

Table of Contents

1	INTRODUCTION	3
	1.1 FEATURES & BENEFITS	3
	1.2 PACKAGE CONTENTS	
	1.3 USB Adapter Description	
	1.4 System Requirements	
	1.5 Applications	-
	1.6 NETWORK CONFIGURATION	6
	a) Ad hoc (peer-to-peer) Mode	
	b) Infrastructure Mode	
2	INSTALL DRIVERS & CLIENT UTILITY	8
	2.1 BEFORE YOU BEGIN	8
	2.2 INSTALLING THE DRIVERS	8
3	USING THE CLIENT UTILITY	20
3		-
	3.1 CURRENT STATUS	
	3.2 PROFILE MANAGEMENT	21
	3.2.1 Scan for available networks	
	3.2.2 Create a New Profile	
	3.2.3 Security 3.2.3.1 Security Disabled	
	3.2.3.1 Security Disabled	
	3.2.3.2 WPA/WPA2 – PEAP (EAP-GTC)	
	3.2.3.4 WPA/WPA2 – PEAP (EAP-MSCHAP-V2)	
	3.2.3.5 WPA/WPA2 – LEAP	.31
	3.2.3.6 WPA/WPA2 – EAP-FAST	
	3.2.3.7 WPA/WPA2 – Passphrase	.34
	3.2.3.8 802.1x – TLS, TTLS.	
	3.2.3.9 802.1x – PEAP (EAP-GTC) 3.2.3.10 802.1x – PEAP (EAP-MSCHAP-V2)	38
	3.2.3.11 802.1x – LEAP	.40
	3.2.3.12 802.1x – EAP-FAST	
	3.2.3.13 Pre-Shared Key (Static WEP)	
	3.2.4 Advanced Settings	
	3.2.4.1 Infrastructure Settings	
	3.2.4.2 Ad Hoc Settings	
	3.3 DIAGNOSTICS	
	3.5 DISABLE TRAY ICON	50
	3.6 DISPLAY SETTINGS	
4	UNINSTALL THE DRIVERS & CLIENT UTILITY	
A	PPENDIX A – SPECIFICATIONS	56
AF	PPENDIX B – FCC INTERFERENCE STATEMENT	57

1 Introduction

This 108Mbps 802.11g High-Gain Wireless USB Adapter supports the IEEE 802.11b/g (2.4GHz) protocol. It provides a high-speed wireless connection with data rates up to 108Mbps.

To protect your wireless connectivity, the high-speed wireless USB adapter supports 64/128/152-bit WEP data encryption and WPA. Dynamic Frequency Selection (DFS) puts your network on the clearest channel in your location. With this 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 108 Mbps in	Capable of handling heavy data payloads
Super G mode	such as MPEG video streaming.
High Output Power up to 23 dBm	A higher power output can increase the range.
Advanced Encryption Standard (AES),	Powerful data security.
Temporal Key Integrity Protocol (TKIP) and	
Wired Equivalent Privacy (WEP)	
IEEE 802.1x Client Support	Enhances authentication and security.
Support for 802.11e standard	Wireless Multimedia Enhancements Quality of
	Service support (QoS)
Advanced Power Management	Low power consumption in power saving
	mode up to 98%.
Support eXtended Range technology	eXtended Range technology provides 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 you need to return the product return. The unit must be returned in its original package.

- > One Wireless LAN USB Adapter
- One USB Cable (Type A to Mini B)
- > One 2dBi Detachable Antenna
- > One Driver and Utility CD-ROM with User's Manual Included
- > One Quick Installation Guide

1.3 USB Adapter Description

This wireless USB adapter fits into your computer's USB 1.1 or 2.0 port. 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 1.1 or 2.0 interface.
- ➤ Windows 2000/XP operating system.
- 20 MB of free disk space for installing the USB adapter driver and utility program.
- CD-ROM Drive
- CPU: 300MHz or above
- ► Memory: 32MB or above

1.5 Applications

. 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 easily installed. 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) Dynamic environments

Show rooms, meeting rooms, retail stores, and manufacturing sites where the workplace is frequently rearranged.

e) Small Office and Home Office (SOHO) networks SOHO users need a cost-effective, easy-to-install 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

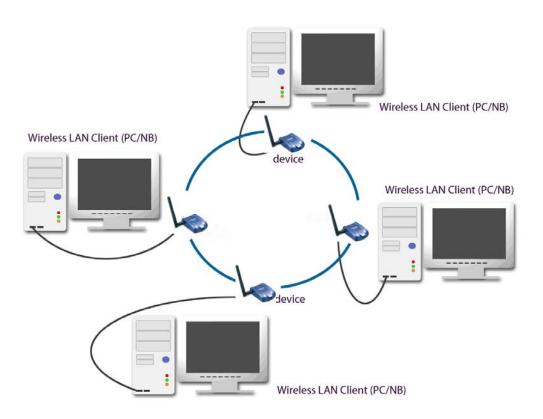
Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

1.6 Network Configuration

To better understand how wireless devices work together to create a wireless network, it might be helpful to depict a few of the possible wireless network configurations. Wireless devices can be configured as:

- a) Ad hoc (or peer-to-peer)
- b) Infrastructure

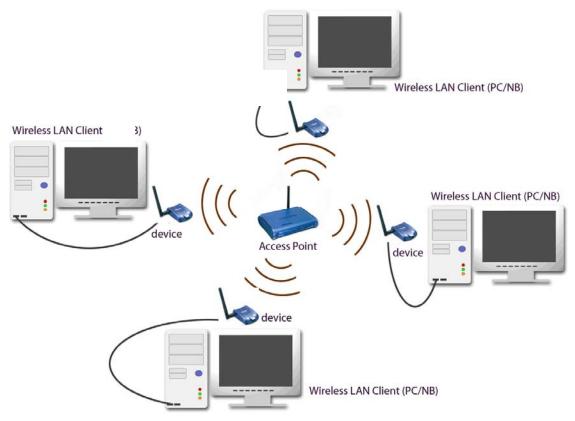
a) Ad hoc (peer-to-peer) Mode



In ad hoc mode, each client is peer-to-peer. The client would only have access to the resources of the other client. Ad hoc mode 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 above depicts a network in Ad hoc mode.

b) Infrastructure Mode

Infrastructure mode requires the use of an access point (AP). In this mode, all wireless communication between clients passes through an 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. The image below depicts a network in infrastructure mode.



