

User's Guide

WebScanX for Windows 3.1x, Windows 95, and Windows NT



Network Security & Management

2805 Bowers Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 A.M. - 6:00 P.M.

COPYRIGHT

Copyright © 1997 by McAfee Associates, 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 Associates, Inc.

TRADEMARK NOTICES

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of McAfee Associates, Inc. WebScan, WebScanX, SiteExpress, BootShield, ServerStor, ScreenScan, WebCrypto, PCCrypto, PCFirewall, NetCrypto, GroupShield, GroupScan, Remote Desktop 32, WebShield, NetRemote, eMail-It, Hunter, ScanPM, and SecureCast are trademarks of McAfee Associates, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

"SABRE" is a trademark of American Airlines, Inc. and is licensed for use to McAfee. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

FEEDBACK

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your feedback to: McAfee Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, send e-mail to documentation@cc.mcafee.com, or send a fax to McAfee Documentation at (408) 970-9727.

Issued August 1997/WebScanX v3.1.0

Table of Contents

Preface.....	vii
Chapter 1. Introducing WebScanX.....	13
What is WebScanX?	13
Why use WebScanX?	13
WebScanX as your online sentry	14
Reporting new items for WebScanX updates	14
How To Contact McAfee	15
Customer service	15
Technical support.....	15
McAfee training	16
International contact information.....	17
Chapter 2. Installing WebScanX.....	18
Before You Begin	18
Basic system requirements.....	18
Installing WebScanX.....	19
Chapter 3. Getting Started	22
WebScanX Components.....	22
Checking Scan Activity	23
WebScanX shortcut menus	23
The WebScanX Status Dialog Box	24
Starting and Quitting WebScanX	26

Chapter 4. Configuring E-mail Scan Properties	28
What is E-mail Scanning?	28
Configuring e-mail scanning	28
Chapter 5. Configuring Download Scan Properties	38
What is Download Scanning?	38
Configuring Download Scan options	38
Chapter 6. Configuring Internet Filter Properties	46
What is Internet Filtering?	46
Configuring Internet filtering	46
Chapter 7. Configuring WebScanX Security Properties	52
What is WebScanX Security?	52
Configuring WebScanX security	52
Chapter 8. Using WebScanX for Windows 3.1x	55
Introducing WebScanX for Windows 3.1x	55
Configuring WebScanX for Windows 3.1x	57
Starting and Quitting WebScanX for Windows 3.1x	58
Appendix A. Preventing Virus Infection	60
Keys to a Secure System Environment	60
Detecting New and Unknown Viruses	61
Updating your WebScanX data files	61
Using SecureCast electronic updating	62
Updating your data files manually	62
Reporting new items for WebScanX updates	63
Appendix B. McAfee Support Services	64
Customer Service Programs	65
Free WebScanX support program	65
Free WebScanX Deluxe support program	66
Free subscription maintenance and support program	66
Optional support plans	67

Professional Services Programs.....	69
Training	69
Consulting.....	69
Jump Start program	70
Enterprise support.....	70
Optional 7 x 24 enterprise support.....	71
Index	72



Preface

The Bits and the Bytes

Computer viruses, most users know, can have a devastating impact on productivity. What many of those same users don't know is basic information that could help them protect themselves from infection—such as where viruses come from and how they operate.

In the beginning

The conceptual foundations for viruses have been around much longer than the virus threat itself. Although virus historians disagree on the specific whens and wheres, most do agree that the ideas were born when computers were still huge and expensive—the domain of large corporations and the government, not the public. And while many of the viruses circulating today are malicious, destruction of data was not part of the original premise.

The researchers who created the first viruses sought to create computer programs that could make copies of themselves, or self-replicate, with the idea that such programs might also “evolve.” If, for example, an error occurred in the replication process, the resulting code (the bits of information that make up the program) would be mutant. Just as mutant genetic code can either enhance or diminish the ability of a biological virus to survive and propagate, mutant digital code might dispose a computer virus to be more or less able to survive in the computer environment. Given enough time, the logical extension of the theory goes, a computer virus could evolve into something approaching artificial intelligence. Science fiction suddenly starts to look more like science and less like fiction.



What viruses really are

At its core, a virus is simply a program with one goal: self-replication. Part of achieving that goal is remaining undetected. Users who find viruses will likely delete them, which puts quite a damper on any self-replicating plans. Just like any other program, a virus has to be run to do its work. And since users will not run a virus intentionally, the virus must attach itself to a file that a user will run. That includes executable files and document files with embedded macros, as we will see in a couple of pages. For a virus to infect any other type of file—say, a plain text file—would be counter-productive: Remember, replication is its primary objective.

Computers with the sniffles?

Consider the similarities between computer and biological viruses. A computer virus infects a host program, just as a biological virus infects a host cell. It writes its own code in among the pieces of code that make up the host program. Then, in much the same way that a biological virus uses resources from its host organism to reproduce, a computer virus runs each time the infected host program runs, and makes copies of itself. Those copies then infect other programs, and the cycle begins again.

Just as biological viruses have detrimental effects, so do their computer counterparts. The first computer viruses were simply experiments by research scientists to test the theory—to see if it could be done. They proved the theory, but they also discovered that viruses had some unfortunate side effects. Viruses got in the way of some of the normal processes of the computer and caused erratic behavior. Many viruses are now specifically programmed to perform some function outside of self-replication. This function, called the payload, can be as innocuous as displaying a message on the computer's monitor or as harmful as destroying data on the system's hard disks. It is delivered when the trigger, an event such as a particular combination of keystrokes, a certain date or a pre-determined number of actions, occurs.



Who writes viruses?

The reason for this change in the behavior of viruses—from innocent experiment to malicious sneak attack—is a result of a change in the type of people who write them. Virus code is now developed by many people who are less interested in studying the possibility of artificial intelligence than in inflicting harm. Some do it out of spite, some because they aspire to be the underground “mad hacker” romanticized in much of pop culture as a freedom fighter of the digital age. The reasons people write virus code are probably as varied and strange as the reasons people perform other destructive acts.

Some virus writers actually choose to identify themselves, such as the Pakistani brothers who wrote the Brain virus. The brothers included the name, address, and telephone number of their software company in the viral code. When the payload was delivered, this information would be displayed for the user. Apparently, the brothers wrote the virus to show how widespread software pirating was. They put it on diskettes leaving their office with the idea that wherever the virus spread, so had their software. Of course, what they overlooked was the fact that the virus spread by infecting programs other than the one it left their office in.

Other virus writers are disgruntled employees seeking revenge. Still others are schoolkids who write just to see if they can. The famous Stoned virus is said to have been written by such a youngster. Having written it, he feared the consequences of unleashing it, so he destroyed all copies of the virus except one, which he kept at his house. His younger brother and a couple of friends managed to lay their hands on it though, and infected some disks as a joke. But the infection spread quickly and soon was impossible to stop.

Whatever the motivation, the number of people capable of writing a virus is growing right alongside the computer industry. Those who stand to be affected by virus infection—anyone who uses a computer—should be alert and wary.



Only getting worse

In part, the fact that so many of us must be on the alert today is what makes virus proliferation possible. When the computer world was made up entirely of huge, expensive machines, a virus did not have very far to go once it got started. But with the advent of the personal computer, viruses suddenly had a lot of places to go. The rapid growth of the Internet, the capability to attach files to e-mail messages, and the increasing degree to which the world depends on its computers all make conditions ever-better for the spread of computer viruses.

New developments

There are other reasons to be especially wary these days. Viruses get increasingly complex and advanced as computers on the whole do the same. Just in the last few years, sophisticated and dangerous new virus families have appeared, such as polymorphic viruses and macro viruses. Polymorphic viruses are especially tricky to detect because they change each time they infect new files. Where once anti-virus software could search for viruses by “signatures” (chunks of code unique to each virus), it now must detect polymorphic viruses that change their signatures each time they infect a file.

Macro viruses infect documents and document templates—new territory for viruses. Documents used to be safe from viral attack because until a few years ago, a document file didn’t have any executable code in it. Now that software applications like Microsoft Word and Microsoft Excel have embedded macro capabilities, viruses can use an application’s own macro language to infect application documents and templates.

On the frontier

Even as viruses grow more sophisticated and continue to threaten the integrity of computer systems we all have come to depend upon, still other dangers have begun to emerge from an unexpected source: the World Wide Web. Once a respository of research papers and academic treatises, the web has transformed itself into perhaps the most versatile and adaptable medium ever invented for communication and commerce.



Because its potential seems so vast, the web has attracted the attention and the developmental energies of nearly every computer-related company in the industry. Convergences in the technologies that have resulted from this feverish pace of invention now give web page designers tools they can use to collect and display information in ways never previously available. Websites can now send and receive e-mail, formulate and execute queries to databases using advanced search engines, send and receive live audio and video, and distribute data and multimedia resources to a worldwide audience.

Much of the technology that makes these features possible consists of small, easily downloaded programs that interact with your browser software and, sometimes, with other software on your hard disk. This same avenue can serve as an entry point into your computer system for other—less benign—programs to use for their own purposes.

Java and ActiveX

These programs, whether beneficial or harmful, come in a variety of forms. Some are special-purpose miniature applications, or “applets,” written in Java, a new programming language first developed by Sun Microsystems. Others are developed using ActiveX, a Microsoft technology that programmers can use for similar purposes.

Both Java and ActiveX make extensive use of prewritten software modules, or “objects,” that programmers can write themselves or take from existing sources and fashion into plug-ins, applets, device drivers and other software needed to power the web. Java objects are called “classes,” while ActiveX objects are called “controls.” The principle difference between them lies in how they run on the host system. Java applets run in a Java “virtual machine” designed especially to interpret Java programming and translate it into action on the host machine, while ActiveX controls run as native Windows programs that link and pass data between existing Windows software.

The overwhelming majority of these objects are useful, even necessary, parts of any interactive website. But despite the best efforts of Sun and Microsoft engineers to design security measures into them, determined programmers can use Java and ActiveX tools to plant harmful objects on websites, where they can lurk until visitors unwittingly allow them access to vulnerable computer systems.



Unlike viruses, harmful Java and ActiveX objects usually don't seek self-replication as their primary goal. The web provides them with plenty of opportunities to spread to target computer systems, while their small size and innocuous nature makes it easy for them to evade detection. In fact, unless you specifically tell your browser software to block them, Java and ActiveX objects automatically download to your system whenever you visit a website that hosts them.

