

User's Guide

WebShieldX Proxy



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.

FAX: (408) 970-9727
BBS: (408) 988-4004

COPYRIGHT

Copyright © 1997-1998 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. ScanPM, WebScan, WebScanX, SiteExpress, BootShield, ServerStor, ScreenScan, ScreamScan, WebCrypto, PCCrypto, NetCrypto, Remote Desktop 32, WebShield, WebShieldX, NetRemote, eMail-It, Hunter, PC Medic, PC Medic 97, 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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Authenticode™ is a trademark of Microsoft Corporation.

“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 documentation 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.

Table of Contents

Preface.....	vi
Chapter 1. Introducing WebShieldX Proxy.....	12
What is WebShieldX Proxy?	12
Why use WebShieldX Proxy?	12
How WebShieldX Proxy Fits Into Your Network.....	13
WebShieldX Proxy features	14
How To Contact McAfee	15
Customer service	15
Technical support.....	15
McAfee training	16
International contact information	17
Reporting new items for WebShieldX Proxy updates	18
Chapter 2. Installing WebShieldX Proxy.....	19
Before You Begin	19
System Requirements.....	19
Installing WebShieldX Proxy	21
Uninstalling and Reinstalling WebShieldX Proxy	25
Chapter 3. Using the Administration Console	27
Starting the Administration Console.....	27
Configuring WebShieldX Proxy.....	29
Choosing Service options	30
Choosing Include options.....	31
Choosing Exclude options	33
Choosing Authenticode options	36
Choosing Java/ActiveX options	38
Choosing HTTP/FTP options	40

Choosing Gopher options	43
Choosing Log/Alert options	45
Choosing Update options	47
Using Alert Manager	50
Viewing the Summary page	51
Forwarding alert messages to another computer	52
Sending network messages	54
Sending alert messages to e-mail addresses	57
Sending alert messages to pagers	61
Sending alert messages to printers	65
Sending alert messages via SNMP	67

Chapter 4. Using a Web Browser to Configure WebShieldX71

Displaying the Configuration Pages	71
Configuring WebShieldX Proxy	73
Viewing the WebShieldX Proxy Information page	74
Choosing Include options	75
Choosing Exclude options	77
Choosing Authenticode options	80
Choosing Java/ActiveX options	82
Choosing HTTP/FTP options	85
Choosing Gopher options	88
Choosing Log options	90
Choosing AutoUpdate options	93
Choosing Alert options	95
Viewing the WebShieldX Proxy log file	95
Getting help	96
Configuring Alert Options	97
Viewing the Summary Page	99
Forwarding alert messages to other computers	99
Sending network messages	102
Sending alert messages to e-mail addresses	104
Sending alert messages to printers	106
Sending alert messages to pagers	108
Sending alert messages via SNMP	111
Choosing Global options	114

Viewing online documentation	116
Returning to WebShieldX Proxy	117
Appendix A. Preventing Virus Infection	118
Keys to a Secure System Environment	118
Detecting New and Unknown Viruses.....	118
Reporting new items for WebShieldX Proxy updates	120
Appendix B. McAfee Support Services	121
Customer Service Programs.....	122
Free WebShieldX support program	122
Free WebShieldX Deluxe support program	123
Free subscription maintenance and support program	124
Optional support plans	125
Professional Services Programs.....	126
Training	126
Consulting.....	126
Jump Start program	127
Enterprise support.....	127
Optional 7 x 24 enterprise support.....	128
Index	129

The Bits and the Bytes

Computer viruses, as you know, can have a devastating impact on productivity. What you might not know is basic information that could help you protect yourself and your colleagues 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

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 repository 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 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.

Introducing WebShieldX Proxy

What is WebShieldX Proxy?

WebShieldX Proxy is McAfee's anti-virus solution for use with network servers that run Microsoft Proxy Server. WebShieldX scans all HTTP, FTP, and Gopher protocol traffic at the Internet gateway, protecting your network from harmful virus infections and malicious code.

WebShieldX Proxy is an important element of a comprehensive security program that includes a variety of safety measures such as regular backups, password protection, training, and awareness. McAfee recommends that you set up and comply with a security program with these elements as a preventive measure to protect your corporate intranet.

Why use WebShieldX Proxy?

The Internet can harbor virus-infected files that have the ability to travel through network servers and even firewalls. Until now, the only defense against these viruses has been powerful virus detection at each desktop to prevent infected files from spreading.

WebShieldX Proxy scans all incoming Internet files at the proxy server. It detects, cleans and isolates copies of infected files and malicious code. It also logs its actions and sends alert messages when it finds harmful agents. Implementing security in this way—at the point of entry—prevents disruption of your network operations.

How WebShieldX Proxy Fits Into Your Network

Figure 1-1 illustrates a typical configuration for a network protected with WebShieldX Proxy

