

User Guide

WU830G

Wireless USB Adapter



This device must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product.

FCC Compliance Class B Digital Device

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 environment. 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.

CAUTION: Changes or modifications not expressly approved by Motorola for compliance could void the user's authority to operate the equipment.

Canadian Compliance

This Class B digital apparatus meets all requirements of the Canadian Interference Causing Equipment Regulations. Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

FCC Declaration of Conformity

Motorola, Inc., Broadband Communications Sector, 101 Tournament Drive, Horsham, PA 19044, 1-215-323-1000, declares under sole responsibility that the WU830G complies with 47 CFR Parts 2 and 15 of the FCC Rules as a Class B digital device. This device complies with Part 15 of FCC Rules. Operation of the device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference that may cause undesired operation.

Wireless LAN and your Health

Caution: Exposure to Radio Frequency Radiation.

To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet, and ankles) must be at least 20 cm (8 inches).

Restrictions on Use of Wireless Devices

In some situations or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, these situations may include:

- Using wireless equipment on board an airplane.
- Using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the applicable policy for the use of wireless equipment in a specific organization or environment (such as airports), you are encouraged to ask for authorization to use the device prior to turning on the equipment.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of interference caused by such unauthorized modification, substitution, or attachment is the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.

FCC Certification

The WU830G contains a radio transmitter and accordingly has been certified as compliant with 47 CFR Part 15 of the FCC Rules for intentional radiators. Products that contain a radio transmitter are labeled with FCC ID and the FCC logo.

Canada - Industry Canada (IC)

The wireless radio of this device complies with RSS 210 and RSS 102 of Industry Canada.

This Class B digital device complies with Canadian ICES-003 (NMB-003).

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada

Europe - European Declaration of Conformity

All products with the CE marking comply with the EMC Directive (89/336/EEC), the Low Voltage Directive (73/23/EEC), and the R&TTE Directive (1999/5/EC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms and the equivalent international standards:

- ETS 300-826, 301 489-1 General EMC requirements for radio devices.
- ETS 300-328-2 Technical requirements for Radio equipment.
- EN 60950 Safety

Caution: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. Contact local authority for regulations.

Copyright © 2004 Motorola, Inc.

All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation or adaptation) without written permission from Motorola, Inc.

Motorola reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of Motorola to provide notification of such revision or change. Motorola provides this guide without warranty of any kind, either implied or expressed, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Motorola may make improvements or changes in the product(s) described in this manual at any time.

MOTOROLA, Intelligence Everywhere, and the Stylized M Logo are registered in the US Patent & Trademark Office. Microsoft, Windows, Windows Me and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Microsoft Windows screen shots are used by permission of Microsoft Corporation. Wi-Fi is a registered trademark of Wireless Ethernet Compatibility Alliance, Inc. All other product or service names are the property of their respective owners. © Motorola, Inc. 2004.

Contents

Section 1: Overview

Features	1-2
Understanding Your User Guide	1-3
Box Contents	1-3
Simple Home Network Diagram	1-4
Wireless Connections	1-5
USB Adapter Physical Description	1-6
Front of USB Adapter	1-6
Back of USB Adapter	1-7

Section 2: Installation

Before You Begin	2-1
Enterprise Business Users	2-1
Small Office/Home Office Users	2-2
Security Options	2-2
Security Example	2-4
Installing Your USB Adapter	2-5
Device Configuration Setup	2-5

Section 3: Configuration

Understanding the Antenna Icons	3-2
Starting the Configuration Utility and Viewing Link Status Information	3-3
Link Status Information	3-4
Connecting to an Available Wireless Network	3-6
Creating a Network Profile	3-8
Configuring Security Settings	3-11
Setting Security for a Wireless Network or a Profile	3-12
Open Authentication	3-13
Shared Authentication	3-14
WPA-PSK Authentication	3-16
WPA Authentication	3-17
Removing a Network from the Profile List	3-21
Viewing Product Information	3-22
Removing the Wireless USB Adapter	3-23

Section 4: Troubleshooting

Contact Us4-1

Register the WU830G4-1

Hardware Solutions.....4-1

My computer is experiencing difficulty connecting to the wireless network4-1

I would like to test if my Internet connection is live.....4-2

Section 5: Glossary

Section 1: Overview

Congratulations on purchasing the Motorola WU830G Wireless USB Adapter!

With the WU830G, your laptop or desktop computer is free to join and enjoy all the benefits of an 802.11b/g wireless home or small office network. Once connected, accessing a single broadband connection with everyone else on the network is simple and fun. You can also share files, pictures, peripherals, printers, and more. You'll need one WU830G for each computer.

Because your WU830G works with USB 2.0 (and is backward compatible with USB 1.0 and 1.1), you'll be able to enjoy blazing fast speeds on your wireless network. Since the WU830G receives its power from the USB port, there is no extra power plug to overload your power strip.

The WU830G complies with the 802.11b and the new, nearly 5-times-faster, 802.11g wireless standard. With Wi-Fi[®] Protected Access (WPA) included, your wireless connections are robust and secure, giving you the confidence to communicate without fear that the signal could be compromised.

After installing the USB adapter, you'll have the ability to wirelessly connect to your network to send and receive emails, print documents, or game online from your computer.

Wireless USB Adapter WU830G



Features

The WU830G has the following features:

- CD-ROM based Installation Wizard to provide easy installation
- Device Configuration and Status Utility
- Wireless security using WPA with TKIP encryption, 802.1X with EAP-type Authentication
- Compatibility with both 802.11g and 802.11b network standards
- Upgradeable firmware to stay current with the latest specifications (as they become available from the Motorola website)

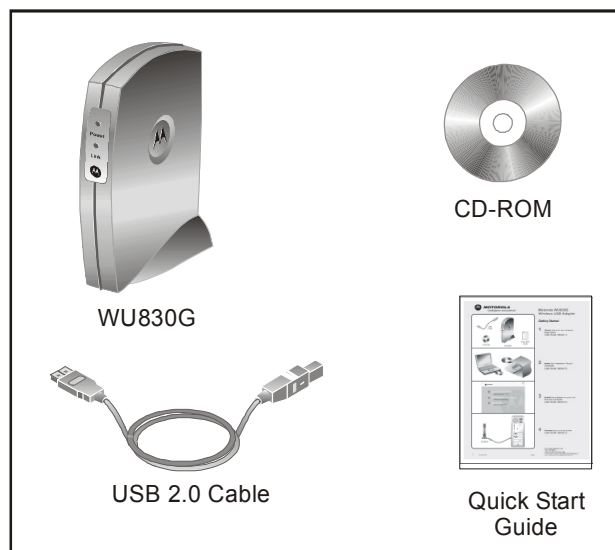
Understanding Your User Guide

The User Guide is divided into the following sections:

Overview	Describes the WU830G and its functions, the technology used, and recommended practices for using it.
Installation	Provides instructions for installing the firmware and hardware and setting up the firmware to get your adapter up and running.
Configuration	Describes the Configuration Utility that manages your WU830G.
Troubleshooting	Provides a list of frequently asked questions and possible solutions.
Glossary	List of terms and acronyms.

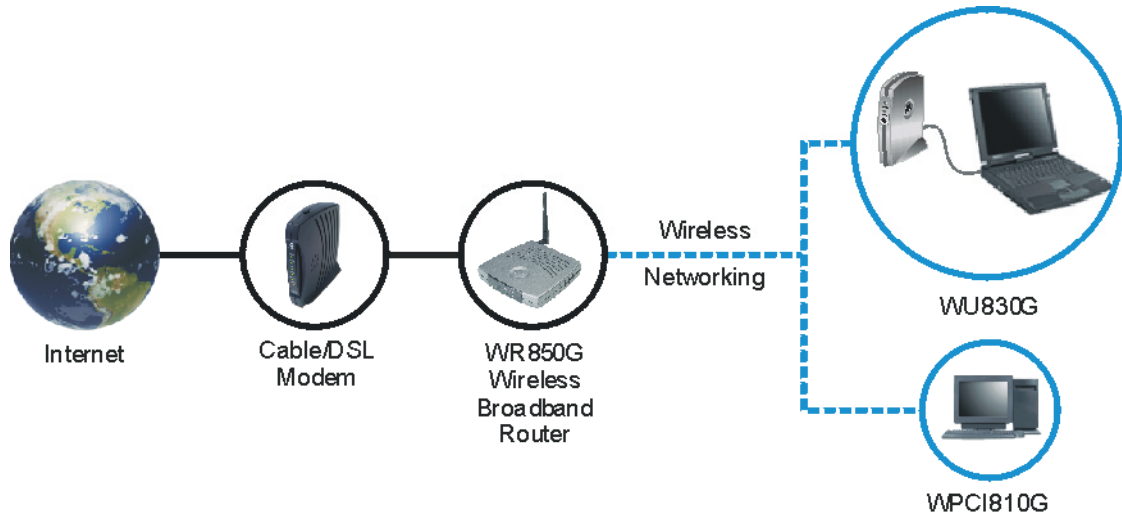
Box Contents

Your box contains the following:



Simple Home Network Diagram

Your wireless USB adapter enables you to access files, printers, and an Internet connection on your network. A sample Local Area Network (LAN) is shown below:



In the example above, the Internet communicates with the modem, which in turn communicates with the wireless router. The wireless router acts as the gateway to your network, sending information to whichever device asks for information. In this example, the USB adapter enables your notebook computer to be part of the wireless network.