Instead, harmful objects exist to deliver their equivalent of a virus payload. Programmers have written objects, for example, that can read data from your hard disk and send it back to the website you visited, that can "hijack" your e-mail account and send out offensive messages in your name, or that can watch data that passes between your computer and other computers.

Where next?

With most of these developments emerging only in the past few years, it's hard to imagine what sorts of dangers lie ahead as the computer becomes more complicated and more a part of everyday life. Luckily, you have purchased the best available protection against virus infections and harm from rogue Java and ActiveX objects. And with McAfee's outstanding support and worldwide anti-virus research teams, you can make sure your protection keeps up with the ever-changing computer world.

1

Introducing WebScanX

What is WebScanX?

WebScanX, a new addition to McAfee's family of security tools, keeps your computing environment secure from viruses and other harmful agents as you explore the Internet, exchange e-mail, and download files from remote computers. WebScanX runs under Windows 3.1, Windows 95 or Windows NT versions 3.51 and 4.0.

Why use WebScanX?

Web page design has advanced considerably in the past few years as the popularity of the Internet has grown; many websites now incorporate interactive elements composed of Java classes and ActiveX controls. At the same time, millions of users now exchange messages, files and other data via e-mail, often using "attachments" that consist of executable files, document templates and other data subject to virus infection.

Along with the excitement and the convenience that these new Internet capabilities bring, however, come some dangers. Executable files infected with viruses can lurk on websites, often without the site owner's knowledge, or can spread via e-mail, whether solicited or not. Sophisticated programmers can design Java applets or ActiveX controls that circumvent the security features built into your browser software to read data stored on your computer's hard disk, forge e-mail messages to others in your name, or cause other harm.

In the face of risks such as these, protecting yourself and your data from harm requires constant vigilance. WebScanX gives you the tools you need to keep your system intact and secure.

WebScanX as your online sentry

WebScanX functions as an online sentry, guarding your system against attacks from viruses and preventing harm caused by Java applets and ActiveX controls you might encounter while browsing websites on the Internet. WebScanX automatically scans e-mail messages and attachments that you receive from the Internet via Lotus cc:Mail, Microsoft Mail or another MAPI-compliant mail client. It filters Java classes and ActiveX controls by comparing those that it encounters with a database of classes and controls known to cause harm. When it detects a match, WebScanX can alert you or it can automatically deny harmful objects access to your system.

WebScanX can also keep your computer from connecting to dangerous Internet sites. Simply designate the sites your browser software should not visit, and WebScanX automatically prevents access. Password protection for your settings prevents unauthorized changes.

WebScanX helps to protect one of your most important assets—your data. It is an important element in a comprehensive security program that includes a variety of safety measures, such as regular use of anti-viral software, backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program.

Reporting new items for WebScanX updates

McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new Java classes, ActiveX controls, dangerous websites, or viruses that WebScanX does not now detect. Please note that McAfee reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

ResearchX@McAfee.com	Use this address to report harmful ActiveX controls and Java classes, or dangerous Internet sites.
AVResearch@McAfee.com	Use this address to report new virus strains.

How To Contact McAfee

Customer service

To order products or obtain product information, we invite you to contact our Customer Care department by calling (408) 988-3832 or by writing to the following address:

McAfee Associates, Inc.
2805 Bowers Avenue
Santa Clara, CA 95051-0963
U.S.A.

Technical support

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

World Wide Web	http://www.McAfee.com
----------------	---

If you do not find what you need or do not have web access, try one of our automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@mcafee.com
McAfee BBS	(408) 988-4004 1200 bps to 28,800 bps 8 bits, no parity, 1 stop bit 24 hours, 365 days a year
CompuServe	GO MCAFEE

1 Introducing WebScanX

How To Contact McAfee

America Online	keyword MCAFEE
Microsoft Network (MSN)	MCAFEE

If the automated services do not have the answers you need, contact McAfee at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 278-6100
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the McAfee technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

McAfee training

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

International contact information

To contact McAfee outside the United States, use the addresses and numbers below.

McAfee Canada

139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Phone: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.

Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: 31 20 586 6100
Fax: 31 20 586 6101

McAfee France S.A.

50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908 737
Fax: 33 1 45 227 554

McAfee Deutschland GmbH

Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 8989 43 5600
Fax: 49 8989 43 5699

McAfee (UK) Ltd.

Hayley House, London
Road
Bracknell, Berkshire
RG12 2TH
United Kingdom
Phone: 44 1344 304 730
Fax: 44 1344 306 902

McAfee Japan KK

4F Toranomori Mori
Bldg. 33
3-8-12 Toranomori
Minato-Ku, Tokyo, 105
Japan
Phone: 81 3 3435 8246
Fax: 81 3 3435 1349

2

Installing WebScanX

Before You Begin


This chapter describes how to install WebScanX. Before you begin, however, please review the basic system requirements outlined below.

Basic system requirements

To run WebScanX, you need an IBM-compatible personal computer with:


- A 486 or later processor
- At least 8MB of random-access memory (RAM)
- At least 7MB of free hard disk space
- One of the following operating systems:
 - Windows 95
 - Windows NT v3.51 or later

A separate, 16-bit version of WebScanX runs under Windows 3.1x. This version does not support Internet filtering and will not scan for harmful ActiveX controls or Java classes, but it uses the same powerful virus scanning technology as the versions for Windows 95 and Windows NT. You can use it to scan for viruses carried in e-mail you receive or files you download from the Internet.

 See Chapter 8, *Using WebScanX for Windows 3.1x*, for more details.

Installing WebScanX

To install WebScanX, follow these steps:

Step	Action
1.	<p>Start your computer, then do one of the following:</p> <ul style="list-style-type: none">■ If installing from files downloaded from a BBS or from the McAfee Web Site, decompress the zipped files into a directory on your network or on your local hard disk.■ If installing from a compact disc, insert it into your CD-ROM drive. <p> <i>The installer's autorun feature prompts you to choose which WebScanX version you want to install. If you choose one of the options listed, the WebScanX installer wizard appears immediately. To continue from that point, skip to step 3.</i></p>
2.	<p>If you are running Windows 95 or Windows NT 4.0, choose Run from the Start menu. If you are running Windows 3.1x or Windows NT 3.51, choose Run from the File menu in the Program Manager. Next, type</p> <p><code>x:\WebScanX\setup.exe</code></p> <p>where x is the drive that contains the CD-ROM. Click OK.</p> <p>If installing from downloaded files, type:</p> <p><code>x:\path\setup.exe</code></p> <p>where x:\path is the location of the files you decompressed. Click OK.</p> <p>Response: The WebScanX installer wizard appears and displays the McAfee Software License Agreement. Read this agreement carefully, then click Yes if you accept its terms.</p>
3.	<p>Choose the type of setup you prefer by selecting Typical, Compact, or Custom.</p>

4. Specify a destination directory for your WebScanX files. If you have other McAfee software installed, you may use an existing McAfee directory to store WebScanX files. Type the path in the text box provided, or click Browse to navigate to the directory of your choice. Click Next to continue.
 5. When prompted, review your settings, then click Next to continue.
- Response:** The installer copies WebScanX files to the directory you designated.
6. Click Yes to review the What's New text file for information on WebScanX. When you have finished reading the file, close the Notepad application window to continue.
 7. Review the modifications made to files on your system, then click Next. The installer notifies you that it has completed the installation.
 8. Select Yes to restart your computer, then click Finish.

Response: The system restarts. WebScanX begins running as soon as Windows finishes its startup.

WebScanX Components

WebScanX consists of three separate, but related, program components that each perform a different type of scanning operation. You may activate all three components at once, or you may run any component by itself. For WebScanX to remain active in your computer's memory, however, you must run at least one program component. The scanning operations each component performs are:

- **E-mail Scan.** This scan type looks for viruses attached to e-mail messages you receive from the Internet via Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant e-mail client software.
- **Download Scan.** This scan type looks for viruses attached to files and e-mail messages that you download or receive from the Internet using browser or e-mail client software that WebScanX supports. This type of scan works with both direct and dial-up connections.
- **Internet Filter.** This scan type examines Java classes and ActiveX controls you encounter as you browse websites and compares them with a database that lists classes and controls known to cause harm. When it finds an item with harmful characteristics, WebScanX blocks its access to your computer. Internet filtering also allows you to designate certain Internet sites as "off limits" to your browser software.

A fourth program component provides security for the other three. With it, you can lock your settings and protect them with a password to prevent unauthorized changes.

Each program component has a corresponding property page in the WebScanX Properties dialog box. See chapters 4 through 7 to learn how to choose settings for each type of scan you want to perform.

Checking Scan Activity

Each active program component can display an icon that tells you the status of WebScanX activity at a glance. The icons are animated and move whenever the corresponding program component performs a scan. Program components running under Windows 95 or Windows NT 4.0 display their icons in the taskbar's system tray, to the left of the clock. Program components running under Windows NT 3.51 display their icons at the lower left corner of the desktop. Here's what each icon looks like:



E-mail Scan



Download Scan



Internet Filter

After installation, WebScanX displays the E-mail Scan icon by default. Settings in the WebScanX Properties dialog box govern whether WebScanX displays other icons. See chapters 4 through 7 for more details.


WebScanX shortcut menus

Each WebScanX activity icon also has a corresponding shortcut menu that gives you quick access to common WebScanX commands. For program components running under Windows 95 or Windows NT 4.0, right-clicking any of the activity icons displays the commands shown below. Click any of the activity icons with your left mouse button when running WebScanX under Windows NT 3.51 to display these same commands:

- **Status.** Choose this to open the WebScanX Status dialog box.
- **Enable/Disable.** Choose this to activate or deactivate a WebScanX program component.
- **Properties.** Choose this to open the WebScanX Properties dialog box.
- **About.** Choose this to display your WebScanX serial number, copyright notices and version numbers.
- **Help.** Choose this to open the WebScanX online help file.

Press Shift on your keyboard as you click an icon to display this additional command:

- **Exit All.** Choose this to stop all scanning activity and quit WebScanX.

