



Wireless-G Business USB Network Adapter with RangeBooster

USER GUIDE

BUSINESS SERIES

Copyright and Trademarks

Specifications are subject to change without notice. Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2006 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

WARNING: This product contains chemicals, including lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. ***Wash hands after handling.***

How to Use this User Guide

This user guide has been designed to make understanding networking with the USB Network Adapter easier than ever. Look for the following items when reading this User Guide:



This checkmark means there is a note of interest and is something you should pay special attention to while using the USB Network Adapter.



This exclamation point means there is a caution or warning and is something that could damage your property or the USB Network Adapter.



This question mark provides you with a reminder about something you might need to do while using the USB Network Adapter.

In addition to these symbols, there are definitions for technical terms that are presented like this:

word: definition.

Also, each figure (diagram, screenshot, or other image) is provided with a figure number and description, like this:

Figure 0-1: Sample Figure Description

Figure numbers and descriptions can also be found in the "List of Figures" section.

Table of Contents

Chapter 1: Introduction	1
Welcome	1
What's in this User Guide?	2
Chapter 2: Planning your Wireless Network	4
Network Topology	4
Roaming	4
Network Layout	5
Chapter 3: Getting to Know the Wireless-G Business USB Network Adapter	6
The LED Indicator	6
Chapter 4: Setting up and Connecting the Wireless-G Business USB Network Adapter	7
Starting the Setup	7
Connecting the Adapter	8
Setting up the Adapter	9
Chapter 5: Using the Wireless Network Monitor	19
Accessing the Wireless Network Monitor	19
Using the Wireless Network Monitors	19
Link Information	19
Profiles	22
Create a New Profile	23
Editing a Profile	32
Site Survey	41
Troubleshooting	42
Administration	42
Chapter 6: The Administrative Functions in the Wireless Network Monitor	45
Accessing the Wireless Network Monitor	45
Using the Administrative Functions in the Wireless Network Monitor	45
Classification	46
Security Monitor	49
Appendix A: Troubleshooting	61
Common Problems and Solutions	61
Frequently Asked Questions	62
Appendix B: Windows XP Wireless Zero Configuration	65

Windows XP Wireless Zero Configuration	65
Appendix C: Wireless Security	68
Security Precautions	68
Security Threats Facing Wireless Networks	68
Appendix D: Windows Help	71
Appendix E: Glossary	72
Appendix F: Specifications	77
Appendix G: Warranty Information	79
Appendix H: Regulatory Information	80
Appendix I: Contact Information	86

List of Figures

Figure 3-1: LED	6
Figure 4-1: Setup Wizard's Welcome Screen	7
Figure 4-2: Setup Wizard's License Agreement	8
Figure 4-3: Connecting the Adapter	8
Figure 4-4: Available Wireless Network	9
Figure 4-5: WEP	10
Figure 4-6: WPA - Personal	10
Figure 4-7: WPA2 - Personal	11
Figure 4-8: Confirm New Settings	11
Figure 4-9: Congratulations	11
Figure 4-10: Creating a Profile	12
Figure 4-11: Network Settings - Wireless Mode	12
Figure 4-12: Ad-Hoc Mode Settings	13
Figure 4-13: Wireless Security - WEP	13
Figure 4-14: Wireless Security - WPA Personal	14
Figure 4-15: Wireless Security - WPA2 Personal	14
Figure 4-16: Wireless Security - WPA Enterprise-EAP-TLS	15
Figure 4-17: Wireless Security - WPA Enterprise-PEAP	15
Figure 4-18: Wireless Security - WPA2 Enterprise-EAP	16
Figure 4-19: Wireless Security - WPA2 Enterprise-PEAP	16
Figure 4-20: Wireless Security - RADIUS - EAP-TLS	17
Figure 4-21: Wireless Security - RADIUS - PEAP	17
Figure 4-22: Wireless Security - LEAP	18
Figure 4-23: Congratulations Screen	18
Figure 5-1: Wireless Network Monitor Icon	19
Figure 5-2: Link Information - Connection	19
Figure 5-3: Link Information - Wireless Network Status	20
Figure 5-4: Link Information - Wireless Network Statistics	21
Figure 5-5: Profiles	22
Figure 5-6: Import a Profile	22
Figure 5-7: Export a Profile	22
Figure 5-8: Creating a Profile - Available Wireless Network	23

Figure 5-9: Creating a Profile - WEP Key Needed	23
Figure 5-10: Creating a Profile - WPA-Personal	24
Figure 5-11: Creating a Profile - Congratulations	24
Figure 5-12: Creating a Profile - Manual Setup - Network Settings	25
Figure 5-13: Creating a Profile - Manual Setup - Wireless Mode	25
Figure 5-14: Creating a Profile - Manual Setup - Wireless Security - Disabled	26
Figure 5-15: Creating a Profile - Manual Setup - Wireless Security - WEP	26
Figure 5-16: Creating a Profile - Manual Setup - Wireless Security - WPA Personal	27
Figure 5-17: Creating a Profile - Manual Setup - Wireless Security - WPA2 Personal	27
Figure 5-18: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - EAP-TLS	28
Figure 5-19: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - PEAP	28
Figure 5-20: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - EAP-TLS	29
Figure 5-21: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - PEAP	29
Figure 5-22: Creating a Profile - Manual Setup - Wireless Security - RADIUS - EAP-TLS	30
Figure 5-23: Creating a Profile - Manual Setup - Wireless Security - RADIUS - PEAP	30
Figure 5-24: Creating a Profile - Manual Setup - Wireless Security - LEAP	31
Figure 5-25: Creating a Profile - Manual Setup - Confirm New Settings	31
Figure 5-26: Creating a Profile - Manual Setup - Congratulations	32
Figure 5-27: Editing a Profile	32
Figure 5-28: Editing a Profile - Wireless Mode	33
Figure 5-29: Editing a Profile - Ad Hoc Mode	33
Figure 5-30: Editing a Profile - Wireless Security	34
Figure 5-31: Editing a Profile - Wireless Security - WEP	34
Figure 5-32: Editing a Profile - Wireless Security - WPA Personal	35
Figure 5-33: Editing a Profile - Wireless Security -WPA2 Personal	35
Figure 5-34: Editing a Profile - Wireless Security - WPA Enterprise - EAP-TLS	36
Figure 5-35: Editing a Profile - Wireless Security - WPA Enterprise - PEAP	36
Figure 5-36: Editing a Profile - Wireless Security -WPA2 Enterprise - EAP-TLS	37
Figure 5-37: Editing a Profile - Wireless Security - WPA2 Enterprise - PEAP	37
Figure 5-38: Editing a Profile - Wireless Security - RADIUS - EAP-TLS	38
Figure 5-39: Editing a Profile - Wireless Security - RADIUS - PEAP	38
Figure 5-40: Editing a Profile - Wireless Security - LEAP	39
Figure 5-41: Editing a Profile - Network Settings	39
Figure 5-42: Editing a Profile - Confirm New Settings	40

Figure 5-43: Editing a Profile - Congratulations	40
Figure 5-44: Site Survey	41
Figure 5-45: Troubleshooting	42
Figure 5-46: Administration	42
Figure 5-47: Administration - Login Access Point Account	43
Figure 5-48: Administration - Modify Access Point Account	43
Figure 5-49: Administration - Security Monitor Account	44
Figure 6-1: Wireless Network Monitor Icon	45
Figure 6-2: Administration - Login Security Monitor Administration - Login Security Monitor Account	45
Figure 6-3: Classification	45
Figure 6-4: AP Classification	46
Figure 6-5: Client Classification	46
Figure 6-6: Trusted Mac Address	47
Figure 6-7: Allowed SSID Configuration	47
Figure 6-8: Allowed Vendor List Configuration	48
Figure 6-9: Allowed SSID Configuration	48
Figure 6-10: Allowed Channel Configuration	49
Figure 6-11: Security Monitor - Channel Usage	49
Figure 6-12: Security Monitor - AP Inventory	50
Figure 6-13: Security Monitor - Client Inventory	50
Figure 6-14: Security Monitor - Alerts Summary	51
Figure 6-15: Security Monitor - POP-UP Alert	51
Figure 6-16: Security Monitor - Alert List	52
Figure 6-17: Alert Details	52
Figure 6-18: Security Monitor - Alert Advice	53
Figure 6-19: Security Monitor - Windows Firewall Screen	60
Figure B-1: Wireless Network Monitor Icon	65
Figure B-2: Windows XP - Use Windows XP Wireless Configuration	65
Figure B-3: Windows XP Wireless Zero Configuration Icon	65
Figure B-4: Available Wireless Network	66
Figure B-5: No Wireless Security	66
Figure B-6: Network Connection - Wireless Security	67

Chapter 1: Introduction

Welcome

Thank you for choosing the Wireless-G Business USB Network Adapter. Setting up your network and your Wireless-G Business USB Network Adapter is easier than ever.

The Wireless-G USB Network Adapter is the simple way to add or upgrade wireless connectivity in your computer. Just connect it into your computer's USB port and enjoy incredible high-speed wireless network access while not having to run cable wires.