2 Install Drivers & Client Utility

2.1 Before You Begin

Before installing your wireless USB adapter, you need to remove all Wireless LAN drivers that you have previously installed.

During the installation, Windows XP/2K/ME/98 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

Windows XP/2000

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

- 1. Insert the provided CD-ROM into your CD-ROM drive. The autorun screen will appear.
- 2. Click Install Utility & Driver and then click Windows 2000/XP.



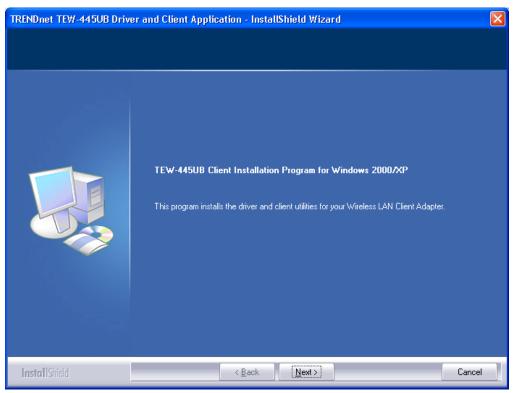
3. Click Run.



4. Click Run.



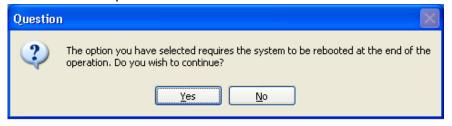
5. Click Next to continue.



6. Select Install Client Utilities and Driver and then click Next.

r TRENDnet TEW-445UB Drive	r and Client Application - InstallShield Wizard	
Setup Type Select the setup type that best s	suits your needs.	
	Click the type of setup you prefer. Install Client Utilities and Driver Install Driver Only	Description Choose this option to install the driver and client utilities. This is the recommended option.
InstallShield	< <u>B</u> ack <u>Next</u> >	Cancel

7. This message informs you that the system must be restarted after the installation is complete. Click **Yes** to continue.



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

TRENDnet TEW-445UB Driver a	nd Client Application - InstallShield Wizard	×
Choose Destination Location Select the folder where the installation	on program will install the files.	
	The installation program will install the client utilities in the following location:	
	Destination Folder- C:\Program Files\TRENDnet\TEW-445UB\ Browse	
Install Shield	< Back Next> Cancel	

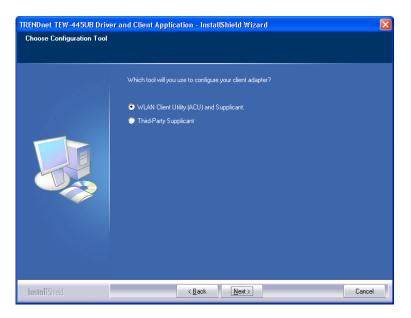
9. Select a program folder for the Start menu, or use the default setting: **WLAN**. Click **Next** to continue.

TRENDnet TEW-445UB Driver	and Client Application - InstallShield Wizard	×
Select Program Folder Select a program folder.		
	The installation program will add program icons to the Program Folder listed below. You may enter a new folder name or select one from the Existing Folders list.	3
	Program Folder: TRENDnet TEW-445UB	
	TRENDhet TEW-4450B	
	Existing Folders:	
	Accessories Acronis	
	Administrative Tools Games Skype Snaglt 8 Startup	
InstallShield	< Back Next> Cancel	

10. The message below 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 **Next** to continue.

TRENDnet TEW-445UB Driver and Client Application - InstallShield Wizard 🛛 🔀	
TEW-445UB Client Installation Program for Windows	
IMPORTANT: Please Read!	
On Windows XP, you can configure your WLAN Wireless LAN Client Adapter through the WLAN Client Utility (ACU) or a third-party supplicant. Because third-party tools may not provide all of the functionality available in the ACU, WLAN recommends that you use the ACU. (Please note that a patch from Microsoft might be required to use the Microsoft tool with WPA security.)	
On the next screen, select whether you want to use the ACU or a third-party tool to configure your client adapter.	
NOTE: If you select a third-party tool, some of the ACU features will not be available. To activate those features, you must install the ACU.	
InstallShield	
< <u>B</u> ack <u>N</u> ext > Cancel	

11. Select one of the options. It is recommended that you select the first option: WLAN Client Utility (ACU) and Supplicant. Click Next to continue.



12. When you reach the screen below, plug in the provided USB cable into the TEW-445UB and into an available USB plug on your computer. Cancel the Found New Hardware Wizard and then click **OK**.

WLAN C	lient 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.
	OK

13. If you are using Windows XP, you will see a message regarding Windows Logo Testing, click on the **Continue Anyway** button to continue.

Software Installation	
<u>.</u>	The software you are installing has not passed Windows Logo testing to verify its compatibility with Windows XP. (<u>Tell me why</u> <u>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 software vendor for software that has passed Windows Logo testing.
	Continue Anyway STOP Installation

14. If you are using Windows 2000, a **Digital Signature Not Found** window appears. Click **Yes** to continue the installation.

