McAfee wirelesshomenetworksecurity

User Guide



COPYRIGHT

Copyright © 2006 McAfee, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE AND DESIGN, CLEAN-UP, DESIGN (STYLIZED D), DESIGN (STYLIZED D), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (AND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSION PREVENTION THROUGH INNOVATION, M AND DESIGN, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE, COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, QUICKCLEAN, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSSCAN, VIRUSSCAN, VAND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, OUR NETWORK, OUR NETWORK, OUR BUSINESS. are registered trademarks of their registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). * Cryptographic software written by Eric A. Young and software written by Eric J. Hudson. * Some software programs that are licensed (or sublicensed) to the user under the GNU ceneral Public Licenses (CPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute do someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software organ that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. * Software organ that are broader than the rights granted in this agreement, then such rights shall take originally written by Hongy 1997 Henry Spencer. * Software developed by the Apache org/license sequencement for this software can be found at www apache-org/licenses/LICENSE-2.0.txl.
 International Components for Unicode ("ICU") Copyright 0 1995-2002 International Business Machines Corporation and others. * Software developed by Thai Open Software Contre Software (Centre 14 and Clark Cooper, © 1998, 1999, 2000. * Software copyrighted by Each Software Copyrighted by Thai Open Source Software (Centre 14 and Clark Cooper, © 1998, 1999, 2000. * Software copyrighted by Soft

Quick Start Card

If you are installing your product from a CD or a Web site, print this convenient reference page.



McAfee reserves the right to change Upgrade & Support Plans and policies at any time without notice. McAfee and its product names are registered trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. © 2006 McAfee, Inc. All Rights Reserved.

For more information

To view the User Guides on the product CD, ensure that you have Acrobat Reader installed; if not, install it now from the McAfee product CD.

- 1 Insert your product CD into your CD-ROM drive.
- 2 Open Windows Explorer: Click **Start** on your Windows desktop, and click **Search**.
- **3** Locate the Manuals folder, and double-click the User Guide .PDF you want to open.

Registration benefits

McAfee recommends that you follow the easy steps within your product to transmit your registration directly to us. Registration ensures that you receive timely and knowledgeable technical assistance, plus the following benefits:

- FREE electronic support
- Virus definition (.DAT) file updates for one year after installation when you purchase VirusScan software

Go to http://www.mcafee.com/ for pricing of an additional year of virus signatures.

 60-day warranty that guarantees replacement of your software CD if it is defective or damaged SpamKiller filter updates for one year after installation when you purchase SpamKiller software

Go to http://www.mcafee.com/ for pricing of an additional year of filter updates.

 McAfee Internet Security Suite updates for one year after installation when you purchase MIS software

Go to http://www.mcafee.com/ for pricing of an additional year of content updates.

Technical Support

For technical support, please visit

http://www.mcafeehelp.com/.

Our support site offers 24-hour access to the easy-to-use Answer Wizard for solutions to the most common support questions.

Knowledgeable users can also try our advanced options, which include a Keyword Search and our Help Tree. If a solution cannot be found, you can also access our FREE Chat Now! and E-mail Express! options. Chat and e-mail help you to quickly reach our qualified support engineers through the Internet, at no cost. Otherwise, you can get phone support information at http://www.mcafeehelp.com/.

Contents

	Quick Start Card iii
1	Getting Started
	Using McAfee Wireless Home Network Security
	Understanding Wireless Home Network Security
	Wireless Home Network Security makes it simple
	Features
	System requirements
	Using McAfee SecurityCenter
2	Installing Wireless Home Network Security
	Installing from a CD
	Installing from the Web site
	Installing from the installation file 15
	Using the configuration wizard 16
3	Using the Summary Page 17
	Viewing your connection
	Viewing your protected wireless network
4	Managing Wireless Networks 19
	Connecting to a network
	Disconnecting from a network
	Using advanced options

5	Configuring Options	21
	Viewing events	21
	Configuring advanced settings	22
	Configuring security settings	22
	Configuring alert settings	23
	Configuring other settings	23
	Revoking access to the network	23
	Repairing security settings	24
	Protecting other computers	24
	Rotating keys	25
	Protecting wireless networks	25
	Unprotecting wireless networks	25
6	Updating Wireless Home Network Security	27
	Automatically checking for updates	27
	Manually checking for updates	27
7	Understanding Alerts	29
7	Understanding Alerts Access revoked	29 29
7	Understanding Alerts	29 29 29
7	Understanding Alerts ************************************	29 29 29 29
7	Understanding Alerts Access revoked Access revoked Computer connected Computer disconnected Computer disconnected Computer secured Computer secured	29 29 29 29 29
7	Understanding Alerts Access revoked Access revoked Computer connected Computer disconnected Computer secured Key rotation failed Computer connected	29 29 29 29 29 29
7	Understanding Alerts Access revoked Access revoked Computer connected Computer disconnected Computer disconnected Computer secured Key rotation failed Key rotation resumed Key rotation resumed	29 29 29 29 29 29 30
7	Understanding Alerts Access revoked Access revoked Computer connected Computer disconnected Computer disconnected Computer secured Key rotation failed Key rotation resumed Key rotation suspended	29 29 29 29 29 30 30
7	Understanding Alerts Access revoked Access revoked Computer connected Computer disconnected Computer secured Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Access revoked	29 29 29 29 29 29 30 30 30
7	Understanding Alerts Access revoked Computer connected Computer disconnected Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Network renamed	29 29 29 29 29 30 30 30 30
7	Understanding Alerts Access revoked Computer connected Computer disconnected Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Network renamed Network repaired	29 29 29 29 29 30 30 30 30 30
7	Understanding Alerts Access revoked Computer connected Computer disconnected Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Network renamed Network repaired Network settings changed	29 29 29 29 30 30 30 30 30 30
7	Understanding Alerts Access revoked Computer connected Computer disconnected Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Network renamed Network settings changed Password changed	29 29 29 29 30 30 30 30 30 30 30
7	Understanding Alerts Access revoked Computer connected Computer disconnected Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Network renamed Network settings changed Password changed Security key rotated	29 29 29 29 30 30 30 30 30 30 30 30 30
7	Understanding Alerts Access revoked Computer connected Computer disconnected Computer secured Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Network renamed Network repaired Network settings changed Password changed Security key rotation frequency changed Security key rotation frequency changed	29 29 29 29 30 30 30 30 30 30 30 30 31 31
7	Understanding Alerts Access revoked Computer connected Computer disconnected Computer secured Computer secured Key rotation failed Key rotation resumed Key rotation suspended Network configuration changed Network renamed Network repaired Network settings changed Password changed Security key rotated Security key rotation frequency changed Wireless router/AP protected Wireless router/AP protected	29 29 29 29 30 30 30 30 30 30 30 31 31 31

