



Wireless Security Corporation

Wireless without worries.™

WSC GuardSM

User Guide

March, 2005

COPYRIGHT INFORMATION

WSC GuardSM User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the End-User License Agreement.

Documentation version: 1.0.4.3

Copyright Notice

Copyright© 2003-2005 Wireless Security Corporation. All rights reserved.

Any technical documentation that is made available by Wireless Security Corporation ("WSC") is the copyrighted work of WSC and is owned by WSC.

NO WARRANTY: The User's Guide is provided to you on an "AS IS" basis without warranty of any kind, express or implied. WSC makes no warranty as to its accuracy or use. Any use of the User's Guide or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. WSC reserves the right to make changes without prior notice.

No part of this User's Guide may be copied without the express written consent of WSC, 643 Bair Island Road, Suite 305, Redwood City, CA 94063.

Trademarks

WSC Guard is a trademark of WSC.

Other product names mentioned in this User's Guide may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Boost Developer's Toolkit

This product utilizes the Boost Developer's Toolkit. © Copyright Greg Colvin and Beman Dawes 1998, 1999. Copyright © 2001, 2002, 2003 Peter Dimov.

Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty, and with no claim as to its suitability for any purpose.

Jetbyte Limited Jbregistry

Copyright 1997 JetByte Limited.

JetByte Limited grants you ("Licensee") a non-exclusive, royalty free, licence to use, modify and redistribute this software in source and binary code form, provided that (i) this copyright notice and licence appear on all copies of the software; and (ii) Licensee does not utilize the software in a manner which is disparaging to JetByte Limited.

This software is provided "AS IS," without a warranty of any kind. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE HEREBY EXCLUDED. JETBYTE LIMITED AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY DAMAGES SUFFERED BY LICENSEE AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE OR ITS DERIVATIVES. IN NO EVENT WILL JETBYTE LIMITED BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR DIRECT, INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE

DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF JETBYTE LIMITED HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

gSOAP

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright © 2001-2003 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Source code from www.open1x.org for a client-side 802.1x implementation supporting EAP/TLS

Copyright © 2002 Bryan D. Payne and Nick L. Petroni Jr. All Rights Reserved

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of Maryland at College Park and its contributors.

- Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

TABLE OF CONTENTS

Chapter 1: Welcome	1
A Quick Overview	3
Types of Wireless Security	5
System Requirements	7
Contacting WSC	8
Chapter 2: Using the Client Software	9
The WSC Guard Notification Icon	10
Log into Your WSC Guard Network	12
The WSC Guard Pop-up Menu	14
Check Network Status	15
Reconnect to a Network	15
View Available Wireless Networks	17
Selecting Options	19
Manage Your Wireless Network	22
Log into Network Management	22
Register a New WSC Member	23
Create a New Network	26
Add an Access Point	29
Check and Manage Network Properties	34
Check Access Point Properties	36
Rename a Network or Access Point	38
Set the Security Fallback Mode	39
Turn on Automatic Fallback	40
Turn On/Off Fallback Mode Manually	42
Remove an Access Point from a WSC Network	46
Remove a WSC Network	47
Disable WSC Guard	48
Go to the WSC Web Site	49

Check for WSC Updates	50
Install a WSC Guard Update	51
Using the WSC Guard Network Selector	52
Sort the Network List	55
Resizing and repositioning the Columns	56
Disconnect from a Network	57
Connect to a Network	57
Add a Wireless Network	59
Modify a Wireless Network	60
Selecting Network Connection Options	62
Listing Preferred Networks	63
Chapter 3: Using the WSC Web Site	67
Logging into the WSC Web Site	68
Viewing Your Personal WSC Home Page	70
Modifying Your WSC Account Profiles	72
Modify Your Member Profile	72
Modify Your Billing Profile	74
Editing Your Renewal Information	75
Notes About Modifying Your Renewal or Billing Information	78
Checking Your Billing History	79
Seeing Which Network You Can Use	80
Managing a WSC Network	81
Network Administration	83
Modify Network User List	90
Provide a Guest Access to the Network	105
Viewing Network Activity Reports	108
Security Countermeasures for Unauthorized Log In Attempts	110

Chapter 4: Troubleshooting	113
WPA Not Supported	113
Login Failed	116
Network Card Cannot Connect to Network	117
Login Failed—Wrong Network Key	118
Login Failed—Wrong Data Encryption Mode	118
Login Failed—Wrong WEP Key	118
Login Failed—Incompatible Network Adapter	119
Cannot Connect to Network	119
Login Fails When You're Offsite	119
XP Wireless Network Support Not Working	120
Access Point Wizard Failed	120
Index	123

CHAPTER 1

Welcome

WSC Guard secures your wireless network. Simply put, WSC Guard keeps out anyone who tries to access your network without your approval and authorization.

Without WSC Guard, wireless networks are particularly vulnerable to hackers and industrial spies. For instance, without security, a hacker could simply park his car outside your office building and, using some well-known techniques, tap directly into your business data. And it usually doesn't take very long to accomplish such break-ins, because many of the wireless access points—the central transmitting devices—are not protected and simply pass data along “in the clear.”

With WSC Guard, not only is the network secured with User Name/Password protection, but the data passing back and forth between Network Members is encrypted. The result? Peace of mind about the privacy of your important business or personal data.

WSC Guard offers these features:

A secure authentication service—WSC maintains a secure database of everyone you designate as a valid Network Member. No one gets into your networks without first getting authentication clearance from the WSC Authentication Center. Think of it as a very large policeman at the front door checking security badges. No badge, no entry.

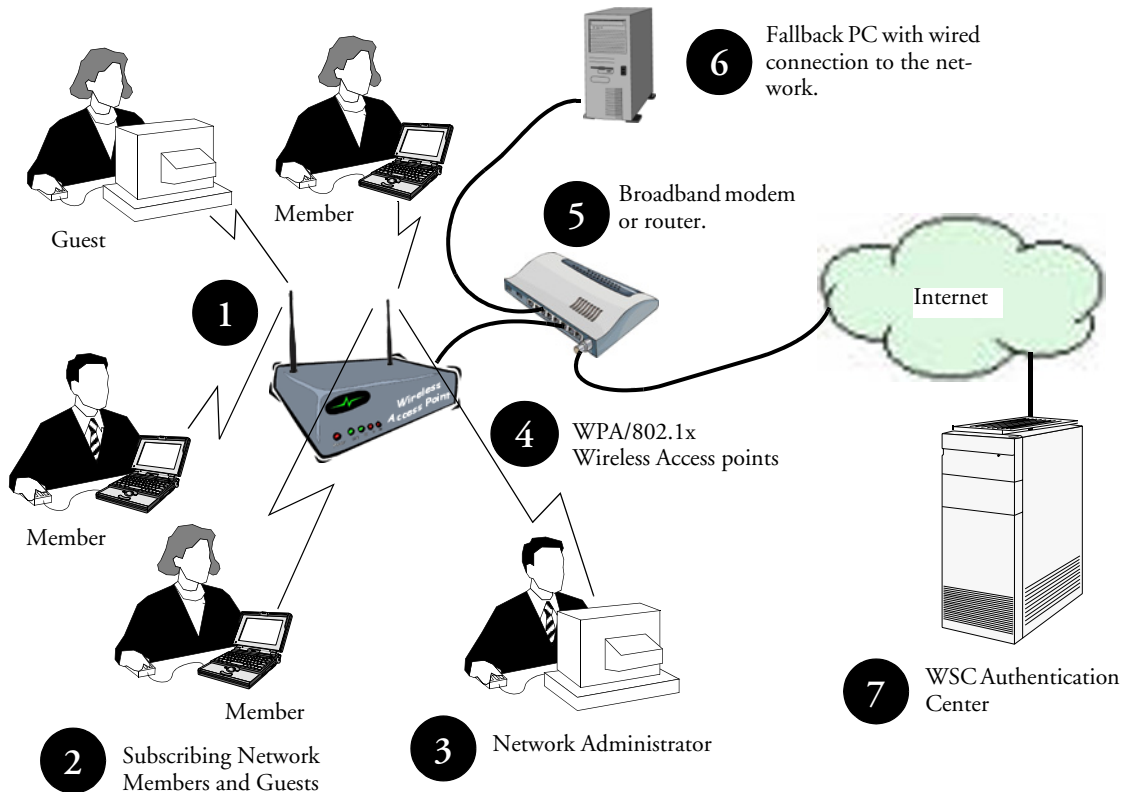
Encrypted data flow—many earlier wireless networks either had no encryption (clear data) or a simple encryption scheme, known as WEP, that hackers can easily crack. WSC Guard, however, uses WPA/802.1x authentication with dynamic key encryption, providing vastly greater security.

Vigilant intrusion detection—the WSC service continuously monitors your network, even at night, and on week-ends and holidays, to detect intruders trying to break in. You set up the sensitivity of the intrusion alarms, and you'll get an email immediately warning you when the intrusions occur.

Easy installation and network management—absolutely no need for an MIS or IT expert. Installation and management is designed to be quick and easy. Plus, an intuitive application provides all the functions you need to assign Members to the network, remove them, and set up Guest status.

A QUICK OVERVIEW

The following figure and explanation provides an overview of the WSC service and its various components.



1. A WSC Guard-Protected Network—a group of access points that are all secured from unauthorized access, and that are programmed by WSC Guard software to the same Network name (or SSID). Grouping the access points together into one WSC Guard-Protected Network in this manner provides a variety of benefits, including: being able to manage all the access point from a single access control list, adding an unlimited number of access points to the Network, and the capability for 802.11 roaming to function among access points without losing connectivity. To achieve these benefits, all access points added to the same WSC Guard-Protected Network must be on the same physical subnet in your

LAN environment. WSC then bills you for the number of Member licenses per WSC Guard-Protected Network that you will use. For information about pricing and billing, visit the WSC web site at www.wirelesssecuritycorp.com and see the Pricing section.

2. Subscribing Network Members—each Network Member registers with the WSC Authentication Center with name, User Name, Password, address, telephone number and so on. That registration information provides a unique identification of each Member. Once Members are logged on, transmissions from each Member's computer to the wireless access point are encrypted, even if two Members sit in the same cubicle.

3. Network Administrator—sets up the access point and the network. Using a simple web-based application, the Network Administrator logs into the WSC Authentication Center and performs the network administration tasks, such as selecting who can have access to the network, how sensitive alarms should be, where to send alarm email, how long Guests can stay on the network and so on. Subscribing Network Members who are not Network Administrators *cannot* perform any network administration.

4. WPA/802.1x Wireless Access Point—The focal point for wireless communication between Subscribing Network Members and to the internet via a broadband modem or router. The access point is secured with a randomly-assigned Password as part of the WSC setup process, plus WPA/802.1x provides strong mutual authentication and dynamic encryption keys, which render it virtually impervious to hacker attacks. The access point has a wired connection to the broadband modem or router. The access point may include a built-in Ethernet hub, providing wired connections to the network.

5. Broadband modem or router—Typically a DSL or Cable modem, or in some cases, a router. Provides the wireless network with a high-speed connection to the internet. The broadband modem or router has a wired connection to the wireless access point. Some broadband modems include a built-in hub, providing for multiple wired connections to the network.

6. Fallback PC—Any PC or laptop that has a wired connection to the network through an Ethernet hub, which may be built-in to the access point or broadband modem. WSC Guard is installed on this PC and configured to run a Fallback agent that monitors internet connectivity. If connectivity is lost, the agent automatically puts the wireless network in Fallback Mode so the Subscribing Network Members can continue communicating with the access point. The network reverts to local authentication using the next best level of security available in the access point. This may be 128-bit WEP or WPA-PSK. When the internet connection is restored, the Fallback agent automatically returns the wireless network to WSC Guard, authenticated and encrypted security.

7. WSC Authentication Center—prior to using your network, everyone must register on the WSC Authentication Center and be added to the secure database. Every attempt to login on your network is checked in the database, authenticated by the WSC Authentication Center, and then approved or disapproved. Disapprovals—that is, failed login attempts—are monitored on a continuous basis. When it looks like your network is under attack, you receive a warning message immediately. Day-to-day network status reports are also available to the owner as part of network administration. All transmissions to and from the WSC Authentication Center are encrypted.

TYPES OF WIRELESS SECURITY

Several different types of wireless security are available. The following definitions help you see what capabilities your wireless technology has. To learn more about wireless technology and terminology, visit www.wirelesssecuritycorp.com/wsc/public/glossary.do.

802.11—a set of IEEE standards for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. Several specifications of 802.11 include 802.11a, 802.11b, 802.11g, and 802.11i, a suite of security standards for all wireless Ethernets.

802.11 a/b/g—802.11a is an extension to 802.11 that applies to wireless LANs and sends data at up to 54 Mbps in the 5GHz band. Although the transmission speed is faster than 802.11b, the distance

covered is much smaller. 802.11b is an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission in the 2.4 GHz band. 802.11g is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 2.4 GHz band.

WPA (Wi-Fi Protected Access)—a specification standard that strongly increases the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, WPA is derived from and is forward-compatible with the upcoming IEEE 802.11i standard. When properly installed, it provides wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network.

WPA-PSK (Wi-Fi Protected Access-Pre-Shared Key)—a special mode of WPA, designed for home use. In a home environment, where there are no network servers, the WPA-PSK mode allows the use of manually entered keys or passwords. This mode is easy to set up. After a password (also called a master key) is entered into the access point or home wireless gateway, and into each computer on the wireless network, Wi-Fi Protected Access security automatically takes over. The password keeps out eavesdroppers and other unauthorized users by requiring all devices to have the matching password. In addition, entering the password starts the advanced encryption process. These processes happen in the background automatically, and completely invisible to the home user.

802.1x—an IEEE standard for authentication on wired and wireless networks, but is most notably used in conjunction with 802.11 wireless networking. This standard provides strong, mutual authentication between a client and an authentication server. In addition, 802.1x can provide dynamic per-user, per-session WEP keys, removing the administrative burden and security risks surrounding static WEP keys.

SYSTEM REQUIREMENTS

The Systems Requirements below are the basic requirements. Visit www.wirelesssecuritycorp.com to see a detailed list of system requirements for supported wireless access points and wireless network adapters.

Computers	IBM PC (or 100-percent compatible) Pentium or equivalent with wireless connectivity (Wi-Fi) hardware either built-in or installed.
RAM	128 MB or greater
Hard Disk Space	At least 50 MB available hard disk space
Operating Systems	Windows XP, 2000, 98, and Me
Internet Connectivity	Broadband DSL or Cable modem or other high-speed connection
Web Browser	Internet Explorer 5.5 or later
Wireless Access Point*	Must be compliant with WPA and/or 802.1x standards, such as: Linksys WRT 54G Linksys WAP 54G Proxim Orinoco AP-600.
Wireless Network Adapter*	Must be a supported wireless network adapter, such as: Linksys WPC 54G/GS Intel 2200 b/g Mini PCI Intel 2100 b Mini PCI NETGEAR WG 511

* See our web site at www.wirelesssecuritycorp.com for more information about compatible wireless access points and wireless network adapters.

CONTACTING WSC

Wireless Security Corporation provides technical support to all registered users at the following numbers and addresses:

Support by Telephone in the US	(877)-717-9213
Support on the web	www.wirelesssecuritycorp.com
Email support	support@wirelesssecuritycorp.com

CHAPTER 2

Using the Client Software

For most routine business activities, using your WSC Guard Network is “transparent.” That is, you start your computer, log into the WSC Guard Network, and begin working.

On occasion, however, you may need to use some of the features of the client software. This chapter explains how to:

- Log into a WSC Guard Network
- View status information for the Network.
- Reconnect to the Network under another name.
- Register another person for WSC Guard Membership.
- Perform a variety of network management functions including adding another access point to the Network and enabling automatic Network Fallback Mode.
- Go to the WSC web site.
- Download and install updates to the WSC Guard software.
- Use the built-in Network Selector application.

THE WSC GUARD NOTIFICATION ICON





The WSC Guard Notification Icon appears at the bottom right corner of your Windows screen (known in Windows XP as the “Notification Area” and in Windows 2000 as the “System Tray”).



WSC Guard Notification Icon

Note: The signal strength icon next to the WSC Guard Notification Icon can be displayed or hidden.

The following table shows how the color and appearance of the WSC Guard Notification Icon indicates the status of your Network connection.

	Gray; not connected.
	Red; connected to a non-WSC network and transmitting data that is not protected by WSC Guard.
	Green with red “x”; connected to the WSC Guard Network, but waiting for authentication. Blinks while authentication is in progress. If the internet connection is running normally, authentication should occur within a few moments.
	Green, not blinking; normal mode; authenticated and connected to a WSC Network; data is secure and encrypted.



Yellow; connected to the WSC Network, but operating in less secure Fallback Mode (using a static WEP key or WPA-PSK). Normally this is due to an internet failure. As soon as the internet failure is resolved, if the WSC automatic Fallback security monitoring is enabled, security is reestablished. If the automatic mode is not enabled, you can manually re-enable full WSC security.



Yellow with “!”; Fallback is needed. You are still connected to the WSC Network, but a problem exists with getting access to the WSC Authentication Center. The most likely cause is an internet interruption, but other possible causes are a loose ethernet cable or the access point needs to be re-booted. If you selected the WSC automatic security option for Fallback Mode, the access point will be reconfigured after a few moments. After that, data is transmitted in the less secure mode built into your wireless access point. If automatic Fallback is not enabled, you can manually enable it. See “Turn On/Off Fallback Mode Manually” on page 42.



Yellow with red “x”; connected to the WSC Network, Network is in Fallback Mode, but Member’s computer does not have Fallback information for the Network yet. Usually, Member has never logged into the Network before.

LOG INTO YOUR WSC GUARD NETWORK

The WSC Guard Login window automatically appears to login to your WSC Guard Network.



1. Enter your User Name and Password.

If you want to login in the future without having to type your password, click **Save Password**. Later, when logging in, as soon as you enter your User Name, your password is automatically entered and all you have to do is click **Login**.

If you want WSC Guard to log you in automatically, click **Enable Auto Login**. With this setting selected, whenever you start your computer, WSC Guard will automatically log you into the Network, and you won't even see this login window.

Note: Auto Login is usually used for home computers, or other machines where access to them is limited. If the Auto Login option is selected for a machine at a work place, anyone who happens to start your computer is automatically logged into the Network.

2. Click **Login**.

The WSC Guard Notification Icon (the “key”) in the Windows Taskbar blinks while the login is proceeding, and then turns green indicating a successful login.



From this point on, whenever you connect to the Network, the WSC Guard Login window will automatically appear to verify your login name and password through the WSC Authentication Center unless you selected the **Enable Auto Login** option to skip this login.

Note: The WSC Login window only appears when you start up your computer in the presence of a WSC-Protected wireless access point. This Login window does not appear when you start up in the presence of an access point that has WEP or Clear security, and of course, it does not appear when you start up your computer in a location that has no wireless access point.

THE WSC GUARD POP-UP MENU

The features of the WSC Client Software are available from the WSC Guard Pop-up menu that appears when you right-click on the WSC Guard Notification Icon.

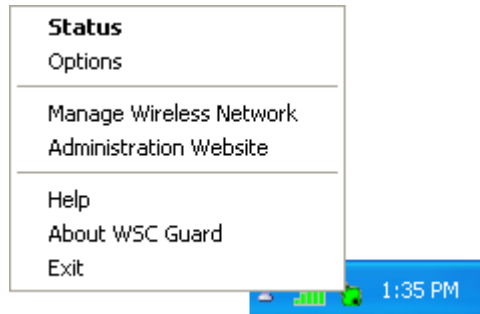
To use the WSC Guard Pop-up menu:

1. Right-click on the **WSC Guard Notification Icon**.



WSC Guard Notification Icon

The WSC Pop-up menu appears.



2. Choose an option from the menu.

Each of the options is described below.

Note: If you activate the WSC Guard Network Selector to configure wireless networks, the menu will have an additional selection, “View Available Wireless Networks.” See “Using the WSC Guard Network Selector” on page 52 for details.