Wireless Connections

Your wireless USB adapter uses a radio transmission technology defined by the Institute of Electrical and Electronics Engineers (IEEE) called 802.11 Wireless Fidelity (Wi-Fi). This standard is subdivided into distinct categories of speed and the frequency spectrum used, designated by the lower case letter after the standard.

For example, your USB adapter can work with both the 'b' and 'g' specifications. The 802.11b specification transmits data rates up to 11 Mbps while the 802.11g specification transmits data rates up to 54 Mbps. Both standards operate in the 2.4 GHz wireless range. These are theoretical speeds so your performance may vary.

A Word About Data Rates: Data rate is the speed at which individual bits of data flow through a channel. It is not the same speed at which entire files are uploaded or downloaded. These speeds will vary, and are often less than the maximum data rate. Upload and download speeds are affected by several factors including, but not limited to: the capacity of and the services offered by your cable operator or broadband service provider, channel capacity, network traffic, computer equipment, type of server, number of connections to server, and availability of Internet router(s).

USB Adapter Physical Description

Front of USB Adapter

The following illustration shows the front of the WU830G:

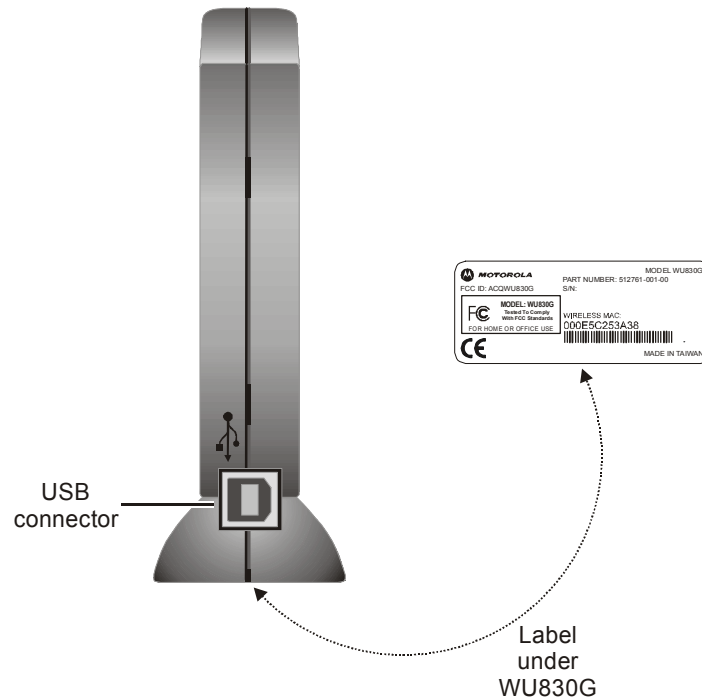


The WU830G has the following features:

	Feature	Description
1	Power LED	Indicates that the USB adapter is powered.
2	Link LED	Indicates the activity of the wireless network traffic.

Back of USB Adapter

The following illustration shows the back of the WU830G:



The following describes the features on the back and bottom of the WU830G:

Feature	Description
USB Connector	Connector for one end of the USB 2.0 cable.
Label	Includes the model number, part number, serial number, and MAC Address.
MAC Address	Located on the label under the words "WIRELESS MAC." This is the MAC Address for the WU830G.

Section 2: Installation

Before You Begin

You need to collect information so that you can setup your WU830G correctly. Depending upon where you are connecting, the type of information required is divided between business (enterprise users) and home settings (small office/home office).

Also, you need to consider the type of security to enable for your wireless connection. A discussion of the types of security available follows this section.

Enterprise Business Users

Obtain the following information from your network administrator:

- Network names (SSID) of the specific wireless networks to which you are going to connect, either WPA or WEP:
 - WPA (Wi-Fi Protected Access) wireless network key information (may include network authentication type, encryption type, and/or network key) for any WPA enabled networks to which you want to connect.
 - WEP (Wired Equivalent Privacy) wireless network key information (network key) for any WEP enabled networks to which you want to connect.
- For Microsoft Windows[®] networking, the customer name and workgroup name.
- For a network account, the domain name, a user name, and a password.
- An IP address (if not using a DHCP server).
- Networks connected to an authentication server, if any.

Small Office/Home Office Users

The access point that communicates with the WU830G has a pre-assigned network name (SSID) that the WU830G recognizes upon startup.

- If you are setting up a new wireless network and want to use WEP (Wired Equivalent Privacy) security, use any string of characters on the wireless router/access point for the network key. This will generate a HEX or ASCII key that you must match when setting up your WU830G.
- If you are connecting to an existing WEP enabled network, obtain the network key from the wireless router/access point.
- If you are connecting to a WPA-enabled access point, obtain the WPA (Wi-Fi Protected Access) wireless network key information (network authentication type, encryption type, network key) from the wireless router/access point.

Security Options

The WU830G is designed for both the home user and business. WPA is a powerful, standards-based, interoperable security technology for wireless local area networks (the subset of the future IEEE Std 802.11i standard) that encrypts data sent over radio waves.

The WPA protocol was developed to overcome the weaknesses of the WEP protocol. Both protocols require the use of network key information, and either protocol can be enabled or disabled, depending on the type of network connection being made.

Various options are available for selecting network authentication and data encryption. It is important for you to understand these options when deciding which (if any) security protocol to use.

The following table lists the network authentication options and the data encryption options available for each type of authentication:

Network Authentication		Data Encryption	
Option	Description	Option	Description
Open	With open authentication there is no data encryption.	Disabled	No encryption is used.
Shared	The network operates in Shared Key authentication mode when a network key is used for data encryption. WEP is the type of encryption used. The Shared Key authentication mode is the least secure.	WEP 64-bit or WEP 128-bit	A network key is used.
WPA-PSK	For infrastructure environments without the RADIUS infrastructure. WPA-PSK supports the use of a pre-shared key. WPA-PSK is the next generation of wireless network security for home and small office environments.	TKIP	A network key is used (more secure).
WPA	The network operates in IEEE 802.1x authentication mode. This mode is for environments with a Remote Access Dial-In User Service (RADIUS) infrastructure. This authentication is usually used by enterprise business systems or large corporations. In a RADIUS environment, various Extensible Authentication Protocols (EAPs) are supported. These may include TLS, TTLS, PEAP, and LEAP.	TKIP with four EAP methods: TLS TTLS PEAP LEAP	A network key is used (more secure).

Security Example

If you want to use a more secure protocol, the wireless network to which you are connecting must also support that protocol. For example, let's say you decide to enable WPA-PSK on your WU830G. However, the slightly older wireless network you want to connect to only supports WEP, which means that you cannot use WPA (and should use WEP) because the security protocols must match between the WU830G and the access point.

For additional information about the options supported by the WU830G, refer to Section 3, Configuration.

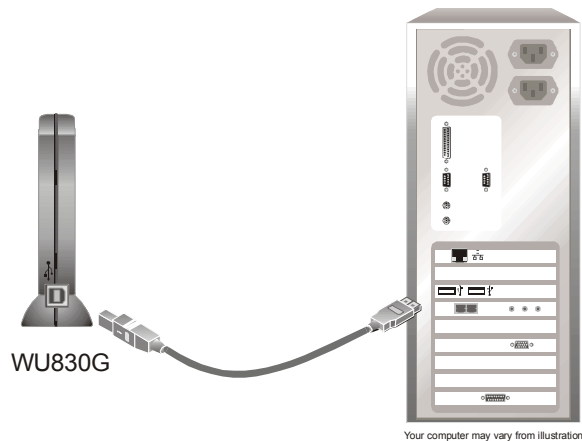
Installing Your USB Adapter

To install the software and hardware:

- 1 Insert the supplied CD-ROM into the CD-ROM drive. The software automatically starts the Installation Wizard program.
- 2 If the software does not automatically start, from your desktop, select **Start > Run > the name of your CD ROM directory:/setup.exe**.
- 3 Follow the prompts to set up your USB adapter.

If Windows 98SE prompts you for the original Windows CD-ROM, insert the CD-ROM, and direct Windows to its proper location (for example, D:\WIN98).