8	Troubleshooting	33
	Installation	33
	Which computers to install this software on	33
	Wireless adapter not detected	33
	Multiple wireless adapters	33
	Unable to download on wireless computers because the network is already secure .	34
	Protecting or configuring your network	35
	Unsupported router or access point	35
	Updating router or access point firmware	35
	Duplicate administrator error	35
	Network appears unsecured	35
	Unable to repair	36
	Connecting computers to your network	37
	Waiting for authorization	37
	Granting access to an unknown computer	37
	Connecting to a network or the Internet	38
	Bad connection to the Internet	38
	Connection briefly stops	38
	Devices (not your computer) losing connection	38
	Prompted to enter the WEP, WPA, or WPA2 key	38
	Unable to connect	38
	Updating your wireless adapter	39
	Weak signal level	40
	Windows cannot configure your wireless connection	40
	Windows showing no connection	40
	Other issues	41
	Network name is different when using other programs	41
	Problems configuring wireless routers or access points	41
	Replacing computers	42
	Software not working after upgrading operating systems	42
9	Glossary	43
	Index	53

Getting Started

Welcome to McAfee Wireless Home Network Security, which offers advanced protection for your wireless network, your personal data, and your computer.

This product is designed for computers with wireless connections. When you install this product on computers that connect to your network using a cable, you do not have full functionality from those wired computers.

McAfee Wireless Home Network Security enhances the privacy of your computing experience by encrypting your personal and private data as it is sent over your protected wireless network, and blocks hackers from accessing your information.

Using McAfee Wireless Home Network Security

Before you protect your network, note the following.

- Cable connections computers that are connected to the router with a cable do not need to be protected, because signals transmitted over a cable cannot be intercepted.
- Wireless connections computers that have wireless connections should be protected, because their data can be intercepted. A wireless computer must be used to protect a network because only a wireless computer can grant access to another wireless computer.

Protecting your network

You do not need to protect your network if you are connected with a cable.

- 1 On your wireless computer, install your wireless adapter and ensure that it is enabled. The wireless adapter can be a card that is inserted on the side of your computer or USB port. Many newer computers come with a built-in wireless adapter, so you do not have to install it.
- 2 Install your wireless router or access point (access points are used to extend the wireless range) and ensure it is turned on and enabled. For a more complete definition of a router and an access point, see *Glossary* on page 43.
- **3** Install McAfee Wireless Home Network Security on every wireless computer in your network. You do not need to install this software on computers that are connected with a cable. See *Installing Wireless Home Network Security* on page 15.

- 4 From one of the wireless computers, protect your network. See *Protecting wireless networks* on page 25.
- **5** Join the network from other wireless computers. See *Protecting other computers* on page 24.

Understanding Wireless Home Network Security

Like many people, you use a wireless network at home because it is convenient and easy. Wireless lets you access the Internet from any room in your house or even your backyard, without the costs and hassles of attaching cables. Wireless networking makes it easy to allow friends and family to access the network.

However, this convenience comes with security vulnerability. Wireless networks use radio waves to transmit data, and these radio waves travel beyond the walls of your house. With specialized antennas, wireless intruders can access your wireless network or intercept your data from miles away.

To protect your wireless network and data, you need to restrict access to your wireless network and encrypt your data. Your wireless router or access point comes with built-in security standards, but the difficulty is properly enabling and managing your security settings. Over sixty percent of wireless networks do not properly use a high level of security like encryption.

Wireless Home Network Security makes it simple

McAfee Wireless Home Network Security activates the security on your wireless network and protects what is sent over it with a simple, one click process that automatically generates a strong encryption key. Most keys that are easy for people to remember can be quickly cracked by hackers. By having the computer remember the key for you, Wireless Home Network Security can use keys that are almost impossible to crack.

Running seamlessly behind the scenes, this software also creates and distributes a new encryption key every few minutes, thwarting even the most determined hackers. Legitimate computers, like those of your friends and family who want access to your wireless network, receive the strong encryption key and all key distributions.

This process offers strong security, while still being simple for an owner of a wireless network at home to implement. With one click, you can block hackers from stealing your data as it is sent over the air. Hackers cannot insert Trojans or other malware into your network. They cannot use your wireless network as a platform to launch spam or virus attacks. Even casual freeloaders cannot use your wireless network, so you will not be erroneously blamed for illegal movie or song downloads.

Other solutions do not offer the simplicity or the strength of security offered by Wireless Home Network Security. Filtering MAC Addresses or Disabling Broadcast SSID only offers cosmetic protection. Even simple hackers can circumvent these mechanisms by downloading freely available tools from the Internet. Other utilities like VPNs do not protect the wireless network itself, so you are still vulnerable to a myriad of attacks.

McAfee Wireless Home Network Security is the first product that truly locks down your home wireless network.

Features

This version of Wireless Home Network Security offers the following features:

- Always on protection automatically detects and protects any vulnerable wireless network that you connect to.
- Intuitive interface protect your network without having to make difficult decisions or knowing complex technical terms.
- Strong automatic encryption only let your friends and family have access to your network and protect your data as it travels back and forth.
- Software only solution Wireless Home Network Security works with your standard wireless router or access point and security software. You do not need to buy additional hardware.
- Automatic key rotation even the most determined hackers cannot capture your information because the key is continuously rotating.
- Addition of network users you can easily grant your friends and family access to your network.
- Intuitive connection tool the wireless connection tool is intuitive and informative, with details about signal strength and security state.
- Event logging and alerts easy to understand reports and alerts offer advanced users more information on your wireless network.
- Suspend mode temporarily suspend key rotation so that particular applications can run without interruption.
- Compatibility with other equipment Wireless Home Network Security automatically updates itself with the latest wireless router or access point modules from the most popular brands including: Linksys[®], NETGEAR[®], D-Link[®], Belkin[®], and others.

System requirements

- Microsoft[®] Windows 98SE, Windows Me, Windows 2000, or Windows XP
- Personal computer with Pentium-compatible processor

Windows 98 or 2000: 133 MHz or higher

Windows Me: 150 MHz or higher

Windows XP (Home and Pro): 300 MHz or higher

RAM

Windows 98SE, Me, or 2000: 64 MB

Windows XP (Home and Pro): 128 MB

- 50 MB hard disk space
- Microsoft Internet Explorer 5.5 or later

NOTE

To upgrade to the latest version of Internet Explorer, visit the Microsoft Web site at http://www.microsoft.com/.

Wireless network

- Standard wireless network adapter
- Standard wireless router or access point, including most Linksys[®], NETGEAR[®], D-Link[®], and Belkin[®] models

Using McAfee SecurityCenter

The McAfee SecurityCenter is your one-stop security shop. You can run SecurityCenter from the McAfee icon in your Windows system tray or from your Windows desktop.