 *WebScanX for Windows 3.1x does not support these shortcut menus. To learn more about using WebScanX for Windows 3.1x, see Chapter 8 later in this manual.*

The WebScanX Status Dialog Box

To see a more detailed report on WebScanX activity, choose Status from the shortcut menu associated with any icon. This opens a tabbed WebScanX Status dialog box (Figure 3-1), where you can see how many files, Internet sites, Java classes and ActiveX controls each program component has examined. The Status dialog box also reports how many viruses WebScanX found in the items it examined, how many it moved or deleted from your system, and how many harmful classes or controls it encountered and blocked.

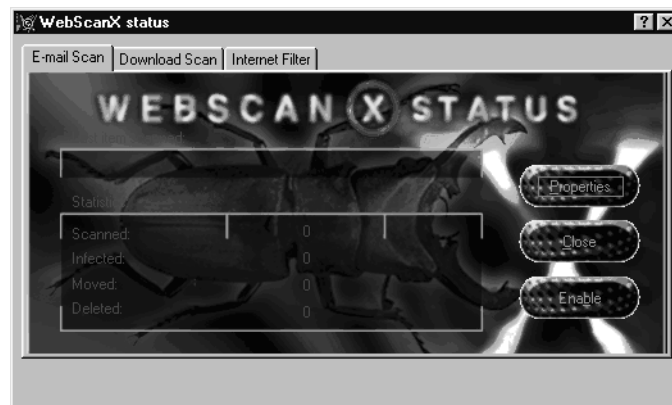



Figure 3-1. WebScanX Status Dialog Box

 *The Status dialog box you see differs from the one shown here if you have set your video display options to 16 colors.*

3 Getting Started

Checking Scan Activity



Click each tab to see a summary of WebScanX activity. The summary is cumulative and continues for an entire session; that is, for as long as you keep the program active. Whenever you quit the program or shut down your computer, the Status dialog box begins its summary over again.


To enable each scan type, select the checkbox at the bottom of the corresponding property page in the Status dialog box. To disable each scan type, clear its checkbox. You may also enable or disable program components from the Properties dialog box or from shortcut menus.

Click Properties to open the WebScanX Properties dialog box, where you can configure settings for each program component. See chapters 4 through 7 to learn how to configure WebScanX to suit your needs. Click Close to close the Status dialog box. Closing this dialog box does **not** quit WebScanX.

Starting and Quitting WebScanX

During installation, WebScanX sets itself to run as soon as Windows has restarted. Once started, WebScanX remains active in your computer's memory, automatically checking for viruses using the configuration options you set (see chapters 4 through 7 for details). To disable WebScanX's "autoload" feature, follow these steps:

- | Step | Action |
|------|--|
| 1. | Click any of the WebScanX activity icons in the system tray or on the desktop. Use your right mouse button if you are running WebScanX under Windows 95 or Windows NT 4.0. Use your left mouse button if you are running WebScanX under Windows NT 3.51. |
| 2. | Choose Properties from the shortcut menu that appears. |
| 3. | Click the switch  beside Load at startup to turn it "off."  This tells WebScanX not to load automatically.

<i> Click the switch again to reactivate the autoloading feature.</i> |
| 4. | Click OK to close the WebScanX Properties dialog box. |

To quit WebScanX, either disable each of the active program components individually, or follow these steps:


- | Step | Action |
|------|--|
| 1. | Press Shift on your keyboard, then click any of the WebScanX activity icons. |
| 2. | Choose Exit All from the shortcut menu that appears. |

Response: WebScanX stops all scanning activity and quits.

If you have disabled the WebScanX autoload feature and have quit WebScanX, you must start it again by choosing it in the Start menu or by locating and double-clicking its program icon. Follow these steps:

- | Step | Action |
|------|---|
| 1. | <p>If you use WebScanX with Windows 95 or Windows NT 4.0, click Start, point to Programs, then point to the McAfee WebScanX folder. Next, choose WebScanX to start the program again.</p> <p>If you use WebScanX with Windows NT 3.51, start the Windows File Manager, then locate the directory that contains WebScanX. If you followed the recommended installation procedure, you should find it here: c:\McAfee\WebScanX. Double-click the WebScanX icon to start the program again.</p> |
| 2. | <p>Choose your user profile from the list beside Profile Name in the Choose Profile dialog box that appears.</p> <p>Your user profile is the collection of settings you use to log on to the various information services available in conjunction with Microsoft Exchange or Microsoft Mail. To learn more about working with user profiles, consult the documentation for Windows Messaging.</p> |
| 3. | <p>Click OK.</p> |

Response: WebScanX starts with the most recent configuration options you have chosen.

 *If you have not yet logged on to your e-mail system, WebScanX first asks you to log on so that it can begin scanning your incoming e-mail. Type your user name, your password, and the path to your post office or mailbox, then click OK to start WebScanX.*

4

Configuring E-mail Scan Properties

What is E-mail Scanning?

WebScanX scans your incoming e-mail and files you download from the Internet for viruses. It also looks for harmful Java classes and ActiveX controls as you browse web pages and other Internet sites. With this combination, you get comprehensive protection for your computer system.

This chapter describes how to configure WebScanX to detect, respond to, alert others about, and log responses to viruses you receive from the Internet via your e-mail system. E-mail scanning works with Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant e-mail client software. To scan e-mail you receive from the Internet via the SMTP or POP-3 protocols, see Chapter 5 to learn how to configure settings for download scanning.

Configuring e-mail scanning

Use the E-mail Scan property page (Figure 4-1, following page) to tell WebScanX which files to scan for viruses and what to do when it finds one.

To open the WebScanX Properties dialog box, click one of the WebScanX activity icons, then choose Properties from the shortcut menu that appears. You'll find the WebScanX icons in one of the following locations:

- When running under Windows 95 and Windows NT 4.0, WebScanX displays its icons in the taskbar's system tray on the bottom right corner of your screen. Right-click any of these icons to reveal its shortcut menu.
- When running under Windows NT 3.51, WebScanX displays its icons on the desktop, at the bottom left corner of your screen. Click any of these icons to reveal its shortcut menu.

4 Configuring E-mail Scan Properties

What is E-mail Scanning?

Although each of the activity icons represents a different program component, you may open the Properties dialog box from any of them.

The WebScanX Properties dialog box appears with the E-mail Scan property page chosen (Figure 4-1).

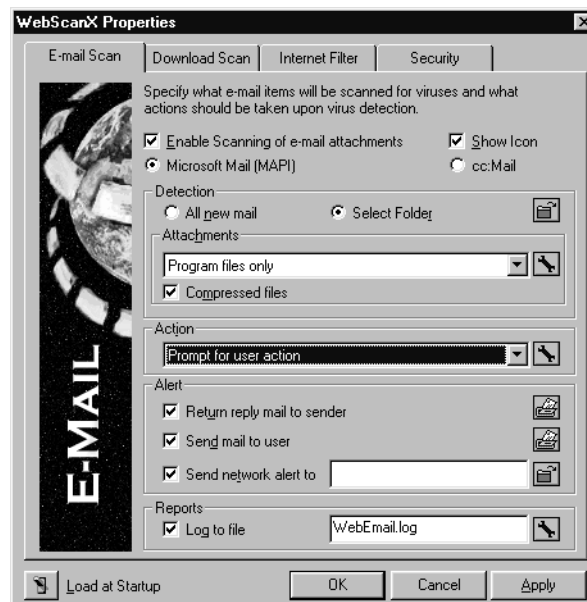




Figure 4-1. E-mail Scan Property Page

4 Configuring E-mail Scan Properties

What is E-mail Scanning?

To configure your settings, follow these steps:



Step	Action
1.	<p>Select the Enable Scanning of E-mail Attachments checkbox to tell WebScanX to scan for viruses in attachments to e-mail messages you receive.</p> <p> <i>When the checkbox is clear, this feature is disabled. You may also disable e-mail scanning from the Status dialog box or by choosing Disable from the shortcut menu that corresponds to this scan type.</i></p>
2.	<p>Select the Show Icon checkbox to display the activity icon for this scan type in the taskbar's system tray or on the Windows NT 3.51 desktop.</p>
3.	<p>Specify which e-mail client software you use by selecting one of the following:</p> <ul style="list-style-type: none">■ Microsoft Mail (MAPI). WebScanX scans messages that you receive from the Internet via Microsoft Mail, or via any MAPI-compliant e-mail client software.■ cc:Mail. WebScanX scans messages that you receive from the Internet via Lotus cc:Mail. <p> <i>WebScanX scans e-mail messages you receive from the Internet—that is, from outside your local area network and your internal mail system. It does not scan messages you receive from within your internal mail system unless that system uses an Internet mail protocol to send and receive mail.</i></p>


4 Configuring E-mail Scan Properties


What is E-mail Scanning?

Setting detection options

To configure WebScanX e-mail virus detection, follow these steps:


- | Step | Action |
|------|--|
| 1. | <p>If you use Lotus cc:Mail, specify how often WebScanX should scan your Inbox. Enter the amount of time between scans in seconds.</p> <p> <i>You can set your Lotus cc:Mail client to poll the cc:Mail server regularly to check for new mail. If you do so, you should set WebScanX to scan your mailbox about twice as frequently as the cc:Mail client does. See the cc:Mail documentation to learn how to set the client software's polling frequency.</i></p> |
| 2. | <p>If you use Microsoft Mail or a MAPI-compliant mail client, select one of the following:</p> <ul style="list-style-type: none">▪ All New Mail. This tells WebScanX to scan all new mail you receive.▪ Select Folder. This tells WebScanX to scan only mail that you receive in a particular folder that you specify. Click  to designate a specific folder. |

WebScanX opens a dialog box you can use to choose a directory or create a new folder within an existing directory. Click the folder you want to use to select it for WebScanX's use. Selected folders look like this . Click the Include Subfolders checkbox to tell WebScanX to examine files deposited into subfolders of the folder you've chosen.

 *If you have not yet logged on to your mail system, WebScanX first asks you to create or specify a user profile it can use to log on to your e-mail system. If you see your user profile listed, choose it, then click OK to close the Choose Profile dialog box. To learn more about how to set up your user profile, consult the documentation for Microsoft Messaging.*

4 Configuring E-mail Scan Properties

What is E-mail Scanning?