RangeBooster technology increases your wireless network's range up to two times, and its throughput by up to 35%. Unlike ordinary wireless technologies that are confused by signal reflections, RangeBooster uses two smart receivers at each end to detect and decode reflected signals at distances where standard technologies give up. You'll find that "dead spots" in the wireless coverage area are reduced, too.

But what does all of this mean?

PCs equipped with wireless cards and adapters can communicate without cumbersome cables. By sharing the same wireless settings, within their transmission radius, they form a wireless network.

Once you're connected, you can keep in touch with your e-mail, access the Internet, and share files and other resources such as printers and network storage with other computers on the network, wherever your work takes you, without cables.

The Advanced security features makes this solution ideal for your business. Advanced wireless security using Wi-Fi Protected Access™ (WPA2 Enterprise) with up to 256-bit encryption, and the new Wireless Security Monitoring functionality gives your business the visibility and protection it needs. When used with a Linksys WAP200, the Wireless Security Monitoring alerts you of possible wireless intruders and vulnerabilities in the wireless network deployment.

The included Setup Wizard walks you through configuring the Adapter to your wireless network settings, step by step. Use the instructions in this Guide to help you set up and connect the Adapter using the Setup Wizard. These instructions should be all you need to get the most out of the Adapter.

adapter: a device that adds network functionality to your PC.

network: a series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

802.11g: a wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

802.11b: a wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

encryption: encoding data transmitted in a network

What's in this User Guide?

This user guide covers the steps for setting up and using the Wireless-G Business USB Network Adapter.

- **Chapter 1: Introduction**
This chapter describes the Adapter's applications and this User Guide.
- **Chapter 2: Planning Your Wireless Network**
This chapter discusses a few of the basics about wireless networking.
- **Chapter 3: Getting to Know the Wireless-G Business USB Network Adapter**
This chapter describes the physical features of the Adapter.
- **Chapter 4: Setting up and Connecting the Wireless-G Business USB Network Adapter**
This chapter instructs you on how to install and configure the Adapter.
- **Chapter 5: Using the Wireless Network Monitor**
This chapter shows you how to use the Adapter's Wireless Network Monitor.
- **Chapter 6: Administration Functions in the Network Monitor**
This chapter shows you how to use the administration features of the Adapter's Wireless Network Monitor.
- **Appendix A: Troubleshooting**
This appendix describes some problems and solutions, as well as frequently asked questions, regarding installation and use of the Adapter.
- **Appendix B: Windows XP Zero Configuration**
This appendix describes how to use the Windows XP Zero Configuration.
- **Appendix C: Wireless Security**
This appendix discusses security issues regarding wireless networking and measures you can take to help protect your wireless network.
- **Appendix D: Windows Help**
This appendix describes how you can use Windows Help for instructions about networking, such as installing the TCP/IP protocol.
- **Appendix E: Glossary**
This appendix gives a brief glossary of terms frequently used in networking.
- **Appendix F: Specifications**
This appendix provides the Adapter's technical specifications.

Wireless-G Business USB Network Adapter with RangeBooster

- **Appendix G: Warranty Information**
This appendix supplies the Adapter's warranty information.
- **Appendix H: Regulatory Information**
This appendix supplies the Adapter's regulatory information.
- **Appendix I: Contact Information**
This appendix provides contact information for a variety of Linksys resources, including Technical Support.

Chapter 2: Planning your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one wireless adapter. Computers in a wireless network must be configured to share the same radio channel. Several PCs equipped with wireless cards or adapters can communicate with each another to form an ad-hoc network.

Linksys wireless adapters also provide users access to a wired network when using an access point or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless PC in an infrastructure network can talk to any computer in a wired network infrastructure via the access point or wireless router.

An infrastructure configuration extends the accessibility of a wireless PC to a wired network, and can double the effective wireless transmission range for two wireless adapter PCs. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network can be doubled.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless PC within your network and the access points will pick up the wireless PC's signal, if they both share the same channel and SSID.

Before you consider roaming, choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

topology: the physical layout of a network.

access point: a device that allows wireless-equipped computers and other devices to communicate with a wired network

ad-hoc: a group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

infrastructure: a wireless network that is bridged to a wired network via an access point.

roaming: the ability to take a wireless device from one access point's range to another without losing the connection.

ssid: your wireless network's name.

Network Layout

Linksys wireless access points and wireless routers have been designed for use with 802.11a, 802.11b, and 802.11g products. With 802.11g products communicating with the 802.11b standard and some products incorporating both “a” and “g”, products using these standards can communicate with each other.

Access points and wireless routers are compatible with 802.11a, 802.11b and 802.11g adapters, such as the PC Cards for your laptop computers, PCI Cards for your desktop PC, and USB Adapters for when you want to enjoy USB connectivity.

When you wish to connect your wired network with your wireless network, the network ports on the access points and wireless routers can be connected to Linksys switches or routers.

With these, and many other, Linksys products, your networking options are limitless. Go to the Linksys website at www.linksys.com for more information about wireless products.

Chapter 3: Getting to Know the Wireless-G Business USB Network Adapter

The LED Indicators

The Network Adapter's LEDs display information about network activity.



Figure 3-1: LEDs

Power *Green.* The Wireless LED lights up when the Adapter is powered on.

Link *Green.* The Link/Act LED lights up when the Adapter has an active connection.

Chapter 4: Setting up and Connecting the Wireless-G Business USB Network Adapter

Starting the Setup

The Wireless-G Business USB Network Adapter Setup Wizard will guide you through the installation procedure. The Setup Wizard will install the driver and Wireless Network Monitor, as well as connect and configure the Adapter.



IMPORTANT: Do not connect the Adapter until you are instructed to do so or the setup will not work correctly.

Insert the **Setup Wizard CD-ROM** into your CD-ROM drive. The Setup Wizard should run automatically, and the *Welcome* screen should appear. If it does not, click the **Start** button and choose **Run**. In the field that appears, enter **D:\setup.exe** (if “D” is the letter of your CD-ROM drive).

On the *Welcome* screen, you have the following choices:

Click Here to Start- Click the **Click Here to Start** button to begin the software installation process.

User Guide - Click the **User Guide** button to open the PDF file of this User Guide.

Exit - Click the **Exit** button to exit the Setup Wizard.

1. To install the Adapter, click the **Click Here to Start** button on the *Welcome* screen.



Figure 4-1: Setup Wizard's Welcome Screen

Wireless-G Business USB Network Adapter with RangeBooster

2. After reading the License Agreement, click the **Next** button if you agree and want to continue the installation, or click the **Cancel** button to end the installation.
3. Windows will begin copying the files onto your PC.

Connecting the Adapter

1. Connect one end of the included USB cable to the Adapter's USB port.
2. Connect the other end of the cable to one of the USB ports on your computer.
3. The Power LED should light up when the Adapter is plugged in.
4. Raise the antennas. Make sure the antennas point straight up into the air, at a 90° angle from the Adapter. This will ensure optimum wireless operating range and performance.
5. Click **Next**. It may take a minute before the next screen appears.

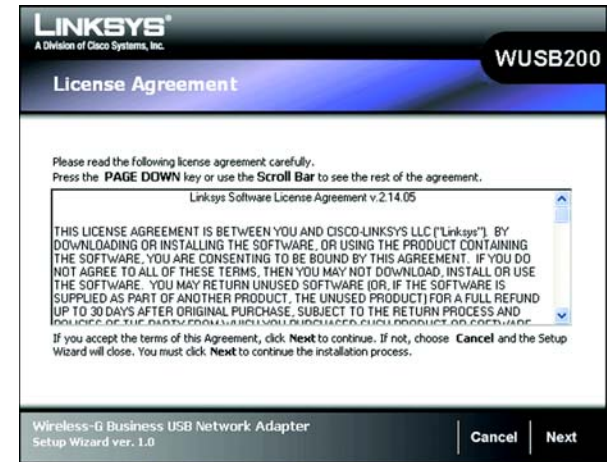


Figure 4-2: Setup Wizard's License Agreement

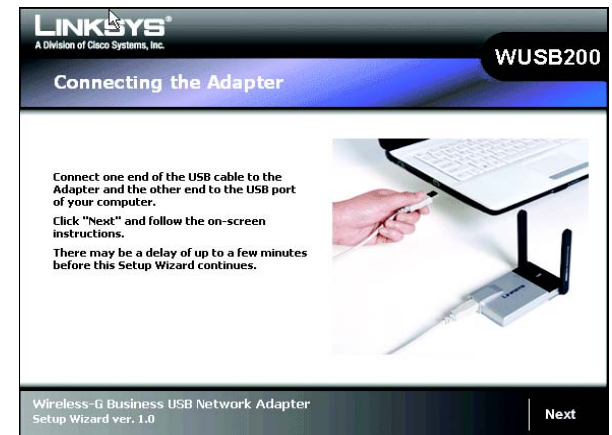


Figure 4-3: Connecting the Adapter

Setting up the Adapter

The next screen to appear will be the *Available Wireless Network* screen.

This screen provides two options for setting up the Adapter.

- **Available Wireless Network. (For most users.)** Use this option if you already have a network set up. The networks available to this Adapter will be listed on this screen. You can choose one of these networks and click the **Connect** button to connect to it. Click the **Refresh** button to update the Available Wireless Network list.
- **Manual Setup.** If your network is not listed on this screen, select **Manual Setup** to set up the adapter manually. This method of setting up the Adapter is intended for Advanced Users only.