CHECK NETWORK STATUS

The Status dialog box shows basic information about your computer's wireless connection. The dialog box also provides buttons to reconnect to the Network under another name, and to view available networks.

To view the Network status:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Status** from the Pop-up menu.



The Status dialog box shows the name of the Network and access point, your user name, the strength of the signal, and the duration of your current network session (how long you have been logged on). If the Network is disconnected, in Fallback mode, or in some other state, the status message tells you the current status.

RECONNECT TO A NETWORK

If you want to reconnect to a Network using a different user name, you can use the Reconnect button on the Status dialog box. For example, if a person is logged in as a Guest in order to sign up and register as a WSC Guard Member, after that process is completed the person can log in under the new Member name.

To reconnect under a new name:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Status** from the Pop-up menu.



3. Click the **Reconnect** button.

Your computer is disconnected from the Network and the login window appears for you to log in under a different name.



4. Enter a new User Name and Password and click **Login**.

Your computer is then reconnected to the Network and you are logged in under the new user name.

VIEW AVAILABLE WIRELESS NETWORKS

Computers running under Windows XP have built-in support for viewing and selecting available wireless networks. Other older Windows operating systems, such as Windows 2000 and Windows 98, do not have that support. With those older systems, connecting to a wireless network can be confusing and complex. Furthermore, the older operating systems do not offer support for WPA security on wireless products.

As one of its added features, WSC Guard has built-in support, called the **Network Selector**, for viewing and selecting available wireless networks for Windows 2000 and the older operating systems. The Network Selector also provides WPA security support so you can use WPA wireless products. You can also use the Network Selector on a Windows XP computer in place of the Windows XP support.

Note: If your computer is running Windows 2000 or one of the older operating systems, the WSC Guard Network Selector is activated by default, and is ready for you to use. If you want to use the Network Selector with Windows XP, you have to activate it first.

To activate the WSC Guard Network Selector:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Status** from the Pop-up menu.

3. Click the **Available Wireless Networks** button.

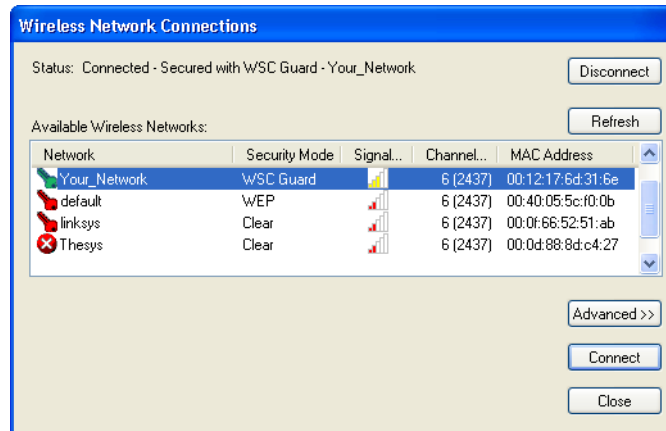


If you haven't activated the Network Selector yet, a dialog box appears so you can activate it now. You can also activate the Network Selector by selecting **Options** from WSC Pop-up menu.



4. Click **Activate Now**.

The main Network Selector window appears. It shows the wireless networks available to your computer, and has buttons for you to connect to, and disconnect from, the selected Network. For a complete description of the features of the Network Selector, please see “Using the WSC Guard Network Selector” on page 52.



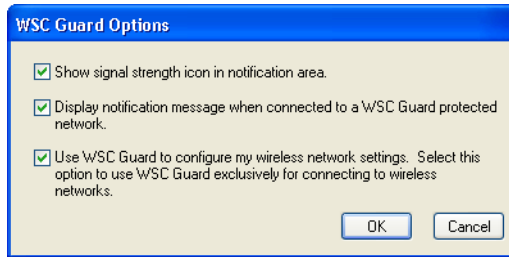
5. Select a Network and click **Connect**.

SELECTING OPTIONS

The Options dialog box has selections for how you want to view and work with the WSC features.

To view the options:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Options** from the Pop-up menu.



3. Choose the options you want and click **OK**.

The options are:

Show signal strength icon in notification area—the signal strength icon represents the current strength of the wireless signal being received by your computer's wireless network adapter. If you select this option, the signal strength icon appears next to the WSC Guard Notification Icon at the bottom right corner of the screen.



Signal Strength icon showing Very Good connection

As shown by the following samples, in addition to showing the signal strength, the icon can also show when the wireless connection is lost.



Signal Excellent



Signal Good



No Wireless Connection

Display notification message when connected to a WSC Guard protected network—selecting this option turns on the messages that appear at the bottom right corner of the screen. The messages tell you when your WSC Guard Network is successfully authenticated, or if the Network is experiencing a problem.

Use WSC Guard to configure my wireless network settings. Select this option to use WSC Guard exclusively for connecting to wireless networks—selecting this option activates the WSC Guard Network Selector that simulates Windows XP wireless network support. Typically this option is for computers running Windows 2000 or other older operating systems. Selecting this option is the same as activating the Network Selector with the button labeled **Available Wireless Networks** on the Status dialog box. Note that if this option is selected, the WSC Guard Pop-up menu has an addition selection—View Available Wireless Networks—that also opens the Network Selector. See “Using the WSC Guard Network Selector” on page 52 for details.



MANAGE YOUR WIRELESS NETWORK

Several network management tasks are controlled from the Manage Wireless Network menu option. These tasks include:

- Register another person with WSC Guard
- Add an access point to a Network
- Check an access point's properties
- Rename a Network or access point
- Delete a Network or access point
- Create a new Network
- Check a Network's properties
- Set up Network security for automated or manual Fallback Mode

LOG INTO NETWORK MANAGEMENT

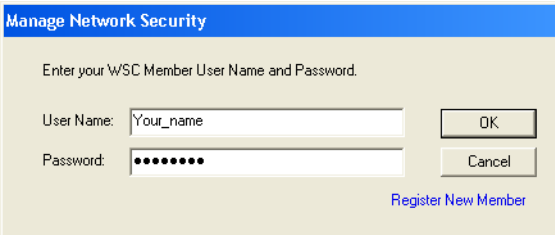
In order to manage wireless networks, you must be:

- Connected to the internet
- The Network Administrator

To log in to the network management functions:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.

The login dialog box appears.



Manage Network Security

Enter your WSC Member User Name and Password.

User Name:

Password:

[Register New Member](#)

3. Enter your User Name and Password.

4. If you want to register a person with WSC, click the link, **Register New Member**.

You can also register a new Member on the Administration web site. See “Adding a Member to a WSC Network” on page 91.

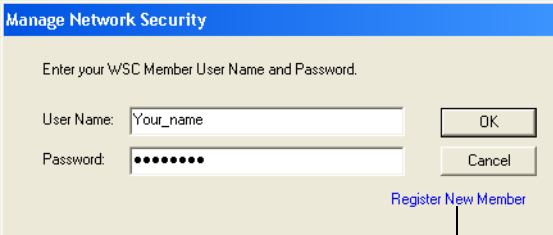
5. If you want to create a new Network, add an access point, or do other network management functions, click **OK**.

REGISTER A NEW WSC MEMBER

As your Network grows, you may need to register new WSC Guard Members in order to add them to the Network. It is the same basic process that you used to register Members when initially installing WSC Guard on your computer.

To register a new WSC Member:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Click the link, **Register New Member**.



Manage Network Security

Enter your WSC Member User Name and Password.

User Name:

Password:

OK

Cancel

[Register New Member](#)

Click this link

The Member Registration wizard screen appears.



4. Click **Next**.

The window for the new Membership information appears.

5. Type the new Member's information in the boxes.

A valid email address is very important because it uniquely identifies the new Member in the WSC Authentication Center.

6. To see our commitment to the privacy of information, click **Privacy Policy**.

Wireless Security Corp values and respects Members' privacy. In keeping with that policy, we have spelled out in detail our information practices as part of our policy.

7. If want the new Member to receive notices of new WSC features or upgrades, do not select the box click the box labelled **Do not send me any promotional email.**
8. Click **Next.**

The next window is where you set up the new Member's user name, password, and security question.

9. Fill in the information.

Make sure the User Name is one the new Member likes. It remains the same for the duration of the WSC Guard membership.

The password must have at least 6 characters and cannot have spaces at its beginning or end.

The security question is a back-up in case the Member forgets the password. If that occurs, instruct the new Member to click the **Forgot your password?** link on the log in window and type the answer to the security question instead.

10. Click the drop-down arrow to see the list of security questions. Type the answer in the box.

Note: Later, the new Member will be able to login to the WSC Member web site and change the password, security question, and answer.

11. Click **Next**.

The next window verifies that you have successfully registered the new Member with WSC Guard.



12. Click **Finish**.

As Network Administrator, you must now add the newly-registered person to your WSC Guard-Protected Network before that person can use your Network.

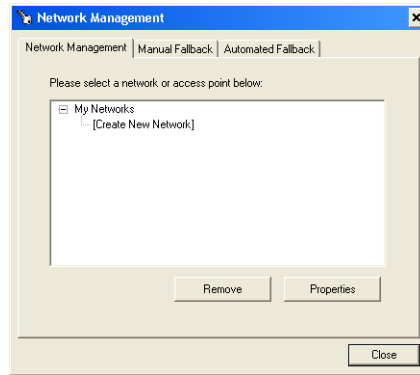
CREATE A NEW NETWORK

The steps to create a new Network are basically the same as when you created an initial Network when installing WSC Guard. You access the process from the WSC Pop-up menu.

To create a new Network:

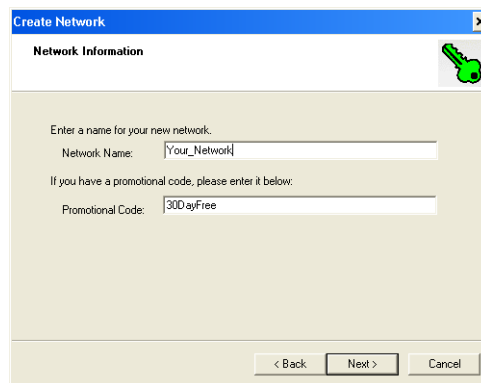
1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

The Network Management dialog box appears.



4. Click **Create New Network**.

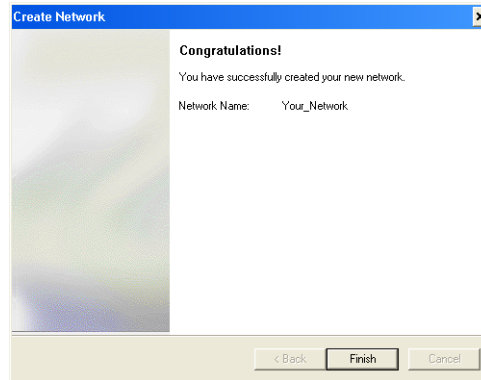
The window for the new Network Information appears.



5. Enter a name for the Network, and use the promotional code provided.

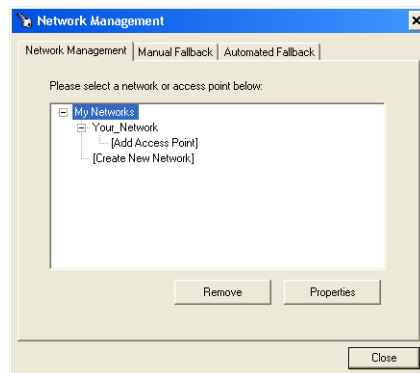
6. Click **Next**.

After a few moments, the new Network is registered at the WSC Authentication Center, and the next screen appears confirming that the Network has been created.



7. Click **Finish**.

The Network Management dialog box now shows your new Network.



Next you probably want to add an access point to the new Network.

ADD AN ACCESS POINT

You can add several access points to a Network. For example, if the wireless computers are spread over a relatively wide area, such as over a full floor in a building, you can add access points at either end of the floor to improve reception.

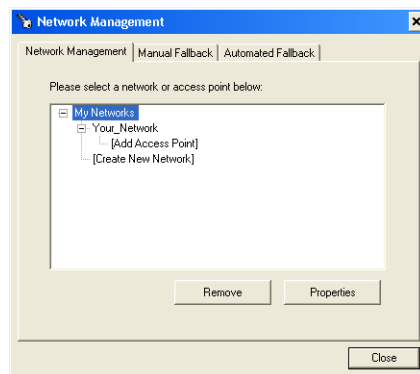
Note: Before adding an access point, it must be configured and connected to the internet according to the manufacturer's instructions.

Note that if you just created a Network and are adding an access point to it, the Network Management window will still be open and you can skip the first three steps of the following process.

To add an access point:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

The Network Management dialog box shows the networks for which you are the Network Administrator.



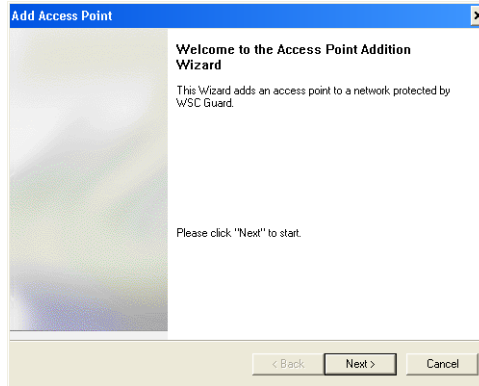
4. To see the information for a Network, click the “+” next to the Network’s name.

The information for each Network includes: the Network name, access point(s) name, and an option to add a new access point.

If you own several networks, scroll down to see them.

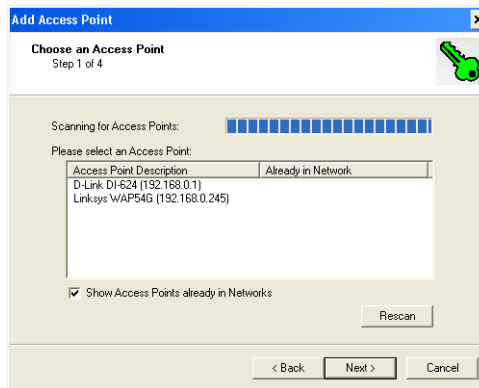
5. Click **Add Access Point**.

The Add Access Point wizard window appears.



6. Click **Next**.

The WSC Guard software scans your Network and finds available, and compatible, access points.

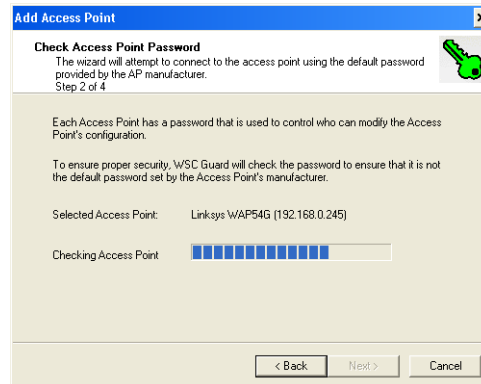


If you have multiple access points, those already assigned to networks will have the Network's name in the **Already in Network** column. You can easily see which access points are not already in a Network because, for them, no Network name will be listed.

The check box **Show Access Points already in Networks** is designed to help you find the new access point quickly in case several are already operating in your business. Unchecking the box limits the list to only those access points not already on networks. So, you can quickly find the new one you're adding without having to scroll through the long list of already-added access points.

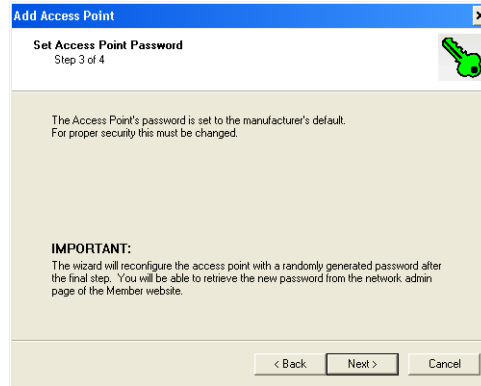
7. Select the WSC-compatible wireless access point that you want to add to the Network, and click **Next**.

The wizard now checks the access point you selected to determine whether its default password was changed when the access point was installed. A wizard window appears briefly while the checking is taking place.



8. Click **Next**.

If the access point is still using the manufacturer's default password, this next wizard window appears.



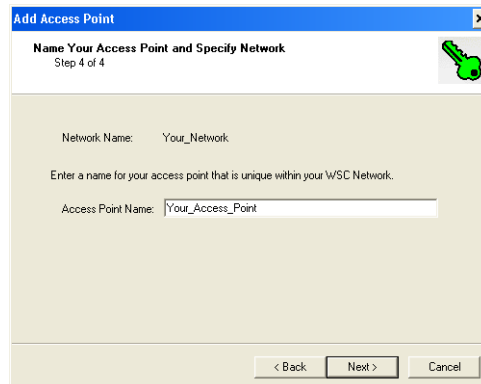
If you've already set the password for the access point, the window will have a box for you to enter the password.

9. Click **Next**.

WSC Guard now automatically generates a random password for the access point. Only you, as the Network Administrator, will be able to see that password if you want to modify the access point's settings later on. You can see this randomly-generated password on the secure section of the WSC web site or on the Access Point's Properties dialog box.

The wizard now displays a window for naming the wireless access point.

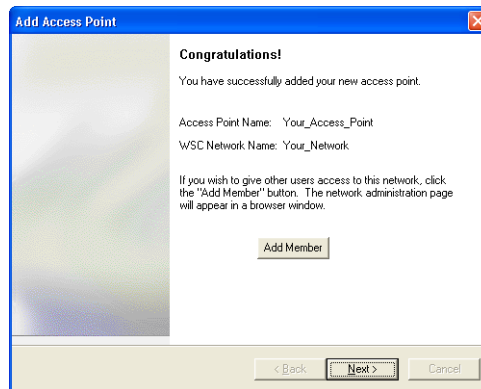
10. Enter a descriptive name for the access point that will help you identify it.



11. Click **Next** to continue.

The final window from the Add Access Point wizard, shown below, now appears, displaying both the name of the access point and the name of the Network to which you have added it.

Important: If a network connection error dialog box appears instead of this final window, you may have lost internet connectivity during the process, or you may have incompatible firmware. If you think the firmware may be at fault, right-click the WSC Guard Notification Icon and choose **Administration Website** from the Pop-up menu. The browser window that appears has a link for checking system requirements. Click the link and follow the steps to check the system requirements. If you think the internet connection was lost, see the problem solution on page 120.



12. If you want to now add a Member to the Network, click **Add Member**.

If you click the **Add Member** button, you'll go to the WSC web site where you can log in to the Member's Section. The Member's Section has the links for going to the Add Member section. See "Adding a Member to a WSC Network" on page 91 for details. If you don't want to add Members now, you can go to the web site later by choosing **Administration Website** from the WSC Pop-up menu.

13. Click **Next**.

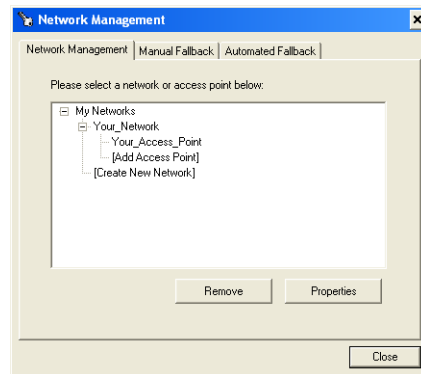
CHECK AND MANAGE NETWORK PROPERTIES

You can see the properties of each Network for which you are the Network Administrator.

To view a Network's properties:

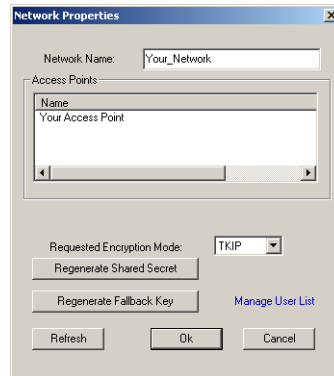
1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

The Network Management dialog box appears.



4. In the list of Networks, select the Network you want to check, and click the **Properties** button.

The Properties dialog box appears for that Network.