3. Specify whether you want WebScanX to examine all file attachments you receive with your e-mail, or only those that are most susceptible to virus infection, by choosing one of these options from the Attachments list:
 - **All Attachments.** This tells WebScanX to scan every attachment that you receive along with your e-mail. This option is your best protection against infection, but it may lengthen the time it takes to scan your entire Inbox.
 - **Program Files Only.** This tells WebScanX to scan only those files most susceptible to virus infection. Click  to specify the filename extensions that WebScanX uses to identify these files.

Response: The Program File Extensions dialog box appears (Figure 4-2).

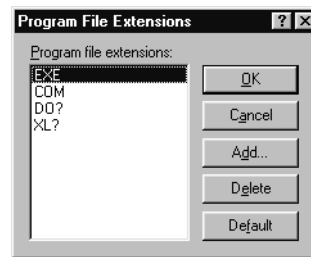



Figure 4-2. Program Extensions Dialog Box

-  *By default, WebScanX identifies files with the extensions .COM, .EXE, .DO? and .XL? as those most susceptible to virus infection. It uses the extensions .DO?, and .XL? to identify Microsoft Word and Excel document and template files, which can contain macro viruses. The ? character is a wildcard.*
- To add a file extension, click Add. Type your new file extension in the dialog box that appears, then click OK. Repeat this procedure until you have entered all of the extensions you want WebScanX to check.
 - To delete an extension, highlight it, then click Delete.
 - To return the extension list to its default state, click Default.

When you finish editing the file extension list, click OK.


4 Configuring E-mail Scan Properties

What is E-mail Scanning?

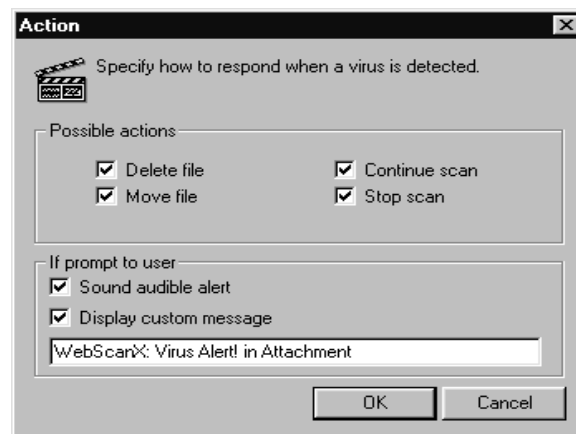
4. Select the Compressed Files checkbox to scan files compressed with PKLITE, LZEXE, PKZIP, LHA, or WinZip.

Responding to infections

To tell WebScanX what to do when it finds a virus in a file attached to an e-mail message, choose a response from the Action list. Your choices are:

- **Prompt for User Action.** Use this option if you expect to be at your computer when WebScanX scans your e-mail. Click  to specify which responses WebScanX will offer you when it finds a virus.

Response: The Action dialog box appears (Figure 4-3).




**Figure 4-3. Action Dialog Box
for Prompt for User Action option**

- ❑ Select the options you want to see when WebScanX detects a virus. Possible actions are: Delete File, Move File, Continue Scan, and Stop Scan.
- ❑ To tell WebScanX to beep when it finds a virus, select the Sound Audible Alert checkbox.
- ❑ To tell WebScanX to display a custom message when it finds a virus, select the Display Custom Message checkbox. Type the message you want to see in the text box provided.

4 Configuring E-mail Scan Properties

What is E-mail Scanning?

- ❑ Click OK to save your settings and return to the E-mail Scan property page. Click Cancel to close the Action dialog box without saving your changes.
- **Move Infected Files to a Folder.** Use this option to tell WebScanX to move infected files to a “quarantine” directory. Click  to choose or create the directory you want to use.

Response: The Action dialog box appears (Figure 4-4).

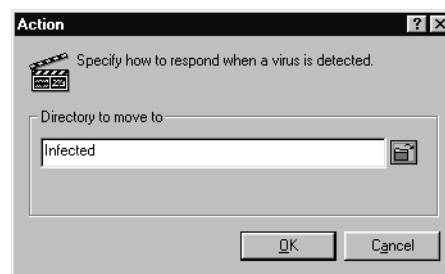





Figure 4-4. Action Dialog Box for Move Infected File option

- ❑ Type a filename and path for your quarantine directory in the text box beneath the label Possible Actions. By default, WebScanX creates a folder in its program directory and gives it the name **Infected**.
 - ❑ To choose a different folder, click . WebScanX opens a dialog box you can use to choose a directory or create a new folder within an existing directory. Click the folder you want to use to select it for WebScanX's use. Selected folders look like this .
-  *If you have not yet logged on to your mail system, WebScanX first asks you to create or specify a user profile it can use to log on to your e-mail system. If you see your user profile listed, choose it, then click OK to close the Choose Profile dialog box. To learn more about how to set up your user profile, consult the documentation for Microsoft Messaging.*
- **Delete Infected Files.** Use this option to tell WebScanX to delete infected files as soon as it detects them.


4 Configuring E-mail Scan Properties

What is E-mail Scanning?

- **Continue Scanning.** Use this option if you plan to leave your computer unattended while WebScanX checks for viruses. If you also activate the WebScanX logging feature (following page), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

Sending alert messages

To tell WebScanX to send alert messages to other users when it finds a virus in your e-mail, follow these steps:

- | Step | Action |
|------|---|
| 1. | To send an alert message to the person who sent you an infected file, select the Return Reply Mail to Sender checkbox. Click  to specify the contents of the message WebScanX sends when it finds a virus. |

Response: The Return Mail Configuration dialog box appears (Figure 4-5).

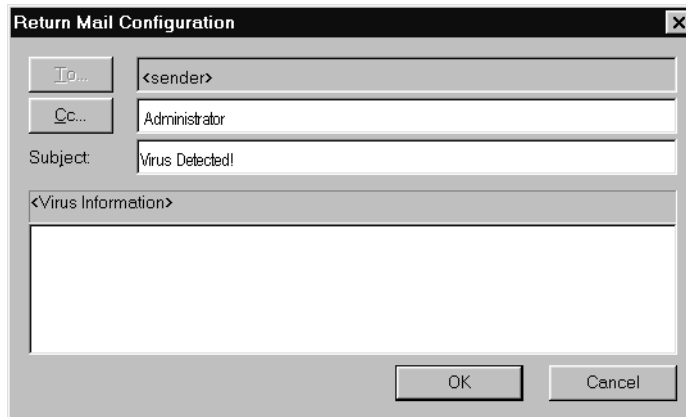



Figure 4-5. Return Mail Configuration Dialog Box

Type a subject for the message, then enter any comments or other text you want to include in the area below the virus information WebScanX sends automatically. You may enter a message up to 1024 characters long. To send a copy of this message to another person, enter an e-mail address in the text box labeled CC. When you finish, click OK.


4 Configuring E-mail Scan Properties


What is E-mail Scanning?

2. Select the Send Mail to User checkbox to send an alert message to another user. Click  to specify the contents and the recipients of the message WebScanX sends when it finds a virus.

Response: The Send Mail to User Configuration dialog box appears.


Type a subject for the message, then enter any comments or other text you want to include in the area below the virus information WebScanX sends automatically. You may enter a message up to 1024 characters long. Enter the e-mail address for each person that you want to receive a copy of this message in the text box labeled To. To send copies of this message to other people, enter e-mail addresses in the text box labeled CC. When you finish, click OK.

3. To tell WebScanX to send a network alert to a server running NetShield, McAfee's server anti-virus solution, select the Send Network Alert To checkbox, then enter the path to the alert file or click  to browse for the correct directory.

 *The directory you choose should contain CENTALRT.TXT, the Centralized Alerting file. To learn more about Centralized Alerting, see the NetShield User's Guide.*

Logging WebScanX actions

To keep a log that details which files WebScanX found viruses in, the names of the infecting viruses, and the actions WebScanX took to respond to the infection, follow these steps:

1. Select the Log to file checkbox.
2. Click  to open the Activity Logging dialog box.

4 Configuring E-mail Scan Properties

What is E-mail Scanning?

Response: The Activity Logging dialog box appears (Figure 4-6).

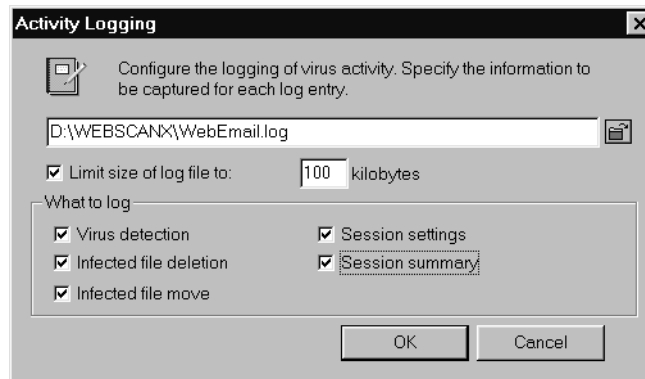




Figure 4-6. Activity Logging Dialog Box

3. Type the filename and path for your log file in the text box provided, or click  to designate a location to store it.
4. Select the Limit Size of Log File checkbox to keep the log file from using excessive hard disk space. Specify a size between 10KB and 999KB. By default, WebScanX sets a limit of 100KB.
5. Select what you want WebScanX to record. Available options are: Virus Detection, Infected File Deletion, Infected File Move, Session Settings, and Session Summary.
6. Click OK to save your changes and close the Activity Logging dialog box.

Click Apply to save the settings you chose for e-mail scanning without leaving the E-mail Scan property page. To save your settings and close the WebScanX Properties dialog box, click OK. To close the Properties dialog box without saving any changes, click Cancel.

 *Clicking Cancel will not undo any changes you have already saved by clicking Apply.*

5

Configuring Download Scan Properties

What is Download Scanning?

WebScanX automatically scans files you download or receive from the Internet, either when you use a Web browser or when you use e-mail client software that receives messages from an Internet mail account. WebScanX works in conjunction with any of these Web browsers:

- **Netscape Navigator**
- **Microsoft Internet Explorer**
- **SPRY Mosaic**
- **America Online Web Browser**

WebScanX tells you when it finds a virus, then gives you the option to delete the infected file or save it to a quarantine folder on your hard disk. If you decide to save files in which WebScanX has detected viruses, we strongly recommend that you use McAfee's VirusScan software to clean the infected files.