- 4 Locate an empty USB port on your computer.
- 5 Connect one end of the USB 2.0 cable to the USB port on the back of the WU830G and connect the other end of the USB 2.0 cable to the USB port on your laptop or desktop computer:



- 6 Complete the installation instructions supplied on the CD-ROM.

Device Configuration Setup

After installing the USB adapter and software, you will need to connect to a network. Refer to Section 3, Configuration for information on how to create detailed connectivity profiles so you can connect to a wireless network, set up security, and set up modes of operation.

Section 3: Configuration

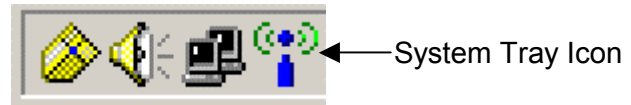
You can use the information in this section to:

- Understand the antenna icons
- Start the Configuration Utility and view link status information
- Connect to an available wireless network
- Create network profiles
- Configure security settings
- Remove a network from the profile list
- View product information
- Remove the WU830G from your computer

The screenshots shown may look slightly different from the ones in your version of the software.







Understanding the Antenna Icons

The icon in your system tray (the area at the bottom right of the screen in your Task Bar) enables you to view the status of the wireless connection and access the Motorola Wireless USB Adapter Configuration Utility.



The following table describes the icons used by the utility.

Antenna Icons

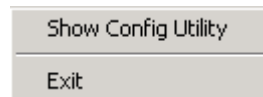
	There are no networks available.
	The signal strength is Very Low (0% to 20% signal strength).
	The signal strength is Low (20% to 40% signal strength).
	The signal strength is Good (40% to 60% signal strength).
	The signal strength is Very Good (60% to 80% signal strength).
	The signal strength is Excellent (80% to 100% signal strength).

Starting the Configuration Utility and Viewing Link Status Information

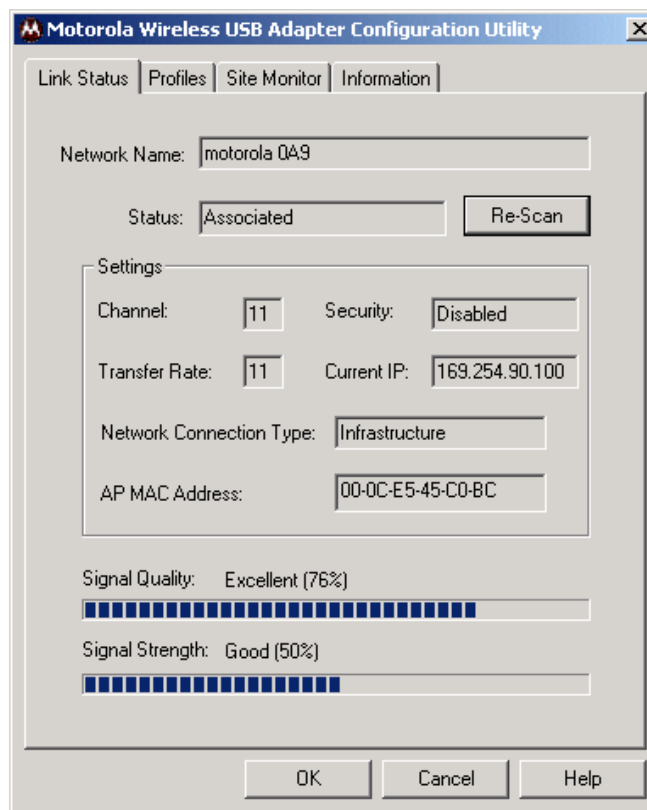
Windows XP users have the option of using the Wireless Zero Configuration utility to manage the wireless network configuration. Motorola's Wireless USB Adapter Configuration Utility provides more wireless information about the network.

To start the Motorola Wireless USB Adapter Configuration Utility:

- 1 Right-click the **antenna icon** in the system tray. The Show Configuration Utility Menu is displayed:



- 2 Select **Show Config Utility**. The Motorola Wireless USB Adapter Configuration Utility window is displayed:



The WU830G automatically detects the available networks and selects the network with the highest signal strength.

Link Status Information

The Link Status window provides:

- Currently connected network information
- Network settings
- MAC Address
- Signal information

The following table describes the fields and buttons on the Link Status window:

Field or Button	Description
Network Name	Displays the Service Set Identifier (SSID) of the network used by the WU830G. When you first access this window, the network with the highest signal strength is displayed. You can select a different network by selecting the Site Monitor tab.
Status	Displays the current connection status of the WU830G.
Re-Scan	Clicking this button enables you to search for the available wireless networks. This is useful if the WU830G was not able to establish a connection to the specified network because the link quality was poor.
Channel	Displays the channel that the WU830G is using. The possible channels are 1 through 11.
Security	Displays the security used on the current wireless connection. For example, WEP. For more information refer to "Configuring Security Settings."
Transfer Rate	Displays the current transfer rate in megabits per second. The possible transfer rates are 1, 2, 5.5, 11, 18, 24, 36, 48, and 54 Mbps. The transfer rate varies dynamically based on the link quality on the wireless connection.

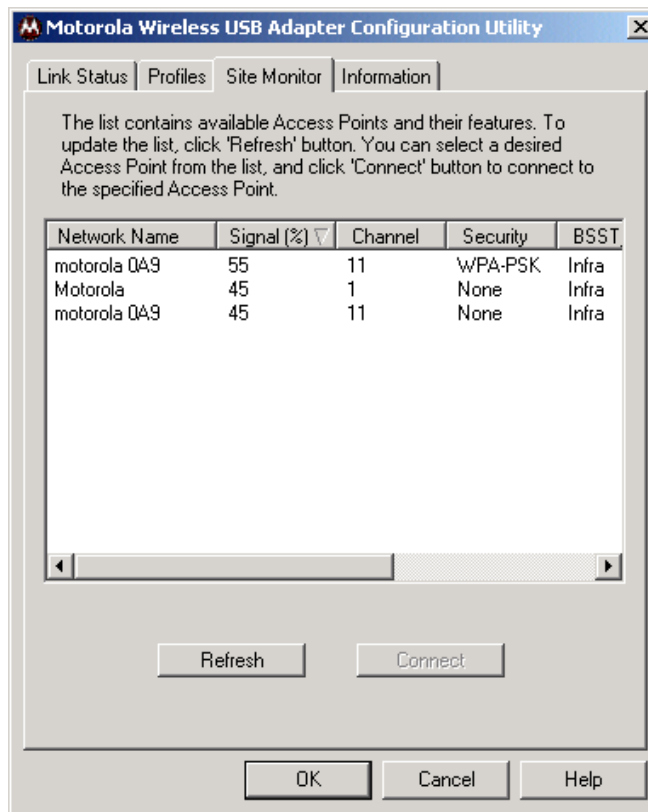
Field or Button	Description
Current IP	Displays the IP address for your current wireless connection.
Network Connection Type	Displays the type of network to which the WU830G is connected. The possible types are Infrastructure and Ad-Hoc.
AP MAC Address	Displays the wireless MAC Address.
Signal Quality	Displays the signal to noise ratio (SNR). The higher the percentage the better the wireless connection.
Signal Strength	Displays the signal strength between the access point and the WU830G. The higher the percentage the better the signal strength. If the percentage is low, try moving your WU830G closer to the access point.

Connecting to an Available Wireless Network

The Motorola Wireless USB Adapter Configuration Utility automatically searches for available wireless networks and connects to the network having the highest signal strength. You may want to select to a different network from a list of available networks.

To connect to an available network:

- 1 Right-click the **antenna icon** in the system tray and select **Show Config Utility**. The Motorola Wireless USB Adapter Configuration Utility window is displayed.
- 2 Click the **Site Monitor** tab. The following window is displayed:



This tab lists the available networks and provides information about each network. The table following this procedure describes the information displayed for each network.

- 3 To ensure that the list is current, click **Refresh**. The updated list of access points is displayed.
- 4 Select the **Network Name** to which you want to connect.
- 5 Click **Connect**. Your WU830G connects to that network.