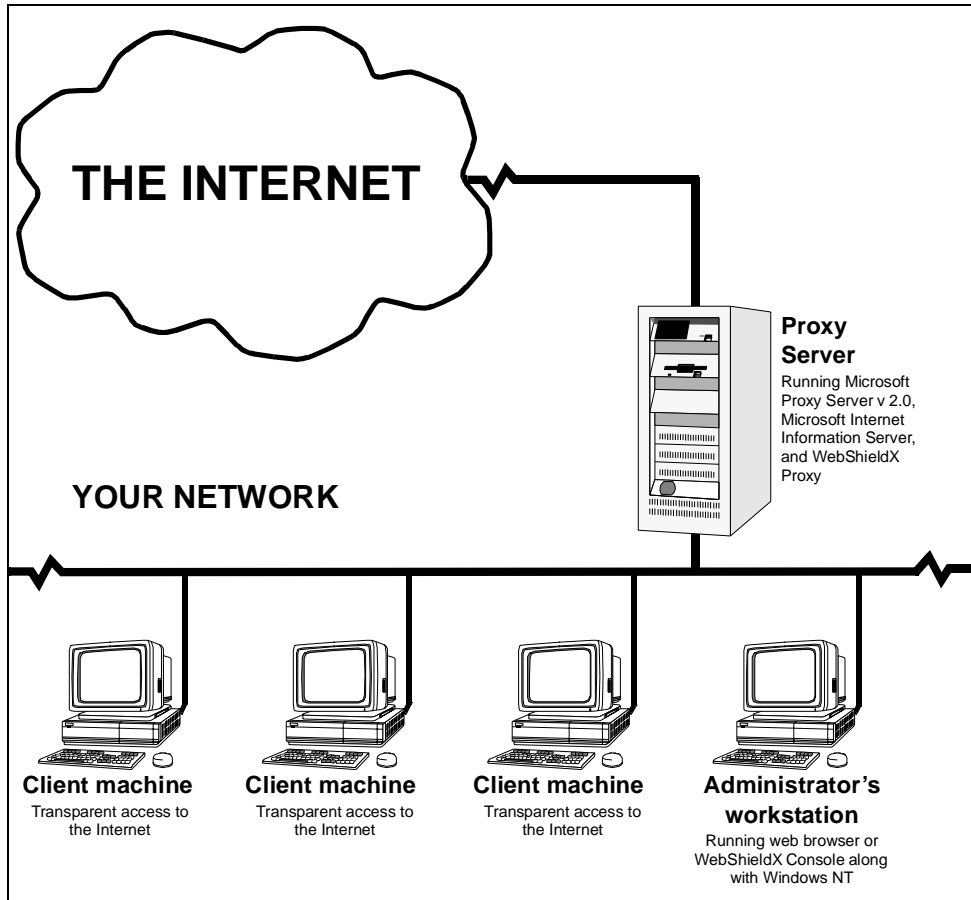


Figure 1-1. Typical WebShieldX Proxy Scheme

WebShieldX Proxy usually runs on the same machine that hosts Microsoft Proxy Server version 2.0. You may configure and manage WebShieldX from an administration console on that same server, or from another server elsewhere on the network. To end users who connect to the proxy server, all Internet traffic downloads transparently.

WebShieldX Proxy features

- Scans all inbound HTTP, FTP, and Gopher protocol traffic from the Internet at the proxy server, stopping viruses, hostile Java and ActiveX objects, and other malicious code before it can spread to your corporate network
- Checks for Microsoft Authenticode verification
- Scans files compressed in these formats: ZIP, LHA, and CAB (compressed application binary)
- Uses McAfee's award-winning Hunter scanning technology to pinpoint macro, polymorphic, boot file, multi-partite, stealth, mutating, and encrypted viruses
- Responds automatically to hostile objects or malicious code by isolating, deleting, or cleaning infected files; sending alert messages; and logging its actions
- Provides two different interfaces you can use to configure and manage scanning functions. You can:
 - Use a console that runs in conjunction with the Microsoft Internet Service Manager; or
 - Use your web browser
- Operates transparently on the network
- Implemented as an ISAPI extension for Microsoft Proxy Server 2.0
- Provides frequent and reliable data file (.DAT) updates for continuous network protection

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
America Online	keyword 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 France S.A.

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

McAfee (UK) Ltd.

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

McAfee Korea

135-090, 18th Fl., Kyoung Am Bldg.
157-27 Samsung-Dong, Kangnam-Ku
Seoul, Korea
Tel: 82 2 555-6818
Fax: 82 2 555-5779

McAfee Europe B.V.

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

McAfee Deutschland GmbH

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

McAfee Japan Co, Ltd.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon
Minato-ku, Tokyo 105
Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0780

McAfee South East Asia

7 Temasek Boulevard
The Penthouse
#44-01, Suntec Tower One
Singapore 038987
Tel: 65 430-6670
Fax: 65 430-6671

Reporting new items for WebShieldX Proxy 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 viruses, Java classes, ActiveX controls, or other malicious code that WebShieldX 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 other malicious code.

AVResearch@mcafee.com

Use this address to report new virus strains.

To report items to our European research office, use this e-mail address:

virus_research_europe@cc.mcafee.com

To report items to our Pacific Rim research office, or our office in Japan, use one of these e-mail addresses:

avert-jp@ccj.mcafee.com

Use this address to report harmful items to our office in Japan.

avert_apac@ccj.mcafee.com

Use this address to report harmful items to our Pacific Rim office.

2

Installing WebShieldX Proxy

Before You Begin

To install WebShieldX, you must first log on to an account with Administrator rights over the Windows NT domain that hosts your proxy server.

WebShieldX Proxy runs in conjunction with other Microsoft software. Before you install WebShieldX Proxy, you must install and configure these Microsoft packages:

- **Windows NT Server 4.0 with Service Pack 3 or later.** Install this on the computer that hosts WebShieldX Proxy, and on the the computer you will use for configuration and management.
- **Proxy Server 2.0.** Install this on the computer you will use as your proxy server.
- **Internet Information Server (IIS) 3.0 or later.** Install this on your proxy server in order to use a web browser for WebShieldX Proxy configuration and management.

System Requirements

WebShieldX Proxy runs on any computer that can run Microsoft Proxy Server 2.0. Microsoft lists these minimum and recommended hardware requirements for Proxy Server 2.0:

- For Intel and compatible systems:
 - 486/33 MHz or later. Pentium or Pentium Pro processor recommended
 - 125MB of available hard disk space
 - 16MB random-access memory (RAM). 24MB recommended
 - CD-ROM drive
 - VGA, Super VGA or video graphics adapter compatible with Windows NT Server 4.0
- For Digital Alpha AXP systems
 - Alpha processor compatible with Windows NT Server 4.0
 - 160MB of available hard disk space
 - 16MB random-access memory (RAM). 32MB recommended
 - CD-ROM drive
 - VGA, Super VGA or video graphics adapter compatible with Windows NT Server 4.0

Additional hardware requirements

Microsoft also recommends reserving sufficient disk space for the proxy cache. This amount varies with the number of client computers that connect to the proxy server, but should include a minimum of 100MB plus 512KB for each client computer.