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. WLAN USB 2.0 Wireless Network Adapter 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?
	Yes <u>N</u> o <u>M</u> ore Info

15. Select Yes, I want to restart my computer now and then click Finish.

TRENDnet TEW-445UB Driver a	nd Client Application - InstallShield Wizard
	InstallShield Wizard Complete The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Select Yes to reboot the system.
	 Yes, I want to restart my computer now. No, I will restart my computer later. Remove any disks from their drives, and then click Finish to complete setup.
InstallShield	< <u>B</u> ack Finish Cancel

Windows ME/98SE

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

- 1. Insert the provided CD-ROM into your CD-ROM drive. The autorun screen will appear.
- 2. Click Install Utility & Driver and then click Windows 98/ME.

	Install Utility & Driver
	Windows 98/ME Windows 2000/XP
	User's Guide
	Bonus
108Mbps 802 11p High Power	Exit
108Mbps 802.11g High Power Wireless USB 2.0 Adapter TEW-445UB	

3. Select Run this program from its current location and then click OK.



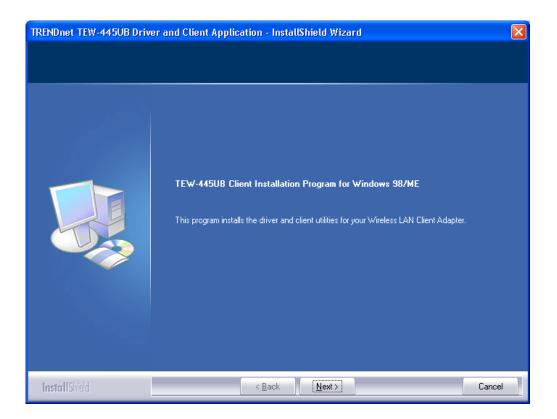
4. Click Yes.



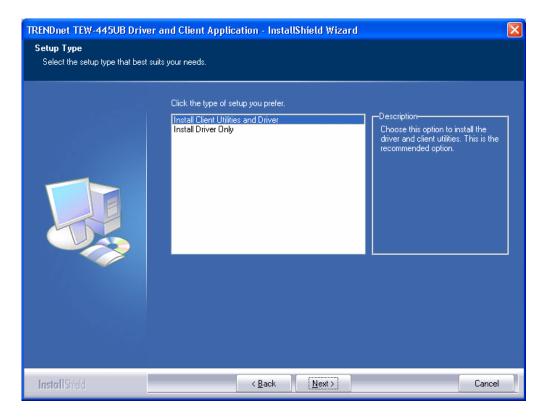
5. Remove the USB adapter from the USB port if it is inserted and then click **OK**.

TRENDnet TEW-445UB Driver and Client Application - InstallShield Wizard 🛛 🛛 🔀	
Please remove the USB Card from the USB slot if it is inserted and insert after installation completes and system reboots	

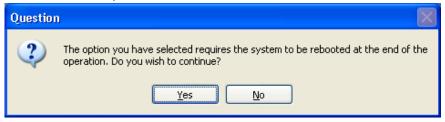
6. Click **Next** to continue.



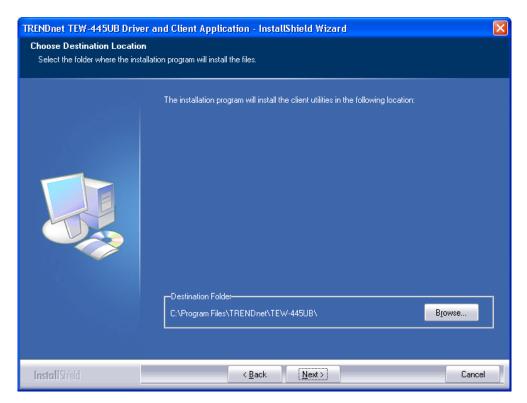
7. Select Install Client Utilities and Driver and then click Next.



8. This message informs you that the system must be restarted after the installation is complete. Click **Yes** to continue.



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



10. Click Next to continue.

TRENDnet TEW-445UB Driver	and Client Application - InstallShield Wizard	3
Select Program Folder Select a program folder.		
	The installation program will add program icons to the Program Folder listed below. You may enter a new folder name or select one from the Existing Folders list.	
	Program Folder: TRENDnet TEW-445UB	
	Existing Folders: Accessories Actonis Administrative Tools Games Skype Snaglt 8 Startup	
InstallShield	< Back Next> Cancel	

11. When you reach the screen below, plug in the provided USB cable into the TEW-445UB and into an available USB port on your computer. Cancel the Found New Hardware Wizard and then click **OK**.

TRENDnet TEW-445UB Driver and Client Application - InstallShield Wizard 🛛 🔀				
⚠	This installation program installs the drivers automatically. Cancel the Found New Hardware Wizard if it appears and proceed with installation			
	<u>(())</u>			

12. Click **OK** to reboot the computer.



3 Using the Client Utility

You will see the Wireless Client Utility icon on your desktop. Double click this icon to open up the utility program.



3.1 Current Status

The **Current Status** tab displays the current status of the wireless radio. The following information is included in this tab:

🛞 802.11g Client Utility - Cur	rent Profile: wlan-g		?×
Action Options Help			
Current Status Profile Management	Diagnostics		
STRENDNET Profile Name:	wlan-g		
Link Status:	Associated		
Wireless Mode:	2.4 GHz 54 Mbps	IP Address: 192.168.223.	100
Network Type:	Infrastructure	Current Channel: 5	
Server Based Authentication:	None	Data Encryption: None	
Signal Strength:		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.
 Note: The profile name and network name (SSID) are not the same.
- Link Status: This indicates the state of the client; associated or not associated.
- Wireless Mode: Displays the 802.11 mode (e.g. "2.4GHz 11 Mbps", "2.4GHz 54 Mbps", "2.4GHz 108Mbps").
- Network Type: Displays the type of network (e.g. "Infrastructure" or "Ad hoc").
- Server Based Authentication: Displays information about the authentication method.
- > IP address: Displays the IP address assigned to this device.
- > Current Channel: Displays the channel of the access point the device is

connected to.