Configuring Download Scan options

Use the Download Scan property page to tell WebScanX which files to scan for viruses among those you receive or download from the Internet and what the program should do when it finds a virus.

5 Configuring Download Scan Properties

What is Download Scanning?

To open the WebScanX Properties dialog box, click one of the WebScanX activity icons, then choose Properties from the shortcut menu that appears. You'll find the WebScanX icons in one of the following locations:

- When running under Windows 95 and Windows NT 4.0, WebScanX displays its icons in the taskbar's system tray to the left of the clock. Right-click any of these icons to reveal its shortcut menu.
- When running under Windows NT 3.51, WebScanX displays its icons on the desktop, at the bottom left corner of your screen. Click any of these icons to reveal its shortcut menu.

Although each of the activity icons represents a different program component, you may open the Properties dialog box from any of them.

Response: The WebScanX Properties dialog box appears.

Click the Download Scan tab to display the correct property page (Figure 5-1).

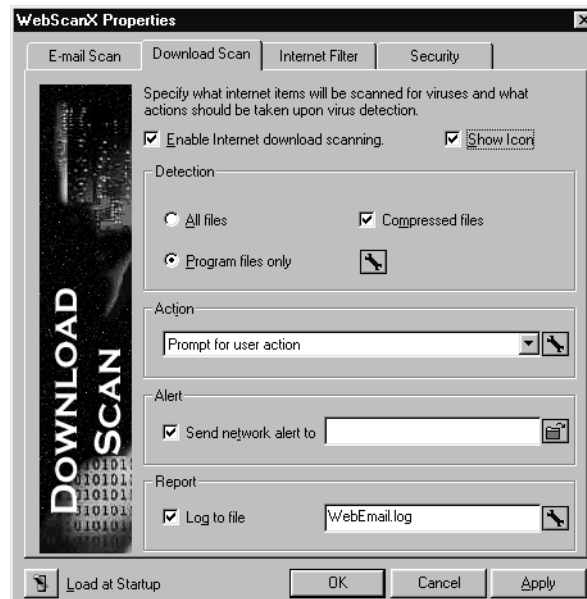



Figure 5-1. Download Scan Property Page

5 Configuring Download Scan Properties


What is Download Scanning?

To configure download scan options, follow these steps:

Step	Action
1.	Select the Enable Internet Download Scanning checkbox to tell WebScanX to scan for viruses in files you receive or download from the Internet.  <i>When the checkbox is clear, this feature is disabled. You may also disable download scanning from the Status dialog box or by choosing Disable from the shortcut menu that corresponds to this scan type.</i>
2.	Select the Show Icon checkbox to display the activity icon for this scan type in the taskbar's system tray or on the Windows NT 3.51 desktop.

Setting detection options

To configure WebScanX virus detection for files you receive or download from the Internet, follow these steps:

Step	Action
1.	<p>Specify whether you want WebScanX to examine all files you receive or download, or only those most susceptible to virus infection, by choosing one of these options from the Attachments list:</p> <ul style="list-style-type: none">▪ All Files. This tells WebScanX to scan every file that you receive or download. This option is your best protection against infection, but it may lengthen the time it takes to download a series of files at once.▪ Program Files Only. This tells WebScanX to scan only the files that are most susceptible to virus infection. Click  to specify the filename extensions that WebScanX uses to identify these files. <p>Response: The Program File Extensions dialog box appears (Figure 5-2, following page).</p>

5 Configuring Download Scan Properties

What is Download Scanning?

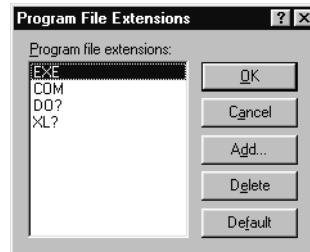



Figure 5-2. Program Extensions Dialog Box

 By default, WebScanX identifies files with the extensions .COM, .EXE, .DO? and .XL? as most susceptible to virus infection. It uses the extensions .DO?, and .XL? to identify Microsoft Word and Excel document and template files, which can contain macro viruses. The ? character is a wildcard.

- ❑ To add a file extension, click Add. Type your new file extension in the dialog box that appears, then click OK. Repeat this procedure until you have entered all of the extensions you want WebScanX to check.
- ❑ To delete an extension, highlight it, then click Delete.
- ❑ To return the extension list to its default state, click Default.

When you finish editing the file extension list, click OK.


2. Select the Compressed Files checkbox to scan files compressed with PKLITE, LZEXE, PKZIP, LHA, or WinZip.

5 Configuring Download Scan Properties

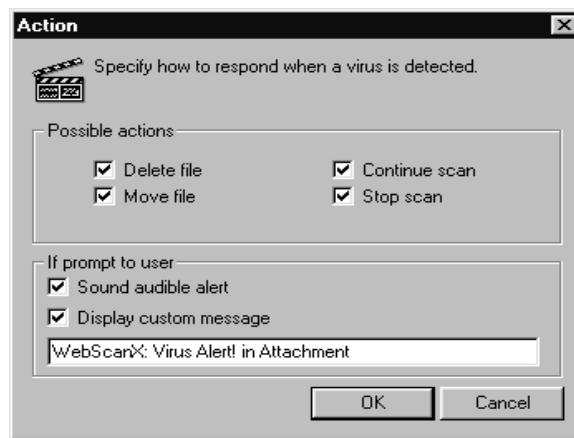
What is Download Scanning?

Responding to infections

To tell WebScanX what to do when it finds a virus in a file you've received or downloaded, choose a response from the Action list. Your choices are:

- **Prompt for User Action.** Use this option if you expect to be at your computer when WebScanX scans incoming files. Click  to specify which responses WebScanX will offer you when it finds a virus.

Response: The Action dialog box appears (Figure 5-3).




**Figure 5-3. Action Dialog Box
for the Prompt for User Action Option**

- ❑ Select the options you want to see when WebScanX detects a virus. Possible actions are: Delete File, Move File, Continue Scan, and Stop Scan.
- ❑ To tell WebScanX to beep when it finds a virus, select the Sound Audible Alert checkbox.
- ❑ To tell WebScanX to display a custom message when it finds a virus, select the Display Custom Message checkbox. Type the message you want to see in the text box provided.
- ❑ Click OK to save your settings and return to the Download Scan property page. Click Cancel to close the Action dialog box without saving your changes.

5 Configuring Download Scan Properties

What is Download Scanning?

- **Move Infected Files to a Folder.** Use this option to tell WebScanX to move infected files to a “quarantine” directory. Click  to choose or create the directory you want to use.

Response: The Action dialog box appears (Figure 5-4).

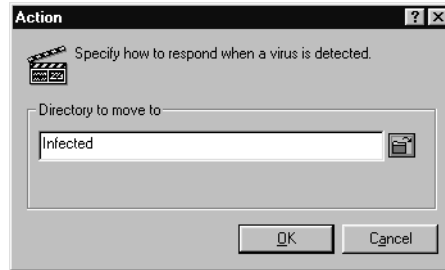




Figure 5-4. Action Dialog Box for the Move Infected File Option


- Type a filename and path in the text box beneath the label Possible Actions. This path can be relative. For example, if you leave the default designation **Infected** in the text box, WebScanX creates a folder with this name, then moves any infected files it finds to this new folder.
- Click  to designate the folder you want to use for your quarantine directory. Click OK to close the Action dialog box once you have chosen a folder to use.
- **Delete Infected Files.** Use this option to tell WebScanX to delete infected files as soon as it detects them.

5 Configuring Download Scan Properties

What is Download Scanning?


Sending network alerts

To tell WebScanX to send a network alert to a server running NetShield, McAfee's server anti-virus solution, select the Send Network Alert To checkbox, then enter the path to the alert file or click  to designate the correct directory.

 *The directory you choose should contain CENTALRT.TXT, the Centralized Alerting file. To learn more about Centralized Alerting, see the NetShield User's Guide.*

Logging WebScanX actions

To keep a log that details which files WebScanX found viruses in, the names of the infecting viruses, and the actions WebScanX took to respond to the infection, follow these steps:

1. Select the Log to File checkbox.
2. Click  to open the Activity Logging dialog box.

Response: The Activity Logging dialog box appears (Figure 5-5).

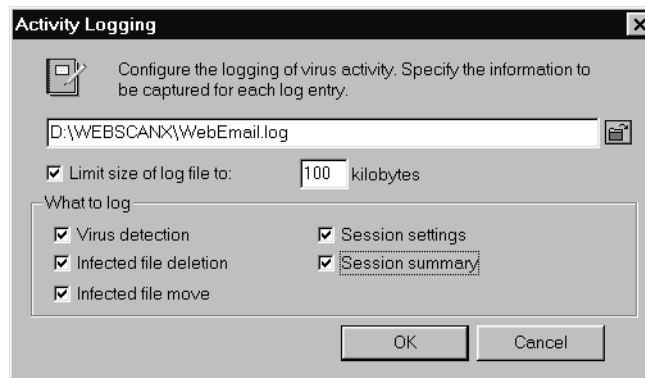



Figure 5-5. Activity Logging Dialog Box


3. Type the filename and path for your log file in the text box provided, or click  to designate a location to store it.

5 Configuring Download Scan Properties

What is Download Scanning?

4. Select the Limit Size of Log File checkbox to keep the log file from using excessive hard disk space. Specify a size between 10KB and 999KB. By default, WebScanX sets a limit of 100KB.
5. Select what you want WebScanX to record. Available options are: Virus Detection, Infected File Deletion, Infected File Move, Session Settings, and Session Summary.
6. Click OK to save your changes and close the Activity Logging dialog box.

Click Apply to save the settings you chose for download scanning without leaving the Download Scan property page. To save your settings and close the WebScanX Properties dialog box, click OK. To close the Properties dialog box without saving any changes, click Cancel.

 *Clicking Cancel will not undo any changes you already saved by clicking Apply.*

6

Configuring Internet Filter Properties

What is Internet Filtering?

WebScanX automatically scans each website you visit and scrutinizes any Java classes and ActiveX controls you encounter for potential danger by comparing them with an internal database of classes and controls known to cause harm. Depending on how you configure it, WebScanX can automatically keep any harmful items it finds away from your system, or it can ask you whether you want to let them through.