WebShieldX Proxy itself requires a minimum of 10MB of hard disk space for its program files and documentation.

Additional options

- Install Internet Explorer version 4.0 on your proxy server to have WebShieldX verify Authenticode digital signatures.
- Use Internet Explorer 3.0 or later, or Netscape Navigator 3.0 or later, to use all available WebShieldX configuration and management options. Other browsers and earlier versions will also work.

Installing WebShieldX Proxy

To install WebShieldX Proxy, follow these steps:

- | Step | Action |
|------|--|
| 1. | Log on to the Windows NT domain that hosts your proxy server, or on to the proxy server itself. You must log on with Administrator rights. |
| 2. | Double-click Setup.exe on the WebShieldX Proxy CD-ROM to start the installation wizard, then click Yes to install WebShieldX Proxy. |

Response: The first WebShieldX Setup window (Figure 2-1) appears.

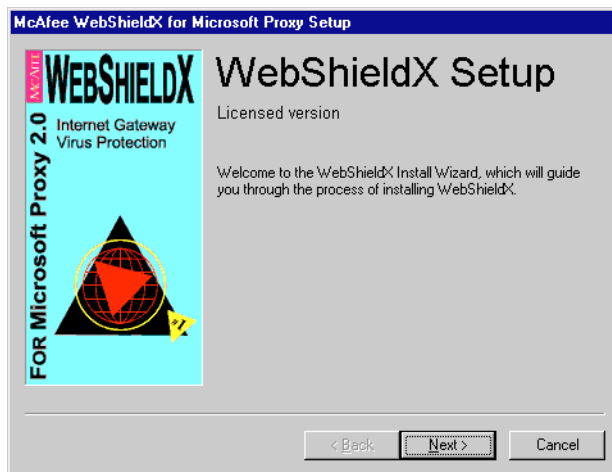


Figure 2-1. WebShieldX Setup

3. Click Next to continue.

Response: The second setup window displays the McAfee WebShieldX license agreement. Read the agreement carefully before you continue. You may scroll or page down through the text to read it.

4. If you agree to the terms of the license, select Yes, then click Next to continue.

Response: The Installation Options window (Figure 2-2) appears.

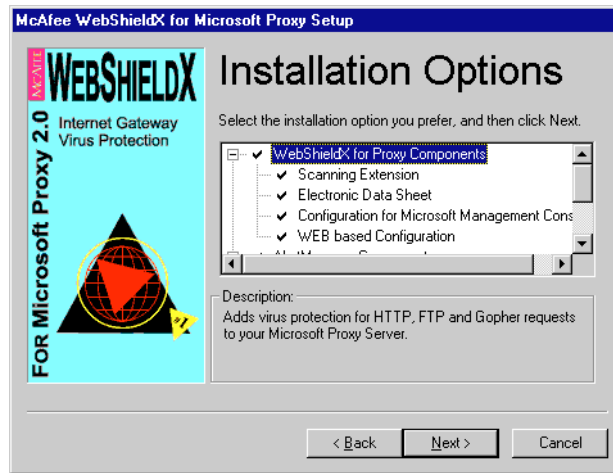


Figure 2-2. Installation Options Window

5. To reveal more options for the first two components shown, click . Click a component's name to highlight it and to view a brief description of it near the bottom of the window.

Components selected for installation show a check mark to the left of their names. To tell the installation wizard not to install one of the listed components, click the check mark to clear it. McAfee recommends that you install all WebShieldX Proxy components.

WebShieldX Proxy runs on any computer that has Windows NT 4.0 and Microsoft Proxy Server 2.0 installed. If you install WebShieldX Proxy on a computer without Microsoft Proxy Server, you will not see these options: Scanning Extension, Electronic Data Sheet, and the Web-based Configuration.

If you have not installed Microsoft's Internet Information Server on your proxy server, you may not use a web browser to configure and manage WebShieldX Proxy, and you will not see an option for Web-based configuration in this window.

6. Click Next to continue.

Response: The Choose Directory dialog box appears.

7. Select the drive and directory where you want to install WebShieldX, then click Next.

Response: The installation wizard appends `WebShieldX` to the directory path you specified, and creates a WebShieldX subdirectory.


The Alert Manager account dialog box appears.



Figure 2-3. Alert Manager Account Login dialog box

8. Select Use Local System Account, or specify which account should receive alert messages when WebShieldX detects a virus or other malicious code. The account you specify must have Administrator rights.

Next, enter account owner's log in domain, username and password in the text boxes provided. Enter the password again for verification, then click Next to continue.


 *If you select Use Local System Account, you will not be able to print or forward alert messages.*

Response: The Finish Installation window (Figure 2-4) appears. It lists the components and subcomponents you have chosen for installation.



Figure 2-4. Finish Installation Window

9. To complete the installation, click Finish.

 *If the installation wizard detects a conflict with a program running in the background, it will prompt you to quit the program before resuming the installation. Note and follow the cautions you see in any alert messages to ensure a complete WebShieldX Proxy installation.*

WebshieldX Proxy is now installed and ready for configuration. To learn how to use the WebShieldX Proxy Administration console, see “Using the Administration Console” on page 27. To learn how to use a web browser to configure WebShieldX, see “Using a Web Browser to Configure WebShieldX” on page 71.