NOTE

For more information about its features, click **Help** in the SecurityCenter dialog box.

To open the McAfee SecurityCenter:

- 1 Right-click the McAfee icon M.
- 2 Click Open SecurityCenter.

To access a Wireless Home Network Security feature:

- 1 Right-click the McAfee icon M.
- 2 Point to Wireless Network Security, and then click the feature you want to use.

Installing Wireless Home Network Security

This section explains how to install Wireless Home Network Security and get started on protecting your network.

When installing Wireless Home Network Security, note the following.

- Install this software on all your wireless computers.
- You do not have to install this software on computers that are connected with a cable.

Installing from a CD

- 1 Insert your product CD into your CD-ROM drive. If the installation does not start automatically, click **Start** on your Windows desktop, then click **Run**.
- 2 In the Run dialog box, type D:\SETUP.EXE (where D is the letter of your CD-ROM drive).
- 3 Click OK.
- 4 Go to Using the configuration wizard on page 16.

Installing from the Web site

When you install Wireless Home Network Security from the Web site, you must save the installation file. This file is used to install Wireless Home Network Security on other computers.

- 1 Go to the McAfee Web site, and click **My Account**.
- 2 If prompted, enter your subscribing e-mail address and password, then click **Log In** to open your **Account Info** page.
- **3** Locate your product in the list, and click **Save Target As...** The installation file is saved on your computer.

Installing from the installation file

If you downloaded the installation package (as opposed to having a CD), you must install the software on all the wireless computers. After the network is protected, wireless computers cannot connect to the network without entering the key. Do one of the following.

- Before protecting the network, download the installation package to every wireless computer.
- Copy the installation file to a USB memory key or a writable CD and install the software on the other wireless computers.
- If the network is already protected, plug a cable in the router to download the file. You can also click View Current Key to see the current key, and connect to the wireless network using this key.

After you install Wireless Home Network Security on all the wireless computers, follow the on-screen instructions. When you click **Finish**, the Configuration wizard appears. Go to *Using the configuration wizard* on page 16.

Using the configuration wizard

The configuration wizard allows you to:

 Protect your network from one of the wireless computers. For more information, see *Protecting wireless networks* on page 25.

If Wireless Home Network Security cannot determine the correct router or access point to protect, you are prompted to Retry or Cancel. Try moving closer to the router or access point you are protecting, and then click **Retry**.

- Join a protected network (this step is not necessary if there is only one wireless computer). For more information, see *Managing Wireless Networks* on page 19.
- Connect to a network. For more information, see Connecting to a network on page 19.

You are notified if your wireless adapter is not detected or your wireless router or access point is not turned on.

Using the Summary Page

To view the status of your connection, right-click the McAfee icon (\overline{M}), point to **Wireless Network Security**, and select **Summary**. The Summary page appears (Figure 3-1).

🖞 McAfee Wireless Home Network Security 📃 🗔 🔀				
McAfee" wirele	🕐 help			
E	Connectio	n		
2	Status:	Connected to network GiancarloWAP		Security Scan
Summary	Security:	McAfee Wireless Security	Duration:	00:10:40
	Speed:	54.0 Mbps	Signal Strength:	Excellent
A	Protected	l Wireless Network		
Available	Connections today: 224 View Netw Key rotations today: 135 Last rotated 7 minutes ago View Curre		work Events	
Networks			rent Key	
	Computer	s secured this month: 74		
	Computer	s:		
10 A 10	Compu	ter	Last Connection	
Options	Å Gianca	rloWAP	07/19/05 16:47:42	
	A Coppi		07/19/05 14:06:06	

Figure 3-1. Summary page

Viewing your connection

The Connection pane shows the status of your connection. If you want to run a scan of your wireless connection, click **Security Scan**.

- Status whether you are connected or disconnected. If you are connected, the name of the network appears.
- Security the security mode of the network.
- Speed connection speed from your wireless NIC (Network Interface Card).
- Duration how long you have been connected to this network.
- Signal Strength strength of your wireless connection.

Viewing your protected wireless network

The Protected Wireless Network pane provides information on your network.

- Connections today how many times users connected to this network today.
- Key rotations today how many times the key has rotated today, including the time elapsed since the key was last rotated.
- Key rotation suspended- key rotation on your network is suspended. To resume key rotation and ensure that your network is fully protected from hackers, click **Resume Key Rotation**.
- Computers secured this month how many computers have been secured this month.
- Computers if you are connected to a protected network, all the computers on the network and when each computer was last connected.

🐕 - the computer is connected.

A - the computer can reconnect without joining the network.

Q - the computer is not connected. The computer must rejoin the network because the key has been updated.

Click View Network Events to view network events. See *Viewing events* on page 21.

Click **View Current Key** to view the key.

If you are connecting wireless devices that Wireless Home Network Security does not support (for example, connecting a wireless handheld computer to your network), follow these steps.

- 1 In the Summary screen, click View Current Key.
- **2** Write down the key.
- **3** Click **Suspend Key Rotation**. Suspending key rotation prevents devices that have been manually connected to the network from being disconnected.
- 4 Enter the key on the device.

When you are done using these devices, click **Resume Key Rotation.** McAfee recommends that you resume key rotation to ensure that your network is fully protected from hackers.

Managing Wireless Networks

To select wireless networks to connect to or join, right-click the McAfee icon (\mathbf{M}), point to **Wireless Network Security**, and select **Available Wireless Networks**. The Available Wireless Networks page appears (Figure 4-1).

🚻 McAfee Wi	reless Home Network Security	×
McAfee' wirele	<mark>ss</mark> home network security	🕐 help
E Summary	Wireless Networks Status: Connected - GiancarloWAP (McAfee Wireless Security) Select a wireless network:	Disconnect
Available Wireless Networks	Network "A" GiancarloWAP "A" Coppi "A" UWNetgear "A" belin54g "A" bugno "A" inksys You are currently connected to this network. Click 'Disconnect' if yo	Signal Strength
Options	from this network.	ect Advanced

Figure 4-1. Available Wireless Networks page

When you are connected to a protected wireless network, the information that is sent and received is encrypted. Hackers cannot intercept the data that is transmitted over the protected network and cannot connect to your network.

- the network is protected.

🛔 - the network is protected using WEP, WPA-PSK, or WPA2-PSK security.

O the network is not protected but you can still connect to it (not recommended).

Connecting to a network

To connect to a network, select the network you want to connect to, and click **Connect**. If you manually configured a pre-shared key for your router or access point, you must also enter the key.