The setup for each option is described, step by step, under the appropriate heading on the following pages.

Click **Exit** to close the Setup Wizard, if you wish to set up the Adapter later.



Figure 4-4: Available Wireless Network

Available Wireless Network

The available networks are listed in the table on the center of the screen by SSID. Select the wireless network you wish to connect to and click the **Connect** button. (If you do not see your network listed, you can click the **Refresh** button to bring the list up again.) If the network utilizes wireless security, you will need to configure security on the Adapter. If not, you will be taken directly to the *Congratulations* screen.

1. If you have wireless security enabled on your network, continue to step 2. Only *One* of these security screens will be shown. If you don't have wireless security enabled, continue to step 3.
2. Wireless Security

If your network has WEP, WPA-Personal, or WPA2-Personal wireless security enabled, then that security screen will appear. Continue to the screen for your wireless security.

WEP

If your network has the wireless security WEP (Wired Equivalent Privacy), RADIUS or LEAP enabled, this screen will appear. For connecting with RADIUS or LEAP, click **Connect**, then continue to the next section "Manual Setup" on page 12.

Security - Select **WEP**.

WEP - Select **64-bit** or **128-bit**.

Then enter a passphrase or WEP key.

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption,

wep (wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.

encryption: encoding data transmitted in a network.

wpa (wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.



Figure 4-5: WEP

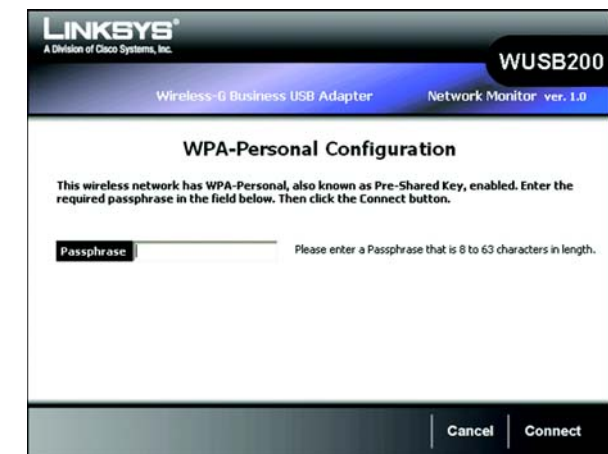


Figure 4-6: WPA - Personal

enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

Then click **Connect** and proceed to Step 3.

WPA-Personal

If your network has the wireless security WPA-Personal (Wi-Fi Protected Access) enabled, this screen will appear.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.



Figure 4-7: WPA2 - Personal



Figure 4-8: Confirm New Settings

WPA2-Personal

If your network has the wireless security WPA2-Personal enabled, this screen will appear.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.



Figure 4-9: Congratulations

3. The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button.

To edit the new settings, click the **Back** button. To exit the Manual Setup through the Wireless Network Monitor, click **Exit**.

4. After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network and return to the Link Information screen.

Click **Return to Profile Screen** to keep the current settings active and return to the *Profiles* screen.

For more information about the Wireless Network Monitor, refer to *Chapter 5: Using the Wireless Network Monitor*.

Congratulations! The installation of the Wireless-G Business USB Network Adapter is complete.

To check the link information, search for available wireless networks, or make additional configuration changes, proceed to Chapter 5: Using the Wireless Network Monitor.



Figure 4-10: Creating a Profile

Manual Setup

If your network is not listed with the available networks, you can use Manual Setup.

1. Click **Manual Setup** on the *Available Wireless Network* screen to set up the adapter manually.
2. The *Network Settings* screen from the Wireless Network Monitor will appear. If your network has a router or other DHCP server, click the radio button next to **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, click the radio button next to **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

IP Address - This IP Address must be unique to your network.

Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.



Figure 4-11: Network Settings - Wireless Mode

Default Gateway - Enter the IP address of your network's Gateway here.

DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

3. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want to connect to a wireless router or access point. Click the **Ad-Hoc Mode** radio button if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

4. If you chose **Infrastructure Mode**, go to Step 5 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.

5. If your wireless network does not have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 6.

If your wireless network has wireless security, select the method of security used: **WEP**, **WPA/WPA2-Personal**, **WPA/WPA2-Enterprise**, **RADIUS**, or **LEAP**. WEP stands for Wired Equivalent Privacy, and WPA



Figure 4-12: Ad-Hoc Mode Settings

encryption: encoding data transmitted in a network.

wep (wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.



Figure 4-13: Wireless Security - WEP

stands for Wi-Fi Protected Access. WPA uses a stronger security method than WEP and WPA2 defines an even stronger encryption, authentication, and key management than WPA. RADIUS stands for Remote Authentication Dial-In User Service. LEAP stands for Lightweight Extensible Authentication Protocol. It uses username and password-based authentication between a wireless client and a RADIUS server. Click the **Next** button to continue or the **Back** button to return to the previous screen.

Proceed to the appropriate section for your security method: WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, RADIUS, or LEAP.

WEP - Select 64-bit or 128-bit encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

Advanced Users

TX Key - The default transmit key number is 1. If your network’s access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 only uses AES for encryption. Select **TKIP** or **AES** for encryption for WPA Personal. Then enter a Passphrase that is 8-63 characters in length.

wpa (wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

wpa2 offers a stronger encryption than wpa by using the AES (Advanced Encryption Standard) which is a block cipher with block sizes of 128, 192 or 256 bits.

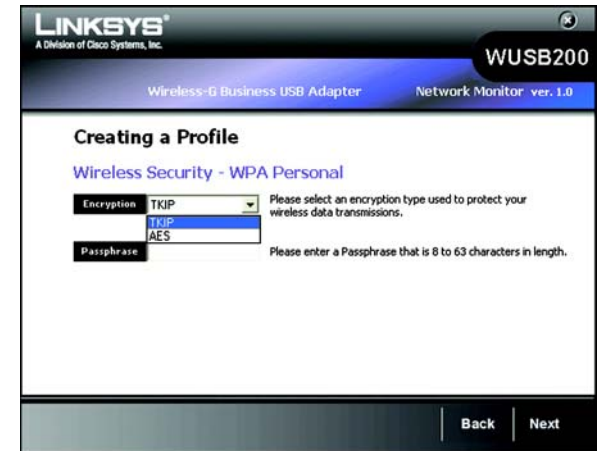


Figure 4-14: Wireless Security - WPA Personal



Figure 4-15: Wireless Security - WPA2 Personal

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

WPA2 Personal

Enter a Pre-shared Key that is 8-63 characters in length.

Pre-shared Key - Enter a Pre-shared Key of 8-63 characters in the *Pre-shared Key* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

The screenshot shows the Linksys WUSB200 Network Monitor interface. The title bar includes the Linksys logo, 'A Division of Cisco Systems, Inc.', and 'WUSB200'. Below the title bar, it says 'Wireless-G Business USB Adapter' and 'Network Monitor ver. 1.0'. The main content area is titled 'Creating a Profile' and 'Wireless Security - WPA Enterprise'. It features several fields: 'Authentication' (EAP-TLS), 'Login Name', 'Server Name', 'Certificate', and 'Encryption' (AES). Each field has a corresponding instruction: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Server Name used for authentication. (Optional)', 'Please select the certificate used for authentication.', and 'Please select the encryption type used to protect the wireless data transmissions.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-16: Wireless Security - WPA Enterprise-EAP-TLS

The screenshot shows the Linksys WUSB200 Network Monitor interface. The title bar includes the Linksys logo, 'A Division of Cisco Systems, Inc.', and 'WUSB200'. Below the title bar, it says 'Wireless-G Business USB Adapter' and 'Network Monitor ver. 1.0'. The main content area is titled 'Creating a Profile' and 'Wireless Security - WPA Enterprise'. It features several fields: 'Authentication' (PEAP), 'Login Name', 'Password', 'Server Name', 'Inner Authen.' (EAP-MSCHAPv2), and 'Encryption' (AES). Each field has a corresponding instruction: 'Please select the authentication method that you use to access your network.', 'Enter the Login Name used for authentication.', 'Enter the Password used for authentication.', 'Enter the Server Name used for authentication. (Optional)', 'Please select the inner authentication method used inside the PEAP tunnel.', and 'Please select the encryption type used to protect the wireless data transmissions.' At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-17: Wireless Security - WPA Enterprise-PEAP

WPA Enterprise

WPA Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP, but only AES encryption method can be used.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

Click the **Next** button to continue or the **Back** button to return to the previous screen.

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The 'Authentication' dropdown is set to 'EAP-TLS'. The 'Encryption' dropdown is set to 'AES'. The 'Login Name' and 'Server Name' fields are empty. The 'Certificate' dropdown is also empty. The 'Back' and 'Next' buttons are at the bottom right.

Figure 4-18: Wireless Security - WPA2 Enterprise-EAP

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA2 Enterprise'. The 'Authentication' dropdown is set to 'PEAP'. The 'Encryption' dropdown is set to 'AES'. The 'Login Name' and 'Server Name' fields are empty. The 'Password' field is empty. The 'Inner Authen.' dropdown is set to 'EAP-MSCHAPv2'. The 'Back' and 'Next' buttons are at the bottom right.