Uninstalling and Reinstalling WebShieldX Proxy

To uninstall or reinstall WebShieldX Proxy or one of its components, follow these steps:

Step	Action
------	--------

- | | |
|----|--|
| 1. | Click Start in the Windows taskbar, point to Programs, then to WebShieldX. Choose Setup. |
|----|--|

Response: The WebShieldX Installation Options window appears.

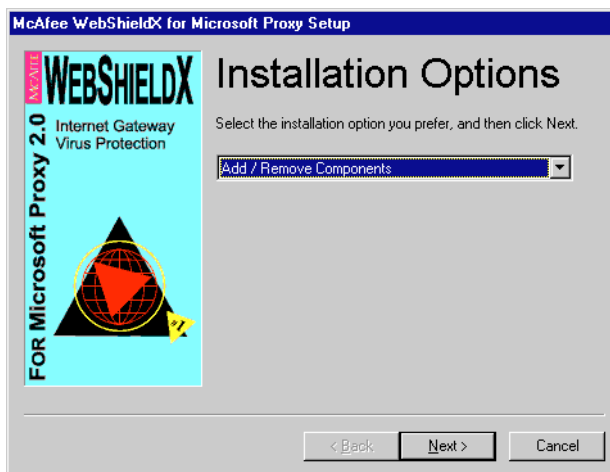


Figure 2-5. Installation Options window

- | | |
|----|--|
| 2. | Choose an installation option from the list, then click Next. Your options are: <ul style="list-style-type: none">■ Add/Remove Components. Choose this to install additional WebShieldX components or remove one or more of the components you installed earlier. |
|----|--|

A second Installation Options window (see Figure 2-2) appears. Choose the components you want to keep or those you want to remove, then follow the installation wizard instructions shown to continue.

- **Remove All Components.** Choose this to uninstall WebShieldX completely.

The Finish Installation window (see Figure 2-4) appears. Click Finish to remove the components shown.

- **Repeat last installation.** Choose this to reinstall WebShieldX with the same options you chose earlier.

The installation wizard starts the installation again from step 7 in “Installing WebShieldX Proxy” (page 23). Continue with the steps listed in this section to complete the installation.

Starting the Administration Console

WebShieldX Proxy offers you two ways to configure and manage its scanning operations. One method allows you to use a web browser to see and change configuration options. To learn how to set up and use that method, see [Chapter 4, “Using a Web Browser to Configure WebShieldX.”](#) The method outlined in this chapter uses the WebShieldX Proxy Administration Console, which runs in conjunction with Microsoft’s Internet Service Manager.

To start the Administration Console, follow these steps:

Step

Action

1. Click Start in the Windows taskbar, point to Programs, then to McAfee WebShieldX. Next, choose Internet Service Manager to open a window that lists the computers with Internet services enabled (Figure 3-1).

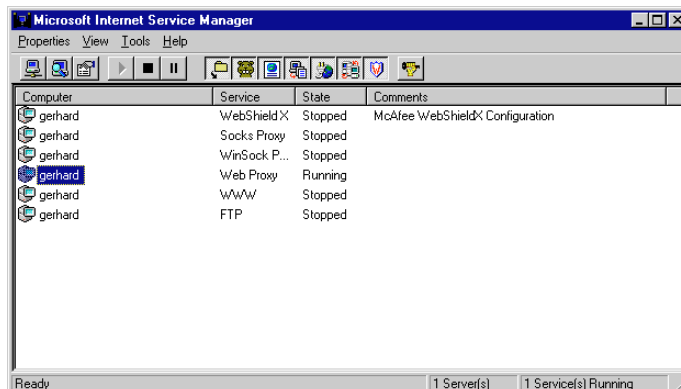



Figure 3-1. The Internet Services Manager window

Locate a computer that lists WebShieldX in the Service column. If you have installed WebShieldX Proxy on more than one computer on the network, you may use any of those available to run the Console.

 *You must have Administrator log in rights to the computer you intend to use.*

2. Double-click the computer you want to use to run the Console, or right-click it, then choose Service Properties in the shortcut menu that appears.

Response: The WebShieldX Proxy Administration Console (Figure 3-2) appears.



Figure 3-2. WebShieldX Proxy Administration Console

Configuring WebShieldX Proxy

Use the property pages provided in the WebShieldX Proxy Administration Console (see Figure 3-2) to configure and manage all program functions. The following summary describes the available property pages:

- **Service.** This page lists WebShieldX Proxy's anti-virus engine and data file specifications, reports the number of files it scanned and the number of viruses it found, and allows you to scan the proxy server cache on demand.
- **Include.** Use this page to specify which file types WebShieldX Proxy should scan for viruses or other malicious code.
- **Exclude.** Use this page to specify which Multipurpose Internet Mail Extension (MIME) types WebShieldX Proxy should skip during scanning operations—audio files, image files or video files, for example. Most MIME files in these categories are not susceptible to virus infection.
- **Authenticode.** Use this page to check incoming files for authentication certificates and to block those without valid certificates. You can check executable files, Java applets and .CAB files. To learn more about Microsoft Authenticode™, see <http://microsoft.com/security>.
- **Java/ActiveX.** Use this page to tell WebShieldX Proxy how to respond when it detects potentially harmful Java or ActiveX objects, or malicious JavaScript code. You can block all objects and scripts, block only objects known to cause harm, or allow all objects and scripts to pass through the proxy server. This page also includes options for logging WebShieldX Proxy actions and sending alert messages.
- **HTTP/FTP.** Use this page to tell WebShieldX Proxy to look for viruses in Internet traffic sent via either or both of these protocols. You can configure WebShieldX Proxy to clean, reject, quarantine, or ignore infected files that it finds. This page also includes options for logging WebShieldX Proxy actions and sending alert messages.
- **Gopher.** Use this page tell WebShieldX Proxy to scan Gopher traffic. This page has the same response options as those for HTTP/FTP scanning.
- **Log/Alert.** Use this page to activate the WebShieldX Proxy activity logs. You can have the program save activity information to a log file or to the Windows NT Event Viewer. Use this page also to specify your quarantine directory.
- **AutoUpdate.** Use this page to schedule data file updates for WebShieldX Proxy. You can update automatically or on demand.