If the network is protected, you must join it before you can connect to it. In order for you to join the network, a user that is already connected to the network must give you permission.

When you join a network, you can reconnect to it without having to join it again. You can also grant permission to other users to join that network.

Disconnecting from a network

To disconnect from the network you are connected to, click **Disconnect**.

Using advanced options

If you want to use advanced connection options, click **Advanced**. The **Advanced Settings** dialog box appears. From this dialog box, you can do the following.

- Change the order of the networks you automatically connect to the network at the top of the list is the one that you last connected to, and is the one that Wireless Home Network Security tries to connect to first. To move a network, select it and click **Move Up** or **Move Down**. For example, if you moved from a location and the network you last connected to is far away and does not have a strong signal, you can move the network that has a stronger signal to the top of your list.
- Remove preferred networks remove networks from this list. For example, if you connected to your neighbor's network by mistake, it is now included in this list. To remove it, select it and click **Remove**.
- Modify network properties if you are having trouble connecting to a network that is not protected, you can modify its properties. Note that this option only applies to networks that are not protected. To modify properties, select a network and click **Properties**.
- Add networks that do not broadcast SSID for example, if you are trying to connect to your friend's wireless network, but it does not appear in the list, click Add and enter the appropriate information. Note that the network that you add cannot be protected by Wireless Home Network Security.

Configuring Options

To configure options, right-click the McAfee icon (M), point to **Wireless Network Security**, and select **Options**. The Options page appears (Figure 5-1).



Figure 5-1. Options page

Viewing events

Actions performed by Wireless Home Network Security are stored in event logs. To view these logs, click **View Network Events**. The information displays in chronological order by default.

In the Events for network box, you can select the type of events that display (all events are still logged), and you can view events for any network that you belong to (if you belong to more than one network).

When an event occurs, an alert appears with a brief description. For more information on alerts, see *Understanding Alerts* on page 29.

Configuring advanced settings

This section is for advanced users. Click **Advanced Settings** to configure security, alert, and other settings.

When you change a setting, click **OK** for the changes to take effect. Note that after you click **OK**, all the computers that are connected temporarily lose connectivity for a few minutes.

Configuring security settings

Use the Security Settings tab to change your security settings.

- Protected Wireless Network Name name of the current protected network. When you change the name of a network, it appears in the Available Wireless Networks list and you must reconnect to the network. See *Managing Wireless Networks* on page 19.
- Security Mode current security. To change the default security (WEP), select another security mode for stronger encryption. Make sure that the routers, access points, and wireless adapters that connect to your network support this mode, or else they will not be able to connect. For more information on updating your adapter, see *Updating your wireless adapter* on page 39.
- Enable automatic key rotation to suspend key rotation, clear this option. To change the frequency of the key rotation, move the slider. For more information on key rotation, see *Viewing your protected wireless network* on page 18.
- Change User Name or Password for security reasons, you can change the default user name or password for the wireless router or access point by selecting it and clicking Change User Name or Password. The default user name or password is the one you used when you logged on and configured your router or access point.

Security mode not supported

If an error states that you selected a security mode that is not supported by the wireless adapter, select a different mode.

- All adapters support WEP.
- Adapters that support WPA implement WPA-PSK TKIP and WPA-PSK AES security modes.
- Adapters that support WPA2 implement WPA security modes, WPA2-PSK AES, and WPA2-PSK TKIP/AES.

Configuring alert settings

Use the Alert Settings tab to change your alert settings.

Select the type of events you want to be alerted to, and click **OK**. If you do not want to be alerted to certain types of events, clear the appropriate box.

Configuring other settings

Use the Other Settings tab to change other settings.

- Display keys in plain text for networks not protected by Wireless Home Network Security. Keys for unprotected networks that appear in the Available Wireless Networks list can be shown in plain text instead of asterisks. If you display keys in plain text, your keys are discarded for security reasons.
- Discard All Saved Keys for networks not protected by Wireless Home Network Security. Delete all the keys that have been saved. Note that if you delete these keys, you must re-enter a key when connecting to WEP, WPA-PSK, or WPA2-PSK networks.
- Leave Network for networks protected by Wireless Home Network Security. You can give up your access rights to a protected wireless network. For example, if you want to leave a network and do not expect to connect to it again, select it from the list and click Leave Network.
- Display notification message when connected to a wireless network when a connection is made, a notification message appears.

Revoking access to the network

To prevent computers that have joined the network, but are not currently connected to it, from accessing your network:

- 1 Click **Revoke Access**. The Revoke Access dialog box appears.
- 2 Click Revoke.

The key rotation for the network is reset, and the computers currently connected receive the new key and remain connected. Computers not currently connected do not receive the updated key and must rejoin the network before they can connect.

When you revoke access to a computer, that computer must rejoin the network before it can connect to the protected network again. To do this, the computer must have Wireless Home Network Security installed (see *Installing Wireless Home Network Security* on page 15), and then connect to the protected network and join it (see *Connecting to a network* on page 19).

Repairing security settings

Repair security settings only if you are having problems with your wireless network. For more information, see *Unable to connect* on page 38.

To fix your router or access point settings on the current network, follow these steps.

- 1 Click **Repair Security Settings.** The Repair dialog box appears.
- 2 Click Repair.
- 3 Click **Close** when you are done.

An error message appears if a connection cannot be made with the network routers or access points. Connect to your network using a cable, then try repairing again. If the password for the router or access point was changed, you are prompted for the new password.

Protecting other computers

To obtain more information on protecting other computers and giving them access to your protected network, click **Protect Another Computer**.

To protect another computer:

- 1 Install McAfee Wireless Home Network Security on the computer you want to protect.
- 2 From the computer you are protecting, right-click the McAfee icon (M), point to Wireless Network Security, and select Available Wireless Networks. The Available Wireless Networks page appears.
- **3** Select a protected network to join, and click **Connect**. Note that a user that is already connected to the network must give you permission to join the network.

When you join a network, you can reconnect to it without having to join it again. You can also grant permission to other users to join that network.

4 Click **OK** in the confirmation dialog box.

If you are connecting wireless devices that Wireless Home Network Security does not support (for example, connecting a wireless handheld computer to your network), follow these steps.

- 1 In the Summary screen, click View Current Key.
- 2 Write down the key.
- 3 Click **Suspend Key Rotation**. Suspending key rotation prevents devices that have been manually connected to the network from being disconnected.

4 Enter the key on the device.

When you are done using these devices, click **Resume Key Rotation**. McAfee recommends that you resume key rotation to ensure that your network is fully protected from hackers.

Rotating keys

To rotate the security key for your network, click Manually Rotate Security Key.

Protecting wireless networks

To protect a router or access point, follow these steps.