The following table describes the information provided on the Site Monitor window:

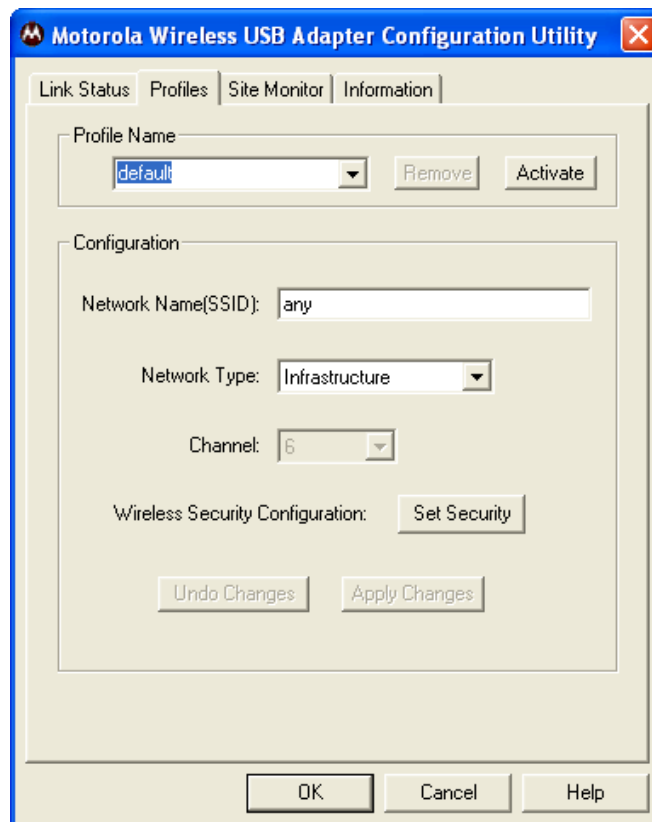
Column Heading	Description
Network Name	Displays the name of the access point.
Signal	Displays the signal strength indicated by percent.
Channel	Displays the channel frequency used by the access point. The possible channels are 1 through 11.
Security	Displays the security type used by the access point. The possible options are None, WEP, WPA-PSK, and WPA.
BSS Type	Displays the network type. The possible options are Infrastructure or Ad-Hoc.
Mode	Displays the wireless mode available with the access point. Possible modes are G or B.
MAC	Displays the MAC address of the access point.

Creating a Network Profile

The Motorola Wireless USB Adapter Configuration Utility enables you to create profile configurations for different working environments. This enables you to enter all the configuration information for a network so you are ready to go as soon as you are in range of that network. For example, this could be useful if you are going to use a wireless network at a trade show.

To create a network profile:

- 1 Right-click the **antenna icon** in the system tray and select **Show Config Utility**. The Motorola Wireless USB Adapter Configuration Utility window is displayed.
- 2 Click the **Profiles** tab. The following window is displayed:



- 3 In the Profile Name field, select **New Entry** from drop down box. The box displays a blinking cursor.
- 4 Type in a **name** for the new profile. The "default" profile contains the initial configuration setting for the WU830G.
- 5 Enter the **Network Name (SSID)**. This is the service set identifier that identifies and announces the wireless network to wireless devices. For more information, refer to the description for Network Name (SSID) in the table following this procedure.

- 6 Select the **Network Type**. The options are Infrastructure or Ad-Hoc. For more information, refer to the description for Network Type in the table following this procedure.
- 7 If your network type is Ad-Hoc, select the **Channel**. For more information, refer to the description for Channel in the table following this procedure.
- 8 Click **Set Security** and configure the security for this profile. For more information, refer to “Configuring Security Settings.”
- 9 Click **Apply Changes** to save the network profile.

The following table provides more information about the fields on the Profiles tab:

Field or Button	Description
Profile Name	The profile setting enables you to save different configurations for different working environments. The “default” profile contains the initial configuration setting for the WU830G.
Network Name (SSID)	The Network Name Service Set Identifier (SSID) identifies and announces the wireless network to wireless devices. This is a case-sensitive identifier, and must not exceed 32 characters. The SSID “any” is a special SSID. It allows your wireless device to connect to any available access point.
Network Type	Select either Ad-Hoc or Infrastructure mode depending on the network type to which you are connecting. <ul style="list-style-type: none"> ▪ Ad-Hoc mode is used for simple peer to peer networks. It allows the sharing of local resources between wireless cards without using a wireless access point. ▪ Infrastructure mode enables a wireless client to be integrated into an existing network through a wireless access point.

Field or Button	Description
Channel	<p>The channel setting is valid only when the Network Type is Ad-Hoc (no access point is being used).</p> <p>When the Network Type is Infrastructure, the channel of the card is automatically set to the same channel as the access point.</p>
Set Security	<p>Enables you to configure the security options for this profile. A security setting box is displayed. For additional information refer to “Configuring Security Settings.”</p>

Configuring Security Settings

There are a series of security windows that enable you to configure the security type for your wireless connection. To access these windows, use one of the following methods:

- By clicking Set Security on the Profiles tab
- When connecting to an access point from the Site Monitor tab and a password or other information is required to connect to that access point, the system automatically displays the correct security window

The WU830G displays windows for you to enter information based on the type of security used by the access point. For example, if you try to connect to an access point with WPA security enabled, the WU830G displays a security window for WPA authentication.

To successfully connect to the wireless network, the WU830G must match the security settings used by the access point.

To establish the security settings you must first choose the authentication option that establishes either an open or secure verification of communication with an access point. The four authentication options are Open, Shared, WPA-PSK and WPA.

After you choose the authentication option, you then choose the data encryption setting.

The following table lists the network authentication options and the data encryption options available for each type of authentication:

Network Authentication		Data Encryption	
Option	Description	Option	Description
Open	With open authentication there is no data encryption.	Disabled	No encryption is used.
Shared	The network operates in Shared Key authentication mode when a network key is used for data encryption. WEP is the type of encryption used. The Shared Key authentication mode is the least secure.	WEP 64-bit or WEP 128-bit	A network key is used.

Network Authentication		Data Encryption	
Option	Description	Option	Description
WPA-PSK	For infrastructure environments without the RADIUS infrastructure. WPA-PSK supports the use of a pre-shared key. WPA-PSK is the next generation of wireless network security for home and small office environments.	TKIP	A network key is used (more secure).
WPA	<p>The network operates in IEEE 802.1x authentication mode. This mode is for environments with a Remote Access Dial-In User Service (RADIUS) infrastructure.</p> <p>This authentication is usually used by enterprise business systems or large corporations.</p> <p>In a RADIUS environment, various Extensible Authentication Protocols (EAPs) are supported. These may include TLS, TTLS, PEAP, and LEAP.</p>	TKIP with four EAP methods: TLS TTLS PEAP LEAP	A network key is used (more secure).

Setting Security for a Wireless Network or a Profile

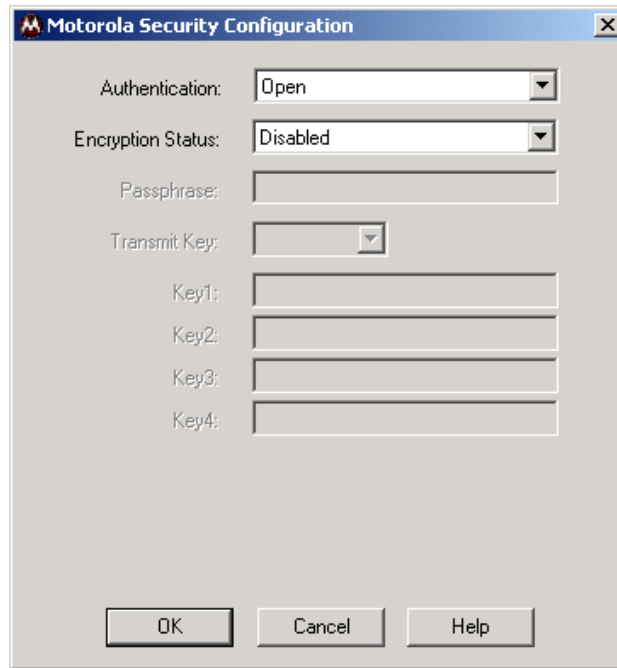
To set up security for a selected wireless network or profile:

- 1 Select a wireless network on the Site Monitor tab and click **Connect** or enter profile information on the Profile tab and click **Set Security**. The Motorola Security Configuration window is displayed.
- 2 Select the **Authentication**.
- 3 Select the **Encryption Status**.
- 4 If necessary, enter additional information to complete the window. For additional information, refer to the topics on Open, Shared, WPA-PSK, and WPA Authentication.
- 5 After completing the security information, click **OK**.

The following subsections describe the security windows for each authentication type.