With WebScanX, you can benefit from the interactive features available at some websites without worrying about possible harm to your system, and without needing to turn off Java or ActiveX access in your browser software.

Configuring Internet filtering

Use the Internet Filter property page to tell WebScanX which items to scan for potential harm, which sites to block and what to do when it locates danger.

To open the WebScanX Properties dialog box, click one of the WebScanX activity icons, then choose Properties from the shortcut menu that appears. You'll find the WebScanX icons in one of the following locations:

- When running under Windows 95 and Windows NT 4.0, WebScanX displays its icons in the taskbar's system tray, to the left of the clock. Right-click any of these icons to reveal its shortcut menu.
- When running under Windows NT 3.51, WebScanX displays its icons on the desktop, at the bottom left corner of your screen. Click any of these icons to reveal its shortcut menu.

6 Configuring Internet Filter Properties

What is Internet Filtering?

Although each of the activity icons corresponds to a different program component, you may open the Properties dialog box from any of them.

Response: The WebScanX Properties dialog box appears.

Click the Internet Filter tab to display the correct property page (Figure 6-1).



Figure 6-1. Internet Filter Property Page

To configure Internet filter options, follow these steps:

- | Step | Action |
|------|---|
| 1. | Select the Enable Java & ActiveX Filter checkbox to tell WebScanX to look for potentially harmful Java classes and ActiveX controls.

<i>✍ When the checkbox is clear, this feature is disabled. You may also disable Internet filtering from the Status dialog box or by choosing Disable from the shortcut menu that corresponds to this scan type.</i> |
| 2. | Select the Show Icon checkbox to display the activity icon for this scan type in the taskbar's system tray or on the Windows NT 3.51 desktop. |

6 Configuring Internet Filter Properties

What is Internet Filtering?


Setting detection options


To configure WebScanX to detect harmful Java classes, ActiveX controls, or dangerous Internet sites, follow these steps:

Step	Action
1.	Specify what you want WebScanX to examine. Select either or both of these options: <ul style="list-style-type: none">▪ ActiveX Controls. Select this button to have the program look for harmful ActiveX or .OCX controls.▪ Java Classes. Select this button to have the program look for harmful Java classes, or applets written in Java.
2.	To block access to Internet sites you know are dangerous, select either or both of the following options: <ul style="list-style-type: none">▪ IP Addresses. Select this checkbox to block access to Internet sites you identify with IP address numbers.▪ Host Names. Select this checkbox to block access to Internet sites you identify with a Uniform Resource Locator (URL). An example of a website URL is www.mydomain.com.

Adding IP addresses or host names

To add an IP address or a URL to the list of Internet sites that WebScanX prevents your browser software from visiting, choose the type of addressing scheme you want to use to designate the site—by IP address or by host name—then follow the steps below.

 *McAfee suggests that you enter a site's URL designation, rather than its IP address, to add it to WebScanX's "banned" list. A URL address is generally a more reliable way to keep track of a site's actual location than a fixed IP address is because the Internet's domain name server system gives you access to a site's current IP address even when it has changed or moved.*

Step	Action
1.	Click  to open the Banned IP Addresses dialog box or the Banned Domain Names dialog box.

6 Configuring Internet Filter Properties

What is Internet Filtering?

2. Click Add to open the Add IP Address dialog box or the Add Domain Name dialog box.
3. To use IP addresses to designate a forbidden site, enter an IP address in the first text box shown. If you know the subnet mask for the site you want to block, enter it in the text box below. The subnet mask defines a range of IP addresses included within a network on the Internet.

An example of a correctly formatted IP address is **123.456.789.10**. If you do not know the subnet mask for the site you want to enter, leave the default value shown.

4. To use domain name addressing to designate a forbidden site, enter the URL for the site in the text box provided.

An example of a URL correctly formatted for WebScanX's use is **www.mydomain.com**. Do not include **http://** or other transport protocol designations in your entry.

5. Click OK to close the Add IP Address or the Add Domain Name dialog box.
6. Repeat steps 2 through 5 to add other IP addresses or domain names to the banned addresses list. The addresses you add to the list appear in the Banned IP Addresses dialog box or in the Banned Domain Names dialog box. To delete any address shown, select it, then click Delete.
7. When you have finished, click OK to return to the Internet Filter property page.


6 Configuring Internet Filter Properties

What is Internet Filtering?


Responding to harmful objects


To tell WebScanX what to do when it encounters a potentially harmful Java class or ActiveX control, choose a response from the Action list. Your choices are:

- **Prompt for User Action.** Choose this to have WebScanX ask you what you want to do when it finds a potentially harmful Java class or ActiveX control.
- **Deny Access to Objects.** Choose this to have WebScanX automatically keep harmful objects away from your computer system.

 *McAfee strongly recommends that you select Deny Access to Objects. This selection allows for no user options, but is the safest choice because it automatically denies access to dangerous objects that you might not even know are present.*


Sending network alerts

To tell WebScanX to send a network alert to a server running NetShield, McAfee's server anti-virus solution, select the Send Network Alert To checkbox, then enter the path to the alert file or click  to browse for the correct directory.

 *The directory you choose should contain CENTALRT.TXT, the Centralized Alerting file. To learn more about Centralized Alerting, see the NetShield User's Guide.*

Logging WebScanX actions

To keep a log that details WebScanX actions during your browsing session:

1. Select the Log to file checkbox.
2. Click  to open the Activity Logging dialog box.

6 Configuring Internet Filter Properties

What is Internet Filtering?

Response: The Activity Logging dialog box appears (Figure 6-2).

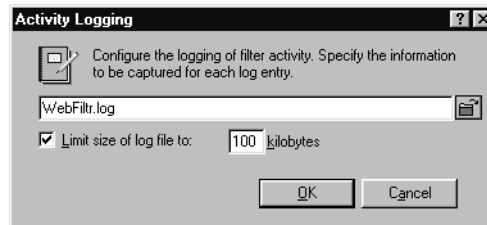




Figure 6-2. Activity Logging Dialog Box

3. Type the filename and path for your log file in the text box provided, or click  to browse for a location to store it.
4. Select the Limit Size of Log File checkbox to keep the log file from using excessive hard disk space. Specify a size between 10KB and 999KB. By default, WebScanX sets a limit of 100KB.
5. Click OK to save your changes and close the Activity Logging dialog box.

Click Apply to save the settings you chose for Internet filtering without leaving the Internet Filter property page. To save your settings and close the WebScanX Properties dialog box, click OK. To close the Properties dialog box without saving any changes, click Cancel.

 *Clicking Cancel will not undo any changes you already saved by clicking Apply.*

7

Configuring WebScanX Security Properties

What is WebScanX Security?

WebScanX lets you set a password to protect the settings you chose in each of the property pages. This feature is particularly useful if you are a system administrator and you want to keep users from tampering with your security measures by changing WebScanX settings.

Configuring WebScanX security

Use the Security property page to keep your WebScanX settings safe from unauthorized changes.

To open the WebScanX Properties dialog box, click one of the WebScanX activity icons, then choose Properties from the shortcut menu that appears. You'll find the WebScanX icons in one of the following locations:

- When running under Windows 95 and Windows NT 4.0, WebScanX displays its icons in the taskbar's system tray to the left of the clock. Right-click any of these icons to reveal its shortcut menu.
- When running under Windows NT 3.51, WebScanX displays its icons on the desktop, at the bottom left corner of your screen. Click any of these icons to reveal its shortcut menu.

Although each of the activity icons corresponds to a different program component, you may open the Properties dialog box from any of them.

Response: The WebScanX Properties dialog box appears.

7 Configuring WebScanX Security Properties

What is WebScanX Security?



Click the Security tab to display the correct property page (Figure 7-1).




Figure 7-1. Security Property Page

To configure WebScanX security options, follow these steps:

- | Step | Action |
|-------------|---|
| 1. | Select the settings you want to protect in the list shown.

You may protect any or all of WebScanX's property pages. Protected property pages display a locked padlock icon  in the security list shown in Figure 7-1. To remove protection from a property page, click the locked padlock icon to unlock it  . |
| 2. | Click Password to open the Specify Password dialog box. |
| 3. | Enter a password in the first text box shown, then enter the same password again in the text box below to confirm your choice. |
| 4. | Click OK to close the Specify Password dialog box. |

Click Apply to save the settings you chose for security without leaving the Security property page. To save your settings and close the WebScanX Properties dialog box, click OK. To close the Properties dialog box without saving any changes, click Cancel.

 *Clicking Cancel will not undo any changes you already saved by clicking Apply.*

8

Using WebScanX for Windows 3.1x

Introducing WebScanX for Windows 3.1x

WebScanX for Windows 3.1x has many of the same features found in WebScanX for Windows 95 and Windows NT, including the ability to scan for viruses in e-mail messages and attachments you receive from the Internet, using identical virus scanning technology. WebScanX also scans files you download with the 16-bit versions of any of these web browsers:

- **Netscape Navigator**
- **Microsoft Internet Explorer**
- **SPRY Mosaic**
- **America Online Web Browser**

The interface for WebScanX for Windows 3.1x, however, differs substantially from the interface for the Windows 95 and Windows NT versions described earlier in this manual. Where the other WebScanX versions require configuration to determine which files they scan and how they respond when they detect infections, WebScanX for Windows 3.1x uses a pre-programmed set of scanning and response options. It scans all incoming e-mail messages and attachments you receive from the Internet through the mail client built into your browser software, or through 16-bit versions of Lotus cc:Mail, and deposits infected files automatically into a quarantine directory.

Other differences between WebScanX for Windows 3.1x and the other WebScanX versions include:

- **Internet Filtering.** WebScanX for Windows 3.1x does not filter Java classes, ActiveX controls, or Internet sites.
- **Network Notification.** WebScanX for Windows 3.1x can notify your Lotus cc:Mail administrator when it finds a virus in e-mail delivered to your Inbox. It cannot, however, issue a network alert to a server running NetShield, McAfee's server anti-virus solution.
- **Other Alerts.** WebScanX for Windows 3.1x does not automatically send alert messages to the person who sent you a message that carried a virus—or to other users—when it detects an infection.
- **Security.** WebScanX for Windows 3.1x does not use password protection.
- **Responses.** WebScanX for Windows 3.1x automatically moves infected files to a quarantine directory called **Infected Files**.
- **Logging.** WebScanX for Windows 3.1x does not include logging features.
- **Supported E-mail Clients.** WebScanX for Windows 3.1x supports e-mail clients included with the supported browsers listed earlier and 16-bit versions of Lotus cc:Mail. It does not, however, support 16-bit MAPI-compliant mail clients.