Figure 4-19: Wireless Security - WPA2 Enterprise-PEAP

WPA2 Enterprise

WPA2 Enterprise features WPA2 security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, Trust Any. Then select the authentication method used inside the PEAP tunnel.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - RADIUS'. The 'Authentication' dropdown is set to 'PEAP' and the 'Inner Authen.' dropdown is set to 'EAP-MSCHAPv2'. The 'Login Name', 'Password', and 'Server Name' fields are empty. The 'Back' and 'Next' buttons are visible at the bottom right.

Figure 4-20: Wireless Security - RADIUS - EAP-TLS

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - RADIUS'. The 'Authentication' dropdown is set to 'PEAP' and the 'Inner Authen.' dropdown is set to 'EAP-MSCHAPv2'. The 'Login Name', 'Password', and 'Server Name' fields are empty. The 'Back' and 'Next' buttons are visible at the bottom right.

Figure 4-21: Wireless Security - RADIUS - PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a user name and password based system.

Login method - Select the login method your network is using, **Manual Login** or **Windows Login**.

If you select manual login, enter the username and password in the username and password field accordingly. Enter the password again in the confirm field.

6. The *Congratulations* screen will appear next. Click **Connect to Network** to implement the new settings and return to the *Link Information* screen. Click **Return to Profile screen** to return to the Creating a Profile screen.

Congratulations! Your manual setup through the Wireless Network Monitor is complete.



The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - LEAP'. At the top, it says 'LINKSYS A Division of Cisco Systems, Inc.' and 'WUSB200'. Below that, it says 'Wireless-G Business USB Adapter' and 'Network Monitor ver. 1.0'. The main heading is 'Creating a Profile' and the sub-heading is 'Wireless Security - LEAP'. There are three input fields: 'User Name' with the instruction 'Enter the Login Name used for authentication.', 'Password' with 'Enter the Password used for authentication.', and 'Confirm' with 'Re-enter the Password again.'. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 4-22: Wireless Security - LEAP



Figure 4-23: Congratulations Screen

Chapter 5: Using the Wireless Network Monitor

Use the Wireless Network Monitor to check the link information, set up profiles of your wireless settings, search for available wireless networks, troubleshoot your wireless connections, or administer the accounts that hold privileges to access the Security Monitor.

Accessing the Wireless Network Monitor

After installing the Adapter, the Wireless Network Monitor icon will appear in the system tray of your computer. If the Wireless Network Monitor is enabled, then the icon will be green. If the Wireless Network Monitor is disabled or the Adapter is not connected, then the icon will be gray.



Figure 5-1: Wireless Network Monitor Icon

Using the Wireless Network Monitors

The opening screen of the Wireless Network Monitor is the **Link Information** screen. From this screen, you can find out how strong the current wireless signal is and how good the connection's quality is. You can also perform configuration changes or create connection profiles by clicking the **Profiles** tab. To view the available wireless networks, click the **Site Survey** tab. To troubleshoot the current connections or view the FAQ pages, click the **Troubleshooting** tab. To perform the administrative tasks of the account information or specify email alert addresses, click the **Administration** tab.

Link Information

The *Connection* screen of the Link Information tab displays signal strength and link quality information of the current connection. It also provides tabs to click for additional connection information.

Signal Strength - The Signal Strength bar indicates signal strength from low to high; low is red, medium is yellow and high is green.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection from low to high; low is red, medium is yellow and high is green.

Click the **Status** or **Statistics** tabs to view additional information about the wireless network connection.



Figure 5-2: Link Information - Connection

Status

Click the **Status** tab to view the *Wireless Network Status* screen. The *Status* screen provides information on your current network settings.

Status- This shows the status of the connection.

SSID - Service Set Identifier, a 32-character unique identifier attached to the header of packets sent over a WLAN. This is the unique name used to identify a network.

Wireless Mode - The mode of the wireless network currently in use is displayed here.

Transfer Rate - This shows the speed at which your wireless network transmits.

Channel - This displays the channel used by your network.

Security - The status of the wireless security feature is displayed here.

Authentication - This is your wireless network's authentication method.

IP Address - The IP Address of the Adapter is displayed here.

Subnet Mask - The Subnet Mask of the Adapter is shown here.

Default Gateway - The Default Gateway address of the Adapter is displayed here.

DNS - This is the DNS (Domain Name Service) address of the Adapter.

DHCP - This shows the status of the DHCP server.

MAC Address- The MAC address of the wireless network's access point or wireless router is shown here.

Click the **Statistics** tab to view the *Wireless Network Statistics* screen. Click the **Connection** button to return to the initial *Link Information* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile.

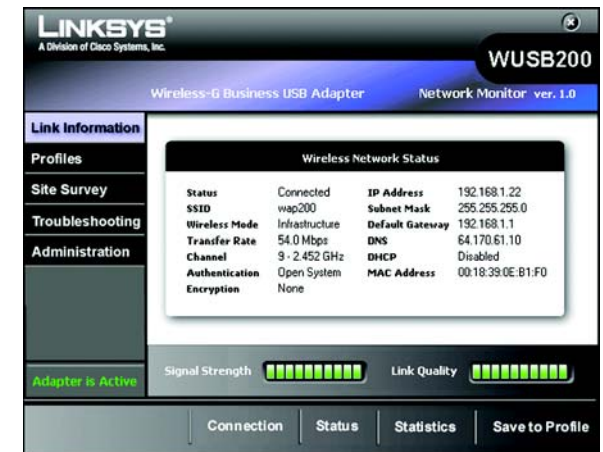


Figure 5-3: Link Information - Wireless Network Status

Statistics

The *Statistics* screen provides statistics on your current network settings.

Transmit Rate - This is the data transfer rate of the current connection. (In Auto mode, the Adapter dynamically shifts to the fastest data transfer rate possible at any given time.)

Receive Rate - This is the rate at which data is received.

Packets Received - This shows the packets received by the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Packets Transmitted - This shows the packets transmitted from the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Bytes Received - This shows the bytes received by the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Bytes Transmitted - This shows the bytes transmitted by the Adapter, in real time, since connecting to the wireless network or since the *Clear Counters* button was last pressed.

Driver Version - This shows the version of the Adapter's driver.

Signal Strength - This is the intensity of the wireless signal received by the Adapter.

Transmit Power - This is the power at which the Adapter transmits.

Total Up Time - This indicates the cumulative total of the Adapter's connection time.

Signal Strength - The Signal Strength bar indicates the signal strength.

Link Quality - The Link Quality bar indicates the quality of the wireless network connection.

Click the **Connection** button to return to the initial *Link Information* screen. Click the **Status** button to go to the *Wireless Network Status* screen. Click the **Save to Profile** button to save the currently active connection settings to a profile. Click the **Clear Counters** button to reset the statistics counter.

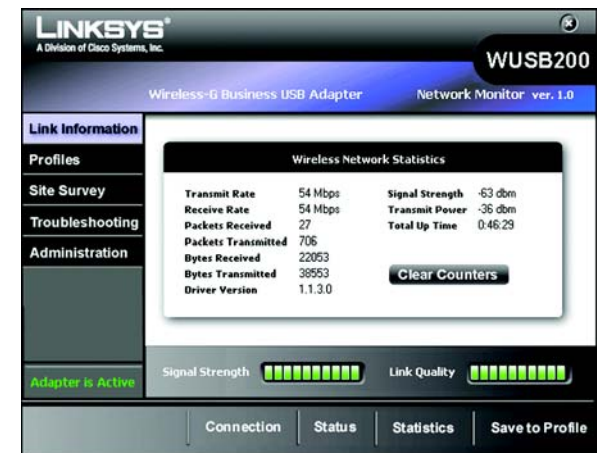


Figure 5-4: Link Information - Wireless Network Statistics

Profiles

The *Profiles* screen lets you save different configuration profiles for different network setups. The table on the left displays a list of available profiles with their profile names and SSIDs.

Profile - The name of the profile is displayed here.

SSID - The SSID or unique name of the wireless network is displayed here.

Profile Information

For each profile selected, the following are listed:

Wireless Mode - This is the mode of the wireless network currently in use.

Transfer Rate - The data transfer rate of the current connection is shown here.

Channel - This is the channel to which the wireless network devices are set.

Authentication - The authentication setting for the network is shown here.

Encryption - The status of the wireless security feature is displayed here.

Connect - To connect to a wireless network using a specific profile, select the profile, and click **Connect**.

New - Click the **New** button to create a new profile. See the next section, “Create a New Profile,” for detailed instructions.

Edit - Select the profile you want to change, and then click the **Edit** button. See the section, “Edit a New Profile,” for detailed instructions.

Import - Click the **Import** button to import a profile that has been saved in another location. Select the appropriate file, and click the **Open** button.

Export - Select the profile you want to save in a different location, and click the **Export** button. Direct Windows to the appropriate folder, and click the **Save** button.

Delete - Select the profile you want to delete, and then click the **Delete** button.



NOTE: If you want to export more than one profile, you must export them one at a time.

NOTE: The default profile cannot be deleted.