The properties are:

Network Name—the name you assigned to the Network. You can click in this box and type a new name if you want to re-name the Network. The Network Name is the SSID used for connecting to the Network.

Access Points—the names of the access points that are on the Network.

Requested Encryption Mode—the type of data encryption that the Network uses to keep your data secure. Click the drop-down arrow to see a list of other encryption modes.

Regenerate Shared Secret—a shared secret is an internally-generated password that is used in a secure manner between the authentication server and access point. Click this button to have WSC Guard create a new shared secret. Usually you use this option if you suspect your Network security has been compromised.

Regenerate Fallback Key—the Fallback key is the encryption key that your computer uses to secure data while in Fallback Mode (that is, either WPA-PSK or standard WEP security mode, whichever

one your access point supports) when internet connectivity is lost. Click this option if you suspect that your Network security has been compromised.

Refresh—click to rescan the Network to find the access points on it. Click this button if the access points list is not complete.

Manage User List—click this link to connect to the WSC Member web site to add or remove users and guests from the Network. See “Modify Network User List” on page 90 for details.

5. Click **Cancel** to close the Network Properties dialog box.

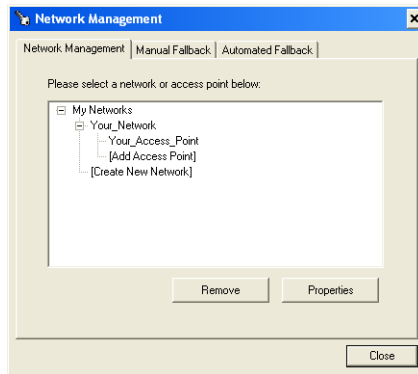
CHECK ACCESS POINT PROPERTIES

You can see the properties of each access point on the Networks for which you are the Network Administrator.

To check an access point’s properties:

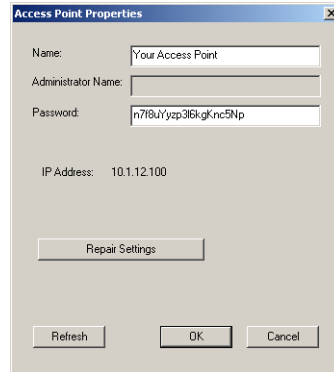
1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

The Network Management dialog box appears.



4. Select the Network that has the access point you want to check and click the **Properties** button.

The Properties dialog box appears for that access point.



The access point Properties are:

Name—the name you assigned to the access point. You can click in this box and type a new name if you want to re-name the access point.

Administrator Name—during initial set-up and configuration, some access points require an administrator name, as well as a password. If your access point has that requirement, the information appears here.

Password—the randomly-generated password generated by WSC that takes the place of the manufacturer's default password. This password is extremely important because, if you want to change the access point's channel or configure other settings to improve connectivity, you will need this password to use the access point's utility program.

IP address—the IP address that the access point has on your Network. The IP address is also necessary for reconfiguring the access point's settings.

Repair Settings—sometimes an access point cannot communicate properly with the WSC Authentication Center. Click this button to reset the access point so it can be used on your WSC Network.

Refresh—click to rescan the Network to update the access point's properties.

5. Click **Cancel** to close the Access Point Properties dialog box.

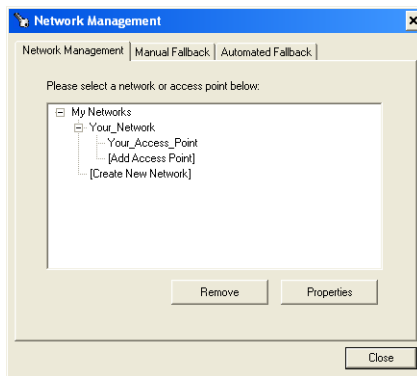
RENAME A NETWORK OR ACCESS POINT

You can change the name of a Network or access point. For example, if an access point was named “3rd Floor West” and you move it to another location, you may want to give it a new name.

To rename an access point or a Network:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

The Network Management dialog box appears.



4. Select the Network or access point that you want to rename.
The text of the name can be edited in the list.

- Simply type a new name for the Network or access point and then click elsewhere on the dialog box.

If you changed the name, inform your Network Members of the new name so they will know which Network to select later on.

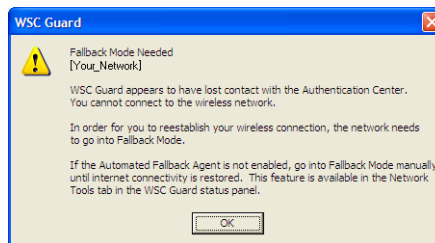
SET THE SECURITY FALLBACK MODE

Your Network uses the WSC Authentication Center over the internet to ensure a high level of security. However, if the internet fails or connectivity to the internet is interrupted, your WSC Guard Network has the ability to switch over to Fallback Mode so that work is not interrupted and people can continue to use the Network locally.

Switching over to Fallback Mode can be done both automatically and manually. Automatic Fallback Mode occurs when the Automated Fallback Agent option is enabled. If the Agent is not enabled and internet connectivity is lost, manually switching over to Fallback Mode is done using the Network Management dialog box. See “Turn On/Off Fallback Mode Manually” on page 42.

The Network Administrator has the authority to initiate Fallback Mode manually, but can also assign that authority to other Network Members. See “Adding a Member to a WSC Network” on page 91 for more about assigning Fallback authority to a Network Member.

If internet connectivity is lost, you will see a warning message:



When this situation occurs, the switchover from WSC Guard security to Fallback Mode is done automatically if the Automated Fallback Agent is enabled. Otherwise, you must switch over manually. In either

case, your Network reverts to local authentication using the next best level of security available in your particular access point. This may be 128-bit WEP or WPA-PSK. Thus, your Network continues to function, but with the lower level of security of the access point instead of the higher-level of WSC Guard protection.

TURN ON AUTOMATIC FALLBACK

The automatic mode uses a Fallback “agent” which is simply a special monitoring program that tests connectivity to the WSC Authentication Center. If a problem occurs, the agent starts the sequence that switches to Fallback Mode.

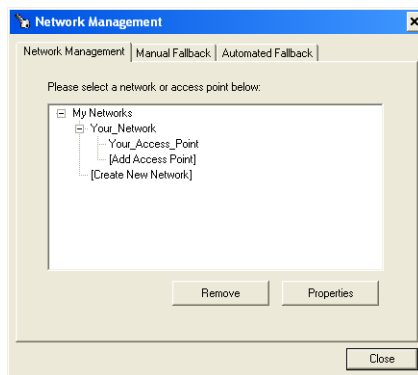
You will need to use a computer that has a wired connection to the Ethernet hub that connects your wireless access point to your broadband modem or router.

To turn on automatic Fallback Mode:

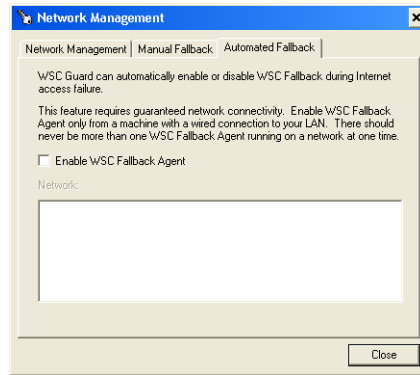
1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

See “Adding a Member to a WSC Network” on page 91 for the steps to assign Fallback authority to a Network Member.

The Network Management dialog box appears.



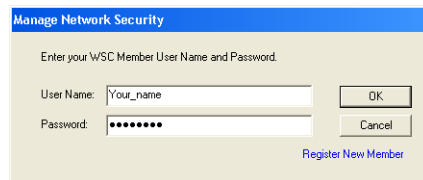
- Click the **Automated Fallback** tab.



- Click **Enable WSC Security Agent**.

Note: Having Automatic Fallback enabled is recommended. However, if you want to turn it off, click the option again to remove the checkmark.

- Enter your User Name and Password and click **OK**.



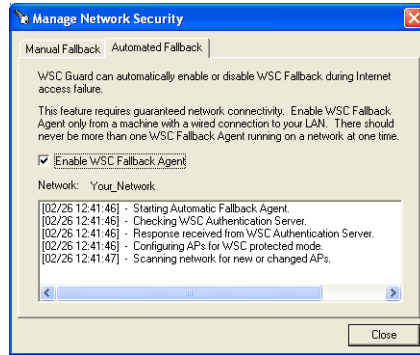
- Select the Network.



Note: You can enable the Automatic Fallback Agent for only one Network per computer. If you want to enable the agent for other Networks, use a different computer for each Network.

8. Click **Enable Wireless Guard Fallback Agent**.

The automatic Fallback agent program starts and you will see information regarding network security activity.



9. Click **Close** to close the Network Management dialog box.

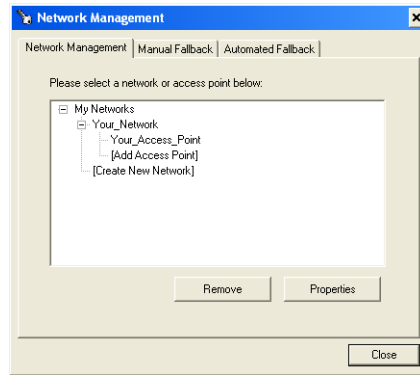
TURN ON/OFF FALLBACK MODE MANUALLY

Although Automatic Fallback Mode is your most likely choice, if you have not activated the Automatic Fallback Agent, you would need to turn on/off Fallback Mode manually if internet connectivity is lost.

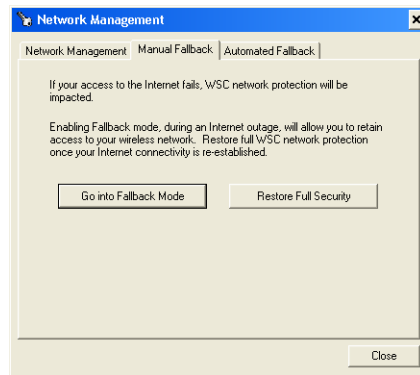
To turn on Fallback Mode manually:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

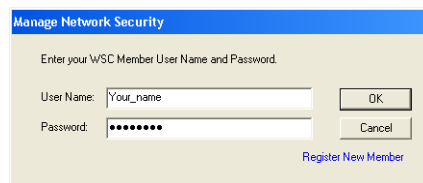
The Network Management dialog box appears.



4. Click the **Manual Fallback** tab.

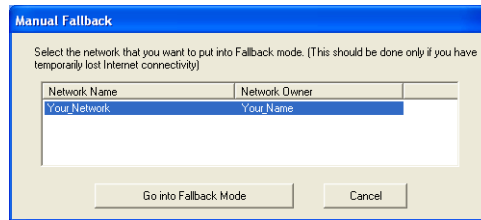


5. Click **Go into Fallback Mode** to manually initiate Fallback.
6. When prompted, enter your User Name and Password and click **OK**.



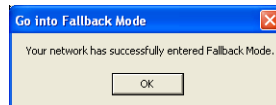
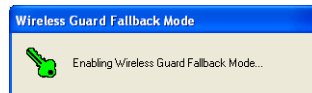
The Manual Fallback dialog box appears.

7. Select the Network.



8. Click **Go into Fallback Mode**.

Messages appear to confirm that the Fallback Mode is successfully initiated.



9. Click **OK**.

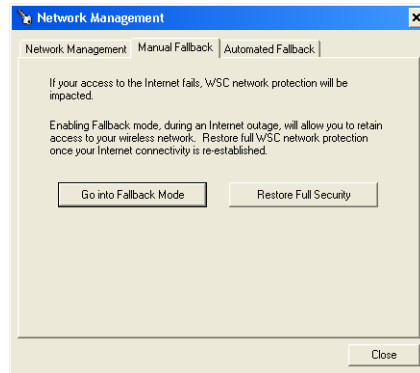
The Network will now run in Fallback Mode.

10. Click **Close** to close the Manage Network Security dialog box.

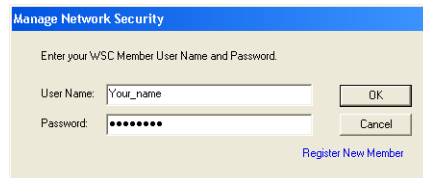
To turn off Fallback Mode manually:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

- Click the **Manual Fallback** tab.



- Click **Restore Full WSC Security**.
- When prompted, enter your User Name and Password and click **OK**.



The Manual Fallback dialog box appears.

- Select the Network.



- Click **Restore Full WSC Security**.
Messages appear to confirm that the Full WSC Security is resumed.
- Click **Close** to close the Network Management dialog box.

REMOVE AN ACCESS POINT FROM A WSC NETWORK

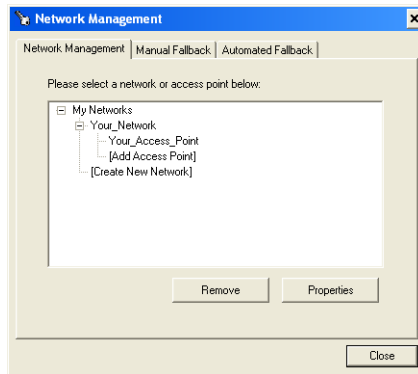
You may need to remove an access point from a Network. For example, you may want to replace one access point with another.

Removing an access point does not physically disable it, but rather only removes it from the WSC Authentication Database. However, when you remove an access point, you will need to give it a new network name (SSID), and set a new password and administrator name, if your type of access point requires it. In addition, the access point's security level is also reset to Clear, which is no wireless security.

To remove an access point:

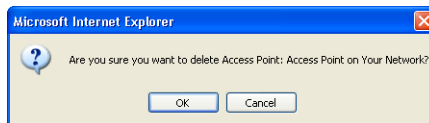
1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.
3. Enter your User Name and Password and click **OK**.

The Network Management dialog box appears.



4. Select the access point to remove and click **Remove**.

A dialog box appears asking you to confirm that you really want to delete the access point.



5. Click **OK**.

A dialog box appears for you to set the access point's new network name (SSID), password and administrator name, if necessary.

When the access point is removed, it will be broadcasting "in the clear" and will not have any wireless security until you reset its security level using the access point's configuration utility, and the new password and administrator name you just assigned to it.

Your access point is now no longer installed as part of the WSC Guard Network.

REMOVE A WSC NETWORK

You must delete all access points from a Network before you can remove the Network. Removing a Network removes it from the WSC Authentication Center, therefore, removing a Network deletes all the information about the Network, including the list of Members you assigned to that Network. If you delete a Network, you cannot recover the lost information.

To recreate the Network, the new Network Administrator will first have to re-add the access point and then re-add Members to it.

But note that if you delete a Network and then recreate it, the WSC Authentication Center treats it as a new Network, with new billing. If the removed Network still had time remaining on its subscription, that time is not carried over to the new Network.

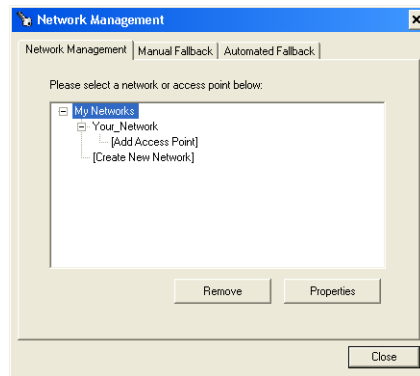
Note: If you delete a Network and then recreate it, the WSC Authentication Center treats it as a new Network, with new billing. Even if the removed Network still had time remaining on its subscription, that time is not carried over to the new Network, and a new billing cycle starts.

To remove a Network:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Manage Wireless Network** from the Pop-up menu.

3. Enter your User Name and Password and click **OK**.

The Network Management dialog box appears.



4. Select the Network you want to remove and click **Remove**.
5. If time remains on the Network's subscription, a message asks you to confirm that you want to remove the Network. Click **Yes**.
If the Network's subscription has expired, the message does not appear.
6. Inform all the people who used that Network that it is no longer available.

DISABLE WSC GUARD

In some instances, you may want to disable WSC Guard. For example, if you take your laptop to another location to give a presentation, and connect to a network there running 802.1x security, the WSC Guard software on your laptop assumes that the access points in that network are protected with the WSC Guard security.

However, trying to login will fail because WSC Guard security is not available on that network. In that case, you simply stop the WSC Guard application so you can login.

Later on, when you want to re-enable WSC Guard security, restart WSC Guard again.

To disable WSC Guard:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Exit**.

To restart WSC Guard:

1. From the Windows Start menu, choose **Wireless Security Corporation**, and choose **WSC Guard**.

If you have set the WSC Guard to automatically login, WSC Guard restarts, otherwise, the login dialog box appears.

2. In the WSC Guard dialog box, enter your User Name and Password and click **Login**.

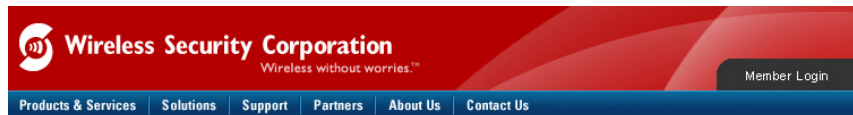
GO TO THE WSC WEB SITE

You can link directly to the WSC web site from the Windows Start menu or from the WSC Guard Notification Icon. Alternatively, you can type the WSC URL directly into your browser.

To connect to the WSC web site from the WSC Guard Notification Icon:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Administration Website**.

The WSC web page opens for you to log in.



3. Click the **Member Login** button.

See “Using the WSC Web Site” on page 67 for details about using the WSC web site.

To connect to the WSC web site from Windows:

1. From the Windows Start menu, choose **Programs**, then **Wireless Security Corporation**.
2. Choose **Membership and Network Administration Website**.

CHECK FOR WSC UPDATES

WSC Guard is constantly being updated with new features, improvements, and enhancements. The WSC Guard application will check periodically to see if updates are available and, if they are, will display a dialog box so you can download the updates. You can also manually check for WSC updates.

When an update is available:

1. A dialog box appears informing you that the update can be downloaded.
2. Click **Download Now** to get the update. It will be stored in a temporary file on your computer.
3. To defer the download for a set time period, click the **Notify me later** down arrow and pick a time when you want to be notified again.

If you don't want to be notified in a specific time period, click **Remind Me Later**.

You will continue to receive reminders until you update your WSC Guard software.

To check for WSC updates manually:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **About WSC Guard**.

The About dialog box opens.



3. Click the **Check for Update** button.

If an update is available, the dialog box for downloading the update appears with buttons to select when to download it.

INSTALL A WSC GUARD UPDATE

WSC Guard update files are downloaded from the internet and stored in a temporary location on your computer until you install the update. The temporary files are then deleted.

Note that updates do not require reconfiguring your Network, access point, list of users, passwords, and so forth. Updating usually fixes any discovered bugs in the software, or adds new enhancements and additional features.

Installation of updates is recommended (but not required) as soon as you download the update files from the internet.

To install a WSC Guard update:

1. A dialog box appears informing you that the update is ready to be installed.
2. Click **Install Now** to install the new software.
3. Follow the instructions on the screen during the update process.

4. If you click **Cancel**, a dialog box appears so you can defer the download for a set time period. Click the **Notify me later** down arrow and pick a time when you want to be notified again.

If you don't want to be notified in a specific time period, click **Remind Me Later**.

You will continue to receive reminders until you install your WSC Guard update software.

USING THE WSC GUARD NETWORK SELECTOR

The WSC Guard Network Selector is activated by default on computers running Windows 2000 or other older Windows operating systems. It is a built-in application within WSC Guard that simulates the Windows XP wireless networking support for viewing and connecting to wireless networks.

Note: You can also use the WSC Guard Network Selector on a computer running Windows XP, by activating it. If you activate the WSC Guard Network Selector, it disables the XP support. You do not have to activate the Network Selector on computers running Windows 2000, 98, or Me. It is already activated as the default.

To activate the WSC Guard Network Selector:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **Status** from the Pop-up menu and click **Available Wireless Networks**.

Or, choose **Options** from the Pop-up menu and select **Use WSC Guard to configure my wireless network settings. Select this option to use WSC Guard exclusively for connecting to wireless networks**.