- > Data Encryption: Displays the type of encryption used.
- > Signal Strength: Displays the strength of the wireless connection.

Click on the **Advanced** button to display more details about the current status. This window includes information such as: Network Name (SSID), AP MAC address, Power Save Mode, Signal Strength, Noise Level, Channel, Frequency, and Channel Set (country). Click **OK** to close the window.

Advanced Status			? 🔀
Network Name (SSID):	kailua	Current Signal Strength:	-91 dBm
Server Based Authentication:	None	Current Noise Level:	-96 dBm
Data Encryption:	WEP	Up Time:	00:48:38
Authentication Type:		802.11b Preamble:	Short & Long
Message Integrity Check:	None	Current Receive Rate:	1.0 Mbps
QoS:	None	Current Transmit Rate:	1.0 Mbps
		Channel:	4
		Frequency:	2.427 GHz
Associated AP MAC Address:	00-11-22-33-44-55	Channel Set:	United States
Power Save Mode:	Normal		
			ОК

3.2 Profile Management

This tab is used to create a new profile, modify an existing profile, remove an existing profile and activate an existing profile.

🛞 802.11g Client Utility - C	urrent Profile: Default		?×
<u>Action Options H</u> elp			
Current Status Profile Manageme	nt Diagnostics		
Sefault		<u>N</u> ew	
		<u>M</u> odify	
		Remove	
		Activate	
⊂ Details			
Network Type:	Infrastructure	Import	
Security Mode:	Disabled		\equiv
Network Name 1 (SSID1):	<empty></empty>	<u>Export</u>	
Network Name 2 (SSID2):	<empty></empty>	Scan	
Network Name 3 (SSID3):	<empty></empty>	<u> </u>	
Auto Select Profiles		Order <u>P</u> rofiles.	

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.

Av	vailable Infrastructure and Ad Hoc Networks 🔹 🔹 🔀				K			
	Network Name (SS Wan-g It net54g TNET Kailua	SID) (୧୦) Sup ଲେଡ ଲେଡ ଲେଡ	: 11 11	nal Strength 29 dB 26 dB 1 dB 4 dB		Channel 5 11 1 4	Wireless M 2.4 GHz 54 2.4 GHz 54 2.4 GHz 11 2.4 GHz 54	
	<		<u>A</u> ctivate	F	Refresh) OK	

If you would like to associate with a specific network, select the network name (SSID) and then click on the **Activate** button.

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 SSID each time.

802.11g Client Utility - C	urrent Profile: Default	?
tion <u>O</u> ptions <u>H</u> elp		
Current Status Profile Manageme	nt Diagnostics	
🐚 Default		<u>N</u> ew
		Modify
		Remo <u>v</u> e
		Ac <u>t</u> ivate
- Details		
Network Type:	Infrastructure	Import
Security Mode:	Disabled	
Network Name 1 (SSID1):	<empty></empty>	<u>E</u> xport
Network Name 2 (SSID2):	<empty></empty>	S <u>c</u> an
Network Name 3 (SSID3):	<empty></empty>	June 1
Auto Select Profiles		Order Profiles

Click on the **New** button to create a new profile. The window below appears:

Profile Management	
General Security Advance	d
← Profile Settings	
Profile Name:	wlan-g
Client Name:	TRENDnet
Network Names	
SSID1:	wlan-g
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 **OK** 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 and 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 encryption key, then select **None** in the security tab, and then click **OK**.

ile Management				
neral Security Adv	vanced			
Set Security Options				
O WPA/WPA2		WPA/WPA2 EAP Type:	LEAP	~
O WPA/WPA2 P	assphrase			
O 802.1x		802.1x EAP Type:	LEAP	~
O Pre-Shared Kej	y (Static WEP)			
None				
Configure		Allow Association to M	iuod Colla	
	Group Policy Delay:		ixed Cells	
				}

3.2.3.2 WPA / WPA2- TLS, TTLS

WPA2 (Wi-Fi Protected Access 2) provides network administrators with a high level of assurance that only authorized users can access the network. 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/WPA2** 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.

ofile Management			?
eneral Security Advanced			
Set Security Options WPA/WPA2 WPA/WPA2 Passphrase	WPA/WPA2 EAP Type:	EAP-TLS EAP-TLS EAP-TLS	~
 802.1x Pre-Shared Key (Static WEP) None 	802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP EAP-FAST	
Configure Group Policy Delay:	Allow Association to M	ixed Cells	

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

Define EAP-TTLS Configuration	? 🗙
Use Machine Information For Domain Logon Trusted Root Certification Authorities	
<any></any>	~
User Information for EAP-TTLS Authentication User Name: james Password: Confirm Password:	
Settings OK Ca	ncel

- ➤ 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: Retype the password.

Click Settings.

Configuration Settings	? 🛛
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 Trusted Root Certification Authorities 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 **OK** to return to the previous window. Click **OK** again to return to the Profile Management window.

3.2.3.3 WPA/WPA2 – 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/WPA2** radio button, and then select **PEAP (EAP-GTC)** from the drop-down list.