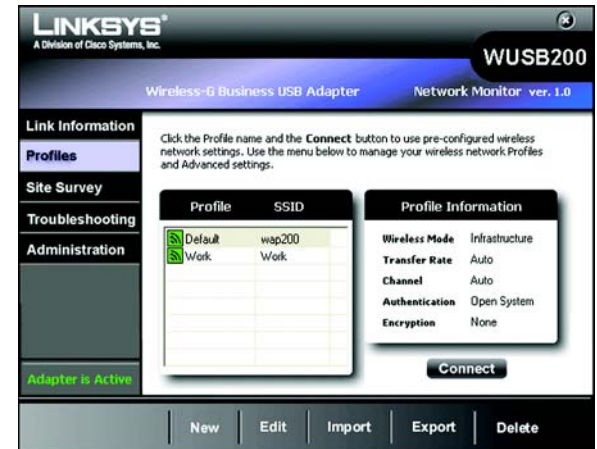


Figure 5-5: Profiles



Figure 5-6: Import a Profile

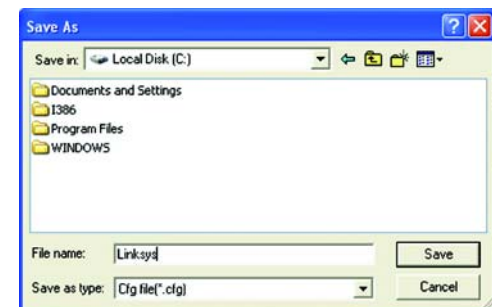


Figure 5-7: Export a Profile

Create a New Profile

When you click the **New** button on the *Profiles* screen, you will need to enter a name for your new profile and click **OK**, then the *Available Wireless Network* screen appears.

This screen provides two options for setting up the Adapter.

- **Available Wireless Network. (For most users.)** Use this option if you already have a network set up. The networks available to this Adapter will be listed on this screen. You can choose one of these networks and click the **Connect** button to connect to it. Click the **Refresh** button to update the Available Wireless Network list.
- **Manual Setup.** If your network is not listed on this screen, select **Manual Setup** to set up the adapter manually. This method of setting up the Adapter is intended for advanced users only.

The setup for each option is described under the appropriate heading on the following pages.

Click **Exit** to return to the *Profiles* screen.

Available Wireless Network

The available networks are listed by SSID. Select the wireless network you wish to connect to and click the **Connect** button. (If your network is not listed, you can click the **Refresh** button to bring the list up again.)

If the network utilizes wireless security, you will need to configure security on the Adapter. If not, you will be taken directly to the *Congratulations* screen.

1. If you have wireless security enabled on your network, continue to step 2. One of these security screens will be shown. If you don't have wireless security enabled, continue to step 3.
2. If your network has WEP, WPA Personal, or WPA2 Personal wireless security enabled, then that security screen will appear. Continue to the screen for your wireless security.
 - **WEP (Wired Equivalent Privacy)**

If your network has the wireless security WEP (Wired Equivalent Privacy), this screen will appear. You must enter the same security settings used on your network.

Select **64-bit** or **128-bit** WEP encryption, then enter a passphrase or WEP key.



Figure 5-8: Creating a Profile - Available Wireless Network

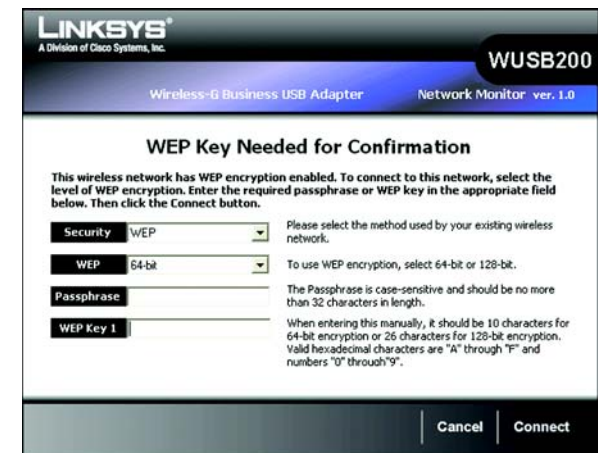


Figure 5-9: Creating a Profile - WEP Key Needed

Passphrase - Enter a passphrase in the *Passphrase* field, to automatically generate a WEP key. The passphrase is case-sensitive and should not be longer than 16 alphanumeric characters. It must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are “0” to “9” and “A” to “F”.

Then click **Connect** and proceed to Step 3.

- **WPA Personal**

If your network has the wireless security WPA Personal (Wi-Fi Protected Access) enabled, this screen will appear. You must enter the same security settings used on your network.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.

- **WPA2 Personal**

If your network has the wireless security WPA2 Personal enabled, this screen will appear. You must enter the same security settings used on your network.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Then click **Connect** and proceed to Step 3.

3. After the software has been successfully installed, the *Congratulations* screen will appear. Click **Connect to Network** to connect to your network, implement the new settings, and return to the *Link Information* screen.

Congratulations! The profile has been successfully configured.

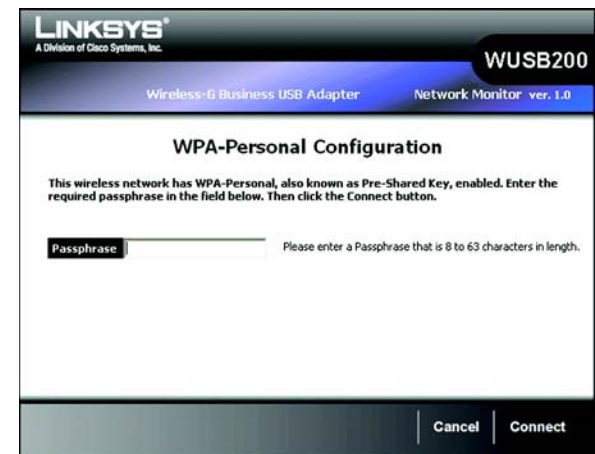


Figure 5-10: Creating a Profile - WPA-Personal

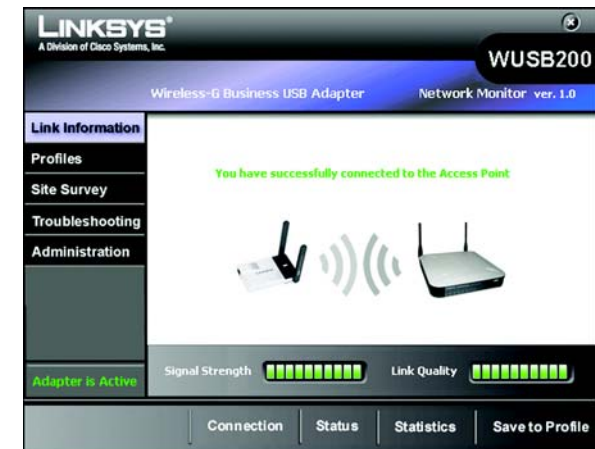


Figure 5-11: Creating a Profile - Congratulations

Manual Setup

If your network is not listed with the available networks, you can use Manual Setup.

1. Click **Manual Setup** on the *Available Wireless Network* screen to set up the adapter manually.
2. The *Network Settings* screen will appear. If your network has a router or other DHCP server, select **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, select **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

IP Address - This IP Address must be unique to your network.

Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

Default Gateway - Enter the IP address of your network's Gateway here.

DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

3. The *Wireless Mode* screen shows a choice of two wireless modes. Select **Infrastructure Mode** if you want to connect to a wireless router or access point. Select **Ad-Hoc Mode**, if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.



Figure 5-12: Creating a Profile - Manual Setup - Network Settings



Figure 5-13: Creating a Profile - Manual Setup - Wireless Mode

- If you chose **Infrastructure Mode**, go to Step 5 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.

- If your wireless network doesn't have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 6.

If your wireless network has wireless security, select the method of security used: **WEP, WPA/WPA2 Personal, WPA/WPA2 Enterprise, RADIUS or LEAP**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA uses a stronger security method than WEP and WPA2 defines an even stronger encryption, authentication, and key management than WPA. RADIUS stands for Remote Authentication Dial-In User Service. LEAP stands for Lightweight Extensible Authentication Protocol. It uses username and password-based authentication between a wireless client and a RADIUS server. Click the **Next** button to continue or the **Back** button to return to the previous screen.

Proceed to the appropriate section for your security method: WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, RADIUS, or LEAP.

WEP

WEP - Select **64-bit or 128-bit** encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

wep (wired equivalent privacy): a method of encrypting network data transmitted on a wireless network for greater security.

wpa (wi-fi protected access): a wireless security protocol using TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

wpa2 offers a stronger encryption than wpa by using the AES (Advanced Encryption Standard) which is a block cipher with block sizes of 128, 192 or 256 bits.



Figure 5-14: Creating a Profile - Manual Setup - Wireless Security - Disabled



Figure 5-15: Creating a Profile - Manual Setup - Wireless Security - WEP

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 only uses AES for encryption. Select **TKIP** or **AES** for encryption for WPA Personal. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

WPA2 Personal

Enter a Pre-shared Key that is 8-63 characters in length.