- 1 Click **Protect Wireless Router/AP**. The Protect Wireless Network dialog box appears. If the router or access point does not appear in the list, click **Refresh**.
- 2 Select the router or access point you are protecting, and click **Protect**.

Unprotecting wireless networks

You must be connected to the wireless router or access point you are unprotecting.

To unprotect a router or access point, follow these steps.

- Click Unprotect Wireless Router/AP. The Unprotect Wireless Router/AP dialog box appears. If the router or access point does not appear in the list, click Refresh.
- 2 Select the router or access point you are unprotecting, and click **Unprotect**.

Updating Wireless Home Network Security

When you are connected to the Internet, Wireless Home Network Security checks for software updates every four hours, then automatically downloads and installs weekly updates without interrupting your work. These updates have a minimal impact on system performance during download.

If a product update occurs, an alert appears. When alerted, you can choose to update Wireless Home Network Security.

Automatically checking for updates

McAfee SecurityCenter is automatically configured to check for updates for all of your McAfee services every four hours when you are connected to the Internet, then notify you with alerts and sounds. By default, SecurityCenter automatically downloads and installs any available updates.

NOTE

In some cases, you are prompted to restart your computer to complete the update. Save all your work and close all applications before restarting.

Manually checking for updates

In addition to automatically checking for updates when you are connected to the Internet, you can also manually check for updates at any time.

To manually check for Wireless Home Network Security updates:

- 1 Ensure your computer is connected to the Internet.
- 2 Right-click the McAfee icon, then click **Updates**. The **SecurityCenter Updates** dialog box appears.
- 3 Click Check Now.

If an update exists, the **McAfee SecurityCenter** dialog box appears. Click **Update** to continue.

If no updates are available, a dialog box tells you that Wireless Home Network Security is up-to-date. Click **OK** to close the dialog box.

- 4 Log on to the Web site if prompted. The **Update Wizard** installs the update automatically.
- 5 Click **Finish** when the update is finished installing.

NOTE

In some cases, you are prompted to restart your computer to complete the update. Save all your work and close all applications before restarting.

Understanding Alerts

Alerts appear when an event occurs, and notify you of changes to the network.

Access revoked

A user has updated the network key. For more information, see *Revoking access to the network* on page 23.

Computer connected

A user has connected to the network. For more information, see *Connecting to a network* on page 19.

Computer disconnected

A user has disconnected from the network. For more information, see *Disconnecting from a network* on page 20.

Computer secured

A user that has access to the protected network has granted someone else access. For example: 'Lance' has given access to 'Mercks' and they can now use the wireless network 'CoppiWAP'.

Key rotation failed

The key rotation failed because:

- The logon information for your router or access point has been changed. If you know the logon information, see *Repairing security settings* on page 24.
- The firmware version of your router or access point has been changed to a version that is not supported. For more information, see *Unable to connect* on page 38.
- Your router or access point is not available. Ensure that the router or access point is turned on, and that it is connected to your network.
- Duplicate administrator error. For more information, see *Duplicate administrator error* on page 35.

If you are having problems connecting to this network, see *Repairing security settings* on page 24.

Key rotation resumed

A user has resumed the key rotation. Key rotation prevents hackers from accessing your network.

Key rotation suspended

A user has suspended the key rotation. McAfee recommends that you resume key rotation to ensure that your network is fully protected from hackers.

Network configuration changed

A user has changed the security mode for the network. For more information, see *Configuring security settings* on page 22.

Network renamed

A user has renamed the network and you must connect to it again. For more information, see *Connecting to a network* on page 19.

Network repaired

A user has attempted to repair the network because they have problems connecting.

Network settings changed

A user is about to change network security settings. Your connection may be briefly interrupted while this occurs. The setting that is being changed can be one or more of the following:

- Name of the network
- Security mode
- Key rotation frequency
- Status of automated key rotation

Password changed

A user has changed the user name or password on a router or access point on the network. For more information, see *Configuring security settings* on page 22.

Security key rotated

The security key for the network has been rotated. McAfee Wireless Home Network Security automatically rotates your network encryption key, making it more difficult for hackers to intercept your data or connect to your network.

Security key rotation frequency changed

The security key rotation frequency for the network has been changed. McAfee Wireless Home Network Security automatically rotates your network encryption key, making it more difficult for hackers to intercept your data or connect to your network.

Wireless router/AP protected

A wireless router or access point has been protected on your network. For more information, see *Protecting wireless networks* on page 25.

Wireless router/AP unprotected

A wireless router or access point has been removed from the network. For more information, see *Unprotecting wireless networks* on page 25.

Troubleshooting

This chapter describes troubleshooting procedures for McAfee Wireless Home Network Security and third-party equipment.

Installation

This section explains how to resolve installation problems.

Which computers to install this software on

Install McAfee Wireless Home Network Security on every wireless computer in your network (unlike other McAfee applications, you can install this software on multiple computers).

You can (but are not required to) install on computers that do not have wireless adapters, but the software is not active on these computers because they do not need wireless protection. You must protect your router or access point (see *Protecting wireless networks* on page 25) from one of your wireless computers to secure your network.

Wireless adapter not detected

If your wireless adapter is not detected when it is installed and enabled, restart your computer. If the adapter is still not detected after restarting your computer, follow these steps.

- 1 Open the Wireless Network Connection Properties dialog box.
- 2 Clear the MWL Filter box and then select it.
- 3 Click OK.

If this does not work, your wireless adapter might not be supported. Update your adapter or buy a new one. To view a list of supported adapters, go to http://www.mcafee.com/router. To update your adapter, see *Updating your wireless adapter* on page 39.

Multiple wireless adapters

If an error states that you have multiple wireless adapters installed, you must disable or unplug one of them. Wireless Home Network Security only works with one wireless adapter.

Unable to download on wireless computers because the network is already secure

If you have a CD, install McAfee Wireless Home Network Security from the CD on all your wireless computers.

If you installed the software on one wireless computer and protected your network before installing the software on all the other wireless computers, you have these options.

- Unprotect your network (see Unprotecting wireless networks on page 25). Then, download the software and install it on all the wireless computers. Protect your network again (see Protecting wireless networks on page 25).
- View the network key (see *Viewing your protected wireless network* on page 18). Then, enter the key on your wireless computer to connect to the network. Download and install the software, and join the network from the wireless computer (see *Protecting other computers* on page 24).
- Download the executable on the computer that is already connected to the network and save it on a USB storage key or burn it to a CD so you can install it on the other computers.

Protecting or configuring your network

This section explains how to troubleshoot problems when protecting or configuring your network.

Unsupported router or access point

If an error states that your wireless router or access point may not be supported, McAfee Wireless Home Network Security was unable to configure your device because it did not recognize it or find it.