Choosing Service options

When you start the Administration Console, the Service property page appears first (Figure 3-3). If you have already started the Console and chosen a different property page, click the Service tab to return to this page.



Figure 3-3. Administration Console–Service page

This page tells you which versions of WebShieldX Proxy's scanning engine and data files you have installed. The page also shows you the number of files that WebShieldX Proxy has scanned and how many viruses it has found.

To have WebShieldX Proxy examine your proxy server's cache immediately, click Scan. The program scans all files in the proxy cache, without regard to the options you choose in the Include and Exclude pages (see "Choosing Include options" on page 31 and "Choosing Exclude options" on page 33 for details).

If it finds an infected file, WebShieldX Proxy does not send an alert message as it does during scheduled scan operations, but it will automatically try to clean the file. If it cannot clean the file, it deletes the file from the proxy cache. WebShieldX Proxy logs its actions during this scan operation according to the options you choose in the Log/Alert page.

The Service page also includes space for you to enter a comment that will identify WebShieldX Proxy in the Comments column in the Internet Service Manager window (see [Figure 3-1 on page 27](#)). By default, the comment reads McAfee WebShieldX Configuration. To change this comment, type your own entry in the text box provided.

Choosing Include options

WebShieldX Proxy can look for viruses or identify harmful agents either in all files on your proxy server, or in those files most likely to contain malicious code. Scanning all traffic that passes through your proxy server provides the best protection for your network, but narrowing the scope of WebShieldX Proxy's scan operations improves its performance. To choose the options you want WebShieldX Proxy to use, follow these steps:

Step	Action
------	--------

- | | |
|----|---|
| 1. | Start the Administration Console, then click the Include tab. |
|----|---|

Response: The Include page ([Figure 3-4](#)) appears.

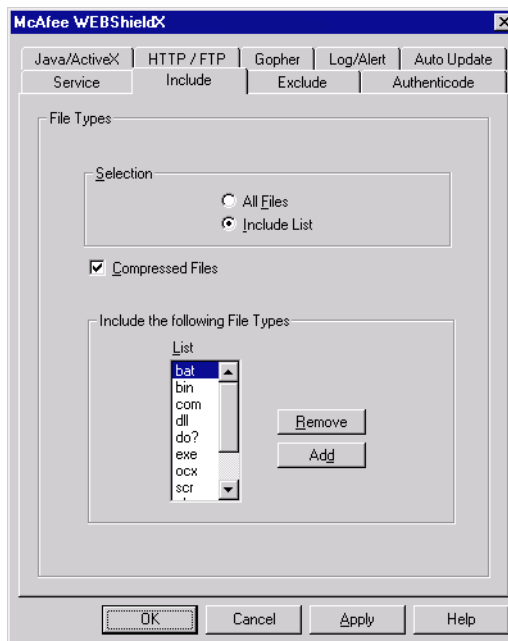



Figure 3-4. Administration Console—Include page

2. Choose which files you want WebShieldX Proxy to scan for viruses or malicious code by selecting one of these options:
 - **All Files.** Select this to tell WebShieldX Proxy to examine all traffic that passes through your proxy server.
 - **Include List.** Select this to tell WebShieldX Proxy to examine only those files most susceptible to virus infection or most likely to contain harmful agents.
3. Select the Compressed Files checkbox to have WebShieldX Proxy look for viruses in files compressed in .ZIP, .LHA or .CAB formats.

To determine which filename extensions WebShieldX Proxy uses to identify files likely to contain malicious code, continue with [Step 4](#). Otherwise, skip to [Step 7](#).

 *By default, WebShieldX Proxy identifies files with the extensions .BAT, .BIN, .COM, .DLL, .EXE, .DO?, .OCX, .SCR, .VBX, .VXD, and .XL? as those most likely to harbor malicious code, which includes viruses, harmful Java or ActiveX objects, and dangerous JavaScript or VBScript. 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.*

4. To remove a filename extension from the default list, select it, then click Remove.
5. To add a filename extension to the default list, click Add.

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

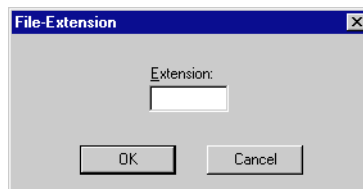




Figure 3-5. File Extension dialog box

6. Type the filename extension you want to add in the text box provided, then click OK.

Response: The filename extension appears in the default list on the Include page.

 *WebShieldX Proxy adds new filename extensions to the bottom of the list, not in alphabetical order.*

7. Click Apply to save the options you chose without leaving the Include page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Choosing Exclude options

Files that contain no executable code—video, audio, and image data, for example—cannot contain viruses or other malicious agents. Because data files of this sort make up a large part of the file attachments that network users receive via e-mail or download from the Internet, excluding them from WebShieldX Proxy scanning operations can improve the program's performance considerably.

WebShieldX Proxy can exclude MIME file attachments—files encoded with the widely supported Multipurpose Internet Mail Extension standard—from its scanning operations by looking at their content-type headers. The content-type header is a portion of a MIME-encoded e-mail message that identifies what sort of file attachment it carries. E-mail software and associated programs use the header information to decide which applications can open and work with the data contained in the file attachment.