Pre-shared Key - Enter a Pre-shared Key of 8-63 characters in the *Pre-shared Key* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

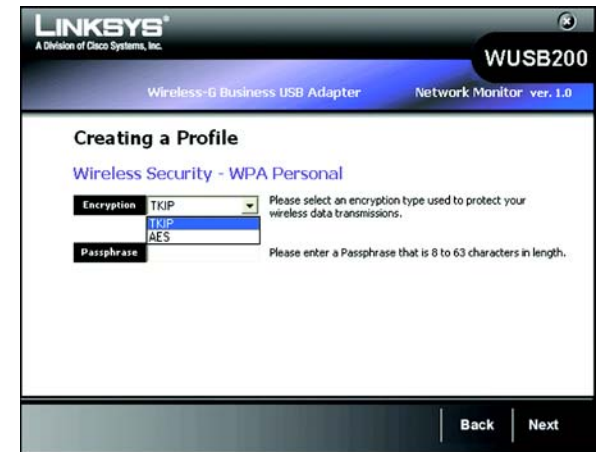


Figure 5-16: Creating a Profile - Manual Setup - Wireless Security - WPA Personal



Figure 5-17: Creating a Profile - Manual Setup - Wireless Security - WPA2 Personal

WPA Enterprise

WPA Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP, but only AES encryption method is used.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). Then select the authentication method used inside the PEAP tunnel. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'EAP-TLS'. Below it are fields for 'Login Name', 'Server Name', 'Certificate', and 'Encryption' (set to 'AES'). There are 'Back' and 'Next' buttons at the bottom right.

Figure 5-18: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - EAP-TLS

The screenshot shows the 'Creating a Profile' screen for 'Wireless Security - WPA Enterprise'. The 'Authentication' dropdown is set to 'PEAP'. Below it are fields for 'Login Name', 'Password', 'Server Name', 'Inner Authen.' (set to 'EAP-MSCHAPv2'), and 'Encryption' (set to 'AES'). There are 'Back' and 'Next' buttons at the bottom right.

Figure 5-19: Creating a Profile - Manual Setup - Wireless Security - WPA Enterprise - PEAP

WPA2 Enterprise

WPA2 Enterprise features WPA2 security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

Click the **Next** button to continue or the **Back** button to return to the previous screen.

The screenshot shows the 'LINKSYS' logo at the top left, 'A Division of Cisco Systems, Inc.' below it, and 'WUSB200' in a black circle at the top right. Below the logo is 'Wireless-G Business USB Adapter' and 'Network Monitor ver. 1.0'. The main heading is 'Creating a Profile' followed by 'Wireless Security - WPA2 Enterprise'. The form includes: 'Authentication' dropdown set to 'EAP-TLS' with a help text: 'Please select the authentication method that you use to access your network.'; 'Login Name' text field with help text: 'Enter the Login Name used for authentication.'; 'Server Name' text field with help text: 'Enter the Server Name used for authentication. (Optional)'; 'Certificate' dropdown with help text: 'Please select the certificate used for authentication.'; and 'Encryption' dropdown set to 'AES' with help text: 'Please select the encryption type used to protect the wireless data transmissions.' At the bottom right are 'Back' and 'Next' buttons.

Figure 5-20: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - EAP-TLS

The screenshot shows the same interface as Figure 5-20. The main heading is 'Creating a Profile' followed by 'Wireless Security - WPA2 Enterprise'. The form includes: 'Authentication' dropdown set to 'PEAP' with a help text: 'Please select the authentication method that you use to access your network.'; 'Login Name' text field with help text: 'Enter the Login Name used for authentication.'; 'Password' text field with help text: 'Enter the Password used for authentication.'; 'Server Name' text field with help text: 'Enter the Server Name used for authentication. (Optional)'; 'Inner Authen.' dropdown set to 'EAP-MSCHAPv2' with help text: 'Please select the inner authentication method used inside the PEAP tunnel.'; and 'Encryption' dropdown set to 'AES' with help text: 'Please select the encryption type used to protect the wireless data transmissions.' At the bottom right are 'Back' and 'Next' buttons.

Figure 5-21: Creating a Profile - Manual Setup - Wireless Security - WPA2 Enterprise - PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

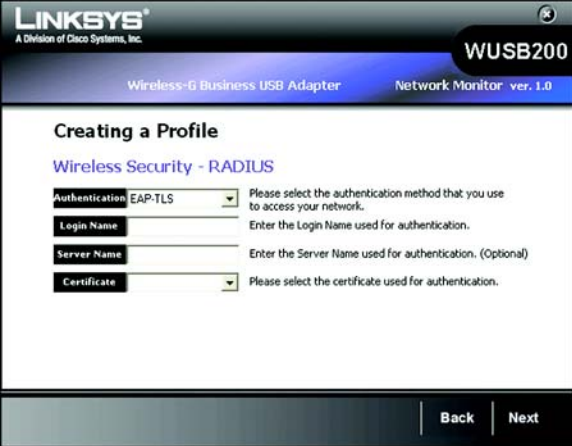
If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

Click the **Next** button to continue or the **Back** button to return to the previous screen.



The screenshot shows the Linksys Network Monitor interface for the WUSB200 adapter. The page title is "Creating a Profile" under "Wireless Security - RADIUS". The "Authentication" dropdown menu is set to "EAP-TLS". Below it are input fields for "Login Name", "Server Name", and "Certificate". The "Certificate" dropdown menu is also visible. At the bottom right, there are "Back" and "Next" buttons.

Figure 5-22: Creating a Profile - Manual Setup - Wireless Security - RADIUS - EAP-TLS



The screenshot shows the Linksys Network Monitor interface for the WUSB200 adapter. The page title is "Creating a Profile" under "Wireless Security - RADIUS". The "Authentication" dropdown menu is set to "PEAP". Below it are input fields for "Login Name", "Password", "Server Name", and "Inner Authen.". The "Inner Authen." dropdown menu is set to "EAP-MSCHAPv2". At the bottom right, there are "Back" and "Next" buttons.

Figure 5-23: Creating a Profile - Manual Setup - Wireless Security - RADIUS - PEAP

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a username and password based system.

Enter the username and password in their fields. Enter the password again in the Confirm field.



Figure 5-24: Creating a Profile - Manual Setup - Wireless Security - LEAP

6. The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button.

To edit the new settings, click the **Back** button. To exit the Manual Setup through the Wireless Network Monitor, click **Exit**.



Figure 5-25: Creating a Profile - Manual Setup - Confirm New Settings

7. The *Congratulations* screen will appear next. Click **Connect to Network** to implement the new settings immediately and return to the *Link Information* screen. Click **Return to Profile Screen** to keep the current settings active and return to the *Profiles* screen.

Congratulations! The profile has been successfully configured.



Figure 5-26: Creating a Profile - Manual Setup - Congratulations

Editing a Profile

On the Profiles screen, select the profile that you would like to edit in the profile list and click on **Edit** button. The next screen would be the Wireless Mode. Follow the steps below to complete the task.

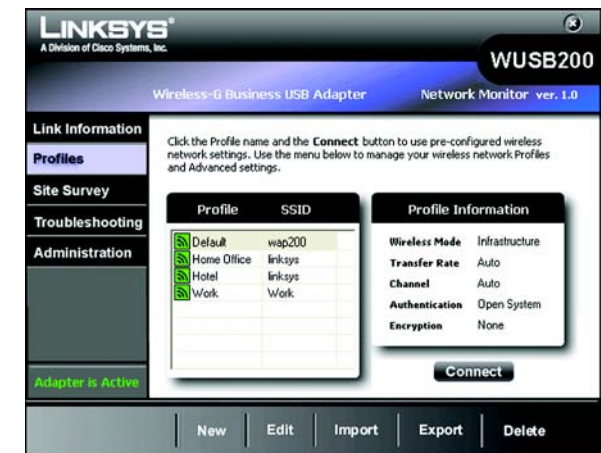


Figure 5-27: Editing a Profile

1. The *Wireless Mode* screen shows a choice of two wireless modes. Click the **Infrastructure Mode** radio button if you want to connect to a wireless router or access point. Click the **Ad-Hoc Mode** radio button if you want to connect to another wireless device directly without using a wireless router or access point. Enter the SSID for your network.

Infrastructure Mode - Use this mode if you want to connect to a wireless router or access point.

Ad-Hoc Mode - Use this mode if you want to connect to another wireless device directly without using a wireless router or access point.

SSID - This is the wireless network name that must be used for all the devices in your wireless network. It is case-sensitive and should be a unique name to help prevent others from entering your network.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

2. If you chose **Infrastructure Mode**, go to Step 3 now. If you chose **Ad-Hoc Mode**, the *Ad-Hoc Mode Settings* screen will appear.

Select the correct operating channel for your wireless network. The channel you choose should match the channel set on the other devices in your wireless network. If you are unsure about which channel to use, keep the default setting.

Click the **Next** button. Click the **Back** button to change any settings.



Figure 5-28: Editing a Profile - Wireless Mode



Figure 5-29: Editing a Profile - Ad Hoc Mode

- If your wireless network doesn't have wireless security, select **Disabled** and then click the **Next** button to continue. Proceed to Step 4.