Open Authentication

The following window displays the Motorola Security Configuration with Open Authentication:

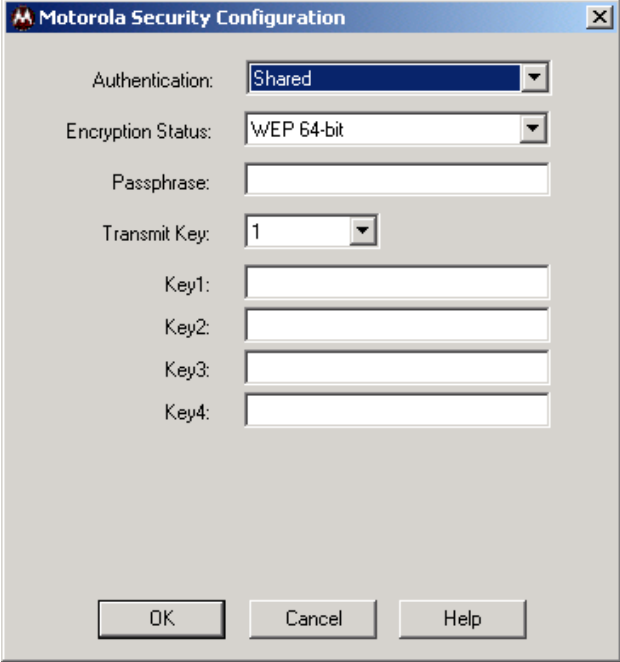


The following table describes the encryption status and the fields that become active with that encryption status:

Encryption Status	Description
Disabled	Selecting this option leaves your wireless connection without any security protection. It is the only option available with Open Authentication. No additional fields become active.

Shared Authentication

The following window displays the Motorola Security Configuration with Shared Authentication:



The image shows a dialog box titled "Motorola Security Configuration". It contains the following fields and controls:

- Authentication: A dropdown menu with "Shared" selected.
- Encryption Status: A dropdown menu with "WEP 64-bit" selected.
- Passphrase: An empty text input field.
- Transmit Key: A dropdown menu with "1" selected.
- Key1: An empty text input field.
- Key2: An empty text input field.
- Key3: An empty text input field.
- Key4: An empty text input field.

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

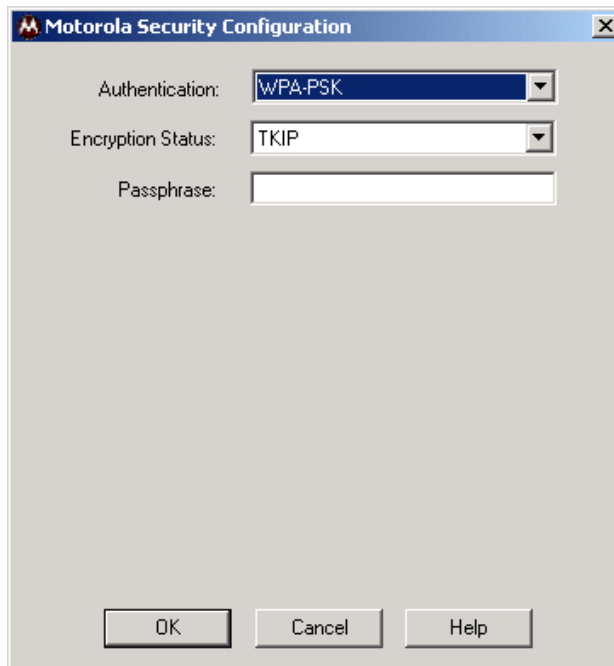
The following table describes the encryption status and the fields that become active with that encryption status:

Encryption Status	Description
WEP 64-bit or WEP 128-bit	Select the same encryption that is used by your access point.
	<hr/> <p>Passphrase Some access points/wireless clients can use a passphrase instead of WEP keys. The passphrase automatically generates the WEP keys.</p> <p>The passphrase should be 8 to 63 characters long.</p> <p>If you use a passphrase, you need to make sure that the WEP keys generated by that passphrase match the keys on the access point.</p> <p>If your wireless router/wireless access point is a Motorola product, the same passphrase will generate the same WEP keys.</p>
	<hr/> <p>Transmit Key There are four available WEP keys. By setting the transmit key, you can specify which key (1 to 4) to use to encrypt the wireless packets. This is also known as the key index on some access points.</p>
	<hr/> <p>Key 1 through Key 4 The key used for packet encryption. If WEP 64-bit encryption is selected, then this field requires ten characters. If WEP 128-bit encryption is selected, then 26 characters are required. The key must be in hexadecimal format.</p> <p>You may have to manually enter the key if the passphrase generates WEP keys that do not match the wireless router/wireless access point.</p> <hr/>

WPA-PSK Authentication

WPA-PSK is a pre-shared key authentication method. To use this method, you need to obtain the passphrase used by the access point to which you want to connect. Packets are encrypted based on the encryption method used.

The following window displays the Motorola Security Configuration with WPA-PSK Authentication:



The following table lists the fields displayed when WPA-PSK authentication is used:

Field	Description
Encryption Status	TKIP is the encryption algorithm used on the packets.
Passphrase	Enter the same passphrase as the access point to which you want to connect. The passphrase should be 8 to 63 characters long.

WPA Authentication

WPA authentication provides both packet encryption and network/user authentication. In this type of security:

- The packets are encrypted using the TKIP algorithm
- The network is authenticated to be the network you want to connect to
- Your identity is authenticated by the network

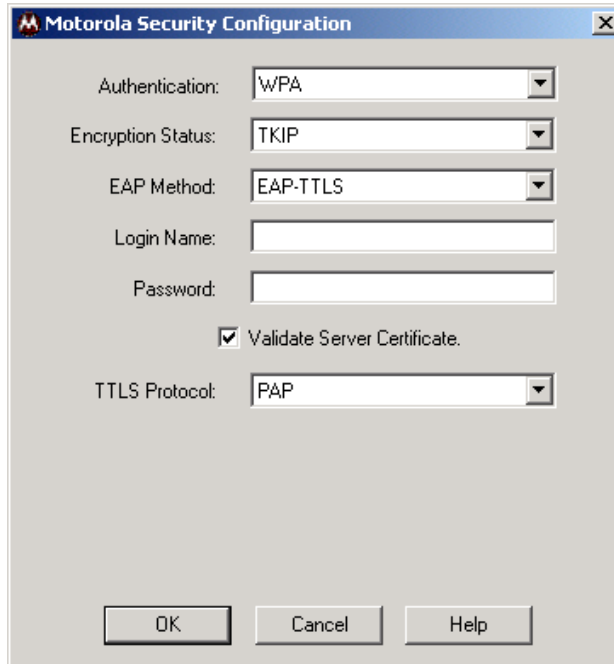
This security method does not require you to obtain a WPA passphrase. The server that authenticates your identity issues a WPA passphrase automatically once it accepts your identity.

There are four different (Extensible Authentication Protocol) EAP methods that you can select on this window:

- EAP-TLS
- EAP-TTLS
- EAP-PEAP
- LEAP

The different EAP methods have been created to support different authentication methods and their associated network security policies. Depending on which EAP method you select, different fields are active.

The following example window displays the Motorola Security Configuration window with WPA Authentication and the EAP-TTLS method selected:



The image shows a dialog box titled "Motorola Security Configuration". It contains the following fields and options:

- Authentication: WPA (dropdown menu)
- Encryption Status: TKIP (dropdown menu)
- EAP Method: EAP-TTLS (dropdown menu)
- Login Name: (text input field)
- Password: (text input field)
- Validate Server Certificate.
- TTLS Protocol: PAP (dropdown menu)

At the bottom of the dialog box are three buttons: OK, Cancel, and Help.

The following table lists the fields displayed when WPA authentication is used:

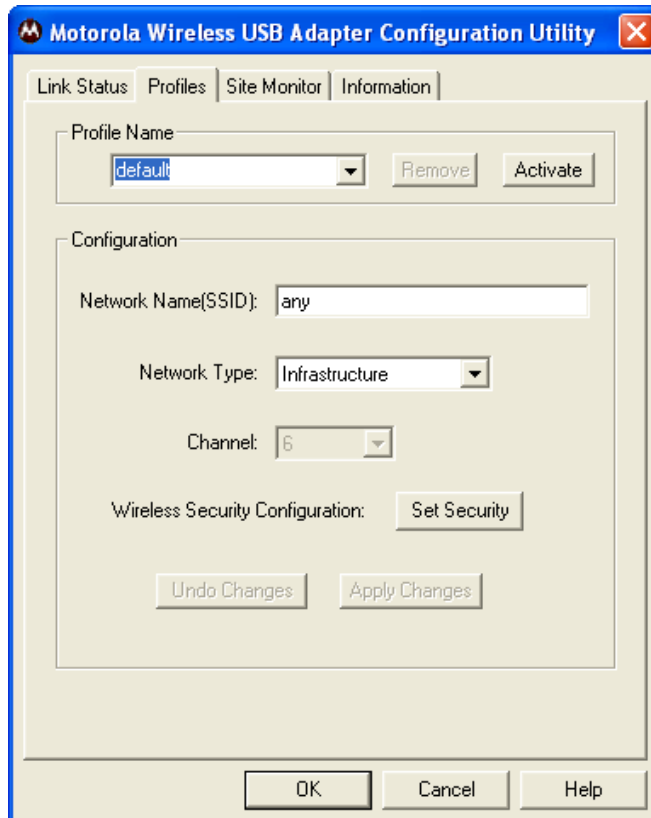
Field	Description				
Encryption Status	TKIP is the encryption algorithm used on the packets.				
EAP Method	There are four different (Extensible Authentication Protocol) EAP methods that you can select on this window: <hr/> <table border="0"> <tr> <td style="vertical-align: top; padding-right: 10px;">EAP-TLS</td> <td> <p>This method requires a Login Name and Certificate issued by the RADIUS server to which you are connecting.</p> <p>Together, the login name and the certificate enable the RADIUS server to authenticate your identity.</p> <p>You can also choose to authenticate the identity of the RADIUS server by enabling the Validate Server Certificate check box.</p> </td> </tr> <tr> <td style="vertical-align: top; padding-right: 10px;">EAP-TTLS</td> <td> <p>This method requires a Login Name and Password.</p> <p>You must also choose an additional TTLS Protocol. The TTLS protocol must match the one on your target RADIUS server. The four TTLS Protocols are:</p> <p>PAP CHAP MS CHAP MS CHAP v2</p> <p>You can also choose to authenticate the RADIUS server identity by checking the Validate Server Certificate check box.</p> </td> </tr> </table> <hr/>	EAP-TLS	<p>This method requires a Login Name and Certificate issued by the RADIUS server to which you are connecting.</p> <p>Together, the login name and the certificate enable the RADIUS server to authenticate your identity.</p> <p>You can also choose to authenticate the identity of the RADIUS server by enabling the Validate Server Certificate check box.</p>	EAP-TTLS	<p>This method requires a Login Name and Password.</p> <p>You must also choose an additional TTLS Protocol. The TTLS protocol must match the one on your target RADIUS server. The four TTLS Protocols are:</p> <p>PAP CHAP MS CHAP MS CHAP v2</p> <p>You can also choose to authenticate the RADIUS server identity by checking the Validate Server Certificate check box.</p>
EAP-TLS	<p>This method requires a Login Name and Certificate issued by the RADIUS server to which you are connecting.</p> <p>Together, the login name and the certificate enable the RADIUS server to authenticate your identity.</p> <p>You can also choose to authenticate the identity of the RADIUS server by enabling the Validate Server Certificate check box.</p>				
EAP-TTLS	<p>This method requires a Login Name and Password.</p> <p>You must also choose an additional TTLS Protocol. The TTLS protocol must match the one on your target RADIUS server. The four TTLS Protocols are:</p> <p>PAP CHAP MS CHAP MS CHAP v2</p> <p>You can also choose to authenticate the RADIUS server identity by checking the Validate Server Certificate check box.</p>				

EAP Method continued	EAP-PEAP	<p>This method requires a Login Name and Password.</p> <p>You must also choose an additional PEAP Protocol. The PEAP protocol must match the one on your target RADIUS server. The three PEAP Protocols are:</p> <p>MD5 Challenge EAP-GTC MS CHAP v2</p> <p>You can also choose to authenticate the RADIUS server identity by checking the Validate Server Certificate check box.</p>
	LEAP	<p>This is a Cisco based EAP method. It only requires a Login Name and Password for user authentication.</p>
Login Name	Required for EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP methods.	
Certificate	Active field for EAP-TLS method.	
Password	Required for EAP-TTLS, EAP-PEAP, and LEAP methods.	

Removing a Network from the Profile List

To remove a wireless network from your network profile list:

- 1 Right-click the **antenna icon** in the system tray and select **Show Config Utility**. The Motorola Wireless USB Adapter Configuration Utility window is displayed.
- 2 Click the **Profiles** tab. The following window is displayed:

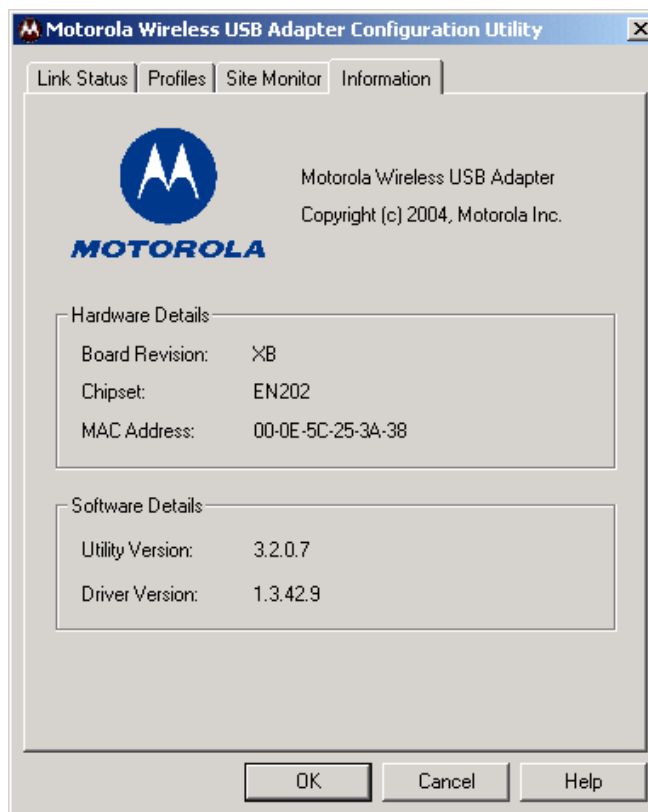


- 3 In the Profile Name field, click the down arrow and select the **profile name** for the network you want to remove.
- 4 Click **Remove**. The network is removed from your network list.
- 5 Click **Apply Changes** or **OK** to save the change.

Viewing Product Information

To view WU830G product information, including the current software versions:

- 1 Right-click the **antenna icon** in the system tray and select **Show Config Utility**. The Motorola Wireless USB Adapter Configuration Utility window is displayed.
- 2 Click the **Information** tab. The Information tab provides the firmware version number and hardware and software details about the Motorola Wireless USB Adapter:

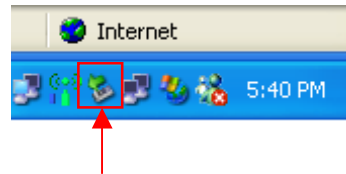


Removing the Wireless USB Adapter

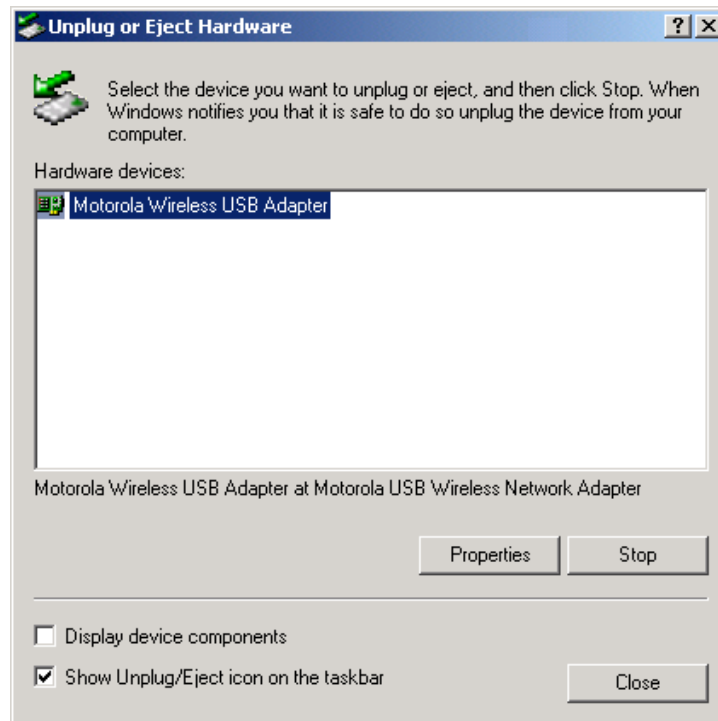
You can safely remove the Wireless USB Adapter while the computer is operating.

To remove the adapter:

- 1 Locate the **device eject icon** located in your system tray. In the illustration below, it is the third icon from the left – the picture of a card and a left-pointing arrow.



- 2 Double-click the **device eject icon**. The Unplug or Eject Hardware window is displayed:



- 3 Highlight the **device** you want to remove.
- 4 Click **Stop**. The Stop a Hardware device window is displayed:



- 5 Confirm that the device listed in the window is the device you want to stop.
- 6 Click **OK**. After you receive a message telling you the device is stopped, you can safely remove the Wireless USB Adapter.

Section 4: Troubleshooting

This section details possible solutions to common problems that may occur in using the WU830G.

Contact Us

If you are unable to locate a solution here, please access our website at www.motorola.com/broadband/consumers for the latest information. You can also reach us 7 days a week, 24 hours a day at 1-877-466-8646.