The content-type header consists of two parts: a “type” designation chosen from a standard list of content type names—“video,” “audio,” or “text,” for example; and a “subtype” designation chosen from a central registry of subtype names. E-mail software and other programs that support the MIME standard can read and interpret these headers, then locate and open the correct application. See RFC 2046 at <http://ds.internic.net/ds/dspg1intdoc.html> for a thorough discussion of MIME content-type headers. See <http://www.iana.org> for a list of registered MIME types and subtypes.

To determine which files WebShieldX Proxy should not scan, follow these steps:

Step	Action
------	--------

- | | |
|----|---|
| 1. | Start the Administration Console, then click the Exclude tab. |
|----|---|

Response: The Exclude page (Figure 3-6) appears.

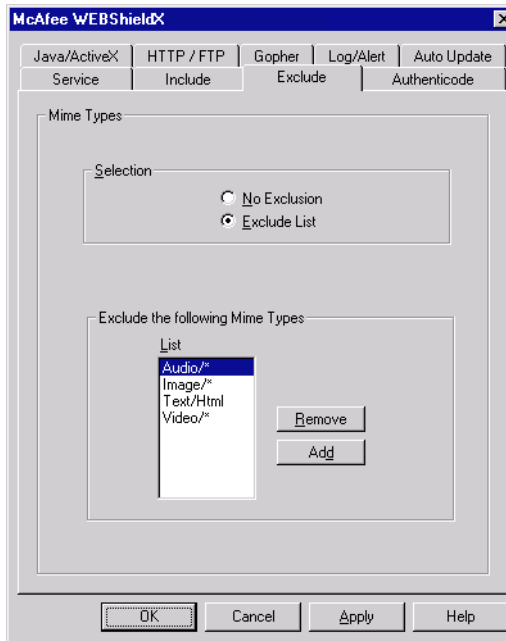



Figure 3-6. Administration Console—Exclude page

- | | |
|----|---|
| 2. | Choose which MIME-encoded files you want WebShieldX Proxy to exclude from its scanning operations by selecting one of these options: <ul style="list-style-type: none"> ■ No Exclusion. Select this to tell WebShieldX Proxy to scan all MIME-encoded files. ■ Exclude List. Select this to tell WebShieldX Proxy to exclude files with the content-type headers specified in the exclusion list at the bottom of the Console page. |
|----|---|

To designate the types of MIME-encoded files WebShieldX Proxy will not scan, continue with [Step 3](#). Otherwise, skip to [Step 6](#).

 *By default, WebShieldX Proxy does not scan files with these content-type headers: Audio/*, Image/*, Text/*, and Video/*.*

3. To remove a MIME content-type header from the exclusion list, select it, then click Remove. WebShieldX Proxy will now scan this file type.
4. To add a MIME content-type header to the default list, click Add. WebShieldX Proxy will not scan files that have the content-type headers you add to the list.

Response: The MIME Extensions dialog box ([Figure 3-7](#)) appears.

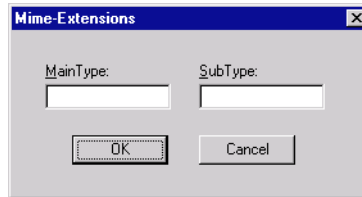




Figure 3-7. MIME Extensions dialog box


5. Enter the content-type header and the subtype you want to add to the exclusion list in the text boxes provided, then click OK.

 *WebShieldX Proxy allows you to specify * as a wildcard designation for all subtypes.*

Response: WebShieldX Proxy adds the MIME content-type header at the bottom of the exclusion list.


 *MIME content-type headers appear in the order you add them to the exclusion list, not in alphabetical order.*

6. Click Apply to save the options you chose without leaving the Exclude page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Choosing Authenticode options

WebShieldX Proxy can look for valid Microsoft Authenticode certificates in file attachments and block those with invalid or missing certificates from access to your proxy server. Authenticode is a Microsoft security standard built into Internet Explorer 3.0 and later that allows software developers to “sign” their products with a tamper-proof digital certificate. WebShieldX Proxy can read and verify these certificates—you can decide whether to allow those with invalid certificates to have access to your proxy server.

 *Authenticode support extends only to certain platforms and development environments. Consult <http://www.microsoft.com/security> for details.*

To configure WebShieldX Proxy to look for Authenticode certificates, follow these steps:

1. Start the Administration Console, then click the Authenticode tab.

Response: The Authenticode page (Figure 3-8) appears.