Set Security Options	WPA/WPA2 EAP Type:	PEAP (EAP-GTC)
WPA/WPA2 Passphrase		EAP-TLS EAP-TTLS
◯ 802.1x	802.1x EAP Type:	DEAD (EAD CTC)
Pre-Shared Key (Static WEP) None		EAP-FAST
Configure	Allow Association to M	ixed Cells
Group Policy De	elay: 60 😂 sec	

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

Define PEAP (EAP-GTC) Configuration	? 🔀
Use Machine Information For Domain Logon Trusted Root Certification Authorities	
<any></any>	~
Set Password O Token O Static Password User Information for PEAP (GTC) Authentication	
User Name: james	
Password:	
Confirm Password:	
Settings OK Can	cel

- ➤ Trusted Root Certification Authorities: Select the appropriate certificate authority from the drop-down list.
- Set Password: Select Token or Static Password radio button. The default setting is Static Password.
- **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: Retype the password.

Click Settings.

Configuration Settings	? 🛛
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 Trusted Root Certification Authorities 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 **OK** to return to the previous window. Click **OK** again to return to the Profile Management window.

3.2.3.4 WPA/WPA2 – 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/WPA2** radio button, and then select **PEAP (EAP-MSCHAP-V2)** from the drop-down list.

eral Security Advanced		
⊙ WPA/WPA2	WPA/WPA2 EAP Type:	PEAP (EAP-MSCHAP V2)
WPA/WPA2 Passphrase		EAP-TLS EAP-TTLS PEAP (EAP-GTC)
◯ 802.1×	802.1x EAP Type:	PEAP (EAP-MSCHAP V2)
O Pre-Shared Key (Static WEP)		LEAP EAP-FAST
O None		
Configure	Allow Association to M	ived Calls
Group Policy Delay:		INCU COIS
encorp i ency e ency.	00	

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

Define PEAP (EAP-MSCHAF	PV2) Configuration	? 🔀
Use Machine Information F Trusted Root Certification Auth	and the second	
<any></any>		~
User Information for PEAP (E User Name:	AP-MSCHAP V2) Authentication	
Password:	•••••	
Confirm Password:	••••	
s	ettings OK Cano	;el

- 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: Retype the password.

Click Settings.

Configuration Settings	? 🛛
Specific Server or Domain: Login Name:	
Logini (and	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 Trusted Root Certification Authorities 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 **OK** to return to the previous window. Click **OK** again to return to the Profile Management window.

3.2.3.5 WPA/WPA2 – 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/WPA2 radio button, and select LEAP from the drop-down list.

General Security Adv	vanced				
Set Security Options					1
⊙ WPA/WPA2		WPA/WPA2 EAP Type:		LEAP	
○ WPA/WPA2 Passphrase ○ 802.1×		802.1x EAP Type:		EAP-TLS EAP-TTLS PEAP (EAP-GTC)	
O Pre-Shared Key	y (Static WEP)			PEAP (EAP-MSCHAP V2) LEAP EAP-FAST	
			siation to M	ixed Cells	
Configure			nation to m		
Configure	Group Policy Delay:		ec		

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

AP Settings		?
Username and Password Se	ttings	
O Use Temporary User	Name and Password	
	ompt for User Name and Password	
O Manually Promp	t for User Name and Password	
Use Saved User Nam	e and Password	
User Name:		
Password:		
Confirm Password:		
Domain:		
	gon Domain with User Name	
No Network Connec	tion Unless User Is Logged In	
А	uthentication Timeout Value (in seconds)	
	ОК С	ancel

- 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: Retype the password.

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

3.2.3.6 WPA/WPA2 – EAP-FAST

EAP-FAST allows customers who cannot enforce a strong password policy to deploy EAP authentication that does not require digital certificates. This method supports a variety of user and password database types and password expiration and change. It is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco LEAP who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks. (See help menu on configuration utility for more details)

Profile Management			? 🗙
General Security Advanced			
Set Security Options			
⊙ WPA/WPA2	WPA/WPA2 EAP Type:	EAP-FAST	
○ WPA/WPA2 Passphrase		EAP-TLS EAP-TTLS	
◯ 802.1x	802.1x EAP Type:	PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
O Pre-Shared Key (Static WEP)		LEAP EAP-FAST	
◯ None			
Configure	Allow Association to M	ived Cells	
Group Policy Delay:			
		ОК	Cancel

EAP-FAST Settings		?×		
⊂Username and Password Se	ttings			
Use Temporary User	Name and Password	_		
O Automatically Pr	ompt for User Name and Password			
🔿 Manually Promp	t for User Name and Password			
Use Saved User Nam	a and Decement			
0				
User Name:				
Password:				
Confirm Password:				
Domain:				
Include Windows Lo	gon Domain with User Name			
🗹 No Network Connec	tion Unless User Is Logged In			
Authentication Timeout Value (in seconds)				
Protected Access Credentials (PAC)				
Allow Automatic PAC Pr	ovisioning for this Profile			
Select a PAC Authority to u	se with this profile			
	Select More			
	OK Cancel			

Click **Configure** to configure the EAP-Fast settings

- Use Temporary User Name and Password: Selecting this option 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:** Retype the password.

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

3.2.3.7 WPA/WPA2 – Passphrase

et Security Options			
 WPA/WPA2 WPA/WPA2 Pa 	WPA/WPA2 EAP Type:	LEAP	×
🔵 802.1x	802.1x EAP Type:	LEAP	~
Configure	Allow Association to Mi	ixed Cells	

Select the WPA/WPA2 Passphrase radio button and then click Configure.

? 🛛
or 64 hexadecimal characters)
OK Cancel

 Enter a WPA/WPA2 passphrase. For ASCII text, enter 8-63 characters, for hexadecimal enter 64 characters).

Click **OK** to return to the previous window. Click **OK** again to return to the Profile Management window.

3.2.3.8 802.1x - 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.