Either method of activating the Network Selector adds the menu option **View Available Wireless Networks** to the Pop-up menu

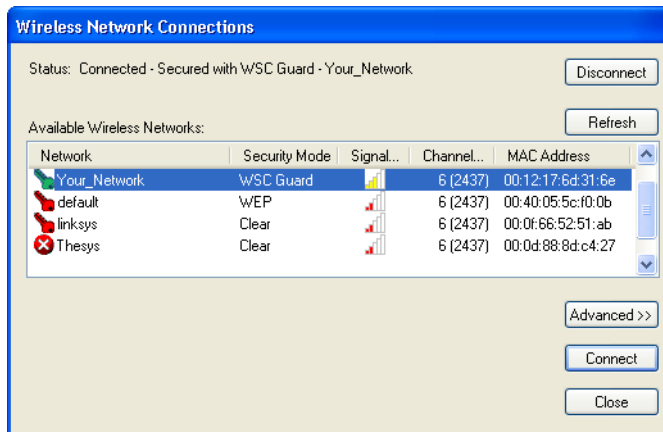
3. See "Check Network Status" on page 15 or "Selecting Options" on page 19 for details about activating the Network Selector.

To open the Network Selector:

1. Right-click on the **WSC Guard Notification Icon**.
2. Choose **View Available Wireless Networks** from the Pop-up menu



The WSC Guard Wireless Network Connections window opens.



Status—shows the name of the current Network and the type of security, such as WSC Guard.

Available Wireless Networks—lists the wireless Networks within range of your computer’s network adapter. The highlighted Network is the one you are currently using (in the example above it is Your_Network).

Network—name of the available Networks. The symbols next to the names indicate the type of Network:



No security. this network is broadcasting “in the clear.”



Protected by WSC Guard.



Protected by WSC Guard, but in Fallback mode.



Not protected by WSC Guard; secured with WEP or WPA-PSK

Note that if you haven't connected to a network before, or are not currently connected, the key may be one color until you connect, and then turns to another color depending on the network's a security state. If your network adapter does not support WPA, all networks appear as in Clear or WEP security mode.

Security Mode—the type of security, if any, being used by the networks.

Signal Strength—the current strength of the wireless signal being received by your computer's network adapter.

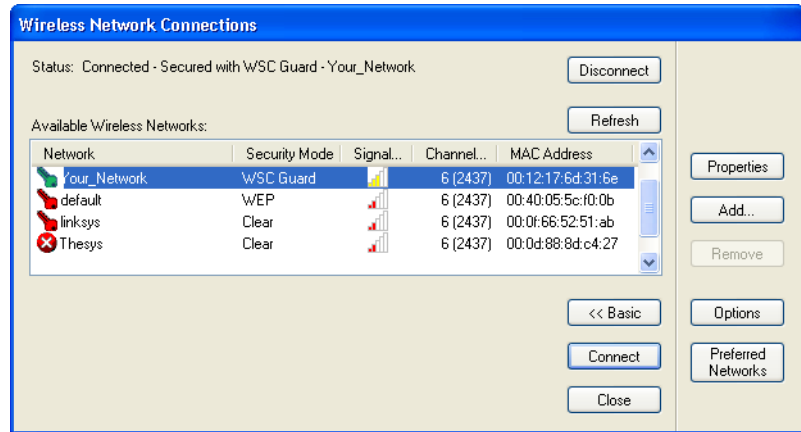
Channel (Frequency MHz)—the wireless channel and radio frequency in MHz being used by the access point to transmit signals over the network.

MAC Address—the wireless MAC (Media Access Control) address of the access point (also the BSSID of the access point).

3. To update the list, click the **Refresh** button.

- To see Advanced features of the Network Selector, click the **Advanced** button.

Extra buttons for the Advanced features appear on the right side of the dialog box, and the Advanced button now is labeled **Basic**. To hide the extra buttons, click the **Basic** button.



SORT THE NETWORK LIST

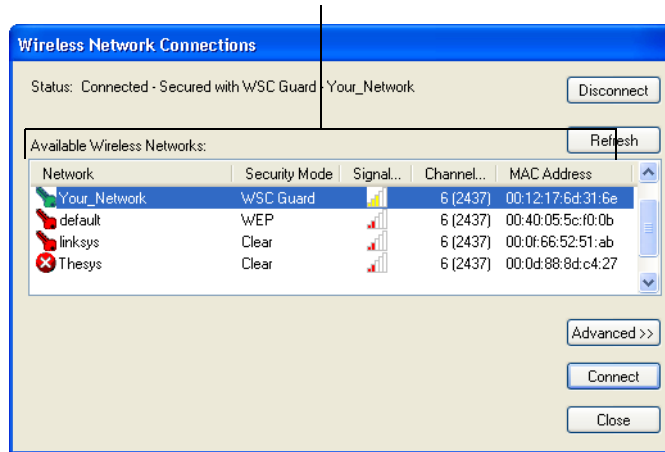
The list of networks can be sorted by the information in any of the five columns.

To sort the list of Available Wireless Networks:

- Click in the column header that you want to use for sorting the data.
- You can sort in ascending or descending order. Clicking the column header toggles between ascending and descending order.

For example, if you want to sort by Security Mode in alphabetical order, click the Security Mode column header. The list rearranges itself in ascending order. Click again to sort in descending order.

Click a column header to sort the list by the information in that column



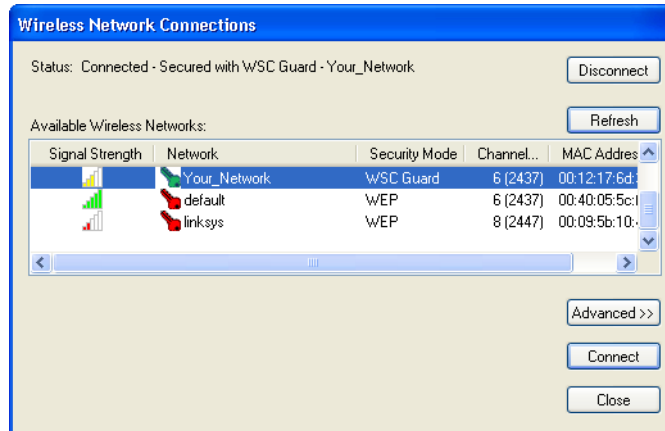
RESIZING AND REPOSITIONING THE COLUMNS

The Available Wireless Networks columns can be resized or repositioned to show the data in the manner you want.

To resize or reposition the list of Available Wireless Networks:

1. To resize a column, drag its edges left or right.
2. To reposition a column, click in the column header, hold down the mouse button and drag the column to a new position.

The following example shows the Signal Strength column resized to show the full column heading, and moved to the first column position.



DISCONNECT FROM A NETWORK

If you want to remove your computer from a wireless network, you use the Disconnect button.

To disconnect from the current wireless Network:

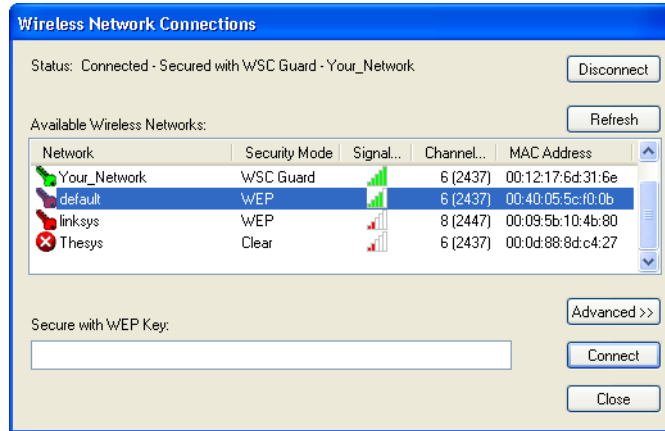
1. Make sure the Network is selected in the list.
2. Click the **Disconnect** button.

CONNECT TO A NETWORK

You can use the WSC Guard Network Selector to connect to non-WSC Networks, even if you don't have a WSC Guard Network. This is essentially a free use of the WSC Guard software.

To connect to another Network:

1. Select the Network in the list of Available Wireless Networks.
2. To connect to a WSC Guard Network, select it in the list and click **Connect**.



3. The WSC Guard login dialog box appears. Fill in your User Name and Password, and click **Login**.

To connect to a non-WSC Guard Network:

1. Select the Network from the list.

If the Network is secured by WEP or WPA-PSK, a box appears on the dialog box for you to enter the security key.

For WEP networks, enter the key as hexadecimal digits. Enter 10 digits for 64-bit keys, and 26 digits for 128-bit keys.

For WPA-PSK keys, enter up to a 30-character key. You can enter regular characters for WPA-PSK keys. The characters do not have to be hexadecimal. For example, the key may be:
ThisKeyisforMeAndNoOneWillKnow

Networks broadcasting in the clear do not need keys.

You only need to enter the security key the first time you connect to a network. The key will appear in the box from then on when you select that network from the list.

2. Click the **Connect** button.
3. Messages inform you of the connection, and remind you to update the keys periodically.

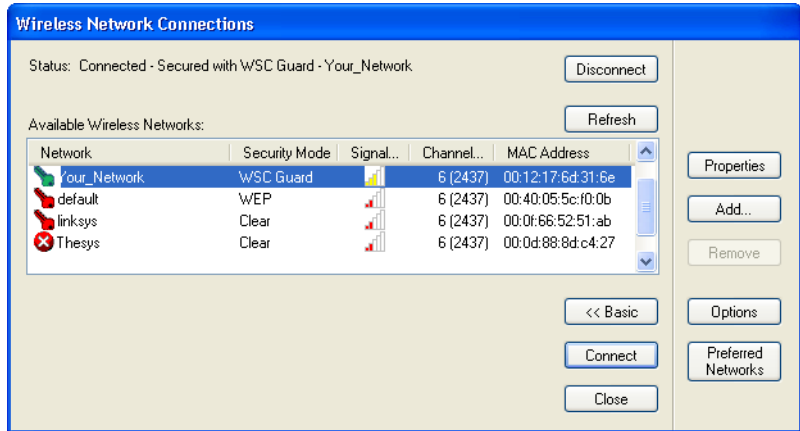
A message then tells you when your computer is connected to the new Network.

ADD A WIRELESS NETWORK

Use this feature if you know that the access point is available, but its broadcast SSID is turned off. When that situation occurs, the Network does not appear in the list and you need to add it.

To add a wireless Network:

1. Click the **Advanced** button on the Network Selector.
2. Click the **Add** button.



The Add Wireless Network dialog box appears.



3. Type a name for the Network in the Network Name (SSID) box.
4. The name must be the exact SSID, including upper and lower case characters.
5. Select the options for the Network from the Security Settings:

Authentication—click the drop-down menu arrow and select the type of authentication to use with the Network. The choices are Open, Shared, Auto, WPA-PSK, and WSC Guard.

Data Encryption—click the drop-down menu arrow and select the type of data encryption to use with the Network. The choices depend on the type of authentication you selected for the Network. For WSC Guard, the choices are WEP, TKIP, and AES.

Security Mode—shows the Security Mode based on your selection of Authentication and Data Encryption.

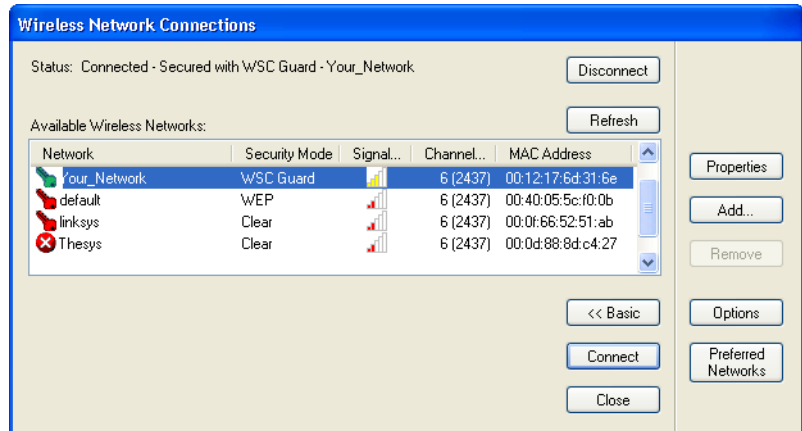
6. Click **OK**. The Network is added to the list of available wireless Networks.

MODIFY A WIRELESS NETWORK

In general, WSC Guard will automatically detect and set the correct settings for all available access points. But if you need to change a Network's properties, you can modify its settings using the advanced features of the Network Selector.

To modify the properties of a wireless Network:

1. Click the **Advanced** button on the Network Selector.
2. Click the **Properties** button.



The Modify Networks dialog box appears.



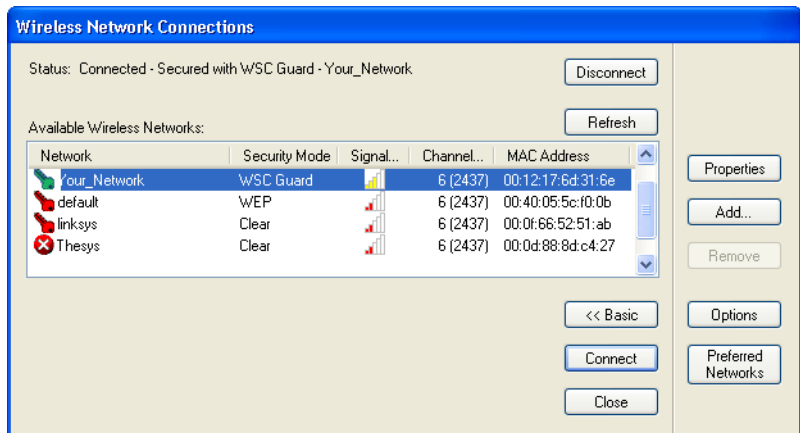
3. Click the drop-down menu arrows and select new security settings for the Network.
4. To use the settings that WSC Guard detects for the Network, click **Revert to Default**.
5. Click **OK**.

SELECTING NETWORK CONNECTION OPTIONS

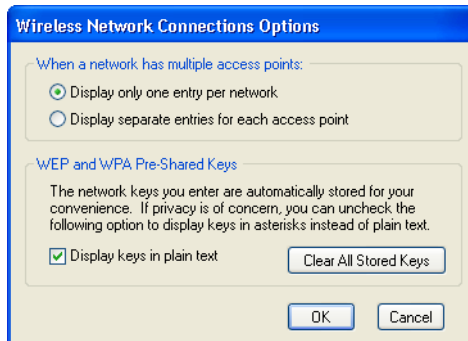
The Network Connection Options provide selections for how you want to display the information on the Network Selector dialog box for each listed Network.

To select options for a wireless Network:

1. Click the **Advanced** button on the Network Selector.
2. Click the **Options** button.



The Wireless Network Connection Options dialog box appears.



3. Select the options you want:

Display only one entry per network/Display separate entries for each access point—if a network has multiple access points with the same SSID, the Network Selector can display only one listing of the match. Click the option you want. Multiple access points with the same SSID is for roaming between them.

Display keys in plain text—check this option to see the actual key characters of the networks' security keys. Uncheck this option to have the characters hidden by asterisks. Usually you uncheck the option if your computer can be accessed by others, and you want to hide the key. However, if you uncheck this option, and then later try to change it to display the keys in plain text, a message tells you that the saved keys will be cleared. This is an extra measure of security to keep an unauthorized person from checking the option and seeing the actual keys in plain text. You will then have to enter the keys again when you connect to a protected network.

Clear all stored keys—select this option periodically to erase all the keys for your Networks. This is similar to changing your password frequently to keep others from getting it. Enter a new key for your Networks when you connect to them.

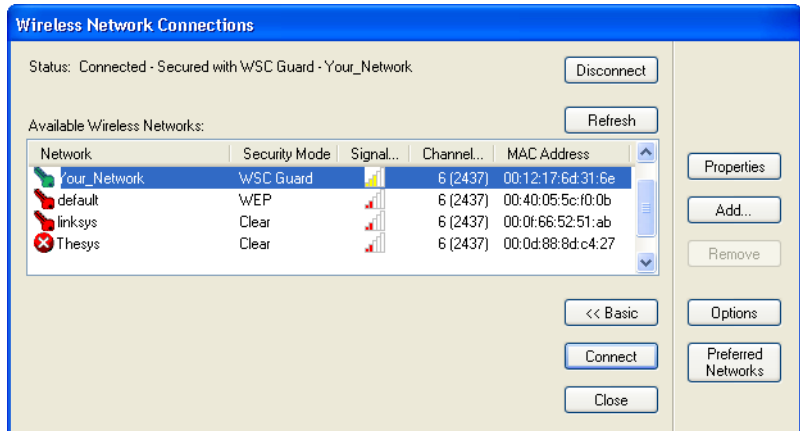
4. Click **OK**.

LISTING PREFERRED NETWORKS

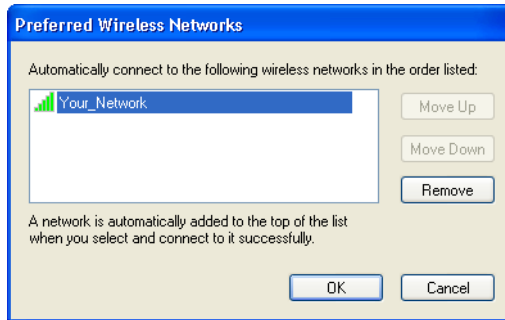
If you have access to several Networks, and your computer loses network connectivity, you can set up a list to try to reconnect to the Networks in a specific, preferred order.

To set the preferred Network order:

1. Click the **Advanced** button on the Network Selector.
2. Click the **Preferred Networks** button.



The Preferred Wireless Networks dialog box appears.



3. Select the Network to be first in the list and click the **Move Up** button until it is at the top of the list.
4. Select the Network to be next in the list and click the **Move Up** or **Move Down** buttons until it is in the second position.

5. Repeat with all of your Networks until they are in the order you want them to be tried for reconnection.

Note that if you connect to different networks in multiple locations, those networks will also be listed even if they are out of wireless range. the Network you most recently encountered is automatically placed at the top of the list.

6. To remove a Network from the preferred list, select it, and then click the **Remove** button.
7. Click **OK** to close the dialog box.

CHAPTER 3

Using the WSC Web Site

This chapter provides reference information and instructions for using the WSC web site. The WSC web site contains two main sections:

- **Public Section**—may be accessed by anyone. The public pages on the WSC web site include information about Wireless Security Corporation, WSC secure wireless networking solutions, customer and technical support, WSC partner information, wireless industry news and events, corporate contact information.
- **Member Center**—only accessible to registered as WSC Guard Members who have a valid user name and password. The Member Center contains web pages specifically designed for use by WSC Network Administrators and Members.

The Member Center includes a set of network administration pages only accessible to WSC Network Administrators (any WSC Guard Member who creates a WSC Guard-Protected Network) for use in managing WSC Networks. Typical management functions include adding a new user, deleting a user (for example when an employee leaves your company), giving a Guest temporary access, setting intrusion alarms, and viewing network reports.

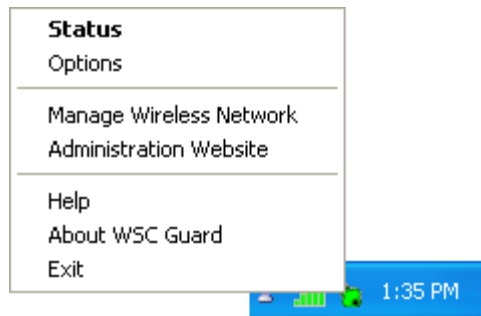
The first section of this chapter provides instructions for logging into the Member' Center. The remaining sections are organized as a reference for the features and functions of the Member Center.

LOGGING INTO THE WSC WEB SITE

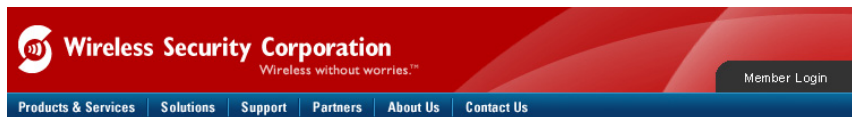
If you have already signed up as a WSC Network Member, you can log into the Member Center of the WSC web site, where you can change your WSC profile information, download new software, and change your contact and account information. Furthermore, if you are a WSC Network Administrator, this is where you can manage the networks that are your responsibility.