Register the WU830G

To register the WU830G, access the following website:

<https://broadbandregistration.motorola.com>

Hardware Solutions

My computer is experiencing difficulty connecting to the wireless network.

- Ensure that both your computer and wireless access point are powered on.
- Ensure that your wireless USB adapter is installed correctly and is active.
- Ensure that your wireless USB adapter and access point radio signals are enabled. Review your access point's documentation for further instructions.
- Ensure that your wireless USB adapter for your computer and the wireless access point have the same security settings that will allow your computer to access the wireless network. Refer to the Configuration information of the documentation that came with your access point.
- Verify that the Access Control List (ACL) is not configured to block your computer. Refer to the Configuration information of the documentation that came with your access point.

- Ensure that your wireless USB adapter is within range of your access point or is not behind an obstruction; for example, metal structures will interfere with the signal, as will 2.4 GHz cordless phones, and microwaves.
- Ensure that your access point antenna is connected.

I would like to test if my Internet connection is live.

Use the *ping* command to test the connection. Before attempting, determine the IP Address of your USB adapter.

- 1 Open a command prompt by clicking **Start** and **Run**.
- 2 For Windows 98 and ME, in the *Open* field, type **command** and press **Enter** or **OK**.

For Windows 2000 and XP, type **cmd**. Or, navigate using your **Start** button to **Programs>Accessories>Command Prompt**.

- 3 In the Command window, type **ipconfig**.
 - You should see an IP address for your adapter, for example:

```
Ethernet Adapter Local Area Connection:

Connection-specific DNS Suffix. . . : Example.example.example.com.

IP Address. . . . . : 192.168.10.10

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.10.1
```

- 4 If using a router at home, in the Command window, type **ping** followed by the **Router's IP address** and press **Enter**. For example, type **ping 192.168.10.1**

The router's IP address is most likely the default gateway.

- If you receive a reply (the first word will be *Reply...*), then your computer is connected to the router. Proceed to Step 4.
- If you do NOT receive a reply, repeat steps 1 – 4 on a different computer to verify that the first computer is not the cause of the problem.

- 5 In the Command window, type **ping** and your **ISP's default gateway IP Address** and press **Enter**. You can determine your ISP's default gateway by examining your modem and or router. Refer to the instructions provided with your modem/router.
 - If you receive a reply (For example, *Reply from 216.109.125.72...*), then your connection to the Internet is live.
 - If you do NOT receive a reply, repeat steps 1 – 5 on a different computer to verify that the first computer is not the cause of the problem.
- 6 If you cannot determine your ISP's default gateway, ping www.yahoo.com or another known web location.

Section 5:Glossary

A

Access Point (AP)

A device that provides wireless LAN connectivity to wireless clients (stations).

Adapter

A device or card that connects a computer, printer, or other peripheral device to the network or to some other device. A wireless adapter connects a computer to the wireless LAN.

Address translation

See *NAT*.

Ad-Hoc Network

A temporary local area network connecting access clients together, usually just for the duration of the communication session. The clients communicate directly to each other and not through an established, such as through a router.

Also known as: IBSS (Independent Basic Service Set).

ASCII

The American Standard Code for Information Interchange refers to alphanumeric data for processing and communication compatibility among various devices; normally used for asynchronous transmission.

B

Bandwidth

The transmission capacity of a medium in terms of a range of frequencies. Greater bandwidth indicates the ability to transmit more data over a given period of time.

bps

Bits Per Second

Broadband

A communications medium that can transmit a relatively large amount of data in a given time period.

BSS

Basic Service Set. A configuration of Access Points that communicate with each other without resorting any infrastructure. Also known as Ad-Hoc networks. Also see *ESS*.

C**CHAP**

Challenge Handshake Authentication Protocol. It is a password-based, challenge-response, mutual authentication protocol that uses the industry-standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses.

Client

In a client/server architecture, a client is a computer that requests files or services such as file transfer, remote login, or printing from the server. On an IEEE 802.11b/g wireless LAN, a client is any host that can communicate with the access point. Also called a CPE. A wireless client is also called a "station." Also see *server*.

Coaxial Cable

A type of cable consisting of a center wire surrounded by insulation and a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference. Coaxial cable has high bandwidth and can support transmission over long distances.

CPE

Customer Premise Equipment: typically computers, printers, etc., that are connected to the gateway at the subscriber location. CPE can be provided by the subscriber or the cable service provider. Also called a client.

Crossover Cable

A crossover cable is a cable that is used to interconnect two computers by "crossing over" (reversing) their respective pin contacts. A crossover cable is sometimes known as a null modem.

D**Default Gateway**

A routing device that forwards traffic not destined to a station within the local subnet.

DHCP

A Dynamic Host Configuration Protocol server dynamically assigns IP addresses to client hosts on an IP network. DHCP eliminates the need to manually assign static IP addresses by “leasing” an IP address and subnet mask to each client. It enables the automatic reuse of unused IP addresses.

DMZ

DeMilitarized Zone. This service opens one IP address to the Internet, usually for online gaming, and acts as a buffer between the Internet and your network.

DNS

The Domain Name System is the Internet system for converting domain names (like www.motorola.com) to IP addresses. A DNS server contains a table matching domain names such as Internetname.com to IP addresses such as 192.169.9.1. When you access the world-wide web, a DNS server translates the URL displayed on the browser to the destination website IP address. The DNS lookup table is a distributed Internet database; no one DNS server lists all domain name to IP address matches.

Domain Name

A unique name, such as motorola.com, that maps to an IP address. Domain names are typically much easier to remember than IP addresses. See *DNS*.

Download

To copy a file from one computer to another. You can use the Internet to download files from a server to a computer.

Driver

Software that enables a computer to interact with a network or other device. For example, there are drivers for printers, monitors, graphics adapters, modems, Ethernet, USB, HPNA, and many others.

DSL

Digital Subscriber Line

DSSS

Direct-Sequence Spread Spectrum. DSSS is a transmission technology used in WLAN transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

Dynamic IP Address

An IP address that is temporarily leased to a host by a DHCP server. The opposite of *Static IP Address*.

E**EAP-GTC**

Extensible Authentication Protocol-Generic Token Card.

EAP-LEAP

Extensible Authentication Protocol-Lightweight Extensible Authentication Protocol is an authentication implementation of 802.1X by Cisco, which provides a challenge-response authentication mechanism and dynamic WEP key assignment.

EAP-PEAP

Extensible Authentication Protocol-Protected EAP is an authentication protocol that requires certificate-based RADIUS server authentication, and supports an extensible set of user authentication methods.

EAP-TLS

Extensible Authentication Protocol-Transport Layer Security is an authentication protocol that requires the station and the RADIUS server to both prove their identities using public key encryption (digital certificates or smart cards).

EAP-TTLS

Extensible Authentication Protocol-Tunneled Transport Layer Security is an authentication protocol that requires certificate-based RADIUS server authentication, and supports an extensible set of user authentication methods.

ESS

An Extended Service Set (ESS) is a set of two or more BSSs that form a single subnetwork. See also *BSS*.

Ethernet

The most widely used LAN type, also known as IEEE 802.3. The most common Ethernet networks are 10Base-T, which provide transmission speeds up to 10 Mbps, usually over unshielded, twisted-pair wire terminated with RJ-45 connectors. Fast Ethernet (100Base-T) provides speeds up to 100 Mbps. “Base” means “baseband technology” and “T” means “twisted pair cable.”

Each Ethernet port has a physical address called the MAC address. Also see *MAC address*.

Event

A message generated by a device to inform an operator or the network management system that something has occurred.

F**Firewall**

A security software system on some devices that enforces an access control policy between the Internet and the LAN for protection.

Firmware

Code written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off. Firmware is upgradeable.

FTP

File Transfer Protocol is a standard Internet protocol for exchanging files between computers. FTP is commonly used to download programs and other files to a computer from web pages on Internet servers.

G**Gateway**

A device that enables communication between networks using different protocols. See also *router*.

GUI

Graphical User Interface

H**Hexadecimal**

A base-sixteen numbering system that uses sixteen sequential numbers (0 to 9 and the letters A to F) as base units before adding a new position. On computers, hexadecimal is a convenient way to express binary numbers.

Host

In IP, a host is any computer supporting end-user applications or services with full two-way network access. Each host has a unique host number that combined with the network number forms its IP address.

Host also can mean:

- A computer running a web server that serves pages for one or more web sites belonging to organization(s) or individuals
- A company that provides this service
- In IBM environments, a mainframe computer

I**ICMP**

Internet Control Message Protocol is a protocol used for error, problem, and informational messages sent between IP hosts and gateways. ICMP messages are processed by the IP software and are not usually apparent to the end-user.