If your wireless network has wireless security, select the method of security used: **WEP, WPA/WPA2 Personal, WPA/WPA2 Enterprise, RADIUS or LEAP**. WEP stands for Wired Equivalent Privacy, and WPA stands for Wi-Fi Protected Access. WPA uses a stronger security method than WEP and WPA2 defines an even stronger encryption, authentication, and key management than WPA. RADIUS stands for Remote Authentication Dial-In User Service. LEAP stands for Lightweight Extensible Authentication Protocol. It uses username and password-based authentication between a wireless client and a RADIUS server. Click the **Next** button to continue or the **Back** button to return to the previous screen.

Proceed to the appropriate section for your security method: WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, RADIUS, or LEAP.

WEP

WEP - Select **64-bit or 128-bit** encryption

Passphrase - Enter a passphrase in the *Passphrase* field, so a WEP key is automatically generated. It is case-sensitive and should not be longer than 16 alphanumeric characters. This passphrase must match the passphrase of your other wireless network devices and is compatible with Linksys wireless products only. (If you have any non-Linksys wireless products, enter the WEP key manually on those products.)

WEP Key - The WEP key you enter must match the WEP key of your wireless network. For 64-bit encryption, enter exactly 10 hexadecimal characters. For 128-bit encryption, enter exactly 26 hexadecimal characters. Valid hexadecimal characters are "0" to "9" and "A" to "F".

Advanced Users

TX Key - The default transmit key number is 1. If your network's access point or wireless router uses transmit key number 2, 3, or 4, select the appropriate number from the *TX Key* drop-down box.

Authentication -The default is set to **Auto**, so it will auto-detect for Shared Key or Open System authentication. For Shared Key authentication, both the sender and the recipient share a WEP key for authentication. For Open System authentication, the sender and the recipient do not share a WEP key for authentication. If you are not sure which authentication method to select, keep the default, **Auto**.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

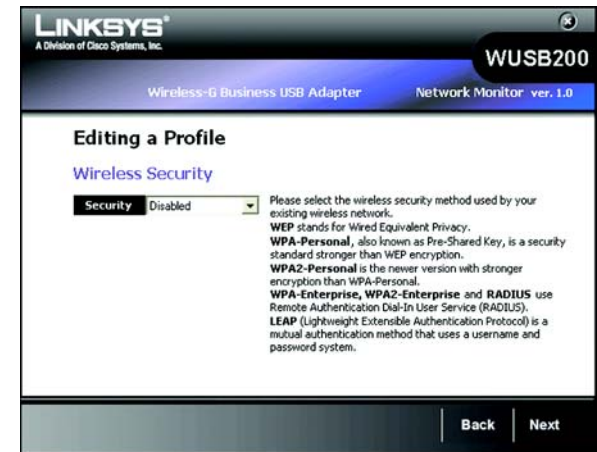


Figure 5-30: Editing a Profile - Wireless Security

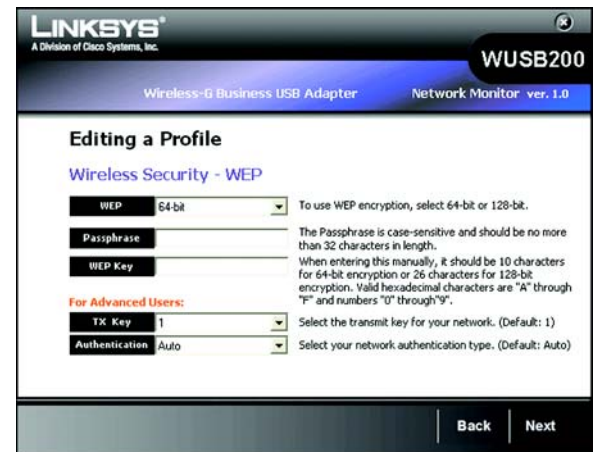


Figure 5-31: Editing a Profile - Wireless Security - WEP

WPA Personal

WPA Personal offers two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 only uses AES for encryption. Select **TKIP** or **AES** for encryption for WPA Personal. Then enter a Passphrase that is 8-63 characters in length.

Encryption - Select the type of algorithm you want to use, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Passphrase - Enter a Passphrase, also called a Pre-shared Key, of 8-63 characters in the *Passphrase* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

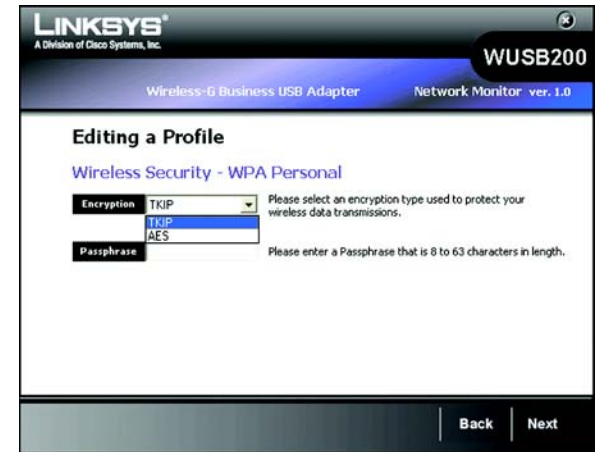


Figure 5-32: Editing a Profile - Wireless Security - WPA Personal

WPA2 Personal

Enter a Pre-shared Key that is 8-63 characters in length.

Pre-shared Key - Enter a Pre-shared Key of 8-63 characters in the *Pre-shared Key* field.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

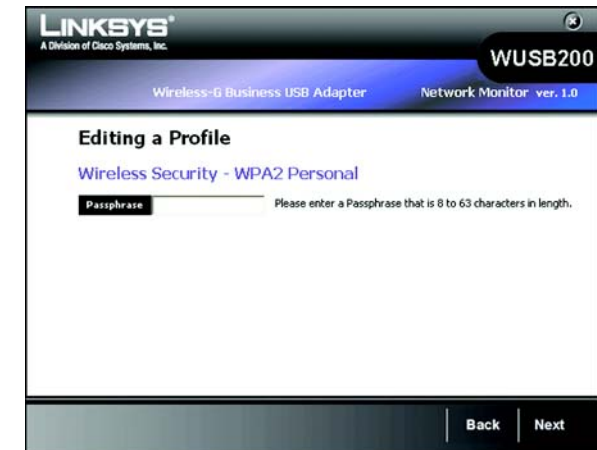


Figure 5-33: Editing a Profile - Wireless Security - WPA2 Personal

WPA Enterprise

WPA/WPA2 Enterprise features WPA security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA Enterprise offers two authentication methods, EAP-TLS and PEAP, as well as two encryption methods, TKIP and AES, with dynamic encryption keys. WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP, but only AES encryption method is used.

Authentication - Select the authentication method your network is using, **EAP-TLS** or **PEAP**.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, **Trust Any**. Then select the authentication method used inside the PEAP tunnel. Select the type of encryption, **TKIP** or **AES**, from the *Encryption* drop-down menu.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

The screenshot shows the 'Editing a Profile' screen for 'Wireless Security - WPA Enterprise' in the Linksys Network Monitor. The interface includes a header with the Linksys logo and 'WUSB200' model name. Below the header, it says 'Wireless-G Business USB Adapter Network Monitor ver. 1.0'. The main content area is titled 'Editing a Profile' and 'Wireless Security - WPA Enterprise'. It contains several fields: 'Authentication' (EAP-TLS), 'Login Name', 'Server Name', 'Certificate', and 'Encryption' (AES). Each field has a corresponding instruction. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-34: Editing a Profile - Wireless Security - WPA Enterprise - EAP-TLS

The screenshot shows the 'Editing a Profile' screen for 'Wireless Security - WPA Enterprise' in the Linksys Network Monitor. The interface is similar to Figure 5-34 but with 'Authentication' set to PEAP. It includes fields for 'Authentication' (PEAP), 'Login Name', 'Password', 'Server Name', 'Inner Authn.' (EAP-MSCHAPv2), and 'Encryption' (AES). Each field has a corresponding instruction. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-35: Editing a Profile - Wireless Security - WPA Enterprise - PEAP

WPA2 Enterprise

WPA2 Enterprise features WPA2 security used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) WPA2 Enterprise offers two authentication methods, EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network; if you want to use any certificate, keep the default setting, Trust Any. Then select the authentication method used inside the PEAP tunnel.

Click the **Next** button to continue or the **Back** button to return to the previous screen.



Figure 5-36: Editing a Profile - Wireless Security - WPA2 Enterprise - EAP-TLS

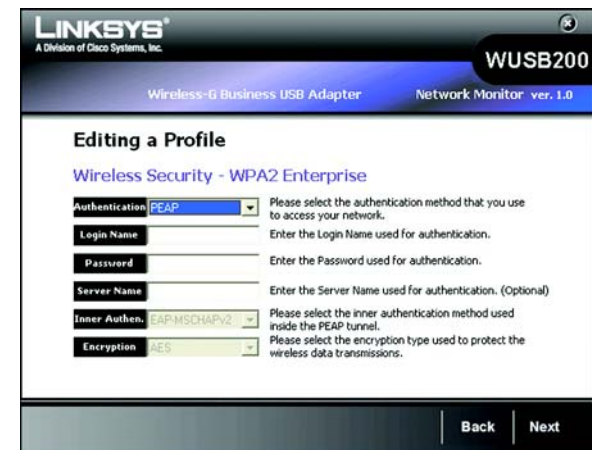


Figure 5-37: Editing a Profile - Wireless Security - WPA2 Enterprise - PEAP

RADIUS

RADIUS features use of a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.) RADIUS offers two authentication types: EAP-TLS and PEAP.

