagnostics		
isable <u>T</u> ray Icon	anagement	hagnosucs		
<u>1</u> anual LEAP Login	Profile Name:	wlan		Total 802
teauthenticate	Link Status:	Associated		AG
. <u>×</u> it				
	Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	192.168.2.233
	Network Type:	Infrastructure	Current Channel:	11
Server Base	ed Authentication:	None	Data Encryption:	None
	Signal Strength:	*******		Excellent

You will then see a confirmation message "The RF signals for the following network card(s) have been successfully disabled".

tion <u>O</u> ptions			
Current Status	Profile Management D)iagnostics	
	Profile Name:		Total 8021
802.	11 WLAN Client Util	lity	N 1
(i		he following network card(s) have	e been successfully disabled:
(i		the following network card(s) have eless Network Adapter	e been successfully disabled:
Q.		eless Network Adapter	e been successfully disabled: No Link

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

To **enable** the radio, click on **Action** in the menu bar, and then click on **Enable Radio**.

A 802.11 WLAN C	lient Utility - (Current Profile: wlan		
Action Options Help				
Enable <u>R</u> adio Disable <u>T</u> ray Icon	anagement [Diagnostics		
Manual LEAP Login	Profile Name:			Total 802.11
<u>R</u> eauthenticate	 Link Status:			AG.
E <u>x</u> it	Wireless Mode:		IP Address:	
	Network Type:		Current Channel:	
Server Based	d Authentication:		Data Encryption:	
	Signal Strength:	Ϋ́.		No Link
	Radio Status:	Software Disabled		Advanced

You will then see a confirmation message "The RF signals for the following network card(s) have been successfully enabled".

🔥 802.11 WLAN Client Utility - Current Profile: wlan	×
Action Options Help	
Current Status Profile Management Diagnostics	
Profile Name: wlan	
802.11 WLAN Client Utility	
The RF signals for the following network card(s) have been successfully enabled: WLAN USB 2.0 Wireless Network Adapter	
Signal Strength: No Link	
Advanced	

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

3.5 Disable Tray Icon

To disable the tray icon, click on **Action** in the menu bar, and then click on **Disable Tray Icon**.

Disable <u>R</u> adio	anagement	Diagnostics		
Disable <u>T</u> ray Icon Manual LEAP Login	Profile Name			Total 80
<u>R</u> eauthenticate	Link Status	Associated		AG
Exit	Wireless Mode Network Type	Infrastructure	IP Address: Current Channel:	192.168.2.233 11
Server Base	d Authentication Signal Strength		Data Encryption:	None Excellent
				Advanced

You will then notice that the tray icon has disappeared from the system tray.

3.6 Display Settings

To change the display settings, click on **Options** in the menu bar, and then click on **Display Settings**.

A 802.11 WLAN Client Utility -	Current Profile: wla	n	
Action Options Help			
Currer Display Settings	liagnostics		
Profile Name:	wlan		Total 802.11
Link Status:	Associated		AG.
Wireless Mode:	2.4 GHz 11 Mbps	IP Address:	192.168.2.233
Network Type:	Infrastructure	Current Channel:	11
Server Based Authentication:	None	Data Encryption:	None
Signal Strength:	******		Excellent
			Advanced

In this window you can change the Signal Strength Display Units from dBm to %,

and increase or decrease the refresh interval rate, as well as displaying the data in a cumulative or relative fashion.

Display Settings		2
Signal Strength Display Units:	0%	<mark>⊙</mark> dBm
Refresh Interval (seconds):		3 🗘
Data Display:	O Relative	 Cumulative
		K Cancel

Click on the **OK** button to return to the previous window.

4 Uninstall the Drivers & Client Utility

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

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

- 1. Click on Start > Settings > Control Panel > Add or Remove Programs
- 2. You will then see the following window. Select the Atheros Utility and then click on **Change/Remove**.

🐻 Add or R	emo	re Programs				X
-	^	Currently installed programs: Show upgat	tes <u>S</u> ort by:	Name	1	*
Change or Remove Programs	in.	A 802.11 WLAN Client Installation Program v1.00		Size Used	<u>0.36MB</u> rarely	^
		To change this program or remove it from your computer, click Change/Remo		sed On	11/8/2005 ge/Remove	
Add <u>N</u> ew Programs		San Acronis True Image		Size	18.02MB	
6	~	谒 ATI - Software Uninstall Utility 			l	~

3. Click on Uninstall the previous installation radio button.



4. Click on the **Next** button to continue. You will then see the following message informing you that you must restart the system after installation.