Configuring WebScanX for Windows 3.1x

During installation, WebScanX asks you to set configuration options for your Lotus cc:Mail client software in the dialog box shown in Figure 8-1. If you do not use Lotus cc:Mail, click Cancel to close this dialog box and skip to the next section of this manual.

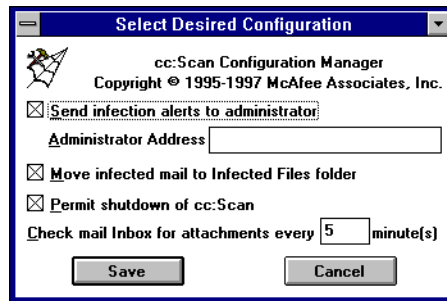


Figure 8-1. The cc:Scan Configuration Manager Dialog Box

Otherwise, follow the steps below to configure WebScanX for Windows 3.1x to scan for viruses in messages you receive from the Internet via cc:Mail:

- | Step | Action |
|-------------|--|
| 1. | Click the Send Infection Alerts to Administrator checkbox to to inform your cc:Mail administrator whenever WebScanX detects a virus in your Inbox. |

Next, enter your administrator's e-mail address in the text box provided. WebScanX sends a standard alert message to this address each time it finds a virus in an e-mail attachment.

- | | |
|-----------|---|
| 2. | Click the Move Infected Mail to Infected Files Folder checkbox to tell WebScanX to move any files that contain viruses to its default quarantine directory. You may delete infected files from this directory at your next opportunity. |
|-----------|---|

Clearing this checkbox tells WebScanX only to inform your cc:Mail administrator when it detects a virus, if you have chosen that option. If you have not, WebScanX takes no action when it detects a virus.

3. Click the Permit Shutdown of cc:Scan checkbox to give yourself the option to stop WebScanX from scanning your cc:Mail Inbox.
4. Enter the amount of time WebScanX should wait between each scan, in minutes, in the text box provided.
5. Click OK to save your settings and close the cc:Scan Configuration Manager dialog box. Click Cancel to close the dialog box without saving any settings.

To change any of the settings you chose, go to the Windows Program Manager, then locate the cc:Scan Configuration Manager program icon in the McAfee WebScanX program group. Double-click the icon to open the Configuration Manager dialog box.

Starting and Quitting WebScanX for Windows 3.1x

Once installed, WebScanX runs automatically as soon as you restart Windows 3.1x. The program might ask you to log on to your cc:Mail mailbox if you have not yet done so. Enter the path to your mailbox, your user name, and your password in the text boxes provided, then click OK to continue. If you do not use cc:Mail, WebScanX simply starts and runs as a Terminate and Stay Resident (TSR) program in your computer's memory.

If you have chosen configuration settings in the cc:Mail Configuration Manager dialog box, WebScanX uses those settings when scanning attachments you receive via cc:Mail. Otherwise, WebScanX runs with a default set of options that tells it to scan all incoming mail you receive from the Internet and move files that contain viruses to its Infected Files folder.

While active, WebScanX displays a minimized icon on the Windows 3.1x desktop at the lower left corner of your screen. To quit WebScanX for Windows 3.1x, click this icon, then choose Close from the menu that appears. To start WebScanX again without restarting Windows, go to the Windows Program Manager, then locate the WebScanX program icon in the McAfee WebScanX program group. Double-click the icon to restart WebScanX.

To disable the program's "autoload" feature and prevent WebScanX for Windows 3.1x from starting when Windows does, you must remove the line in your `win.ini` file that reads

```
load=c:\mcafee\webscanx\webscn16.exe
```

You should find this line in the `[windows]` section of the file. To restore the autoload feature, replace this line in the file.

A


Preventing Virus Infection

Keys to a Secure System Environment

WebScanX is an effective tool for preventing virus infections and harm from Java classes, ActiveX controls, and dangerous Internet sites. It is most effective, however, when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

To create a secure system environment and minimize your chance of infection, McAfee recommends that you

- Install WebScanX and other McAfee anti-virus software
- Create a shortcut to webscanx.exe and place it in your Windows StartUp folder so that WebScanX starts automatically whenever Windows does.

 *The WebScanX installer automatically sets WebScanX to run when Windows finishes its startup if you followed the recommended installation procedures. To configure WebScanX to start when Windows 3.1x or Windows NT 3.51 loads, you might need to alter your AUTOEXEC.BAT file. See your Windows documentation for more details.*

- Make frequent backups of important files. Even with WebScanX scanning for viruses, some viruses (as well as fire, theft, or vandalism) can render data unrecoverable without a recent backup.

Detecting New and Unknown Viruses

There are two ways for you to deal with new and unknown viruses and harmful applets that might affect your system:

- Update your WebScanX virus data files
- Update your WebScanX Internet filter data files

Updating your WebScanX data files

To offer the best virus protection possible, McAfee continually updates the files WebScanX uses to detect viruses and harmful applets. After a certain time period, WebScanX will notify you to update its virus definition, or .DAT, file. For maximum protection, you should update these files on a regular basis.

Why would I need a new data file?

New viruses and harmful applets are discovered at a rate of more than 200 per month. Often, older data files cannot assist WebScanX in detecting these new variations. The data files that came with your copy of WebScanX, for example, may not detect a virus or harmful Java applet that was discovered after you bought the product.

McAfee's virus researchers are working constantly to update these data files with more and better virus definitions and with lists of Java classes and ActiveX controls known to cause harm. New data files are released monthly.

 *McAfee cannot guarantee that the WebScanX .DAT files included with this release will work with previous WebScan or WebScanX versions.*

Using SecureCast electronic updating

McAfee's SecureCast software gives you several options for keeping your WebScanX installation up-to-date, with varying levels of user interaction. One option, which uses BackWeb's Internet "push" technology, automatically updates your installation on a regular basis. If you choose this option, you will install BackWeb's client software, which performs invisible downloads of updates whenever you are connected to the Internet. If you are not connected long enough for a full download at one time, the software automatically pieces out the work and notifies you when a complete update package has arrived.


You can also wait until WebScanX warns you it is time to update, then use the convenient one-button electronic update option available at that time. Or you can choose to update your files manually at any time by following the procedure below. Information on SecureCast is available from the McAfee Web Site.

Updating your data files manually

You can use either of the following methods to update your data files without using SecureCast:


- **Use one-button updating.** WebScanX suggests that you update your data files with a notice that appears approximately every 30 days. Click the Update button you see on this notice to connect directly to the McAfee Web Site.
- **Connect to the McAfee Web Site whenever you wish.** Start your favorite browser software, then go to <http://www.McAfee.com> to download the latest data files and read up-to-the-minute news.

Once you've connected, follow the steps below to download and install your new data files.

 *Please note that your access to these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.*

- | Step | Action |
|------|--|
| 1. | Download the data file (for example, DAT-3007.ZIP) from one of McAfee's electronic services. On most services, you'll find it in the anti-virus area. |
| 2. | Copy the file to a new directory. |
| 3. | The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don't have the decompression software, you can download PKUNZIP (shareware) from one of McAfee's electronic sites. |
| 4. | Locate the directories on the hard drive where WebScanX is currently installed. Typically, the files are stored in

C:\Program Files\McAfee\WebScanX |
| 5. | Copy the new files into the appropriate directory or directories, overwriting the old data files.

<i> There might be part of the software in more than one directory. If so, place each updated file in the appropriate directory.</i> |
| 6. | Reboot your computer so that changes take place immediately. |

Reporting new items for WebScanX updates

McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new Java classes, ActiveX controls, dangerous websites, or viruses that WebScanX does not now detect. Please note that McAfee reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:


- | | |
|-----------------------|--|
| ResearchX@McAfee.com | Use this address to report harmful ActiveX controls and Java classes, or dangerous Internet sites. |
| AVResearch@McAfee.com | Use this address to report new virus strains. |

B

McAfee Support Services

McAfee offers several flexible support programs to meet your needs. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal support plan, McAfee helps to ensure that you receive the level of technical assistance you require.

McAfee also offers a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, enterprise support, and a Jump Start program. Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you or your business.

 *The term “update” refers only to the virus definition files; the term “upgrade” refers to product version revisions, executables, and definition files. McAfee offers free online virus signature file updates (.DATs) for the life of your product. We cannot, however, guarantee backward compatibility of the signature files with previous versions’ executable files (.EXEs). By upgrading your software to the latest product version and updating to the latest .DAT files regularly, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

Customer Service Programs

Free WebScanX support program

All registered owners of single-node (one computer) WebScanX products purchased at local retail stores or downloaded from the McAfee Web Site, are entitled to:

- Unlimited free online virus updates (new .DAT files) for the life of your product
- One year of unlimited free online product upgrades (product version revisions) with the newest features
- Free support services listed below

Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
 - Automated voice and fax system: (408) 988-3034
 - McAfee BBS (electronic bulletin board system): (408) 988-4004
 - World Wide Web site: <http://www.McAfee.com>
 - CompuServe: GO MCAFEE
 - Microsoft Network: MCAFEE
 - America Online: keyword MCAFEE
- 90 days of free technical support phone assistance, available during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.

Free WebScanX Deluxe support program

All registered owners of single-node (one computer) WebScanX Deluxe products purchased at local retail stores or downloaded from the McAfee Web Site, are entitled to:


- Unlimited free online virus updates (new .DAT files) for the life of the product
- Two years of unlimited free online product upgrades (product version revisions) with the newest features
- Free support services listed below

Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
 - Automated voice and fax system: (408) 988-3034
 - McAfee BBS (electronic bulletin board system): (408) 988-4004
 - World Wide Web site: <http://www.McAfee.com>
 - CompuServe: GO MCAFEE
 - Microsoft Network: MCAFEE
 - America Online: keyword MCAFEE
- 90 days of free technical support phone assistance, available during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally-trained support representatives at (408) 988-3832.

Free subscription maintenance and support program


McAfee offers all registered owners of licensed multiple-node (ten computers or more) subscription products the following free support services and maintenance during the two-year term of the software subscription.