To log into the WSC web site:

1. Right-click the **WSC Guard Notification Icon** in the Windows notification area at the lower right corner of your desktop, and choose **Administration Website**.



Alternatively, using a web browser you can navigate to the WSC web site at: <http://www.wirelesssecuritycorp.com> and then click the **Member Login** button.



The Login page appears.



Products & Services Solutions Support Partners About Us Contact Us

Secure Wireless Member Login

User Name:

Password:

Forgot your password? [Click here.](#)

Interested in:

- [System Requirements](#)
- [Product Downloads and Documentation](#)
- [FAQs](#)

2. Enter your User Name and Password.

Note: Your login has an automatic “time out” if you don’t use the web application within that time. This is simply an additional measure of security in case you leave your computer unattended and forget to log out of the application. After the time-out expires, you must login again.

3. Click **Login**.

Upon successful login, you are switched from the insecure Public section to the secure Member Center of the WSC web site, as indicated by the **Member Center** label at the top of the page. Also note that the Login button now says **Member Log Out**.



VIEWING YOUR PERSONAL WSC HOME PAGE

When you log in to the Member’s section of the WSC web site, you arrive at the “My Home” page, which contains a personalized greeting at the top (Hello and your name).

Wireless Security Corporation
Member Center

Member Log Out

My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

My Home

Network Activity Summary

Since your last login on **02/25/05 14:33:17 PST**, your networks have experienced the following activity:

Network Name	Successful Attempts	Failed Attempts
Your_Network	25	5

For additional information go to [Network Admin](#) and select Reports.

We want to hear from you!

EARN \$25

What is your experience with WSC Guard? We want to hear from you.

Earn \$25 by taking a 15 minute phone survey to tell us about your experience.

Call (650) 482-5588 or [send us an email](#) to schedule a time to talk.

[Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#) | [Site Map](#)

The “My Home” page is your personal home page in the Member Center of the WSC web site. If you are a Network Administrator, the left side of this page contains a Network Activity Summary table, and the right side contains news and information from WSC that is updated periodically.

The Network Activity Summary table provides a quick overview of the number of successful and failed logon attempts for each of your WSC Guard Networks. From this information, you can determine at a glance if an unauthorized person has been trying to log into your secure Network. See “Setting Intrusion Detection Alarms” on page 85 to see how to set up alarms for email notification of break-in attempts.

If you are a WSC Network Member, but not a Network Administrator, the Network Activity Summary table is empty and displays the message: “You are not a network administrator.”

The navigation tabs in navigation bar across the top of the page link to pages with the following information:

- **My Home:** brings you back to your personal home page in the WSC Member Center.

- **My Account:**

For all network users: provides access to your Member information for the WSC Guard service. This is where you can change your password and contact information.

For Network Administrators only: the My Account tab also has a drop-down menu for seeing the pages to update your membership and billing information, check the status of your account, and change your Network's subscription.

- **Networks:**

For all network users: shows which networks you can access.

For Network Administrators only: for managing each WSC wireless Network for which you are listed as the Network Administrator. This is where you add more Network users and guests, change access rights, set up reports of possible security intrusions, and so forth. Network management is only for Network Administrators. Network users who are not Network Administrators cannot change any of the network management settings.

- **Downloads:** provides links to get the software for new users, documentation, or updates as new versions are released.
- **Member Log Out:** click to log out of the Member Center and return to the Public section of the WSC web site.
- **Help:** shows help information for the various web pages in the Member's section of the WSC web site.

MODIFYING YOUR WSC ACCOUNT PROFILES

Your WSC account profiles contain all your membership information. The Member Profile is available to every WSC Guard Member; but the Billing Profile and Billing History pages are only available to Network Administrators.

MODIFY YOUR MEMBER PROFILE

Changes to your Member profile include changing your password and updating your address information. These functions are available to all WSC Guard Members.

Tip: As another security precaution, we recommend changing your login password often. It is a simple, easy process with the WSC web application.

To modify your Member profile:

1. *All Network Users:* Log into the WSC web application and click the **My Account** tab.

Network Administrators Only: Log into the WSC web application and click the **My Account** tab and choose **Member Profile** from the drop-down menu.

The screenshot shows the WSC web application interface. At the top, there is a navigation bar with tabs for 'My Home', 'My Account', 'Networks', and 'Downloads'. A 'Help' icon is visible in the top right corner. Below the navigation bar, the user is greeted with 'Hello Your Name'. The 'My Account' tab is selected, and a dropdown menu is open, showing options for 'Member Profile', 'Billing Profile', and 'Billing History'. Below the navigation bar, there is a 'Network Activity Summary' section. It contains a message: 'Since your last login on 02/25/05 14:33:17 PST, your networks have experienced the following activity.' Below this message is a table with the following data:

Network Name	Successful Attempts	Failed Attempts
Your_Network	25	5

Below the table, there is a link to 'Network Admin' and a note to 'select Reports.' To the right of the 'Network Activity Summary' section, there is an 'Update for WSC Guard now available!' section. It contains a message: 'To review a features list and release notes, click here'. Below this message, there is a link to 'support@wirelesssecuritycorp.com'. Below the link, there is a message: 'Click here to Update Now.' Below the message, there is a note: 'Not sure which version you're currently running? Right-click on the key icon in the Notification Area and select About WSC Guard.'

The page with your Member profile appears. Unless you've already changed it, the page contains the same information you filled in when initially signing up for the WSC Guard service.

The screenshot displays a web interface for editing a member profile. At the top, there are navigation tabs: 'My Home', 'My Account', 'Networks', and 'Downloads'. A 'Hello Your Name (Your_Name)' greeting is visible. The main heading is 'Member Profile'. Below this, the 'Account ID' section contains the following fields: 'User Name*' (pre-filled with 'Your_Name'), 'Password*' (6 characters min., masked with dots), 'Confirm Password*' (masked with dots), 'Email*' (pre-filled with 'you@your_corp.com', with a note '(required for account modification notifications)'), 'Security Question*' (a dropdown menu with 'What is your first favorite sports team?' selected), and 'Security Answer*' (masked with dots). A checkbox labeled 'Do not send me any promotional email.' is checked. The 'Account Contact Information [Optional]' section includes: 'First Name:' (pre-filled with 'Your'), 'Last Name:' (pre-filled with 'Name'), 'Address 1:' (pre-filled with '1234 5th Street'), 'Address 2:' (empty), 'City:' (pre-filled with 'Anytown'), 'State/Province:' (a dropdown menu with '<-Select a State->' selected), 'Zip or Postal Code:' (pre-filled with '12345'), 'Country:' (a dropdown menu with 'USA' selected), and 'Phone:' (pre-filled with '415-555-1212'). At the bottom of the form are 'Submit' and 'Cancel' buttons.

2. Click in any box where you want to make changes and type the new information.

Note: You cannot change your User Name. It is the name that the WSC Guard service uses to identify you.

3. To change the Security Question, click the drop-down arrow and choose a new question. Type the answer in the Security Answer box.
The security question is a back-up in case you forget your password. If that occurs as you're logging onto a WSC Guard Network, or the WSC Guard Member's web site, click the **Forgot your password?** link and type the answer to your security question instead.
4. When all the changes are complete, click **Submit**. Your new profile is now active.

Note: New users added to a Network should visit their Member Profile page soon after being added in order to enter their name, select a security question, and set a new password.


MODIFY YOUR BILLING PROFILE

Typical changes to your billing profile include changing your credit card information or billing address.

To modify your billing profile, log into the WSC web application, click the **My Account** tab, and choose **Billing Profile** from the drop-down menu.

The screenshot shows the WSC web application interface. At the top, there is a navigation bar with tabs: **My Home**, **My Account**, **Networks**, and **Downloads**. A **Help** icon is in the top right corner. Below the navigation bar, the user is greeted with "Hello Your Name". A dropdown menu is open under the **My Account** tab, showing options: **Member Profile**, **Billing Profile** (which is highlighted), and **Billing History**. Below the menu, there are two main sections. On the left, a **Network Activity Summary** section states: "Since your last login on 02/25/05 14:33:17 PST, your networks have experienced the following activity:" followed by a table:

Network Name	Successful Attempts	Failed Attempts
Your_Network	25	5

Below the table, it says: "For additional information go to [Network Admin](#) and select Reports." On the right, an **Update for WSC Guard now available!** section provides instructions: "To review a features list and release notes, click [here](#). For technical support, contact 877-717-9213 or email support@wirelesssecuritycorp.com. Click [here](#) to Update Now. Not sure which version you're currently running? Right-click on the key icon  in the Notification Area and select About WSC Guard."

The page with your billing profile appears. It shows your current billing information. If you are the Network Administrator of more than one Network, the page shows the billing profile for each Network.

The screenshot shows the **Network Billing Profiles** page. At the top, the navigation bar is the same as in the previous screenshot. Below the navigation bar, the user is greeted with "Hello Your Name (Your_Name)". The main heading is **Network Billing Profiles**. Below this, there is a section for **Network Name: Your_Network** with a **[Do Not Renew]** link. The page is divided into two columns of information:

Renewal Information	[Edit]	Billing Information	[Edit]
Network Status:	Active	No credit card specified.	
Renewal Date:	03/06/05	Billing Contact No Billing Contact Information	
Total Renewal Billing Rate:	\$ 11.00	Promotions Promotional Code: WSC-10free (10 days left in free trial)	
Billing Interval:	Annually		
Renewal Network Size:	1 members		
Current Network Size:	1 members		
Renewal Rate:	\$ 11.00 per User		

At the bottom center of the page, there is a **Home** button.

EDITING YOUR RENEWAL INFORMATION

Your WSC renewal information includes the number of Members on your Network, the current size of your subscription (which can be more than the number of users on your Network), credit card information used for billing, payment schedule, and so on. Only the Network Administrator can change the information.

Each Network has its own billing information. Therefore, a Network Administrator responsible for two Networks could pay for them with two different credit cards. Likewise, the billing profile of one Network does not pertain to any other Network, even if the Network Administrator is the same person.

To edit your renewal information:

1. On the Network Billing Profiles page, click the **Edit** link for Renewal Information.

Click Edit to edit the Renewal information

The screenshot shows a web interface for 'Network Billing Profiles'. At the top, there are navigation tabs: 'My Home', 'My Account', 'Networks', and 'Downloads'. A 'Help' icon is in the top right. Below the navigation, it says 'Hello Your Name (Your_Name)'. The main heading is 'Network Billing Profiles'. Underneath, there's a sub-heading 'Network Name: Your_Network' with a '[Do Not Renew]' link. The 'Renewal Information' section is highlighted and includes an '[Edit]' link. The details for Renewal Information are: Network Status: Active; Renewal Date: 03/06/05; Total Renewal Billing Rate: \$ 11.00; Billing Interval: Annually; Renewal Network Size: 1 members; Current Network Size: 1 members; Renewal Rate: \$ 11.00 per User. To the right, the 'Billing Information' section has an '[Edit]' link and shows: No credit card specified; Billing Contact: No Billing Contact Information; Promotions: Promotional Code: WSC-10free (10 days left in free trial). A 'Home' button is at the bottom center.

The page for editing your renewal information appears. If you haven't filled in billing information yet, the page includes the section for your billing information.

My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

Modify Renewal Information Current Network Members: 1 Maximum Network Size: 1

Network Name: Your_Network

Network Subscription Renewal Information

Subscription Size: * 1 member(s)

Billing Plan Interval: * Monthly Annually

Card Type: * Visa Mastercard AMEX [Purchase Orders](#)

Promotional Code: WSC-10free (10 days left in free trial)

Card Number: *

Expiration Date: * 01 2007

Name on Card: *

Security Code: *
3 digit number after credit card number on back of card.

Your Total Billing Rate is: \$ 11.00 Annually (1 members at \$ 11.00 per member)

Billing Contact Information

First Name: * Your

Last Name: * Name

Title:

Company:

Address 1: * 1234 5th Street

Address 2:

City: * Anytown

State/Province: * California

Zip or Postal Code: * 12345

Country: * USA

Email: * you@your_corp.com

Primary Phone: * 415-555-1212

Secondary Phone:

2. Edit the information you want to change.

- **Increase the subscription size so more people can use the network**—enter a number in the Subscription Size box. You do **not** have to increase the subscription size here prior to adding more Network users. But if you expect to add a group of people, you could “pre-allocate” Network “slots” for them. Adding people to the Network automatically increases the subscription size.
- **Change the billing interval**—select the option for monthly or annually.
- **Change the credit card you use for billing**—enter the new credit card information.
- **Change the contact information**—edit or enter the information in the bottom portion of the page. The information will only be in this section if you filled in the Member Profile before creating the Network.

3. Click **Continue**.

A confirmation page appears so you can check your changes.

My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

Modify Renewal Information

Network Name: Your_Network

Confirm Network Subscription Renewal Information

On your next billing date, 02/09/06, you will be billed for 2 Members at \$ 11.00 per Member, for a total of \$ 22.00.

Billing Information [Edit]

Visa: 0000-0000-0000-1111
Expires: 10/05

Billing Contact

Your Name
network.
Shortly, network will also
have a billing history., CA.12345

Submit Cancel

4. Click **Submit** if the information is correct.

To edit your billing information:

1. On the Network Billing Profiles page, click the **Edit** link.

Click Edit to edit the
Billing information

My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

Network Billing Profiles

Network Name: Your_Network [Do Not Renew]

Renewal Information		Billing Information	
[Edit]		[Edit]	
Network Status:	Active	No credit card specified.	
Renewal Date:	03/06/05	Billing Contact	
Total Renewal Billing Rate:	\$ 11.00	No Billing Contact Information	
Billing Interval:	Annually	Promotions	
Renewal Network Size:	1 members	Promotional Code: WSC-10free (10 days left in free trial)	
Current Network Size:	1 members		
Renewal Rate:	\$ 11.00 per User		

Home

The page for editing your billing information appears and shows your current information.

Note: Updating your billing information will update on both the Renewal Information page and the Billing information page so you don't have to update twice.

The screenshot shows a web browser window with the following content:

- Navigation tabs: My Home, My Account, Networks, Downloads, Help.
- Greeting: Hello Your Name (Your_Name)
- Section: **Network Billing Information**
- Network Name: Your_Network
- Section: **Credit Card Information**
 - Card Type:
 - Visa
 - Mastercard
 - AMEX
 - [Purchase Orders](#)
 - Card Number: 12345678910111213
 - Expiration Date: 01 / 2005
 - Name on Card: Your_Name
 - Security Code: 123
 - 3 digit number after credit card number on back of card.
- Section: **Billing Contact Information**
 - First Name: Your
 - Last Name: Name
 - Title:
 - Company:
 - Address 1: 1234 5th Street
 - Address 2:
 - City: Anytown
 - State/Province: California
 - Zip or Postal Code: 12345
 - Country: USA
 - Email: you@your_corp.com
 - Primary Phone: 415-5551212
 - Secondary Phone:
- Buttons: Submit, Cancel

2. Click in any box where you want to make changes and type the new information.
3. When all the changes are complete, click **Submit**.

NOTES ABOUT MODIFYING YOUR RENEWAL OR BILLING INFORMATION

The Renewal Subscription Size is the number of current Members of your Network. If you change the current size of your subscription, the subscription is renewed at the new size. If you increase the subscription size, you will be billed at a pro-rated amount. A decreased size is reflected at the next billing due date.

Usually there's no need to increase the subscription size until you add new Members. Then, the size is updated automatically.

If you want to cancel your Network subscription, click the **Do Not Renew** link on the Network Billing Profile page. Your account will stay in effect until your billing term is completed. After that, your account will not be renewed. The Do Not Renew option is only available to the Network Administrator.

CHECKING YOUR BILLING HISTORY

You can see the transactions of your account from its inception to the current date.

Log into the WSC web application, click the **My Account** tab, and choose **Billing History** from the drop-down menu.

The screenshot shows the WSC web application interface. At the top, there are navigation tabs: 'My Home', 'My Account', 'Networks', and 'Downloads'. A 'Help' icon is in the top right. Below the tabs, a user greeting 'Hello Your Name' is visible. A dropdown menu is open under 'My Account', showing options: 'Member Profile', 'Billing Profile', and 'Billing History'. The 'Billing History' option is highlighted. Below the menu, there are two main sections. On the left, a 'Network Activity Summary' section contains a red warning message: 'Since your last login on 02/25/05 14:33:17 PST, your networks have experienced the following activity:'. Below this is a table with columns 'Network Name', 'Successful Attempts', and 'Failed Attempts'. The table shows one row for 'Your_Network' with 25 successful and 5 failed attempts. Below the table is a link to 'Network Admin'. On the right, an 'Update for WSC Guard now available!' notification provides instructions on how to update the software, including a link to a features list and technical support contact information.

Network Name	Successful Attempts	Failed Attempts
Your_Network	25	5

The page with your billing history appears. It shows the transactions for your Network.

The screenshot shows the 'Network Subscription Billing History' page. At the top, there are navigation tabs: 'My Home', 'My Account', 'Networks', and 'Downloads'. A 'Help' icon is in the top right. Below the tabs, a user greeting 'Hello Your Name (Your_Name)' is visible. The main section is titled 'Network Subscription Billing History' and contains a table with columns: 'Date', 'Network Name', 'Card Type', 'Card Number', 'Amount', and 'Transaction Id'. The table lists three transactions for 'Your_Network' on 03/18/2005, with amounts of \$22.00, \$22.00, and \$80.00. Below the table is a 'Continue' button.

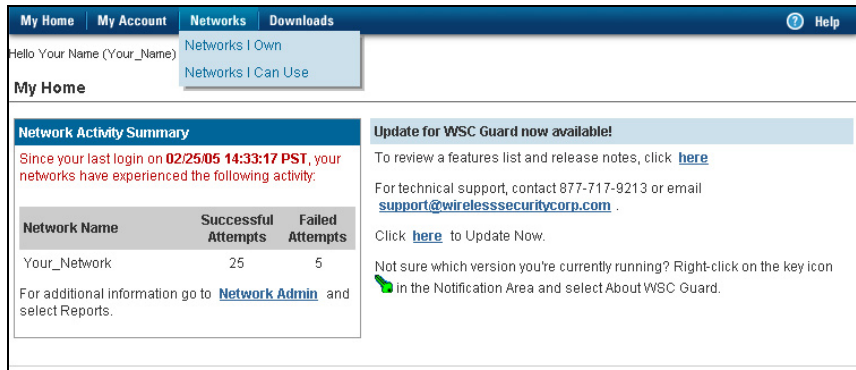
Date	Network Name	Card Type	Card Number	Amount	Transaction Id
03/18/2005	Your_Network	Visa	x000-x000-x000-1111	\$22.00	V64E77913119
03/18/2005	Your_Network	Visa	x000-x000-x000-1111	\$22.00	V64E77913042
03/18/2005	Your_Network	Visa	x000-x000-x000-1111	\$80.00	V64E77912839

SEEING WHICH NETWORK YOU CAN USE

You may have access to more than one WSC Guard Network.

To see which Networks you can use:

Log into the WSC web application, click the **Networks** tab, and choose **Networks I Can Use** from the drop-down menu.

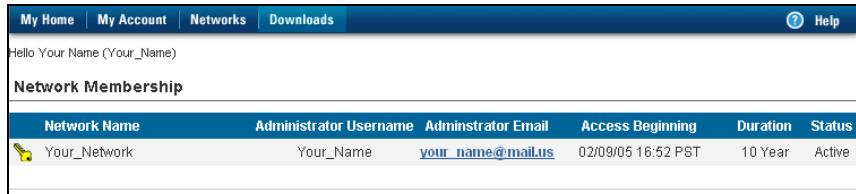


The screenshot shows the WSC web application interface. The top navigation bar includes 'My Home', 'My Account', 'Networks', and 'Downloads'. A dropdown menu is open under 'Networks', showing 'Networks I Own' and 'Networks I Can Use'. The main content area is titled 'My Home' and contains a 'Network Activity Summary' section. This section includes a message about the user's last login and a table of network activity.