Verify that you have the latest version of Wireless Home Network Security by requesting an update (McAfee constantly adds support for new routers and access points). If your router or access point appears in the list at http://www.mcafee.com/router and you still receive this error, you are experiencing communication errors between your computer and the router or access point. See *Unable to connect* on page 38 before protecting your network again.

Updating router or access point firmware

If an error states that the firmware revision of your wireless router or access point is not supported, your device is supported, but the firmware revision of the device is not. Verify that you have the latest version of Wireless Home Network Security by requesting an update (McAfee constantly adds support for new firmware revisions).

If you have the latest version of Wireless Home Network Security, refer to the manufacturer Web site or support organization for your router or access point and install a firmware version that is listed on http://www.mcafee.com/router.

Duplicate administrator error

After you configure your router or access point, you must log off the administration interface. In some cases, if you do not log off, the router or access point acts as if another computer is still configuring it and an error message appears.

If you cannot log off, unplug the power from the router or access point and then plug it in again.

Network appears unsecured

If your network is showing as unsecured, it is not protected. You must protect the network (see *Protecting wireless networks* on page 25) to secure it. Note that McAfee Wireless Home Network Security only works with compatible routers and access points (see http://www.mcafee.com/router).

Unable to repair

If the repair fails, try the following. Note that each procedure is independent.

- Connect to your network using a cable, then try repairing again.
- Unplug the power from the router or access point, plug it in again, then try connecting.
- Reset the wireless router or access point to its default setting and repair it.
- Using the advanced options, leave the network from all the computers and reset the wireless router or access point to its default settings, then protect it.

Connecting computers to your network

This section explains how to troubleshoot problems when connecting computers to your network.

Waiting for authorization

If you try to join a protected network and your computer remains in waiting for authorization mode, verify the following.

- A wireless computer that already has access to the network is turned on and connected to the network.
- Someone is present to grant access on that computer when it appears.
- The computers are within wireless range of each other.

If **Grant** does not appear on the computer that already has access to the network, try granting from another computer.

If other computers are not available, unprotect the network from the computer that already has access, and protect the network from the computer that did not have access. Then, join the network from the computer that originally protected the network.

Granting access to an unknown computer

When you receive a request from an unknown computer to grant access, verify that they are familiar. Someone might be trying to illegitimately access your network.

Connecting to a network or the Internet

This section explains how to troubleshoot problems when connecting to a network or the Internet.

Bad connection to the Internet

If you cannot connect, try accessing your network using a cable, and then connect to the Internet. If you still cannot connect, verify the following:

- your modem is turned on
- your PPPoE (see *Glossary* on page 43) settings are correct
- your DSL or Cable line is active

Connectivity problems such as speed and signal strength can also be caused by wireless interference. Try changing the channel of your cordless telephone, eliminate possible sources of interference, or change the location of your wireless router, access point, or computer.

Connection briefly stops

When your connection briefly stops (for example, during an online game), the key rotation might be causing brief network delays: Momentarily suspend key rotation. McAfee recommends that you resume key rotation as soon as you can to ensure that your network is fully protected from hackers.

Devices (not your computer) losing connection

If some devices are losing their connection when you are using McAfee Wireless Home Network Security, suspend the key rotation.

Prompted to enter the WEP, WPA, or WPA2 key

If you have to enter a WEP, WPA, or WPA2 key to connect to your network, you probably did not install the software on your computer. To function correctly, Wireless Home Network Security must be installed on every wireless computer in your network. See *Protecting or configuring your network* on page 35.

Unable to connect

If you are unable to connect, try the following. Note that each procedure is independent.

- If you are not connecting to a protected network, verify that you have the correct key and enter it again.
- Unplug the wireless adapter and plug it in again, or disable it and re-enable it.

- Turn off the router or access point, and turn it on again, then try connecting.
- Verify that your wireless router or access point is connected, and repair the security settings (see *Repairing security settings* on page 24).

If the repair fails, see *Unable to repair* on page 36.

- Restart your computer.
- Update your wireless adapter or buy a new one. To update your adapter, see Updating your wireless adapter on page 39. For example, your network could be using WPA-PSK TKIP security, and your wireless adapter might not support the network's security mode (the networks show WEP, even though they are set to WPA).
- If you are unable to connect after you upgraded your wireless router or access point, you might have upgraded it to an unsupported version. Verify that the router or access point is supported. If it is not supported, downgrade it to a supported version, or wait until a Wireless Home Network Security update is available.

Updating your wireless adapter

To update your adapter, follow these steps.

- 1 From your desktop, click **Start**, point to **Settings**, and then select **Control Panel**.
- 2 Double-click the **System** icon. The **System Properties** dialog box appears.
- **3** Select the **Hardware** tab, and then click **Device Manager**.
- 4 In the Device Manager list, double-click your adapter.
- 5 Select the **Driver** tab and note the driver you have.
- **6** Go to the Web site of the adapter's manufacturer and see if an update is available. Drivers are usually found in the Support or Downloads section.
- **7** If a driver update is available, follow the instructions on the Web site to download it.
- 8 Go back to the **Driver** tab and click **Update Driver**. A Windows wizard appears.
- **9** Follow the on-screen instructions.

Weak signal level

If your connection drops or is slow, your signal level might not be strong enough. To improve your signal, try the following.

- Ensure that your wireless devices are not blocked by metal objects such as furnaces, ducts, or large appliances. Wireless signals do not travel well through these objects.
- If your signal is going through walls, make sure that it does not have to cross at a shallow angle. The longer the signal travels inside a wall, the weaker it gets.
- If your wireless router or access point has more than one antenna, try moving the two antennas perpendicular to each other (one upright and one horizontal, at a 90 degree angle).
- Some manufacturers have high-gain antennas. Directional antennas provide longer range, while omni-directional antennas offer the most versatility. Consult your manufacturer's installation instructions for installing your antenna.

If these steps are not successful, add an Access Point to your network that is closer to the computer you are trying to connect to. If you configure your second AP with the same network name (SSID) and a different channel, your adapter automatically finds the strongest signal and connects through the appropriate AP.

Windows cannot configure your wireless connection

When you get a message saying that Windows cannot configure your wireless connection, you can ignore it. Use Wireless Home Network Security to connect to, and configure wireless networks. In the Windows Wireless Network Connection Properties dialog box, under the Wireless Networks tab, ensure that the **Use Windows to configure my wireless network setting** box is clear.

Windows showing no connection

If you are connected, but the Windows Network icon is showing an X (no connection), ignore this. You have a good connection.

Other issues

This section explains how to troubleshoot problems with other issues.

Network name is different when using other programs

If the name of the network is different when viewed through other programs (for example, _SafeAaf is part of the name), this is normal. Wireless Home Network Security marks networks with a code when they are protected.