Question	n 🛛 🐹
2	The option you have selected requires the system to be rebooted at the end of the operation. Do you want to continue?
	Yes No

5. Click on the **Yes** button to continue. You will then see the following message asking you if you would like to remove the application.

Confirm Uninstall			
Do you want to complete	ely remove the OK	selected application an	d all of its features?

6. Click on the **OK** button to continue. You will then see the following message asking you if you would like to remove the driver and all the existing profiles.

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

7. Click on the **Yes** button to continue. You must then restart your system to complete the Uninstallation.

802.11	WLAN Client Installation Program	×
1	The Installation Program has successfully performed the selected operations, but the system needs to be reboor before all of the changes will take effect. Click OK to reboot the system. OK	oted

8. Remove the device form your computer and then click on the **OK** button. The Uninstallation process is complete.

Appendix A – Specifications

Data Rates

802.11a: 6, 9, 12, 18, 24, 36, 48, 54, 72, 96 & 108 (Super A) Mbps

802.11g: 6, 9, 12, 18, 24, 36, 48, 54, 72, 96 & 108 (Super G) Mbps

802.11b: 1, 2, 5.5, 11Mbps

Standards / Compliance

IEEE802.11, IEEE802.11a, IEEE802.11g, IEEE802.11b, draft IEEE 802.11e, f, h, and i standards, IEEE802.1x

Regulation Certifications

FCC Part 15/UL, ETSI 300/328/CE

Operating Voltage

5 V ± 0.25V

Status LEDs

RF link activity

Drivers

Windows 98SE/ME/2000/XP

RF Information

Frequency Band

802.11a: 5.15~5.25GHz, 5.25~5.35GHz, 5.47~5.725GHz, 5.725~5.825GHz **802.11b/g:** U.S., Europe and Japan product covering 2.4 to 2.484 GHz, programmable for different country regulations

Media Access Protocol

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Modulation Technology

802.11a/g: OFDM (64-QAM, 16-QAM, QPSK, BPSK)

802.11b: DSSS (DBPSK, DQPSK, CCK) Operating Channels

11 for North America, 14 for Japan, 13 for

Europe, 2 for Spain, 4 for France

Receive Sensitivity (Typical)

5.15~5.825GHz

6Mbps@ -90dBm; 54Mbps@ -74dBm

2.412~2.472GHz (IEEE802.11g) 6Mbps@ -92dBm; 54Mbps@ -76dBm

2.412~2.472GHz (IEEE802.11b) 11Mbps@ -92dBm; 1Mbps@ -96dBm

Available transmit power

5.15~5.35 GHz 20 ± 1dBm @6~24Mbps

- 19 ± 1dBm @36Mbps
- 18 ± 1dBm @48Mbps
- 17 ± 1dBm @54Mbps

5.47 ~ 5.725GHz

19 ± 1dBm @6~24Mbps

- 18 ± 1dBm @36Mbps
- 17 ± 1dBm @48Mbps
- 16±1dBm @54Mbps

5.725 ~ 5.825GHz

18 ± 1dBm @6~24Mbps

- 17 ± 1dBm @36Mbps
- 16 ± 1dBm @48Mbps
- 15 ± 1dBm @54Mbps

2.412~2.472GHz (IEEE802.11g)

- 23 ± 1dBm @6~ 24Mbps 22 ± 1dBm @36Mbps 21 ± 1dBm @48Mbps
- 20 ± 1dBm @54Mbps

2.412~2.472GHz (IEEE802.11b)

23 ± 1dBm @1~11Mbps

Antenna

Dipole antenna

Networking

Topology

Ad-Hoc, Infrastructure

Security

IEEE802.1x support for LEAP/PEAP WPA – Wi-Fi Protected Access (AES, 64,128,152-WEP with shared-key authentication)

Physical

Form Factor

USB 2.0 Dimensions

75.2(L) mm x 53.9(W) mm x 14(H) mm

Weight

40 g/ 1.5oz

Environmental

Temperature Range

Operating: -0°C to 55°C Storage: -20°Cto 75°C

Humidity (non-condensing)

5%~95% Typical

Package Contents

One USB Adapter One USB Cable One Quick Start Guide One CD-ROM with User's Manual and Drivers

Appendix B – FCC Interference Statement

Federal Communication Commission Interference Statement

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

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

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

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

IMPORTANT NOTE: FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This device complies with FCC RF Exposure limits set forth for an uncontrolled environment, under 47 CFR 2.1093 paragraph (d)(2).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.