Network Name	Successful Attempts	Failed Attempts
Your_Network	25	5

Additional information is provided in the 'Update for WSC Guard now available!' section, including links for technical support and update instructions.

The page shows the Networks you can use. A yellow key next to your name means you have the authority to put that Network into Fallback Mode if necessary.



The screenshot shows the 'Network Membership' section of the WSC web application. It displays a table with columns for Network Name, Administrator Username, Administrator Email, Access Beginning, Duration, and Status.

Network Name	Administrator Username	Administrator Email	Access Beginning	Duration	Status
 Your_Network	Your_Name	your_name@mail.us	02/09/05 16:52 PST	10 Year	Active

You can also see the Network Administrator's user name and email address. If you want to send the Administrator an email, just click the Administrator Email link and your email application opens.

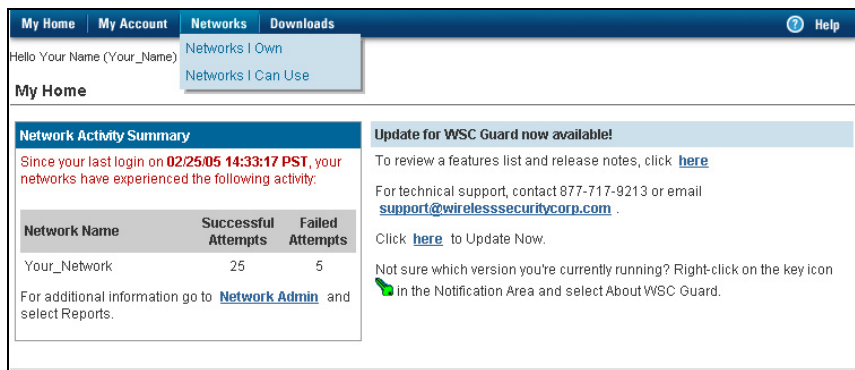
MANAGING A WSC NETWORK

Network management includes adding and deleting users, providing Guests with temporary access, setting the intrusion detection and reporting, transferring the Network to a different Administrator, and so forth.

You can only manage the WSC Guard Networks for which you are the Network Administrator.

To manage a Network:

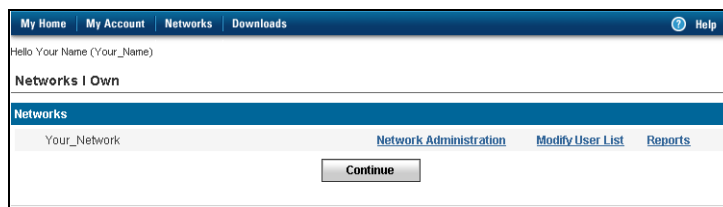
1. Log into the WSC web application and click the **Networks** tab.
2. Choose **Networks I Own** from the drop-down menu.



The screenshot shows the WSC web application interface. The top navigation bar includes 'My Home', 'My Account', 'Networks', and 'Downloads'. A dropdown menu is open under 'Networks', showing 'Networks I Own' and 'Networks I Can Use'. Below the navigation, there is a 'My Home' section with a 'Network Activity Summary' table and an 'Update for WSC Guard now available!' notification.

Network Name	Successful Attempts	Failed Attempts
Your_Network	25	5

The page for managing your Network(s) appears. It shows the Networks for which you are the Network Administrator.



The screenshot shows the 'Networks I Own' section of the WSC web application. It features a table with one network entry and a 'Continue' button below it.

Networks
Your_Network

3. Click the link for the management task you want to do.

- **Network Administration**—Click this link to see access points, set the Network Administrator name, see your access point’s randomly-generated password, and set intrusion detection parameters. The section, “Network Administration” on page 83 describes the options available in this section.
- **Modify User List**—Click this link to add Members or Guests to your Network or to modify or delete their access rights. The section, “Modify Network User List” on page 90, describes the options available in this section.
- **Reports**—Click this link to view reports on network activity. See the section, “Viewing Network Activity Reports” on page 108 for more information about reports.

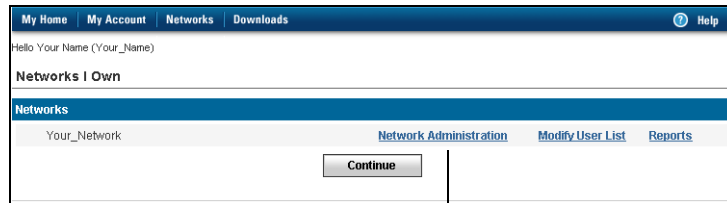
NETWORK ADMINISTRATION

The Network Administration page contains three options:

- Check the access point configuration and password.
- Set intrusion alarms.
- Transfer the Network to a different Administrator

To use the Network Administration functions:

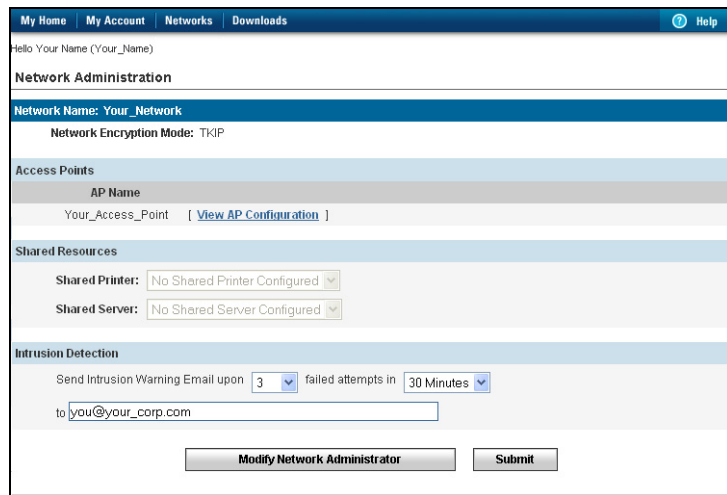
1. On the **Networks I Own** page, click the **Network Administration** link.



Network Administration link

If you have more than one Network, click the link for it.

The Network Administration page appears for that particular Network and shows the current network settings.




CHECKING AN ACCESS POINT'S CONFIGURATION AND PASSWORD

On the Network Administration page, you can view configuration information about the access point(s) on your Network, including its randomly-generated password.

To check an access point's settings:

1. On the **Networks I Own** page, click the **Network Administration** link.
2. On the Network Administration page, click the **View AP Configuration** link for the Network.

The Access Point Configuration parameters are listed.



The screenshot shows a web interface with a navigation bar at the top containing 'My Home', 'My Account', 'Networks', and 'Downloads'. A 'Help' icon is on the right. Below the navigation bar, it says 'Hello Your Name (Your_Name)'. The main content area is titled 'Access Point Configuration' and shows 'Network Name: Your_Network'. Below this is a section titled 'AP Configuration Parameters' with a table of settings:

Network Name:	Your_Network
Access Point Name:	Your_Access_Point
Manufacturer:	Linksys
Manufacturer Model:	WAP54G
Firmware Revision:	Version: 2.07
Access Point Password:	0fInIxQ trVDz6vdljuNr
Mac Address:	00-0c-41-17-33-e0

The line labelled **Access Point Password** shows the password that WSC Guard randomly generated for your access point. Because this page is only visible to the Network Administrator, no one else can see the password. Thus, you have sole access to the access password and no one else can change any of the access point's settings.

If you do need to change the access point's settings not available from WSC Guard, such as the access point's IP address, then use the utility program that you received with the access point that you used to set it up in the first place.

Note: To modify the access point's settings from now on, you will need its password first. For example, to use the utility program that you received with the access point, you must first supply this password to the utility when it opens. You can also see an access point's password using the WSC Guard Pop-up menu. See "Check Access Point Properties" on page 36.

Note: You can copy and paste the access point password from the web page into the access point utility's box for entering the password. This helps avoid errors in re-typing the long, randomly-generated string of characters.

SETTING INTRUSION DETECTION ALARMS

One of the key elements of network security is knowing when your Network is under attack by outsiders trying to break in. You can set up intrusion alarms that warn you that someone is trying to get in.

To set up intrusion detection:

1. On the Network Administration page, click the drop-down menus and choose the number of failed attempts and the time period that triggers an alarm email.

The screenshot shows the 'Network Administration' interface. At the top, there's a navigation bar with 'My Home', 'My Account', 'Networks', and 'Downloads'. Below that, a greeting says 'Hello Your Name (Your_Name)'. The main section is 'Network Administration', which includes 'Network Name: Your_Network' and 'Network Encryption Mode: TKIP'. There are sections for 'Access Points' (with an 'AP Name' field and a 'View AP Configuration' link) and 'Shared Resources' (with 'Shared Printer' and 'Shared Server' dropdowns). The 'Intrusion Detection' section is highlighted, showing 'Send Intrusion Warning Email upon 3 failed attempts in 30 Minutes' and an email address field 'to you@your_corp.com'. At the bottom of this section are 'Modify Network Administrator' and 'Submit' buttons.

Failed attempts setting

Time Period setting

2. Enter an email address where you want to receive notification of the attempted intrusion.

You can enter multiple email addresses. Separate them by commas or semicolons.

Note: Failed attempts include valid users who type the wrong password. Therefore, setting the number of failed attempts too low can trigger unnecessary intrusion alarms.

3. Click **Submit**.

Now the WSC Guard Network is monitored continuously and will let you know when intrusions are detected.

See the section, “Viewing Network Activity Reports” on page 108 and “Security Countermeasures for Unauthorized Log In Attempts” on page 110 for more about detecting intrusions and taking countermeasure steps.

TRANSFERRING THE NETWORK TO A NEW NETWORK ADMINISTRATOR

If you want to relinquish responsibility for the Network, you can transfer it to someone else using the Network Administration page.

Note: After you relinquish network responsibility, you cannot regain control of it unless the new Network Administrator goes through the same steps below to re-establish you as the Network Administrator.

To transfer the Network to a new Network Administrator:

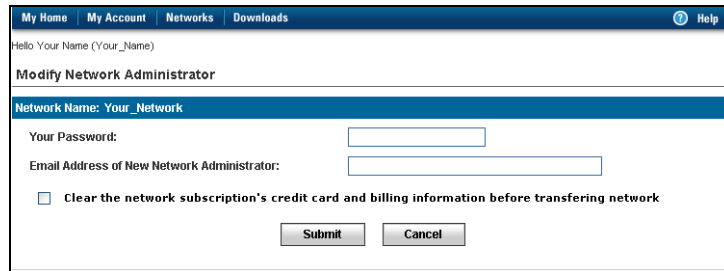
1. On the Network Administration page, click the **Modify Network Administrator** button at the bottom of the page.

The screenshot shows the Network Administration page with the following sections:

- Network Name:** Your_Network
- Network Encryption Mode:** TKIP
- Access Points:** AP Name: Your_Access_Point | [View AP Configuration](#)
- Shared Resources:**
 - Shared Printer:** No Shared Printer Configured
 - Shared Server:** No Shared Server Configured
- Intrusion Detection:**
 - Send Intrusion Warning Email upon: 3 failed attempts in 30 Minutes
 - to: you@your_corp.com

At the bottom of the page, there are two buttons: **Modify Network Administrator** and **Submit**.

The Modify Network Administrator page appears.



The screenshot shows a web browser window with a dark blue header containing navigation links: "My Home", "My Account", "Networks", and "Downloads". A "Help" icon is in the top right. Below the header, the text "Hello Your Name (Your_Name)" is displayed. The main heading is "Modify Network Administrator". A blue bar below the heading contains the text "Network Name: Your_Network". The form contains three input fields: "Your Password:" (a small text box), "Email Address of New Network Administrator:" (a larger text box), and a checkbox labeled "Clear the network subscription's credit card and billing information before transferring network". At the bottom of the form are two buttons: "Submit" and "Cancel".

2. Enter your current WSC password.
3. Enter the email address of the person who will be the new Network Administrator. That person must be a WSC Guard Member.
4. Use the **Clear the network subscription's credit card and billing information before transferring network** in the following manner:
 - Select this option if you want the new Network Administrator to pay for the Network. Your credit card information will be removed from the network billing information, and the new Administrator will have to enter new credit card information. The new Administrator will also be able to see the billing history for the Network's subscription.
 - Do not select this option if you want your credit card to continue to be billed for the Network.
5. Click **Submit**.

6. Click **Yes**.

You are now no longer the Network Administrator.

An email message will be sent to you and the new Network Administrator informing you both of the change.

Note: The email address for receipt of alarm detection reports is not automatically changed to the new Network Administrator's email address. The new Network Administrator should change that address using the steps in the section "Setting Intrusion Detection Alarms" on page 85.

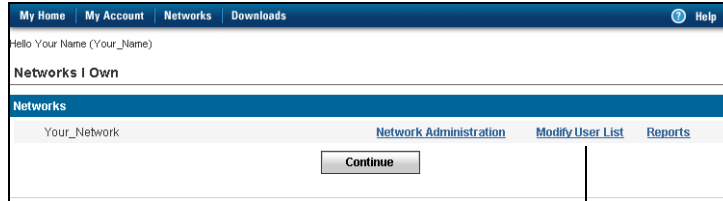
MODIFY NETWORK USER LIST

The Network Administrator controls access to the Network, including who gets access, and the level of access privileges granted to each user. The tasks associated with access control are:

- Adding and removing users from the Network
- Modifying the access rights granted to a user
- Adding and removing Guests from the Network

To use the Modify User List functions:

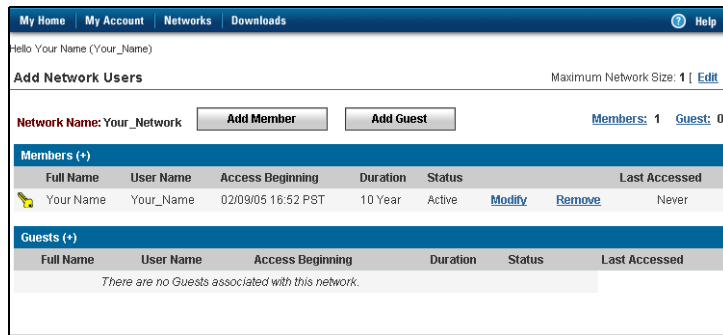
1. On the **Networks I Own** page, click the **Modify User List** link



Modify User List link

If you have more than one Network, click the link for it.

The Add Network Users page appears for that Network and shows the current list of users.



- **Full Name**—the person's name as listed in the person's profile. Note that you don't add users' names when adding people to a Network. That is for new users to do themselves once you inform them that they are part of the Network.
- **Yellow key icon**—the yellow key icon next to a person's name indicates that person has the authority to put the Network into Fallback Mode in the event that the Network loses internet access. That authority can be assigned when the person is initially added to the Network, or later when modifying that person's access.
- **User Name**—the person's Member name used to log into the Network. You assign this name, and that person is now a WSC Guard Member with that User Name. The User Name is permanent as long as the person is a WSC Guard Member.
- **Access Beginning**—the date and time when the Member or Guest's access duration begins.
- **Duration**—the length of the duration; maximum guest duration is 48 hours unless renewed.
- **Status**—whether the access is still available in the duration.
- **Last Access**—the date and time that the person last logged onto the Network.

ADDING A MEMBER TO A WSC NETWORK

For someone to have day-to-day access to your WSC secure wireless Network, that person must first be granted access to the Network by the Network Administrator.

Note: You do **not** have to manually increase the number of Network Members prior to adding more Members. Adding new Members automatically increases the size of your Network subscription.

To add a Member to your Network:

1. On the **Networks I Own** page, click the **Modify User List** link, then click the **Add Member** button.

The screenshot shows the 'Add Network Users' page. At the top, there are navigation tabs: 'My Home', 'My Account', 'Networks', and 'Downloads'. Below the navigation, the user is greeted with 'Hello Your Name (Your_Name)'. The page title is 'Add Network Users' and it indicates 'Maximum Network Size: 1 | Edit'. The network name is 'Your_Network'. There are two buttons: 'Add Member' and 'Add Guest'. The current status is 'Members: 1 Guest: 0'. Below this, there are two sections: 'Members (+)' and 'Guests (+)'. The 'Members (+)' section contains a table with the following data:

Full Name	User Name	Access Beginning	Duration	Status	Last Accessed
Your Name	Your_Name	02/09/05 16:52 PST	10 Year	Active	Never

The 'Guests (+)' section is currently empty, with the text 'There are no Guests associated with this network.'

The Add Network Users page appears.

The screenshot shows the 'Add Network Users' page with the form to add new members. At the top, there are navigation tabs: 'My Home', 'My Account', 'Networks', and 'Downloads'. Below the navigation, the user is greeted with 'Hello Your Name (Your_Name)'. The page title is 'Add Network Users' and it indicates 'Current Network Members: 1 Maximum Network Size: 1'. The network name is 'Your_Network'. Below this, there is a section titled 'Add Network Users' with the instruction 'Enter the email addresses of the people you'd like to add to your network.' and a note: 'If they are not already WSC Guard members, you will be prompted in subsequent screens for the information needed to create their membership.' Below this, there is a table with the following columns: 'Email Address', 'Access Duration', and 'Can Initiate Network Fallback'. There are five rows, each with an empty text input field for the email address, a dropdown menu for the access duration (set to '10 Year'), and a checkbox for 'Can Initiate Network Fallback'. At the bottom, there is a note: 'Note: You have no empty network slots that you have already purchased. Additional members will increase your network size.' and two buttons: 'Submit' and 'Cancel'.

2. Enter a valid email address for each new Network Member.
3. Select the access duration for each Member.
4. Click the option **Can Initiate Network Fallback** if you want a Member to have that authority.

Generally, Fallback Authority should be limited to Network Administrators and their assistants.

5. Click **Submit**.

- *If the new users are already WSC Guard Members and your Network has enough empty “slots” to accept them, that’s all you have to do.* The list of users is simply updated. A typical situation when this might occur is when you remove one employee from a Network and add another. The Network has an empty “slot” from the removed employee which the new employee gets. Furthermore, because both employees were already WSC Guard Members, with valid passwords and user names, you don’t have to do anything else. The cost of the subscription also does not change because you’ve already paid for the “slot” and the Network size remains the same.
- *If the new users are already WSC Guard Members but your Network does not enough empty “slots” to accept them, the Network size will be updated automatically.* A billing confirmation page will tell you how much the increased Network size will cost and, if you accept, a receipt page appears. The receipt will be emailed to the address shown on the page. You will be billed a pro-rated amount for the increased Network size. A typical situation for adding existing Members is in a two-network office, when you want some people to have access to both networks. Adding more people to the smaller network will increase its size, but you don’t have to re-enter each person’s username and password because they are already WSC Guard Members.
- *If the new users are not WSC Guard Members, you need to register them with WSC, as well as give them Network access.* This is one of the most common situations, especially if you start with a Network just for yourself and a few others, and then add more people later. The Network size is increased automatically as you add the new Members. After you provide the necessary information to register each new WSC Guard Member, a billing

confirmation message shows how much the increased Network size will cost. When you accept, the receipt page appears. The steps below show this process.

For users who are not already WSC Guard Members, the page appears to register them now with the WSC Authentication Center. Providing the users email addresses, assigning the new user names and passwords registers them as WSC Guard Members.

The screenshot shows a web browser window with a dark blue header containing navigation links: 'My Home', 'My Account', 'Networks', and 'Downloads'. A 'Help' icon is on the right. Below the header, the page content includes a greeting 'Hello Your_Name', the title 'Add Network Users', and status information 'Current Network Members: 1' and 'Maximum Network Size: 1'. The 'Network Name' is set to 'Your_Network'. A blue banner indicates 'Step 1 - Collect New Member Information'. The instructions state: 'To create and add the new members to 'Your_Network' network: Fill in the member's information. Click 'Continue' to create the new members.' There are three input fields: 'Email Address' (containing 'User2_Name@your_corp.com'), 'User Name' (containing 'User2_Name'), and 'Password (6 Characters Minimum)' (containing 'welcome'). Below the fields are 'Back', 'Continue', and 'Cancel' buttons.