Problems configuring wireless routers or access points

If an error appears when configuring your router or access point or adding multiple routers on the network, verify that all the routers and access points have a distinct IP address.

If the name of your wireless router or access point appears in the Protect Wireless Router or Access Point dialog box, but you get an error when you configure it: Verify that your router or access point is supported. To view a list of supported routers or access points, go to http://www.mcafee.com/router.

If your router or access point is configured, but does not seem to be on the correct network (for example, you cannot see other computers attached to the LAN), verify that you configured the appropriate router or access point, and not your neighbor's. Unplug the power from the router or access point, and ensure that the connection drops. If the wrong router or access point was configured, unprotect it and then protect the correct router or access point.

If you are unable to configure or add your router or access point, but it is supported, some changes you performed might be preventing it from being properly configured.

- Follow the manufacturer's directions to configure your wireless router or access point to DHCP, or to configure the correct IP address. In some cases, the manufacturer provides a configuration tool.
- Reset your router or access point to factory defaults and try repairing your network again. You might have changed the administration port on the router or access point, or turned off wireless administration. Ensure that you are using the default configuration, and that wireless configuration is enabled. Another possibility is that the http administration is disabled. In this case, verify that the http administration is enabled.
- If your wireless router or access point does not appear in the list of wireless routers or access points to protect or connect to, enable broadcast SSID and verify that the router or access point is enabled.
- If you get disconnected, or cannot establish a connection, MAC filtering might be enabled. Disable MAC filtering.

 If you cannot perform network operations (for example, share files or print to shared printers) across two computers with wireless connection to the network, verify that you have not enabled AP Isolation. AP Isolation prevents wireless computers from being able to connect to each other over the network.

Replacing computers

If the computer that protected the network has been replaced and there are not any computers that have access (you cannot access the network), reset the wireless router or access point to its factory defaults and protect your network again.

Software not working after upgrading operating systems

If Wireless Home Network Security does not work after upgrading operating systems, uninstall it and then reinstall it.

Glossary

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, a standard for up to 54 Mbps networking in the 5Ghz band, 802.11b, a standard for up to 11 Mbps networking in the 2.4 Ghz band, 802.11g, a standard for up to 54 Mbps networking in the 2.4 Ghz band, 802.11i, a suite of security standards for all wireless Ethernets.

802.11a

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

An extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission in the 2.4 GHz band. 802.11b is currently considered the wireless standard.

802.11g

An extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 2.4 GHz band.

802.1x

Not supported by Wireless Home Network Security. 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.

A

Access Point (AP)

A network device that allows 802.11 clients to connect to a local area network (LAN). APs extend the physical range of service for a wireless user. Sometimes referred to as wireless router.

Authentication

The process of identifying an individual, usually based on a user name and password. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

B

Bandwidth

The amount of data that can be transmitted in a fixed amount of time. For digital devices, the bandwidth is usually expressed in bits per second (bps) or bytes per second. For analog devices, the bandwidth is expressed in cycles per second, or Hertz (Hz).

Brute-Force Attack

Also known as brute force cracking, a trial and error method used by application programs to decode encrypted data such as passwords through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or crack, a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

С

Cipher Text

Data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key.

Client

An application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

D

Denial of Service

On the Internet, a denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. A denial of service attack can also destroy programming and files in a computer system. Although

usually intentional and malicious, a denial of service attack can sometimes happen accidentally. A denial of service attack is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money.

Dictionary Attack

These attacks involve trying a host of words from a list to determine someone's password. Attackers don't manually try all combinations but have tools that automatically attempt to identify someone's password.

Ε

Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, a person must have access to a secret key or password that enables them to decrypt it. Data that is not encrypted is called plain text; encrypted data is referred to as cipher text.

ESS (Extended Service Set)

A set of two or more networks that form a single subnetwork.

F

Firewall

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially an intranet. All messages entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

G

Н

Hotspot

A specific geographic location in which an access point (AP) provides public wireless broadband network services to mobile visitors through a wireless network. Hotspots are often located in heavily populated places such as airports, train stations, libraries, marinas, conventions centers, and hotels. Hotspots typically have a short range of access.

I

Integrated Gateway

A device that combines the functions of an access point (AP), router, and firewall. Some devices may also include security enhancements and bridging features.

IP Address

An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 192.168.1.100 could be an IP address.

IP Spoofing

Forging the IP addresses in an IP packet. This is used in many types of attacks including session hijacking. It is also often used to fake the e-mail headers of SPAM so they cannot be properly traced.

J

Κ

Key

A series of letters and/or numbers used by two devices to authenticate their communication. Both devices must have the key. See also WEP, WPA, WPA2, WPA-PSK, and WPA2-PSK.

L

LAN (Local Area Network)

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

Most LANs connect workstations and personal computers generally through simple hubs or switches. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices (e.g., printers) anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, for example, by sending e-mail or engaging in chat sessions.

Μ

MAC (Media Access Control or Message Authenticator Code)

For the former, see MAC Address. The latter is a code that is used to identify a given message (e.g., a RADIUS message). The code is generally a cryptographically strong hash of the contents of the message which includes a unique value to insure against replay protection.

MAC Address (Media Access Control Address)

A low-level address assigned to the physical device accessing the network.

Man-in-the-Middle Attack

The attacker intercepts messages in a public key exchange and then retransmits them, substituting their own public key for the requested one, so that the two original parties still appear to be communicating with each other directly. The attacker uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the messages, or enable the attacker to modify them before transmitting them again. The term is derived from the ball game where a number of people try to throw a ball directly to each other while one person in between attempts to catch it.

Ν

Network

A collection of Access Points and their associated users, equivalent to an ESS. Information about this network is maintained in McAfee Wireless Home Network Security. See ESS.

NIC (Network Interface Card)

A card that plugs into a laptop or other device and connects the device to the LAN.

0

Р

PCI Wireless Adapter Cards

Connects a desktop computer to a network. The card plugs into a PCI expansion slot inside the computer.

PPPoE

Point-to-Point Protocol Over Ethernet. Used by many DSL providers, PPPoE supports the protocol layers and authentication widely used in PPP and enables a point-to-point connection to be established in the normally multipoint architecture of Ethernet.

Plain Text

Any message that is not encrypted.

Protocol

An agreed-upon format for transmitting data between two devices. From a user's perspective, the only interesting aspect about protocols is that their computer or device must support the right ones if they want to communicate with other computers. The protocol can be implemented either in hardware or in software.

Q

R

RADIUS (Remote Access Dial-In User Service)

A protocol that provides for authentication of users, usually in the context of remote access. Originally defined for use with dial-in remote access servers, the protocol is now used in a variety of authentication environments, including 802.1x authentication of a WLAN user's Shared Secret.