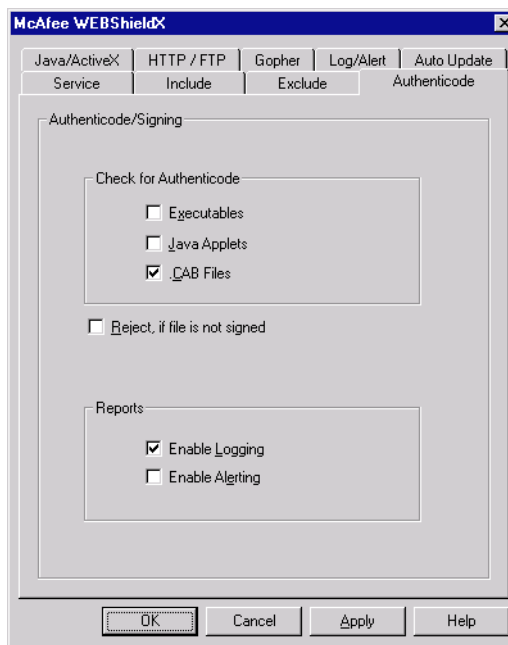



Figure 3-8. Administration Console—Authenticode page

2. In the Check For Authenticode area, select the items you want WebShieldX Proxy to verify. Clear the checkboxes beside items you do not want verified. You may choose all, any, or none of these items:
 - **Executables.** Select this to have WebShieldX Proxy verify certificates for ActiveX controls and other executable files.
 - **Java Applets.** Select this to have WebShieldX Proxy verify certificates for Java classes and applets.
 - **CAB Files.** Select this to have WebShieldX Proxy verify certificates for files archived in the compressed application binary (.CAB) format.
3. Select the Reject If File Is Not Signed checkbox to tell WebShieldX Proxy to block any files that do not have valid Authenticode certificates. Clearing this checkbox allows unverified files to pass through to your proxy server.
4. To have WebShieldX Proxy generate alert messages when it detects invalid or missing Authenticode certificates and to log its actions, select either or both of these checkboxes:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked, how many had valid Authenticode certificates and how many files it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which options you choose in the Log/Alert page. See [“Choosing Log/Alert options” on page 45](#).
 - **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected a file with an invalid Authenticode certificate. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy’s Alert Manager. See [“Using Alert Manager” on page 50](#) for details.
5. Click Apply to save the options you chose without leaving the Authenticode page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Choosing Java/ActiveX options

WebShieldX Proxy can examine any Java classes, ActiveX controls or JavaScript code on your proxy server for potential danger. You can choose to filter Java classes and ActiveX controls by comparing them with an internal database of classes and controls known to cause harm. You can also choose to block all harmful objects and script code, or let it pass through your proxy server unimpeded. With WebShieldX Proxy's scanning features, your network users benefit from the interactive features available at some websites without your having to worry about possible harm to the network, and without needing to turn off Java or ActiveX access in each user's browser software.

To configure WebShieldX Proxy to examine Java and ActiveX objects and script code—such as JavaScript or VBScript—follow these steps:

Step

Action

1. Start the Administration Console, then click the Java/ActiveX tab.

Response: The Java/ActiveX page (Figure 3-8) appears.

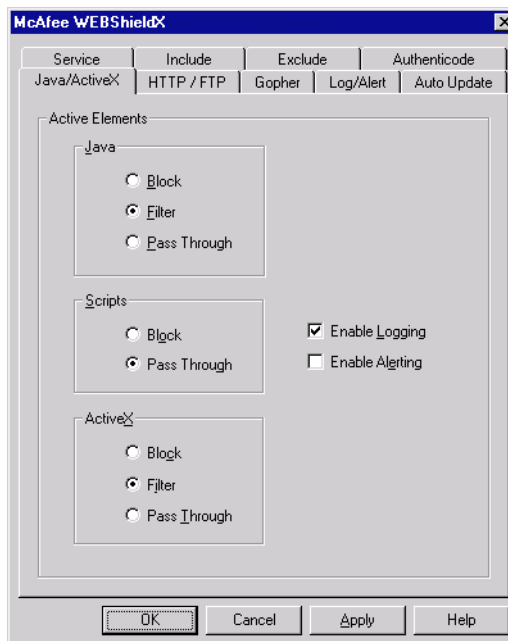



Figure 3-9. Administration Console—Java/ActiveX page

2. In the Active Elements area, select the actions you want WebShieldX Proxy to take when it finds potentially harmful objects or malicious code. You can have WebShieldX Proxy respond in different ways to each element.
 - To respond to harmful Java classes or ActiveX controls, select one of the following actions:
 - **Block.** Select this to deny all Java and ActiveX objects access to your proxy server.
 - **Filter.** Select this to compare Java and ActiveX objects to a database of objects known to cause harm. WebShieldX Proxy then allows only those objects not likely to cause harm on to your proxy server.
 - **Pass Through.** Select this to allow Java and ActiveX objects access to your proxy server whether they could cause harm or not. Depending on how you have configured its logging and alert options, WebShieldX Proxy can still log its actions and can send alert messages when it discovers a harmful object. (See Step 3, below.)
 - To respond to harmful script code, select one of the following actions:
 - **Block.** Select this to deny all script code access to your proxy server.
 - **Pass Through.** Select this to allow script code to remain on your proxy server whether it could cause harm or not. This option could expose your network users to harm from malicious code.

Depending on how you have configured its logging and alert options, WebShieldX Proxy can still log its actions and can send alert messages when it discovers a harmful Java object. (See Step 3, below.)

3. To tell WebShieldX Proxy to send alert messages and log its actions when it detects potentially harmful objects or malicious code, select either or both of these checkboxes:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked and how many files it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which options you choose in the Log/Alert page. See “Choosing Log/Alert options” on page 45 for details.
 - **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected a potentially harmful object or malicious code. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy’s Alert Manager. See “Using Alert Manager” on page 50 for details.
4. Click Apply to save the options you chose without leaving the Java/ActiveX page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Choosing HTTP/FTP options

WebShieldX Proxy can look for viruses in all network traffic sent via Hyper Text Transfer Protocol (HTTP) or File Transfer Protocol (FTP), then respond with the actions you specify here when it finds a virus. You can configure scanning operations for each protocol separately, telling WebShieldX Proxy to block infected files from access to your proxy server, to allow files to pass through the server unimpeded, to quarantine infected files in a particular directory, or to remove viruses from infected files before allowing them onto your server.

To configure WebShieldX Proxy to look for viruses in HTTP and FTP traffic, follow these steps:

- | Step | Action |
|------|--|
| 1. | Start the Administration Console, then click the HTTP/FTP tab. |

Response: The HTTP/FTP page (Figure 3-10) appears.