6. Enter a user name and password for each new user.

Once assigned, the user names cannot be changed. Later on, new Members should add their full names and change their passwords using the Member Profile page. See “Modify Your Member Profile” on page 72.

7. Click **Continue**.

The confirmation page shows who will be added and, if adding the Members increases the Network size, the effect on billing.

My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

Add Network Users Current Network Members: 1 Maximum Network Size: 1

Network Name: Your_Network

Step 2 of 3 - Confirm New Network Subscription Size

You have not been billed yet for your WSC Guard network subscription.

You are currently in your free trial. On your initial billing date, 02/09/17, you will be billed for 2 Members at \$ 40.00 per Member, for a total of \$ 80.00.

Billing Information [Edit]
No credit card specified.

Billing Contact
No Billing Contact Information

New User Information

Email	Username	Password
User2_Name@your_corp.com	User2_Name	welcome

Back Submit Cancel Print

Note the Edit link for the Billing Information on the right hand side of the page. Click that link if you want to update or change your credit card information before accepting the new charges.

8. Click **Submit**.

The next page is your receipt. It shows who will be added and the effect on the size of your Network and subsequent billing. You will receive an email version of the receipt.

My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

Modify Renewal Information

Network Name: Your_Network

Billing Receipt

Congratulations! You have successfully modified the network renewal information for network **Your_Network**. A copy of this invoice will be emailed to 'user1@your_corp.com'.

On 03/01/2005 you purchased:

Item Description	Price
Changed the Network Subscription size of Network "Your_Network" to 2. A charge will be made to your credit card on 03/01/05.	\$ 80.00

Billing Payment Information:
No credit card specified.

Billing Contact Information:
No Billing Contact Information

Continue

9. Click **Continue**.

Your Network is now updated to include the new Members.

The Network size is updated when you add new Members

My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

Add Network Users Maximum Network Size: 2 [[Edit](#)]

Network Name: Your_Network [Members: 2](#) [Guest: 0](#)

Members (+)							
Full Name	User Name	Access Beginning	Duration	Status			Last Accessed
	Your_Name	02/24/05 11:07 PST	10 Year	Active	Modify	Remove	02/24/05 12:14 PST
	User2_Name	02/24/05 13:23 PST	10 Year	Active	Modify	Remove	Never

Guests (+)							
Full Name	User Name	Access Beginning	Duration	Status			Last Accessed
<i>There are no Guests associated with this network.</i>							

In the example above, the user has not yet accessed the Network as indicated by the “Never” in the column labelled Last Accessed.

That new user has access privileges on your WSC secure wireless Network until the duration time you set runs out. After that, the Member will not be able to log into your Network unless you reset their access duration.

Note: WSC Guard Members can be part of any WSC Guard-Protected Network without having to sign up again. For example, if you have a WSC Guard Network at work and another one at home, you can be a Member of both networks without having to sign up a second time. To be part of a Network, the Network Administrator simply adds a person to a Network. The Member does not have to sign up for WSC again.

NOTES ABOUT ADDING MEMBERS TO A NETWORK

Existing WSC Guard Members (who are part of another WSC Network) are added to your Network for free, if your subscription size already has enough room for them. If your Network size does not have enough room, the subscription size is automatically increased. The billing confirmation page shows the effect of adding the new user.

Billing for increased Network size is prorated to your billing renewal date.

When you renew a subscription, it automatically renews at the current number of Members on the Network, plus any empty “slots” if you have them.

In the event of a billing error, such as an expired or cancelled subscription or the need for new credit card information, additional web site pages walk you through the process to resolve the error.

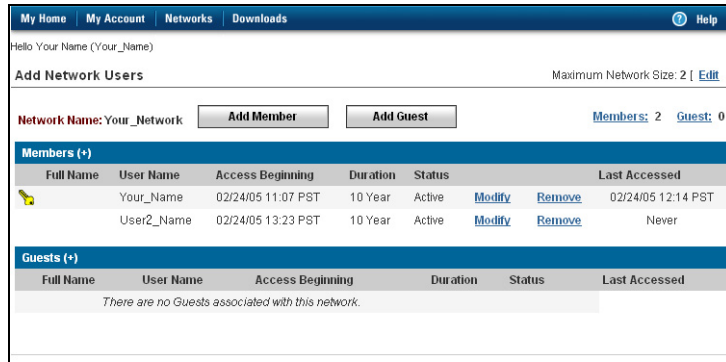
If you inadvertently let the subscription expire or a problem occurs with the billing, you can see the Members of the Network, but cannot modify the Network Users list, or make any other changes until the subscription is renewed. Note that the list of Members is not lost during this process so you do not have to re-enter all their information again after renewal.

REMOVING A MEMBER FROM A WSC NETWORK

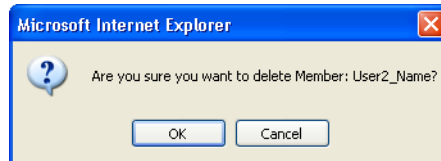
A typical instance for removing a Member from your secure WSC Guard Network is when an employee leaves your business and you no longer want that person to have access to the Network.

To remove a Member from the Network:

1. On the **Networks I Own** page, click the **Modify User List** link.
2. Click the **Remove** button of the Member to remove.



3. A message asks if you're sure you want to remove that Member from the Network. Click **OK**.



The Member's Network access privileges are immediately removed from the WSC Authentication Database, and any subsequent attempts by the user to log into the Network will fail.

Note that billing does not change when you remove a Member from the Network because the Network "slot" that person occupied is already paid for through the end of the current subscription.

Note: Typically, the Member's access is invalidated in less than an hour. But, if a user is logged into the Network at the same time you remove them, the time it takes depends on whether or not the access point automatically re-authenticates users—and, if so, how often the re-authentication occurs. For access points that re-authenticate periodically, the user is logged off when the re-authentication fails. In that case, the WSC Guard Notification Icon will turn green with an “x” through it, and Windows will display a warning that local Network access has become unavailable, and from that point on the user is no longer allowed access. However, some access points do not automatically re-authenticate at all. Users already logged into this type of access point will not be affected by termination of their access privileges until they log off the Network and then try to log back on.

If you inadvertently remove the wrong Member from a wireless Network, simply click the **Add Member** button and reinstate that person's access privileges. As noted above, that person's Network access may or may not be temporarily interrupted, but as soon as you reinstate access privileges, the Network will immediately be able to authenticate that Member again.

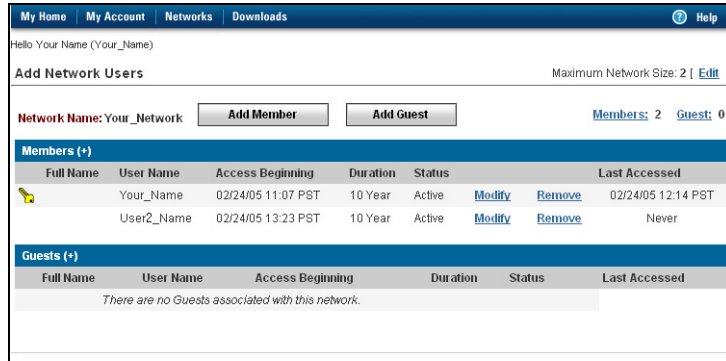
MODIFYING MEMBER ACCESS DURATION AND FALLBACK AUTHORITY

Once you have added a Member to your Network, you can modify the access duration setting for that Member at any time. If the Member's access duration time shows an “expired” status (that is, their allocated access time runs out), the Member will no longer be able to log into your Network. However, the Member remains in the WSC Authentication Database, and you, as Network Administrator, can reinstate the Member's access rights by simply resetting their access duration.

You can also modify a Member's authority to initiate or cancel Fallback in the event the Network loses its internet connection. It will “fall back” to WEP or WPA-PSK security until the internet connection is restored.

To modify a Member's access duration or Fallback authority:

1. On the **Networks I Own** page, click the **Modify User List** link.
2. Click the **Modify** link for the Member. The Modify Member page appears.




My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

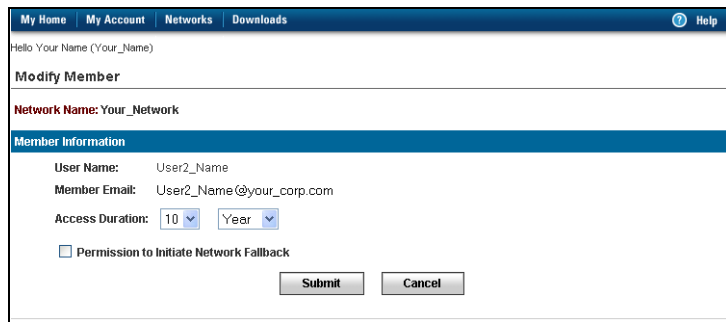
Add Network Users Maximum Network Size: 2 | [Edit](#) |

Network Name: Your_Network [Members: 2](#) [Guest: 0](#)

Members (+)						
Full Name	User Name	Access Beginning	Duration	Status		Last Accessed
	Your_Name	02/24/05 11:07 PST	10 Year	Active	Modify	02/24/05 12:14 PST
	User2_Name	02/24/05 13:23 PST	10 Year	Active	Modify	Never

Guests (+)						
Full Name	User Name	Access Beginning	Duration	Status		Last Accessed
<i>There are no Guests associated with this network.</i>						

3. Use the drop-down menus for setting the Access Duration.
4. To give the Member Fallback authority, click the checkbox.



My Home My Account Networks Downloads Help

Hello Your Name (Your_Name)

Modify Member

Network Name: Your_Network

Member Information	
User Name:	User2_Name
Member Email:	User2_Name@your_corp.com
Access Duration:	10 Year
<input type="checkbox"/>	Permission to Initiate Network Fallback

5. Click **Submit**. The new access duration and Fallback authority setting for the Member are now in force.

ADDING A TEMPORARY GUEST TO A WSC NETWORK

Network Guests are people who will have temporary access (up to 48 hours) to your Network. Guests might include people visiting your office to make a presentation or employees from another office visiting

for a meeting. With the WSC management options, you can not only provide the person with temporary access, you can also specifically limit the duration of the access.

To add a temporary Guest:

1. On the **Networks I Own** page, click the **Modify User List** link.
2. Click the **Add Guest** button.

The Add Guest page appears.

The Add Guest page has fields for the Guest's information and drop-down menus for setting the access level and duration.

- **Guest User Name**—assign the Guest a temporary User Name. The Guest’s user name cannot be the same as another Guest or Member.
 - **Guest First Name/Last Name**—enter the first and last name of the Guest. These names do not have to be unique.
 - **Password/Password Verify**—assign a Guest a password of at least six characters, and then type that password in both the Password and Password Verify boxes.
 - **Access Duration**—this is where you set up the duration of the Guest’s access. Guest access is available for a maximum of 48 hours. Click the drop down arrows for the number to choose the number of hours of access. When the Guest’s access duration expires, the Guest will no longer be able to login to your Network.
3. Enter the email address in the section for the Guest Access Notification.

Adding the email address in this section provides the Guest with an email that includes the link to the WSC web site, and instructions for getting set up to use your WSC Guard network. Thus, upon arriving at your site, the Guest’s computer will be ready for WSC Guard login, and all you have to do is provide the User Name and password.

4. Click **Submit**. The new access rights for the Guest are now in force.
5. Help the Guest connect to your wireless Network.

See the section “Provide a Guest Access to the Network” on page 105.

6. Give the Guest the User ID and password you created.

The Guest can now log into the Network on a temporary basis until the access period expires.

MODIFYING A GUEST’S ACCESS DURATION TO A WSC NETWORK

The Network User List displays a list of all the Guests you have added to your Network, as well as the Members. You can modify or reinstate the access duration for any Guest on the list.

To modify a Guest's access:

1. On the **Networks I Own** page, click the **Modify User List** link.
2. Click the **Modify** link for the Guest.

The screenshot shows the 'Add Network Users' page for a network named 'Your_Network'. It displays a table of members and a table of guests. The 'Members' table has columns for Full Name, User Name, Access Beginning, Duration, Status, and Last Accessed. The 'Guests' table has the same columns. The 'Add Member' and 'Add Guest' buttons are visible at the top.

Full Name	User Name	Access Beginning	Duration	Status	Last Accessed
User2_Name	User2_Name	03/02/05 16:54 PST	6 Month	Active	Never
Your Name	Your_Name	02/09/05 16:52 PST	10 Year	Active	Never

Full Name	User Name	Access Beginning	Duration	Status	Last Accessed
Guest Employee	Guest1	03/14/05 15:30 PST	8 Hour	Active	Never

The Modify Guest page for access duration and other information appears. Note that the Guest User Name cannot be changed.

The screenshot shows the 'Modify Guest' page for a guest named 'Guest1'. It displays a form with fields for Guest User Name, User First Name, User Last Name, Password, Password Verify, Access Duration, and Guest's e-mail (optional). The 'Access Duration' is currently set to 8 hours.

Guest Information

Guest User Name: Guest1
 User First Name: Guest
 User Last Name: Employee
 Password: [masked]
 Password Verify: [masked]
 Access Duration: 8 [v] Hour [v]

Guest Access Notification [Optional]
 Optionally, you can enter guest's user e-mail address to notify the guest about granted access. The e-mail address will not be stored.
 Guest's e-mail: [optional] [input field]

Submit Cancel

3. Make the modifications you want.

For example, if the Guest's access duration is about to expire, you can set a new duration. If you make other changes, the duration is automatically renewed.

4. Click **Submit**. The modifications are now in force.

REMOVING A GUEST FROM YOUR WSC SECURE NETWORK

Like Members, Guests whose access duration has run out remain in the WSC Authentication Database, with “expired” status. If you know that a particular Guest will not be returning or will no longer need access to your WSC secure Network, you can remove them permanently from the WSC Authentication Database.

To remove a Guest from your WSC Network:

1. On the **Networks I Own** page, click the **Modify User List** link.
2. Click the **Modify** link for the Guest.

The screenshot shows the 'Add Network Users' page in the WSC web interface. The page has a navigation bar with 'My Home', 'My Account', 'Networks', and 'Downloads'. Below the navigation bar, there is a greeting 'Hello Your Name (Your_Name)' and a 'Maximum Network Size: 2 | Edit' link. The 'Add Network Users' section includes a 'Network Name: Your_Network' and two buttons: 'Add Member' and 'Add Guest'. Below this, there are two tables: 'Members (+)' and 'Guests (+)'. The 'Members (+)' table has columns for Full Name, User Name, Access Beginning, Duration, Status, and Last Accessed. It lists two members: 'User2_Name' and 'Your Name'. The 'Guests (+)' table has the same columns and lists one guest: 'Guest Employee' with a duration of 8 hours and an active status. The 'Modify' link for the guest is highlighted.

Members (+)						
Full Name	User Name	Access Beginning	Duration	Status		Last Accessed
	User2_Name	03/02/05 16:54 PST	6 Month	Active	Modify	Remove
	Your Name	02/09/05 16:52 PST	10 Year	Active	Modify	Remove

Guests (+)						
Full Name	User Name	Access Beginning	Duration	Status		Last Accessed
	Guest Employee	03/14/05 15:30 PST	8 Hour	Active	Modify	Remove

3. Click the **Remove** link of the Guest you want to remove.

The Guest’s Network access privileges are immediately removed from the WSC Authentication database, and any subsequent attempts by the Guest to log into the Network will fail. See the note on page 99.

The time it takes for authentication removal to affect a user who is already logged into the Network depends on whether or not the access point automatically re-authenticates users—and if so, how often the re-authentication occurs. If re-authentication fails while a user is logged into the Network, the WSC Guard Notification Icon will turn green with an “x” through it, and Windows will display a warning that local Network access has become unavailable. Some access points do not

automatically re-authenticate at all. Users already logged into this type of access point will not be affected by termination of their access privileges until they log off the Network and then try to log back on.

If you inadvertently remove the wrong Guest from a wireless Network, simply click the **Add Guest** button and re-enter that person's access information. As noted above, that person's Network access may or may not be temporarily interrupted, but as soon as you reinstate Guest access, the Network will immediately be able to authenticate that Guest once again.

PROVIDE A GUEST ACCESS TO THE NETWORK

Once a Guest has a User Name and Password for the Network, the Guest will need to get access to the Network. The three options are:

- Download and install the WSC Guard software (Windows XP/2000/98/Me).
- Automatically configure the Guest's computer from the WSC web site (Windows XP only).
- Manually configure the Guest's computer to connect to the Network (Windows XP only).

Note: If you had WSC Guard send an Access Notification email when you registered the Guest, the Guest's computer should already be set up for use on the WSC Guard Network. See "Adding a Temporary Guest to a WSC Network" on page 100 for details.

To download and install the WSC Guard software:

1. Go to the WSC Guard web site at:
www.wirelessecuritycorp.com.
2. Click the Downloads link.
3. Click the link: Windows XP/2000/ME/98 WSC Guard Installer.
4. Save the WSC Guard 4.0 WSC Setup.exe file to the hard drive.

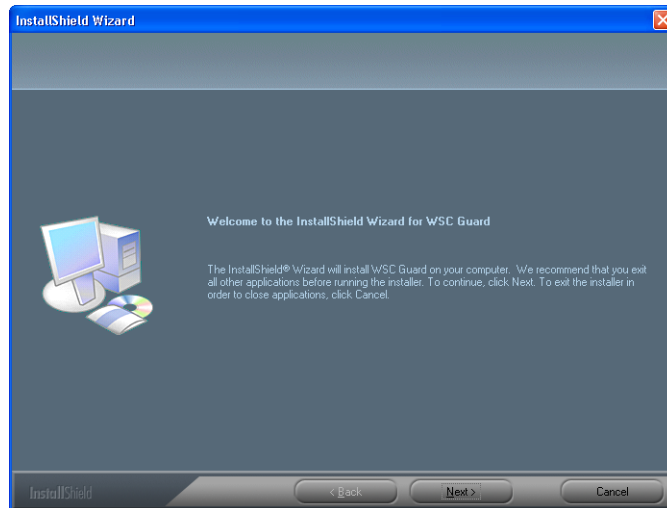
5. Double-click the WSC Guard 4.0 Setup icon to launch the installer.



WSC Guard
4.0 WSC
Setup

The first installation window appears.

6. Click **Next** and Follow the instructions on the windows.



7. When installation is complete, have the guest reboot the computer. A Wizard window appears. Follow the instructions for the Guest's computer to connect to the WSC Guard-Protected network.

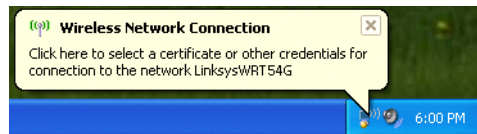
To automatically configure a Guest's XP computer:

1. Go to the WSC Guard web site at: **www.wirelessecuritycorp.com**.
2. Click the Downloads link.
3. Click the link: **Windows XP Guest Client Configuration Wizard**.

4. Save the software to the hard drive.
5. Double-click the icon for the WSCGuestClient.exe that you just saved and run the software.

The software automatically configures the Guest's computer for use with the WSC Guard Network.

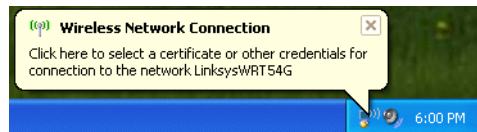
6. When the following message bubble appears on the screen, *make sure the Guest clicks it before it closes*.



7. A login dialog box appears. The guest logs in using the appropriate User Name and Password.

To manually configure a Guest's XP computer:

1. Go to the WSC Guard web site at:
www.wirelessecuritycorp.com.
2. Click the Downloads link.
3. In the Support section, click the link **Guest Access**.
4. Click the link for instructions to **manually configure Wireless Zero config for guest access**.
5. Follow the instructions.
6. When the following message bubble appears on the screen, *make sure the Guest clicks it before it closes*.



The software automatically configures the Guest's computer for use with the WSC Guard Network.