 *You must be a registered owner to receive these services.*

Support services

- Electronic and online support, available 24 hours a day, seven days a week on each of the forums listed below:
 - Automated voice and fax system: (408) 988-3034
 - McAfee BBS (electronic bulletin board system): (408) 988-4004
 - World Wide Web site: <http://www.McAfee.com>
 - CompuServe: GO MCAFEE
 - The Microsoft Network: MCAFEE
 - America Online: keyword MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.–6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Two years of free online product upgrades with the newest features and virus definition data. If you upgrade your operating system, you can also upgrade your product version to one that runs on your new platform.

Optional support plans

 *Contact McAfee for current pricing structures.*


Option 1: One-year personal support plan

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical telephone support, download the latest virus protection updates each month, and periodically download upgrades from any of McAfee's registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product version to one that runs on your new platform.

Option 2: One-year quarterly disk/CD-ROM maintenance and support programs

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of Option 1, while adding a quarterly mailing of software upgrade diskettes or CD-ROMs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus data files without having to download from an online service.

Each optional support plan begins as soon as you purchase the product and is good for one year, at which time you can renew your support program through McAfee's Customer Care department at (408) 988-3832.

 *McAfee reserves the right to change part or all of its Customer Service Programs at any time without notice.*

Professional Services Programs

McAfee Professional Services provide a wide range of on-site services. Whether for short-term assistance or long-term strategic planning, a highly qualified consultant can help you achieve positive results. McAfee consultants are trained on NetWare, Microsoft NT Advanced Server, Windows 95, and a multitude of desktop applications.

Before work begins, a project manager discusses the project scope and objective with you and comes to a mutual agreement on the job objective. When the consultant leaves the site, you can be sure that the objective has been achieved.

Training

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of its computing resources. McAfee offers on-site training on all McAfee products, network management seminars, anti-virus seminars, customized curricula for site-specific applications as well as product and personnel certification. McAfee's consultants provide extensive training with a curriculum tailored to your organization's needs.

Consulting

McAfee Professional Services offer a number of hourly and daily consulting services including:

- Troubleshooting an existing installation
- Writing PowerScript or SaberBASIC scripts
- Planning and designing networks
- Installing and configuring McAfee products
- Configuring Windows 95
- One-on-one consulting

McAfee Professional Services are available on a quotable time and materials basis to perform project management, product research, and a number of other consulting services.

Jump Start program

This fixed-fee consulting program is designed to get clients up and running on McAfee products as soon as possible. It includes training, installation, and configuration services as needed on a single server. It is designed to demonstrate how to connect various PCs to the LAN, train administrators how to use the program, and master the roll-out process.

Enterprise support

McAfee's Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.


The Enterprise Support Program offers the following features:

- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. central time, Monday through Friday
- Five designated McAfee contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount
- VIP issues review list
- Beta site (if desired)

Every Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.

Optional 7 x 24 enterprise support

Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hours.

 *McAfee reserves the right to change part or all of its Professional Services Programs at any time without notice.*

A

- about WebScanX 23
- Action dialog box
 - Move Infected Files to a Folder option 34, 43
 - Prompt for User Action option 33, 42
- ActiveX controls
 - filtering 48
- activity icons, location and appearance of 23
- activity logging 36, 44, 50
- alert messages
 - Centralized Alerting 36, 44, 50
 - reply mail 35
 - sending to other users 36
 - sending to your network administrator 36, 44, 50, 57
- autoload
 - disabling in WebScanX for Windows 3.1x 59
- autoload, enabling and disabling for WebScanX 26

B

- backups, use of in security program 60
- Bulletin Board System (BBS) 15

C

- cc:Mail
 - scanning with WebScanX for Windows 3.1x 57
- cc:Mail checkbox 30
- CENTALRT.TXT 36, 44, 50
- checking scan activity 23
 - WebScanX Status dialog box 24
- closing WebScanX 24, 26
- commands available in shortcut menus 23
- Compressed Files checkbox 33, 41
- configuring options
 - Download Scan 38
 - E-mail Scan 28
 - Internet Filter 46
 - Security 52
- Customer Care
 - contacting 15
 - programs 65

D

- data (.DAT) file, updating 61
- desktop, location of WebScanX activity icons on 23, 28, 38, 46, 52
- disabling WebScanX program components 23, 25
- Display Custom Message checkbox 33, 42
- domain names
 - filtering or blocking 48
- Download Scan options, configuring 38
- download scanning
 - features of 38

E

- E-mail Scan options, configuring 28
- e-mail scanning
 - features of 28
- enabling WebScanX program components 23, 25
- enterprise support 70
- Exit All, shortcut menu command 24, 26



F

filtering

- ActiveX controls 48
- host names or domain names 48
- IP addresses 48
- Java classes 48

G

- getting started with WebScanX 22

H

- hardware requirements for WebScanX 18
- host names
 - filtering or blocking 48

I

- icons
 - activity icons 23
 - security locks 53
- installing WebScanX 19
- Internet
 - dangers from 13
- Internet Filter options, configuring 46
- Internet filtering
 - features of 46
- IP addresses
 - filtering or blocking 48

J

- Java classes
 - filtering 48

L

- load at startup, enabling and disabling 26
- logging
 - Download Scan activity 44
 - E-mail Scan activity 36
 - Internet Filter activity 50
- Lotus cc:Mail
 - scanning with WebScanX for Windows 3.1x 57

M

- McAfee
 - consulting services 69
 - contacting
 - BBS 15
 - Customer Care 15
 - outside the United States 17
 - via America Online 16
 - via CompuServe 15
 - via the Microsoft Network (MSN) 16
 - within the United States 16
 - enterprise support 70
 - jump start program 70
 - support services 64
 - training 16, 69

menus

- displaying 23
- Download Scan 38
- E-mail Scan 28
- Internet Filter 46
- use of Shift key with 24, 26
- Microsoft Mail (MAPI) checkbox 30
- Microsoft Messaging, user profile for 34
- monitoring scan activity 23
- WebScanX Status dialog box 24

N

- NetShield, use of with WebScanX 36, 44, 50
- network alert, sending 36, 44, 50

O

- one button updating 62
- operating system requirements for WebScanX 18

P

- password
 - entering 53
 - using to protect settings 52
- personal support plan 67



professional services
 consulting 69
 enterprise support 70
 jump start program 70
 training 69

program components in
 WebScanX
 Download Scan 22, 38
 E-mail Scan 22, 28
 Internet Filter 22, 46
 Security 22, 52

program file extensions
 adding 32, 41
 default 32, 41

Properties dialog box
 opening 23, 25, 28, 38,
 46, 52

property pages for
 WebScanX
 Download Scan 38, 39
 E-mail Scan 28, 29
 Internet Filter 46, 47
 protecting from
 unauthorized
 changes 53
 Security 52, 53

Q

quarantine directory
 creating or choosing 34,
 43
 default in WebScanX for
 Windows 3.1x 57
quitting WebScanX 24, 26

R

reporting WebScanX
 activity 36, 44, 50
responding to harmful
 objects 50
responding to virus
 infections
 Download Scan 42
 E-mail Scan 33
restarting WebScanX 27

S

scan activity, checking 23
 WebScanX Status
 dialog box 24
SecureCast
 using for updates 62
securing your system
 environment 60
security
 features of 52
Security options, configuring
 52
setting options
 Download Scan 38
 E-mail Scan 28
 Internet Filter 46
 Security 52
setup for WebScanX 19
Shift key, use of with
 shortcut menus 24, 26

shortcut menus
 displaying 23
 Download scan icon 38
 E-mail Scan icon 28
 Internet Filter icon 46
 use of Shift key with 24,
 26
Show Icon checkbox 30, 40
shutting down WebScanX
 for Windows 3.1x 58
software license
 agreement 19
Sound Audible Alert
 checkbox 33, 42
starting WebScanX
 automatically 26
Status dialog box
 appearance of 24
 opening 23
stopping WebScanX scans
 24, 26
subscription maintenance
 program 66
summary of scan activity
 23, 24
Support
 programs 65
switch button, using to
 enable or disable
 autoloading 26
system requirements 18
system tray, WebScanX
 activity icons in 23, 28, 38,
 46, 52



T

- taskbar, location of activity icons in [23](#), [28](#), [38](#), [46](#), [52](#)
- technical support
 - e-mail address [15](#)
 - free support policies [65](#)
 - information needed from user [16](#)
 - McAfee Bulletin Board System (BBS) [15](#)
 - online [15](#), [65](#)
 - programs [64](#)
- Training
 - scheduling [16](#)
- training for McAfee products [16](#)

U

- Uniform Resource Locator (URL)
 - using to designate forbidden sites [48](#)
- update, definition of [64](#)
- updating WebScanX [61](#)
 - automatically [62](#)
 - manually [62](#)
 - one-button updating [62](#)
- upgrade, definition of [64](#)
- user profile for Microsoft Messaging
 - use of in WebScanX [34](#)

V

- Viruses
 - preventing infection [60](#)
 - reporting new and unknown [61](#)

W

- WebScanX
 - activity icons [23](#)
 - as a part of security program [60](#)
 - getting started [22](#)
 - installing [19](#)
 - introducing [13](#)
 - overview of features [13](#)
 - program components in
 - Download Scan [22](#), [38](#)
 - E-mail Scan [22](#), [28](#)
 - Internet Filter [22](#), [46](#)
 - Security [22](#), [52](#)
 - reporting items not detected [14](#)
 - reporting items not detected by [63](#)
 - restarting [27](#)
 - shortcut menus [23](#)
 - software license agreement [19](#)
 - starting and quitting [26](#)
 - Status dialog box [24](#)
 - system requirements for [18](#)
 - updating [61](#)
 - automatically [62](#)
 - manually [62](#)
 - What's New text file [20](#)

- WebScanX for Windows 3.1x
 - as a TSR program [58](#)
 - browsers supported [55](#)
 - configuring [57](#)
 - feature and interface differences [56](#)
 - icons for [58](#)
 - interface differences [55](#)
 - running [55](#)
 - shutting down [58](#)
 - starting and quitting [58](#)
- why use WebScanX? [13](#)
- win.ini file, editing in Windows 3.1x [59](#)
- Windows 3.1x
 - running WebScan under [55](#)