Set Security Options	WPA/WPA2 EAP Type:	LEAP	
 WPA/WPA2 Passphrase 802.1x Pre-Shared Key (Static WEP) None Configure 	802.1× EAP Type:	EAP-TTLS EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP EAP-FAST	
Group Policy Delay:	Allow Association to M	Host Based EAP]

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 **Configure** to configure the TTLS settings.

efine EAP-TTLS Configur	ation 🤗
Use Machine Information Fo	or Domain Logon
Trusted Root Certification Auth	
<any></any>	*
User Information for EAP-TTL	_S Authentication
User Name:	james
Password:	
Confirm Password:	
s	ettings OK 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.
- Password: Enter the password that corresponds with the user name for the certificate authority.
- > Confirm Password: Retype the password.

Click Settings.

Configuration Settings	? 🛛
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 Trusted Root Certification Authorities 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 **OK** to return to the previous window. Click **OK** again to return to the Profile Management window.

3.2.3.9 802.1x – 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. 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.

rofile Management			?
General Security Advanced			
○ WPA/WPA2 ○ WPA/WPA2 Passphrase	WPA/WPA2 EAP Type:	LEAP	
 802.1x Pre-Shared Key (Static WEP) None 	802.1x EAP Type:	PEAP (EAP-GTC)	
Configure Group Policy Delay:	Allow Association to M	LEAP	
		ок с	Cancel

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

Define PEAP (EAP-GTC) Configuration	? 🗙
Use Machine Information For Domain Logon	
Trusted Root Certification Authorities	
<any></any>	~
Set Password	
O Token	
Static Password	
User Information for PEAP (GTC) Authentication	
User Name: james	
Password:	
Confirm Password:	
Settings OK Ca	ancel

► **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 Settings.

Configuration Settings	? 🔀 🤉
Specific Server or Domain:	
Login Name:	iames
	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 Trusted Root Certification Authorities 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 **OK** to return to the previous window. Click **OK** again to return to the Profile Management window.

3.2.3.10 802.1x – 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 Management			? 🗙
General Security Advanced			
 ○ WPA/WPA2 ○ WPA/WPA2 Passphrase 	PA/WPA2 EAP Type:	LEAP	*
 802.1x Pre-Shared Key (Static WEP) None Configure 	802.1х ЕАР Туре:	PEAP (EAP-MSCHAP V2) EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP EAP-FAST	
Group Policy Delay: 60	Allow Association to Mi:	Host Based EAP	
		ОК	Cancel

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

Define PEAP (EAP-MSCHAR	P V2) Configuration	? 🔀
Use Machine Information F Trusted Root Certification Auth		
<any></any>		~
User Information for PEAP (E User Name: Password: Confirm Password:	AP-MSCHAP V2) Authentication	
s	ettings OK Cano	cel

- ➤ 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: Retype the password.

Click Settings.

Configuration Settings	2 🛛
Specific Server or Domain:	james
Login Name:	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 Trusted Root Certification Authorities 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 **OK** to return to the previous window. Click **OK** again to return to the Profile Management window.

3.2.3.11 802.1x – 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.

Set Security Options	WPA/WPA2 EAP Type: LEAP	×
O WPA/WPA2 Passphrase		
 802.1x Pre-Shared Key (Static Wf None Configure 	802.1x EAP Type: LEAP EAP-TLS EAP-TLS PEAP (EAP-GTC) PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2) LEAP EAP-FAST Host Based EAP	×
Group P	olicy Delay: 60 📚 sec	

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

LEAP Settings	? 🗵
Username and Password Set	
	mpt for User Name and Password for User Name and Password
Saved User Nam	e and Password
User Name:	
Password:	
Confirm Password:	
Domain:	
No Network Connect	ion Domain with User Name ion Unless User Is Logged In thentication Timeout Value (in seconds)
	OK Cancel

- Use Temporary User Name and Password: Selecting this option 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: Retype the password.

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

3.2.3.12 802.1x - EAP-FAST

EAP-FAST allows customers who cannot enforce a strong password policy to deploy an 802.1X EAP type that does not require digital certificates. This method supports a variety of user and password database types and password expiration and change. It is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco LEAP who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks. (See help menu on configuration utility for more details)

Profile Management			? 🗙
General Security Advanced			
Set Security Options			
○ WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	
○ WPA/WPA2 Passphrase			
	802.1x EAP Type:	EAP-FAST	
O Pre-Shared Key (Static WEP)		EAP-TLS EAP-TTLS	
◯ None		PEAP (EAP-GTC) PEAP (EAP-MSCHAP V2)	
Configure	Allow Association to Mi	LEAP EAP-FAST	
Group Policy Delay:	60 🗢 sec	Host Based EAP	
		ок с	ancel

- Use Temporary User Name and Password: Selecting this option 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: Retype the password.

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

EAP-FAST Settings		?×
Username and Password Se	ttings	
O Use Temporary User	Name and Password	
	ompt for User Name and Password t for User Name and Password	
💿 Use Saved User Nam	e and Password	
User Name:		
Password:		
Confirm Password:		
Domain:		
Include Windows Lo	gon Domain with User Name	
🗹 No Network Connec	tion Unless User Is Logged In	
A	uthentication Timeout Value (in seconds)	
Protected Access Credential	< (PAC)	
Allow Automatic PAC Pr		
Select a PAC Authority to u	-	
	Select More	
	OK Can	cel

3.2.3.13 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 the 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.

Profile Management			? 🛛
General Security Advanced			
Set Security Options			
◯ WPA/WPA2	WPA/WPA2 EAP Type:	LEAP	~
○ WPA/WPA2 Passphrase			
◯ 802.1×	802.1x EAP Type:	LEAP	~
Pre-Shared Key (Static WEP)			
O None			
Configure			
Group Policy D	Allow Association to M	ixed Lelis	
		F	
			OK Cancel

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

rd character	rs)	
AL/E	P Key S	line:
64		152
•	0	0
•	0	0
•	0	0
•	0	0
	 ○ ○ ○ 	● ○● ○● ○

- 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 **OK** 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 wireless mode, power save mode, and network type.