IEEE

The Institute of Electrical and Electronics Engineers, Inc. (<http://www.ieee.org>) is an organization that produces standards, technical papers, and symposiums for the electrical and electronic industries and is accredited by ANSI. 802.11b and 802.11g are examples of standards they have produced.

Internet

A worldwide collection of interconnected networks using TCP/IP.

IP

Internet Protocol is a set of standards that enable different types of computers to communicate with one another and exchange data through the Internet. IP provides the appearance of a single, seamless communication system and makes the Internet a virtual network.

IP Address

A unique 32-bit value that identifies each host on a TCP/IP network. TCP/IP networks route messages based on the destination IP address.

For a Class C network, the first 24 bits are the network address and the final 8 bits are the host address; in dotted-decimal format it appears “network.network.network.host.”

ISDN

Integrated Services Digital Network

ISP

Internet Service Provider

L**LAN**

Local Area Network. A local area network provides a full-time, high-bandwidth connection over a limited area such as a home, building, or campus. Ethernet is the most widely used LAN standard.

LEAP

Lightweight Extensible Authentication Protocol (LEAP) is an authentication implementation of 802.1X by Cisco, which provides a challenge-response authentication mechanism and dynamic WEP key assignment.

M**MAC Address**

The Media Access Control address is a unique, 48-bit value permanently saved in the ROM at the factory to identify each Ethernet network device. It is expressed as a sequence of 12 hexadecimal digits printed on the unit's label. You need to provide the MAC Address to the cable service provider. Also called an Ethernet address, physical address, hardware address, or NIC address.

MB

One megabyte; equals 1,024 x 1,024 bytes, 1,024 kilobytes, or about 8 million bits.

Mbps

Million bits per second (megabits per second). A rate of data transfer.

MS CHAP v2

Microsoft's implementation of Challenge Handshake Authentication Protocol.

MTU

The Maximum Transmission Unit is the largest amount of data that can be transmitted in one discrete message on a given physical network. The MTU places an upper bound on the size of a message that can be transferred by the network in a single frame. Messages exceeding the MTU must be fragmented before transmission, and reassembled at the destination.

Multicast

A data transmission sent from one sender to multiple receivers. See also *broadcast* and *unicast*.

N**NAT**

Network Address Translation is an Internet standard for a LAN to use one set of IP addresses for internal traffic and a second set of IP addresses for external traffic. NAT provides some security because the IP addresses of LAN computers are invisible on the Internet.

Network

Two or more computers connected to communicate with each other. Networks have traditionally been connected using some kind of wiring.

NIC

A Network Interface Card converts computer data to serial data in a packet format that it sends over the LAN. A NIC is installed in an expansion slot or can be built-in. Every Ethernet NIC has a MAC address permanently saved in its ROM.

P**PAP**

Password Authentication Protocol.

Packet

The unit of data that is routed between the sender and destination on the Internet or other packet-switched network.

PCMCIA

The Personal Computer Memory Card International Association sets international standards for connecting peripherals to portable computers. Laptop computers typically have a PCMCIA slot that can hold one or two PC Cards to provide features such as Ethernet or wireless connectivity.

PING

A network utility that tests host reachability by sending a small packet to the host and waiting for a reply. If you PING a computer IP address and receive a reply, you know the computer is reachable over the network. It also stands for "Packet Internet Groper."

Port Triggering

A mechanism that allows incoming communication with specified applications.

PPP

Point-to-Point Protocol is used to transport other protocols, typically for simple links over serial lines. It is most commonly used to access the Internet with a dial-up modem.

PPPoE

Point-to-Point Protocol over Ethernet. Used by many DSL Internet Service Providers for broadband connection.

PPTP

Point-to-Point Tunneling Protocol encapsulates other protocols. It is a new technology to create VPNs developed jointly by several vendors.

Private IP Address

An IP address assigned to a computer on the LAN by the DHCP server for a specified lease time. Private IP addresses are invisible to devices on the Internet. See also *Public IP Address*.

Protocol

A formal set of rules and conventions for exchanging data. Different computer types (for example PC, UNIX, or mainframe) can communicate if they support common protocols.

Public IP Address

The IP address assigned by the service provider. A public IP address is visible to devices on the Internet. See also *Private IP Address*.

R**RADIUS**

Remote Access Dial In User Service. This is a widely deployed protocol for network access authentication, authorization, and accounting.

RJ-11

The most common type of connector for household or office phones.

RJ-45

An 8-pin modular connector; the most common connector type for 10Base-T or 100Base-T Ethernet networks.

Roaming

The ability to transfer your wireless session from one AP to another AP seamlessly.

ROM

Read-Only Memory.

Router

On IP networks, a device connecting at least two networks, which may or may not be similar. A router is typically located at a gateway between networks. A router operates on OSI network layer 3. It filters packets based on the IP address, examining the source and destination IP addresses to determine the best route on which to forward them.

A router is often included as part of a network switch. A router can also be implemented as software on a computer.

Routing Table

A table listing available routes that is used by a router to determine the best route for a packet.

RTS

Request To Send.

S**Server**

In a client/server architecture, a dedicated computer that supplies files or services such as file transfer, remote login, or printing to clients. Also see *client*.

Service Provider

A company providing Internet connection services to subscribers.

SMTP

Simple Mail Transfer Protocol is a standard Internet protocol for transferring e-mail.

Static IP Address

An IP address that is permanently assigned to a host. Normally, a static IP address must be assigned manually. The opposite of *Dynamic IP Address*.

Station

IEEE 802.11b term for wireless client.

Subscriber

A user who accesses television, data, or other services from a service provider.

Subnet Mask

A methodology that determines what the router will examine for the destination of an IP address. A router delivers packets using the network address.

Switch

On an Ethernet network, a switch filters frames based on the MAC address, in a manner similar to a bridge. A switch is more advanced because it can connect more than two segments.

T**TCP**

Transmission Control Protocol on OSI transport layer four, provides reliable transport over the network for data transmitted using IP (network layer three). It is an end-to-end protocol defining rules and procedures for data exchange between hosts on top of connectionless IP. TCP uses a timer to track outstanding packets, checks error in incoming packets, and retransmits packets if requested.

TCP/IP

The Transmission Control Protocol/Internet Protocol suite provides standards and rules for data communication between networks on the Internet. It is the worldwide Internetworking standard and the basic communications protocol of the Internet.

Tunnel

To place packets inside other packets to send over a network. The protocol of the enclosing packet is understood by each endpoint, or tunnel interface, where the packet enters and exits the network. VPNs rely on tunneling to create a secure network.

Tunneling requires the following protocol types:

- A carrier protocol, such as TCP, used by the network that the data travels over
- An encapsulating protocol, such as IPSec, L2F, L2TP, or PPTP, that is wrapped around the original data
- A passenger protocol, such as IP, for the original data

U**UDP**

User Datagram Protocol. A method used along with the IP to send data in the form of message units (datagram) between network devices over a LAN or WAN.

Unicast

A point-to-point data transmission sent from one sender to one receiver. This the normal way you access websites. See also *multicast*.

USB

Universal Serial Bus is a computer interface for add-on devices such as printers, scanners, mice, modems, or keyboards. USB supports data transfer rates of 12 Mbps and plug-and-play installation. You can connect up to 127 devices to a single USB port.

V**VoIP**

Voice over Internet Protocol is a method to exchange voice, fax, and other information over the Internet. Voice and fax have traditionally been carried over traditional telephone lines of the PSTN (Public Switched Telephone Network) using a dedicated circuit for each line. VoIP enables calls to travel as discrete data packets on shared lines. VoIP is an important part of the convergence of computers, telephones, and television into a single integrated information network.

VPN

A virtual private network is a private network that uses “virtual” connections (tunnels) routed over a public network (usually the Internet) to provide a secure and fast connection; usually to users working remotely at home or in small branch offices. A VPN connection provides security and performance similar to a dedicated link (for example, a leased line), but at much lower cost.

W**WAN**

A wide-area network provides a connection over a large geographic area, such as a country or the whole world. The bandwidth depends on need and cost, but is usually much lower than for a LAN.

WAP

Wireless Access Point or Wireless Access Protocol. See also *Access Point*.

WEP

Wired Equivalent Privacy encryption protects the privacy of data transmitted over a wireless LAN. WEP uses keys to encrypt and decrypt transmitted data. The access point must authenticate a client before it can transfer data to another client. WEP is part of IEEE 802.11b.

Wi-Fi®

Wireless fidelity (pronounced why-fy) brand name applied to products supporting IEEE 802.11b/g.

WLAN

Wireless LAN.

WPA

Wi-Fi Protected Access. A security regimen developed by IEEE for protection of data on a WLAN.

WWW

World Wide Web. An interface to the Internet that you use to navigate and hyperlink to information.

Visit our website at:
www.motorola.com/broadband/consumers



512708-001
03/04

MGBI