Authentication - Select the authentication method your network is using, EAP-TLS or PEAP.

EAP-TLS

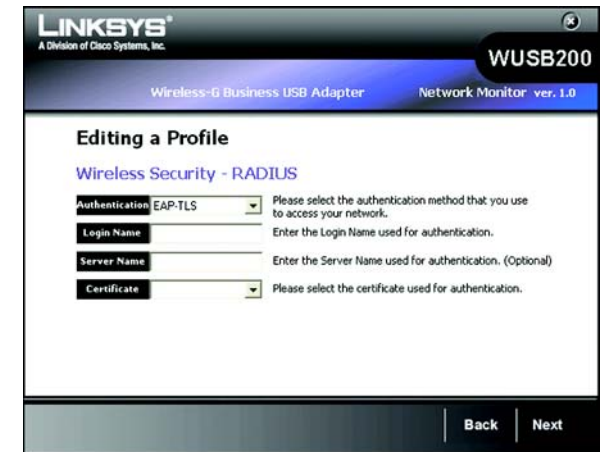
If you selected EAP-TLS, enter the login name of your wireless network in the *Login Name* field. Enter the name of the authentication server in the *Server Name* field (this is optional). From the *Certificate* drop-down menu, select the certificate you have installed to authenticate you on your wireless network.

Click the **Next** button to continue or the **Back** button to return to the previous screen.

PEAP

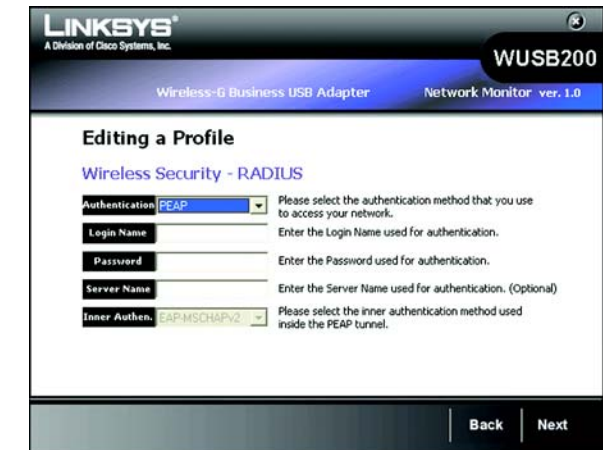
If you selected PEAP, enter the login name of your wireless network in the *Login Name* field. Enter the password of your wireless network in the *Password* field. Enter the name of the authentication server in the *Server Name* field (this is optional).

Click the **Next** button to continue or the **Back** button to return to the previous screen.



The screenshot shows the 'Editing a Profile' screen for 'Wireless Security - RADIUS'. The 'Authentication' dropdown menu is set to 'EAP-TLS'. Below it are fields for 'Login Name', 'Server Name', and 'Certificate'. The 'Certificate' dropdown menu is also visible. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-38: Editing a Profile - Wireless Security - RADIUS - EAP-TLS



The screenshot shows the 'Editing a Profile' screen for 'Wireless Security - RADIUS'. The 'Authentication' dropdown menu is set to 'PEAP'. Below it are fields for 'Login Name', 'Password', 'Server Name', and 'Inner Authen.'. The 'Inner Authen.' dropdown menu is set to 'EAP-MSCHAPV2'. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 5-39: Editing a Profile - Wireless Security - RADIUS - PEAP

LEAP

Lightweight Extensible Authentication Protocol is a mutual authentication method that uses a username and password based system.

Enter the username and password in the username and password field accordingly. Enter the password again in the *Confirm* field.



Figure 5-40: Editing a Profile - Wireless Security - LEAP

4. The *Network Settings* screen from the Wireless Network Monitor will appear. If your network has a router or other DHCP server, click the radio button next to **Obtain network settings automatically (DHCP)**.

If your network does not have a DHCP server, click the radio button next to **Specify network settings**. Enter an IP Address, Subnet Mask, Default Gateway, and DNS addresses appropriate for your network. You must specify the IP Address and Subnet Mask on this screen. If you are unsure about the Default Gateway and DNS addresses, leave these fields empty.

IP Address - This IP Address must be unique to your network.

Subnet Mask - The Adapter's Subnet Mask must be the same as your wired network's Subnet Mask.

Default Gateway - Enter the IP address of your network's Gateway here.

DNS 1 and **DNS 2** - Enter the DNS address of your wired Ethernet network here.

Click the **Next** button to continue, or click the **Back** button to return to the previous screen.

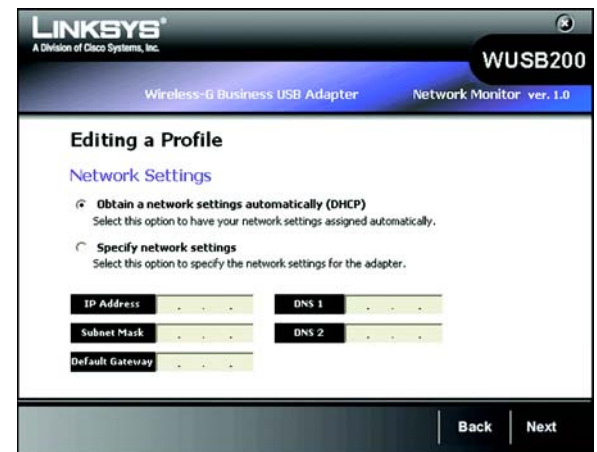


Figure 5-41: Editing a Profile - Network Settings

- The *Confirm New Settings* screen will appear next and show the new settings. To save the new settings, click the **Save** button.

To edit the new settings, click the **Back** button. To exit the Manual Setup through the Wireless Network Monitor, click **Exit**.



Figure 5-42: Editing a Profile - Confirm New Settings

- The *Congratulations* screen will appear next. Click **Connect to Network** to implement the new settings immediately and return to the *Link Information* screen. Click **Return to Profile Screen** to keep the current settings active and return to the *Profiles* screen.

Congratulations! The profile has been successfully configured.



Figure 5-43: Editing a Profile - Congratulations

Site Survey

The *Site Survey* screen displays a list of available networks in the table on the left. The table shows each network's SSID, Channel, and the quality of the wireless signal the Adapter is receiving. You may click **SSID**, **CH** (Channel), or **Signal**, to sort by that field.

SSID - The SSID or unique name of the wireless network is displayed here.

CH - This is the channel that the network uses.

Signal - This is the percentage of signal strength, from 0 to 100%.



The Access Points in the Site Survey list will be represented with different icons that will indicate Access Points in various states of classification. For instance, trusted Access Points are green, untrusted Access Points are red, and unclassified Access Points are blue. And if there is a lock next to it, it indicates the Access Point has a security method enabled.



Figure 5-44: Site Survey

For more information about classification of the Access Points, refer to “AP Classification” section of “Chapter 6: The Administrative Functions in the Wireless Network Monitor.”

Site Information

For each network selected, the following settings for each SSID are listed:

Wireless Mode - This is the mode of the wireless network currently in use.

Network Type - The type of your network connection in either wireless-b or wireless-g is displayed here.

Security - The status of the wireless security feature is displayed here.

MAC Address- The MAC address of the wireless network's access point is displayed here.

Refresh - Click the **Refresh** button to perform a new search for wireless devices.

Connect - Click the **Connect** button to connect to a selected network.

Troubleshooting

The *Troubleshooting* screen lets you troubleshoot your wireless connection.

Address Type - This shows the addressing method of your client.

IP Address - This shows the current IP Address of your client.

Subnet Mask - This shows the subnet mask of your IP addressing.

Default Gateway - This shows the default gateway of your IP addressing.

You may click **Repair** to troubleshoot your connection to the wireless network. Repair will disconnect your client from the network and then reconnect, in order to re-establish an IP address. You may also click **FAQ** to view the FAQ pages from the Linksys website.



Figure 5-45: Troubleshooting

Administration

The *Administration* screen lets you administer your Security Monitor account and classification functions, and modify your Access Point's username and password in Account Management. Select on a button to log in to either the Security Monitor account or Account Management as the Access Point's administrator.

Log in to the Security Monitor account to access the classification and Security Monitor functions:

Enter the Security Monitor's account name and password in the *username* and *password* fields, then retype the password in the *confirm* field. Click Next to continue to the administrative options.

After a successful login, the Classification and Security Monitor tab appears. Only the login screens are provided in this section. To use the Administration tab, continue to Chapter 6: The Administrative Functions in the Wireless Network Monitor.



Figure 5-46: Administration

Log in as the Access Point's administrator:

Enter the Access Point's administrative account and password and retype the password in the confirm field (default account name is *admin* and password is *admin*). Click **Next** to continue to the administrative options.

Access Point Account

This screen appears when you click the Access Point button on the Security Monitor Account screen. This will let you modify your Access Point's username and password.



Figure 5-47: Administration - Login Access Point Account



Figure 5-48: Administration - Modify Access Point Account