3.2.4.1 Infrastructure Settings

Profile Management				? 2
General Security Ad	lvanced			
Power Save Mode:	Normal	×		
Network Type:	Infrastructure	*		
802.11b Preamble:	💿 Short & Long	O Long Only]	
Wireless Mode	ps	- Wireless Mode W	hen Starting Ad Ho	c Network
💌 2.4 GHz 11 Mb	ps	O 2.4 GHz 11 M	lbps	
 ✓ Super G ✓ eXtended Ran 	ge (XR) TM	◯ 2.4 GHz 54 M	lbps	Channel: Auto
QoS		802.11 Authentica O Auto	ation Mode	◯ Shared
				Preferred APs
				OK Cancel

- > Wireless Mode: Place a check in the preferred frequency and data rate.
- 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.
- Network Type: Select Infrastructure from the dropdown list if the wireless client is connecting to an access point.
- 802.11b 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 OK 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

Profile Management				? 🔀
General Security Advanced				
Power Save Mode: Off	S	1		
Network Type: Ad Hoc	8	/		
802.11b Preamble: 💿 Short & Long	🔘 Long Only			
⊂Wireless Mode ✓ 2.4 GHz 54 Mbps	Wireless Mode V	When Starting Ad Ho	c Network	
2.4 GHz 11 Mbps	💿 2.4 GHz 11 I	Mbps		
✓ Super G ✓ eXtended Range (XR) TM	🔿 2.4 GHz 54 I	Mbps	Channel: Auto	
₽ QoS	802.11 Authentio	cation Mode ③ Open	O Shared	
			Preferred APs	
			OK Ca	incel

- Wireless Mode: Place a check next to the preferred frequency and data rates.
- Network Type: Select Ad hoc from the drop-down list if the wireless client is connecting to another wireless client
- ➤ 802.11b Preamble: This setting should be the same as the other wireless client. If you are not sure of that setting, select Short & Long.

Click **OK** 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.

on <u>O</u> ptions <u>H</u> elp		
urrent Status Profile Mana	gement Diagnostics	
Transmit		A destas la francision
Multicast Packets:	12	Adapter Information
Broadcast Packets:	1796	Advanced Statistics
Unicast Packets:	1298	
Total Bytes:	154059	
Receive		
Multicast Packets:	464	
Broadcast Packets:	4773	
Unicast Packets:	88	
Total Bytes:	706605	

Click on **Adapter Information** to view information about the wireless USB adapter (e.g. Card Name, MAC address, Driver, Driver Version and Driver Date).

Adapter Informa	tion ? 🔀
Card Name:	WLAN USB 2.0 Wireless Network Adapter
MAC Address:	00-02-6F-3C-31-EB
Driver:	C:\WINDOWS\System32\DRIVERS\ar5523.sys
Driver Version:	1.5.0.102
Driver Date:	05 Jan 2006 16:56:08
Client Name:	SW
	(maintain)
	OK

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

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

Fransmit			
Frames Transmitted OK:	3208	RTS Frames:	1
Frames Retried:	215	CTS Frames:	1
Frames Dropped:	1569	No CTS Frames:	0
No ACK Frames:	96	Retried RTS Frames:	0
ACK Frames:	3208	Retried Data Frames:	215
Receive			
Beacons Received:	24376	Authentication Time-Out:	0
Frames Received OK:	7778	Authentication Rejects:	0
Frames Received with Errors:	39853	Association Time-Out:	0
CRC Errors:	4865	Association Rejects:	0
Encryption Errors:	98	Standard MIC OK:	0
Duplicate Frames:	36	Standard MIC Errors:	0
AP Mismatches:	0	CKIP MIC OK:	0
Data Rate Mismatches:	0	CKIP MIC Errors:	0

Click OK to return to the previous window

3.4 Enable / Disable Radio

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

802.11g Client Utility - Cur	rent Profile: Default		?×
Action Options Help			
Disable Radio Disable Tray Icon	Diagnostics		
Exit Profile Name:	Default		
Link Status:	Associated		
Wireless Mode:	2.4 GHz 54 Mbps	IP Address: 192.168.1.18	
Network Type:	Infrastructure	Current Channel: 4	
Server Based Authentication:	None	Data Encryption: WEP	
Signal Strength:		Fair	
		Advanced	

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

WLAN Client Utility	X
The RF signals for the following network card(s) have been suc WLAN USB 2.0 Wireless Network Adapter	cessfully disabled:
ОК	

Click **OK** to continue.

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

🛞 802.11g Client Utility - Curi	rent Profile: Default	? 🔀
Action Options Help		
Enable Radio Disable Tray Icon	Diagnostics	
Exit Profile Name:		
Link Status:	Not Associated	
Wireless Mode:	IP Add	ress:
Network Type:	Current Char	nnel:
Server Based Authentication:	Data Encryp	ition:
Signal Strength:		
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".

WLAN Client Utility	
The RF signals for the follow WLAN USB 2.0 Wireless Net	een successfully enabled:

Click **OK** 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**.

📀 802.11g Client Utility - Cur	rent Profile: Default	? 🛛
Action Options Help		
Disable Radio Disable Tray Icon	Diagnostics	
Exit Profile Name:	Default	
	Associated	
	2.4 GHz 54 Mbps	IP Address: 192.168.1.18
Network Type:	Infrastructure	Current Channel: 4
Server Based Authentication:	None	Data Encryption: WEP
Signal Strength:		Fair
		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**.

left for the second sec	? 🛛
Action Options Help	
Currer Display Settings Diagnostics	
STRENDNET Profile Name: Default	
Link Status: Associated	
Wireless Mode: 2.4 GHz 54 Mbps	IP Address: 192.168.1.18
Network Type: Infrastructure	Current Channel: 4
Server Based Authentication: None	Data Encryption: WEP
Signal Strength:	Fair
	Advanced

In this window you can change the Signal Strength Display Units from dBm to %, and increase or decrease the refresh interval rate. You can also display date in a cumulative or relative format.