Roaming

The ability to move from one AP coverage area to another without interruption in service or loss in connectivity.

Rogue Access Points

An access point that a company does not authorize for operation. The trouble is that a rogue access points often don't conform to wireless LAN (WLAN) security policies. A rogue access point enables an open, insecure interface to the corporate network from outside the physically controlled facility.

Within a properly secured WLAN, rogue access points are more damaging than rogue users. Unauthorized users trying to access a WLAN likely will not be successful at reaching valuable corporate resources if effective authentication mechanisms are in place. Major issues arise, however, when an employee or hacker plugs in a rogue access point. The rogue allows just about anyone with an 802.11-equipped device on the corporate network. This puts them very close to mission-critical resources.

Router

A network device that forwards packets from one network to another. Based on internal routing tables, routers read each incoming packet and decide how to forward it. To which interface on the router outgoing packets are sent may be determined by any combination of source and destination address as well as current traffic conditions such as load, line costs, bad lines. Sometimes referred to as access point (AP).

S

Shared Secret

See also RADIUS. Protects sensitive portions of RADIUS messages. This shared secret is a password that is shared between the authenticator and the authentication server in some secure manner.

SSID (Service Set Identifier)

Network name for the devices in a wireless LAN subsystem. It is a clear text 32-character string added to the head of every WLAN packet. The SSID differentiates one WLAN from another, so all users of a network must supply the same SSID to access a given AP. An SSID prevents access by any client device that does not have the SSID. By default, however, an access point (AP) broadcasts its SSID in its beacon. Even if SSID broadcasting is turned off, a hacker can detect the SSID through sniffing.

SSL (Secure Sockets Layer)

A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data which is transferred over the SSL connection. Both Netscape Navigator and Internet Explorer use and support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:

Т

TKIP (Temporal Key Integrity Protocol)

A quick-fix method to overcome the inherent weaknesses in WEP security, especially the reuse of encryption keys. TKIP changes temporal keys every 10,000 packets, providing a dynamic distribution method that significantly enhances the security of the network. The TKIP (security) process begins with a 128-bit temporal key shared among clients and access points (APs). TKIP combines the temporal key with the (client machine's) MAC address and then adds a relatively large 16-octet initialization vector to produce the key that encrypts the data. This procedure ensures that each station uses different key streams to encrypt the data. TKIP uses RC4 to perform the encryption. WEP also uses RC4.

U

USB Wireless Adapter Cards

Provide an expandable Plug and Play serial interface. This interface provides a standard, low-cost wireless connection for peripheral devices such as keyboards, mice, joysticks, printers, scanners, storage devices, and video conference cameras.

V

VPN (Virtual Private Network)

A network constructed by using public wires to reunite nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

W

Wardriver

Interlopers armed with laptops, special software, and some makeshift hardware, who drive through cities, suburbs and business parks in order to intercept wireless LAN traffic.

WEP (Wired Equivalent Privacy)

An encryption and authentication protocol defined as part of the 802.11 standard. Initial versions are based on RC4 ciphers and have significant weaknesses. WEP attempts to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed.

Wi-Fi (Wireless Fidelity)

Used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is used by the Wi-Fi Alliance.

Wi-Fi Certified

Any products tested and approved as Wi-Fi Certified (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. A user with a Wi-Fi Certified product can use any brand of access point (AP) with any other brand of client hardware that also is certified. Typically, however, any Wi-Fi product using the same radio frequency (for example, 2.4GHz for 802.11b or 11g, 5GHz for 802.11a) works with any other, even if not Wi-Fi Certified.

Wi-Fi Alliance

An organization made up of leading wireless equipment and software providers with the mission of (1) certifying all 802.11-based products for inter-operability and (2) promoting the term Wi-Fi as the global brand name across all markets for any 802.11-based wireless LAN products. The organization serves as a consortium, testing laboratory, and clearinghouse for vendors who want to promote inter-operability and the growth of the industry.

While all 802.11a/b/g products are called Wi-Fi, only products that have passed the Wi-Fi Alliance testing are allowed to refer to their products as Wi-Fi Certified (a registered trademark). Products that pass are required to carry an identifying seal on their packaging that states Wi-Fi Certified and indicates the radio frequency band used. This group was formerly known as the Wireless Ethernet Compatibility Alliance (WECA) but changed its name in October 2002 to better reflect the Wi-Fi brand it wants to build.

Wireless adapter

Contains the circuitry to enable a computer or other device to communicate with a wireless router (attach to a wireless network). Wireless adapters can be built into the main circuitry of a hardware device or they can be a separate add-on that can be inserted into a device through the appropriate port.

WLAN (Wireless Local Area Network)

See also LAN. A local area network using a wireless medium for connection. A WLAN uses high-frequency radio waves rather than wires to communicate between nodes.

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 compatible with, the IEEE 802.11i standard. When properly installed, it provides wireless LAN users with a high level of assurance that their data remains protected and that only authorized network users can access the network.

WPA2

See also WPA. WPA2 is an update of the WPA security standard and is based on the 802.11i IEEE standard.

WPA-PSK

A special WPA mode designed for home users who do not require strong enterprise-class security and do not have access to authentication servers. In this mode, the home user manually enters the starting password to activate Wi-Fi Protected Access in Pre-Shared Key mode, and should change the pass-phrase on each wireless computer and access point regularly. See also WPA2-PSK and TKIP.

WPA2-PSK

See also WPA-PSK and WPA2. WPA2-PSK is similar to WPA-PSK and is based on the WPA2 standard. A common feature of WPA2-PSK is that devices often support multiple encryption modes (e.g., AES, TKIP) simultaneously, while older devices generally supported only a single encryption mode at a time (i.e., all clients would have to use the same encryption mode). Y Z

Index

Α

advanced settings alerts, 23 other, 23 security, 22 alerts, 29 Available Wireless Networks page, 19

С

configuration wizard, using, 16 connection, viewing, 17

Е

events, viewing, 21

F

features, 11

G

glossary, 43

Κ

keys, rotating, 25

Μ

McAfee SecurityCenter, 13

Ν

network connecting, 19 disconnecting, 20 protecting, 25 revoking access, 23 unprotecting, 25 viewing, 18

0

options advanced, 20 configuring, 21 Options page, 21

Ρ

protecting computers, 24

Q

Quick Start Card, iii

S

settings, repairing, 24 Summary page, 17 system requirements, 12

Т

troubleshooting, 33

U

updating Wireless Home Network Security automatically checking for updates, 27 manually checking for updates, 27

W

Wireless Home Network Security installing, 15 introduction, 10 using, 9