7. A login dialog box appears. The guest logs in using the appropriate User Name and Password.

VIEWING NETWORK ACTIVITY REPORTS

Your WSC Guard secure Network collects activity information continuously. With that information you can see, at a glance, how many successful and failed log in attempts occurred over some time period.

When you first log into the WSC web site as the Network Administrator, a table on your “My Home” page updates Network activity dynamically and shows you the number of successful logins and number of failed attempts. The following sample shows an example of the table that lists 25 successful attempts and 5 failed attempts.

Wireless Security Corporation
Member Center

Member Log Out

My Home | My Account | Networks | Downloads | Help

Hello Your Name (Your_Name)

My Home

Network Activity Summary

Since your last login on **02/25/05 14:33:17 PST**, your networks have experienced the following activity:

Network Name	Successful Attempts	Failed Attempts
Your_Network	25	5

For additional information go to [Network Admin](#) and select Reports.

We want to hear from you!

EARN \$25

What is your experience with WSC Guard? We want to hear from you.

Earn \$25 by taking a 15 minute phone survey to tell us about your experience.

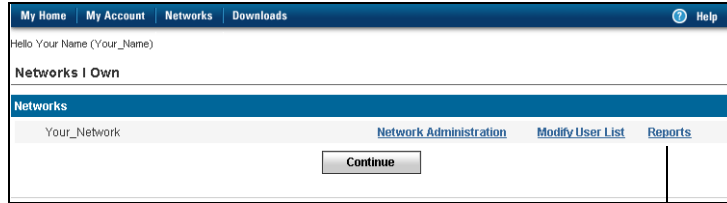
Call **(650) 482-5588** or [send us an email](#) to schedule a time to talk.

[Terms of Use](#) | [Privacy Policy](#) | [Contact Us](#) | [Site Map](#)

You can also generate reports about the Network to monitor it. The reports are available as part of the Network Administration functions.

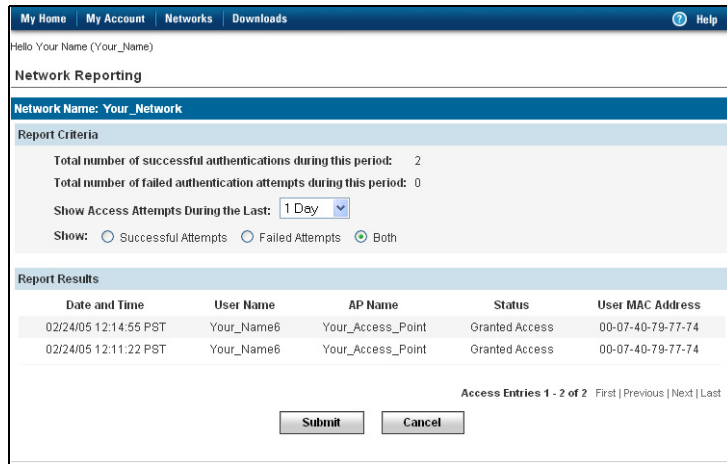
To see Network Reports:

1. On the **Networks I Own** page, click the **Reports** link for the appropriate Network



Reports link

The Network Reporting page appears for that Network.



2. To see the number of attempts over a certain time period, click the drop-down menu for the time period and select the one you want. You can choose to view only the successful attempts, only the failed attempts, or both, by clicking the appropriate choices.
3. Click **Submit** to get the data for your choices.

4. Click the navigation arrows at the bottom right of the table to page through the data.

Note: In the report, you can see the User IDs and MAC addresses of all access attempts— both successful and failed. If you see a stream of denied attempts using the same User ID/MAC address, it is likely that someone using that User ID is trying various passwords to break into the Network. The MAC Address identifies the NIC in the computer being used to log in to the Network.

The date/time stamp of the attempts can also be used to analyze when attacks occur. You may find, for example, that most attacks occur late at night when no one is around to receive warning email.

SECURITY COUNTERMEASURES FOR UNAUTHORIZED LOG IN ATTEMPTS

You can use the information in the Network Reports to analyze unauthorized attempts to log into your Network. The following steps explain how to detect unauthorized attempts and the action to take to assure that your Network remains secure.

If your Network appears to be under attack:

1. When you receive an email alert of intrusions, log into the WSC web site, click the **Networks** button, choose **Networks I Own**, and click the **Reports** link for the appropriate Network.

See “Setting Intrusion Detection Alarms” on page 85 to set up the email alert settings.
2. If the log shows repeated failures for a valid account on the Network, make a note of the MAC address and User ID associated with the failed log in attempts.
3. Compare the MAC address to prior successful authentications for that User ID.

4. If the MAC address is the same as for the earlier successful authentications, but now the log in attempts for that User ID/MAC address keep failing, the person assigned that User ID probably forgot his or her password and is repeatedly trying to guess it incorrectly.
5. If the MAC address for the failed attempts is different than earlier successful attempts, contact the person with that User ID to see if the wireless card (and therefore the MAC address) in the computer has been changed. If a new wireless card has been installed, then the person has probably forgotten his or her password.

In either of the above two cases, tell the person to use the “Forgot Your Password?” assistance on the WSC Guard Log in screen, or alternatively, to contact WSC Support to have the password reset.

6. However, if the person with the User ID did not recently change the wireless card and the reports show subsequent successful authentications for that User ID from the MAC address in question, an illegal break-in attempt may have occurred.

In that case, remove the user from the Network User List immediately, because the User Name has possibly been compromised.

7. If the Access Point for the Network has advanced filtering capabilities, you may be able to block the offending MAC address, rather than disabling the account. See the documentation you received with that Access Point for details. As an added precaution, tell the person whose account has been compromised to change to a stronger password.

CHAPTER 4

Troubleshooting

If you try the troubleshooting procedures described in this section and still have problems, please visit the WSC Guard web site and click the link for Support. You can receive answers to your questions about technical issues as well as billing and subscription issues.

WPA NOT SUPPORTED

When I use a non-WPA wireless adapter, a message says:

Your wireless adapter does not support WPA <your network adapter name and its driver version>.

What do I do?

Solutions: This usually occurs when you insert a non-WPA wireless adapter in your computer or reboot your computer with a non-WPA wireless adapter installed. Several solutions may remedy this problem. Try the following:

- Go the WSC web site at **www-wirelesssecuritycorp.com**, or just select **Administration Website** from the WSC Guard Pop-up menu.
1. Click the Support button, then click the System Requirements link.



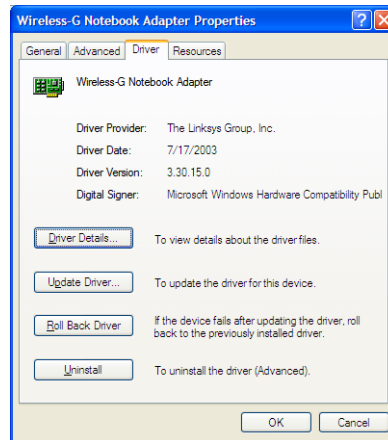
2. Follow the instructions to have WSC Guard test your network adapter for the latest driver and compatibility with WSC Guard.
3. If the system check reveals that your network adapter needs an updated driver, follow the next steps.

■ Update your network adapter's driver.

The driver version for your adapter is very important. If you need to update your wireless network adapter's driver, follow the steps below.

1. From the Windows **Start** menu, choose **Settings** and then **Control Panel**.
2. Double-click the **System** icon to see the System Properties dialog box.
3. Click the **Hardware** tab, and then click the **Device Manager** button.
4. In the list of hardware devices, click on **Network Adapters** and double-click on the adapter in your computer.
5. On the dialog box, click the **Driver** tab.

The following shows an example of the dialog box listing the driver version.



To update the adapter driver:

1. Go to the web site of the adapter's manufacturer.
2. Follow the instructions on the web site and download the newer driver.

Note: Drivers are often available on a web site in sections named Support or Downloads.

3. Then, follow the same steps as above to check the driver version of your adapter.
4. On the dialog box, click the **Update Driver** button.
5. A Windows wizard window appears and walks you through the process to update the adapter's driver.

LOGIN FAILED

When I try to login to the network, I get a message that the login failed. What do I do?

Solutions: Several possible problems can cause a "Login Failed" message. Try the following causes and solutions to remedy the problem.

- **Your access point does not have internet connectivity.** If internet connectivity is lost, you cannot login to the WSC Authentication Center. In that case, your network needs to go into Fallback Mode so you can continue working, but at a lower level of security. Once internet connectivity returns, you will be able to log in at full security.
- **A network firewall is configured to block the RADIUS port used by the authentication process.** Some firewalls block the RADIUS port on your computer that the WSC Authentication Center uses. Please see your Network Administrator to change the settings of the firewall application to allow connection with the WSC Authentication Center. The documentation that you received with the firewall application should also explain how to change the settings.
- **If you are using an access point, the access point may not be able to communicate with the Authentication Center because:**

It is not physically connected to your network router. Check the cables between the access point and the network router to make sure they are securely connected. Also check the status lights on the router to make sure the connection port for the access point's cable is working.

It is configured with an incorrect gateway address. Your access point must have the proper gateway address. Please see your access point's setup utility for setting the gateway address.

It is in an "inconsistent" state, thus requiring a restart or repair. WSC Guard has an access point Repair Settings button just for this purpose. See "Check Access Point Properties" on page 36 for the steps to "repair" an access point's settings so it can be used on the network. You can also reboot your access point.

NETWORK CARD CANNOT CONNECT TO NETWORK

When I try to connect to a WEP or WPA-PSK network, I get the following message:

Your network card has indicated it had a problem connecting to the wireless network. Please verify that you correctly entered your key and try again.

What do I do?

Solutions: The key that you typed to connect to the network is incorrect. Try one of the following:

- Re-set the key on the access point and your computer.
- Update the network card's driver to a more recent version. See the steps beginning on page 115.
- Eject and reinsert your computer's wireless network adapter, or disable then re-enable the adapter.
- Reboot your computer.

LOGIN FAILED—WRONG NETWORK KEY

When I try to login to the network, I get the following message:

The key you entered doesn't appear to match the key programmed on your wireless network. Please verify that you correctly entered your key and try again.

What do I do?

Solution: The key that you typed to connect to the network is incorrect. Retype the key correctly.

LOGIN FAILED—WRONG DATA ENCRYPTION MODE

When I try to login to the network, I get the following message:

You have manually set the Data Encryption mode to <an encryption mode such as AES>, but your wireless network is configured to <an encryption mode such as TKIP>. Please use the same Data Encryption settings and try again.

What do I do?

Solution: Remove the network from the list of preferred networks. See “Listing Preferred Networks” on page 63.

LOGIN FAILED—WRONG WEP KEY

When I try to login to the network, I get the following message:

You may have entered the wrong WEP key, or your wireless adapter is not compatible with the network you are trying to connect to.

What do I do?

Solution: Your network adapter does not have WPA capability and mistakenly shows an access point set to WPA as being set to WEP security. The key you typed is being interpreted as a WEP key instead of the needed WPA key. You need to either upgrade your adapter to have WPA security, or set the access point to have WEP security.

LOGIN FAILED—INCOMPATIBLE NETWORK ADAPTER

When I try to login to the network, I get the following message:

Your wireless adapter may not be compatible with the network you are trying to connect to.

What do I do?

Solution: You need to upgrade your access point's driver to a more recent version. See the steps beginning on page 115.

CANNOT CONNECT TO NETWORK

I cannot connect to the network. A message says that “Invalid key detected.” What do I do?

Solutions: Your network adapter driver did not accept the WEP key or PSK key that is sent to the driver during a connection attempt. Try these possible solutions:

- If you're using a removable network card, eject it and re-insert it into your computer.
- Your adapter driver may need to be updated with a newer version. Please visit the web site of the manufacturer of your adapter to see if updates are available.
- The WEP key or PSK key on your access point and the WSC client may not match. Re-set the key on them both. See your access point's setup utility for the steps to reset its keys.

LOGIN FAILS WHEN YOU'RE OFFSITE

When I try to login to a network at a different site, I get a message that the login failed. What do I do?

Solution: Usually the reason the login fails is because the network at the site also has 802.1x security, but it is not secured with WSC Guard. Your computer sees the 802.1x security and tries to logon using WSC Guard, which is not available so the login fails.

To solve the problem, choose Exit from the WSC Guard Pop-up menu to stop the WSC Guard security. You should then be able to log onto the other network. Later, when you return to your network, re-start WSC Guard from the Windows Start menu.

XP WIRELESS NETWORK SUPPORT NOT WORKING

My Windows XP wireless network support is no longer working. What's wrong?

Solutions: You either activated the WSC Guard Network Selector, or your network adapter disabled Windows XP support. Try the following solutions:

- If you activated the WSC Guard Network Selector application, it took the place of the Windows XP wireless network support. You need to deactivate the WSC Guard Network Selector.

Choose **Options** from the WSC Guard Pop-up menu and uncheck the box labeled: **Use WSC Guard to configure my wireless network settings. Select this option to use WSC Guard exclusively for connecting to wireless networks. Click OK.**

Your Windows XP wireless network support will now be active. Right-click on a wireless network icon in the Windows notification area at the lower right of your computer screen and choose **View Available Wireless Networks**.

- You may have installed a network adapter that disabled Windows XP network support. See the documentation that you received with the adapter.

ACCESS POINT WIZARD FAILED

When I was setting up my access point, I got a message that says the Access Point Wizard failed. What do I do?

Solutions: If an error dialog appeared during the final step of the Access Point Setup wizard, instead of the final wizard window, it is possible that Windows became “disoriented” due to having multiple open network connections (wired and wireless) simultaneously. In this case,

in order to proceed, you will first need to manually disable your connection to the new access point, so that only the wired Ethernet connection to your broadband hub remains active. You can then proceed all the way through the Access Point Setup wizard. Finally, you will need to disconnect the Ethernet patch cable (wired connection), re-enable the wireless connection, and then you can proceed with the final network configuration, connect to the wireless network, and log in. Following are the steps for this manual connection detour.

To manually disable and re-enable the wireless connection during network configuration:

1. From the Windows XP **Start** menu, choose **Control Panel**.

In Windows 2000, choose **Start->Settings->Control Panel**.

2. In the Windows XP Control Panel, double-click on the **Network Connections** icon to view the Network Connections Control Panel.

In Windows 2000, double-click on the **Network and Dial-up Connections** Control Panel.

3. In the Control Panel, locate the icon for your wireless network adapter, right-click on its icon, and choose **Disable**.

A dialog appears, confirming that the connection has been disabled. You can now close all Control Panel windows.

4. Once again, follow the steps to add an access point.

At this point, the final Add Access Point wizard window should be displayed on your screen, showing the names you gave to both the access point and to the new wireless network.

5. From the Windows XP Start menu, choose **Control Panel**.

In Windows 2000, choose **Start->Settings->Control Panel**.

6. In the Windows XP Control Panel, double-click on the **Network Connections** icon to view the Network Connections Control Panel.

In Windows 2000, double-click on the **Network and Dial-up Connections** Control Panel.

7. In the Control Panel, locate the icon for your wireless network adapter, right-click on its icon, and choose **Enable**. Then close the Control Panel windows.
8. Unplug the Ethernet patch cable between your computer and the Ethernet hub that connects your wireless access point to your broadband modem or router.
9. Now, if you're installing WSC Guard for the first time, continue with the steps to automatically select and configure your wireless network.

INDEX**Numerics**

- 802.11 5
- 802.11a/b/g 5
- 802.1x 4, 6

A

- Access Beginning 91
- access duration 99
 - guest 102
- access point 4
 - add new 29
 - administrator name 37
 - built-in security 39
 - configuration 84
 - default password 31
 - delete 46
 - IP address 37
 - multiple 31
 - name 32
 - password 31, 32, 37, 84
 - wizard failure 120
- access point password 37, 84
- account profile 72
- account renewal 78
- adapter
 - driver version 115
- add access point 29
- Add Access Point wizard 30
- add guest 100
- Add Member 33, 92, 98, 100, 101, 103, 104
- Add Network Users page 92
- add new user 91
- add wireless network 59
- Administration Website 68
- alarm detection report
 - email address 89
- alarms 85
- attack on network 110
- automated fallback 41
- automated fallback agent 39
- automatic time out 69

available wireless networks 18

B

- billing history 79
- billing information
 - transfer 88
- billing interval 76
- billing profile 74

C

- cancel subscription 79
- change password 73
- Channel 54
- check access point properties 36
- check system requirements 33
- Clear security 13
- connect network 57
- create network 26

D

- date/time stamp 110
- delete access point 46
- delete network 47
- disable WSC Guard 48
- disconnect network 57
- driver version 115
- Duration 91

E

- enable auto login 12, 13
- Enable WSC Security Agent 41
- encryption mode 35

F

- failed login attempts 108
- fallback 5
 - enabling automatic security 40
 - enabling/disabling 39
- fallback agent 40, 41
- fallback key 35
- fallback mode 5, 91
 - enabling/disabling network security 39
 - manually enabling/disabling 42
- Forgot password 73

G

guest 100
 guest access duration 102
 Guest User ID 102

I

illegal break-in 111
 illegal log in 110
 internet failure 33
 intrusion detection 5, 70, 85, 108
 alarms 86
 countermeasures 110

K

key icon 10, 12

L

Last Access 91
 login 69
 automatic 13
 login password 69, 72
 login under new name 15

M

MAC Address 54, 110
 manual fallback 43, 45
 manual fallback mode 39, 43
 member 4
 register 94
 remove 97
 member profile 72
 membership 24
 modem 4
 Modify Access Control 82
 modify guest access 102
 Modify Member page 100
 Modify Network Setup 82
 modify profile 72, 73, 78
 Modify User Link 90
 Modify User List 90
 modify wireless network 60
 my account 71
 My Home page 70

N

network
 administration 83
 can use 80
 connect 57
 connect non-WSC 58
 connection options 62
 create 26
 delete 47
 disconnect 57
 empty slots 93
 preferred 63
 remove guest 104
 renewal 75
 network activity 82, 108
 network activity summary 70
 network activity summary table 70
 Network Administration 86, 87
 network administration 67
 network administrator 4, 71
 access point password 84
 transfer 88
 network administratorname 87
 network guest 100
 Network Member 4
 network properties 34
 network re-authentication 99
 Network Reporting page 109
 Network Reports 109
 network security 39
 Network Selector 17, 21, 52
 activate 19
 Network User List 102
 Networks
 own 81
 networks to use 71
 new name 15
 new user
 add 91
 normal operating mode 10
 notification area 10
 notification icon 10, 12

O

Options 18, 19
options dialog box 19

P

password 25, 69, 72
 access point 84
 change 73
 forgotten 25
 randomly-generated 32
preferred networks 63
profile 72
 modify 72, 73, 78

R

re-authentication 99, 104
reconnect to network 15
register WSC member 23, 94
remove guest 104
remove member 97
rename access point 38
rename network 38
renewal information 75
repair settings 38
Reports 82, 108
Reports Link 109, 110
reposition columns 56
resize columns 56
restore full WSC security 45
router 4

S

save password 12
security countermeasures 110
security key 63
security question 25
setup fails 120
shared secret 35
Signal Strength 54
signal strength icon 20
sort networks list 55
SSID 35, 47, 59
Status 15, 91

status dialog box 15
status icon 10
subscription 27
 cancel 79
subscription size 76
system requirements 7

T

temporary access 101
transfer network 87

U

User Name 25, 73, 91
user name 73

V

View Available Wireless Networks 17, 52

W

WEP 13
Windows 2000 alternate setup 121
Windows XP alternate setup 121
wired network connection 121
Wireless Network Connections window 53
WPA 4, 6
WPA-PSK 6
WSC Authentication Center 5, 24, 39
WSC Authentication Database 46, 98, 104
WSC contact numbers 8
WSC Guard Notification Icon 10, 12
WSC Guard Pop-up menu 14
WSC personal page 70
WSC updates 50
WSC URL 49
WSC Web site 49
 log in URL 68
 member's section 67
 personal home page 70
 public section 67
 time out 69

Y

yellow key icon 91