Display Settings	?	
Signal Strength Display Units:	O% ⊙ ₫₿	Ĵ
Refresh Interval (seconds):	3 🗘	
Data Display:	O Relative O Cumulative	
	OK Cancel]

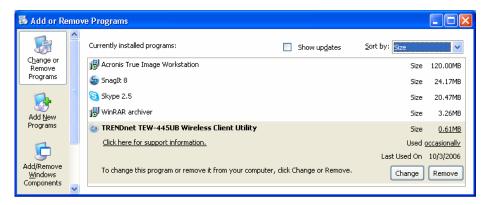
Click **OK** to return to the previous window.

4 Uninstall the Drivers & Client Utility

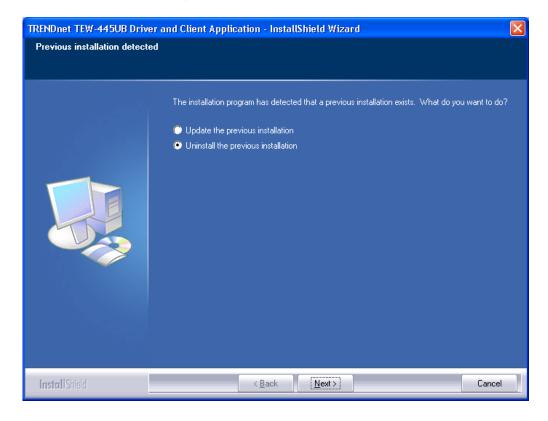
If the device installation is unsuccessful for any reason, the best way to solve the problem is to completely uninstall the device and its utility and repeat the installation procedure again.

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

- 1. Click on Start > Settings > Control Panel > Add or Remove Programs
- You will then see the following window. Select the TRENDnet TEW-445UB Wireless Client Utility and then click **Remove**.



3. Select Uninstall the previous installation radio button. Then click Next.



4. Click OK.



5. Click Yes.

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

6. Remove the device from your computer and then click **OK**.

TRENDnet TEW-445UB Driver and Client Application - InstallShield Wizard 🛛		
♪	The Installation Program has successfully performed the selected operations, but the system needs to be rebooted before all of the changes will take effect. Click OK to reboot the system.	
	ОК	

Appendix A – Specifications

Data Rates

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, IEEE802.11g, IEEE802.11b, draft IEEE 802.11e, 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 XP/2K/ME/98

RF Information

Frequency Band

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

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

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

11 for North America, 13 for Europe and Japan

Receive Sensitivity (Typical)

- 2.412~2.472G(IEEE802.11g)
 6Mbps@ -91dBm;
 54Mbps@ -76dBm
- 2.412~2.472G(IEEE802.11b)
 11Mbps@ -91dBm;
 1Mbps@ -96dBm

Available transmit power

FCC

2.412~2.472G(IEEE802.11g)
 22 dBm @ 6 ~ 24 Mbps
 21 dBm @ 36 Mbps
 20 dBm @ 48 Mbps

19 dBm @ 54 Mbps

2.412~2.472G(IEEE802.11b)
 22 dBm @1~11Mbps

ETSI

- 2.412~2.472G(IEEE802.11g)
 20 dBm @ 6 ~ 24 Mbps
 20 dBm @ 36 Mbps
 20 dBm @ 48 Mbps
 19 dBm @ 54 Mbps
- 2.412~2.472G(IEEE802.11b)
 20 dBm @1~11Mbps

Antenna

Detachable Dipole antenna (2dBi Gain)

Networking

Topology

Ad hoc, Infrastructure

Security

IEEE802.1x support for LEAP/PEAP WEP 64,128,152bit WPA (PSK, TKIP) WPA2 (AES)

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 (Type A to Mini B) One CD-ROM with User's Manual and Drivers One Quick Installation Guide One 2dBi Detachable Antenna

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 radiates radio frequency energy. If not installed and used in accordance with the instructions, it 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 and correct the interference by one or more of the following measures:

- 1. Reorient or relocate the receiving antenna.
- 2. Increase the distance between the equipment and the receiver.
- 3. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- 4. 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.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

If a product does not operate as warranted above during the applicable warranty period, TRENDnet shall, at its option and expense, repair the defective product or deliver to customer an equivalent product to replace the defective item. All products that are replaced will become the property of TRENDnet. Replacement products may be new or reconditioned.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product through any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet office within the applicable warranty period for a Return Material Authorization (RMA) number, accompanied by a copy of the dated proof of the purchase. Products returned to TRENDnet must be pre-authorized by TRENDnet with RMA number marked on the outside of the package, and sent prepaid, insured and packaged appropriately for safe shipment.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO

EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California. <u>Note</u>: AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1-Year Warranty

TRENDNET

TRENDnet Technical Support

US · Canada

Toll Free Telephone: 1(866) 845-3673

24/7 Tech Support

rechnical Support

Europe (Germany · France · Italy · Spain · Switzerland · UK)

Toll Free Telephone: +00800 60 76 76 67

English/Espanol - 24/7 Francais/Deutsch - 11am-8pm, Monday - Friday MET

Worldwide

Telephone: +(31) (0) 20 504 05 35

English/Espanol - 24/7 Francais/Deutsch - 11am-8pm, Monday - Friday MET

Product Warranty Registration

Please take a moment to register your product online. Go to TRENDnet's website at http://www.trendnet.com

TRENDNET

3135 Kashiwa Street Torrance, CA 90505 USA

Copyright ©2006. All Rights Reserved. TRENDnet.