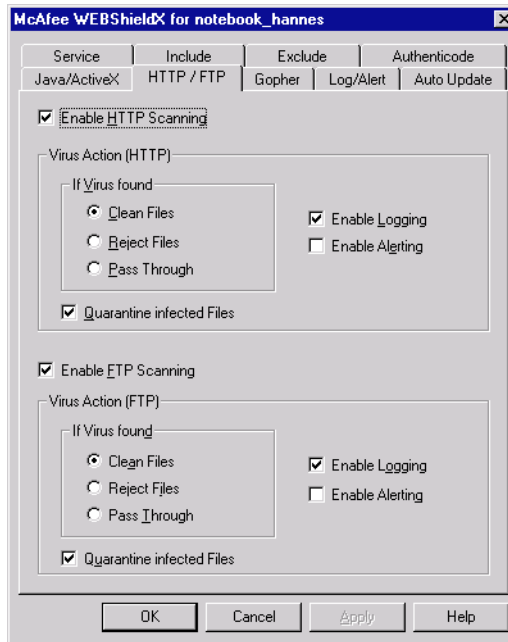



Figure 3-10. Administration Console—HTTP/FTP page

2. Select the Enable HTTP Scanning checkbox or the Enable FTP Scanning checkbox, or both, to have WebShieldX Proxy monitor each type of traffic.
3. Select the actions you want WebShieldX Proxy to take when it finds infected files—you can tell the program to respond in different ways for each protocol. Your options are:
 - ❑ **Clean Files.** Select this to have WebShieldX Proxy remove virus code from infected files. The cleaned files remain on your proxy server.
 - ❑ **Reject Files.** Select this to deny infected files access to your proxy server. The rejected files do not remain on your server.

- ❑ **Pass Through.** Select this to allow infected files to remain on your proxy server whether they could cause harm or not. Although this can expose your network users to the risk of virus infection, you can quarantine infected files (see Step 4 below) and keep them in a directory separate from your proxy cache.

Depending on how you have configured its logging and alert options, WebShieldX Proxy can also log its actions and can send alert messages when it discovers a harmful object. (See Step 5, below.)

4. Select either or both of the Quarantine Infected Files checkboxes to have WebShieldX Proxy preserve copies of infected files found in each type of traffic. The program can quarantine files regardless of how else you ask it to respond when it finds infections.
5. To have WebShieldX Proxy send alert messages and log its actions, select either or both of these checkboxes for each type of traffic:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked, how many infected files it found, how many it cleaned, and how many it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which options you choose in the Log/Alert page. See “Choosing Log/Alert options” on page 45 for details.
 - **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected an infected file. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy’s Alert Manager. See “Using Alert Manager” on page 50 for details.
6. Click Apply to save the options you chose without leaving the HTTP/FTP page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Choosing Gopher options

WebShieldX Proxy can look for viruses in all network traffic sent to your proxy server from Gopher servers, then respond with the actions you specify here when it finds a virus. You can tell WebShieldX Proxy to block infected files from access to your proxy server, to allow files to pass through the server unimpeded, to quarantine infected files in a particular directory, or to remove viruses from the infected files before allowing them onto your server.

To configure WebShieldX Proxy to look for viruses in Gopher traffic, follow these steps:

- | Step | Action |
|------|--|
| 1. | Start the Administration Console, then click the Gopher tab. |

Response: The Gopher page (Figure 3-11) appears.

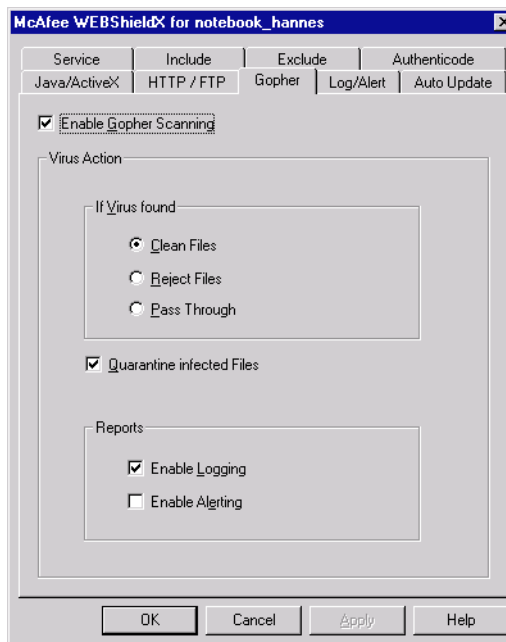



Figure 3-11. Administration Console–Gopher page

2. Select the Enable Gopher Scanning checkbox to have WebShieldX Proxy monitor Gopher traffic on your proxy server.
3. Select the actions you want WebShieldX Proxy to take when it finds infected files. The program can respond in any of these ways:
 - ❑ **Clean Files.** Select this to have WebShieldX Proxy remove virus code from infected files. The cleaned files remain on your proxy server.
 - ❑ **Reject Files.** Select this to deny infected files access to your proxy server. The rejected files do not remain on your server.
 - ❑ **Pass Through.** Select this to allow infected files to remain on your proxy server whether they could cause harm or not. Although this can expose your network users to the risk of virus infection, you can quarantine infected files (see Step 4 below) and keep them in a directory separate from your proxy cache.

Depending on how you have configured its logging and alert options, WebShieldX Proxy can also log its actions and can send alert messages when it discovers a harmful object. (See Step 5, below.)

4. Select the Quarantine Infected Files checkbox to have WebShieldX Proxy preserve copies of infected files found in Gopher traffic. The program can quarantine files regardless of how else you ask it to respond when it finds infections.
5. To have WebShieldX Proxy send alert messages and log its actions, select either or both of these checkboxes:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked, how many infected files it found, how many it cleaned, and how many it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which options you choose in the Log/Alert page. See “Choosing Log/Alert options” on page 45 for details.

- **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected an infected file. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy's Alert Manager. See "Using Alert Manager" on page 50 for details.
6. Click Apply to save the options you chose without leaving the Gopher page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Choosing Log/Alert options

WebShieldX Proxy can record its actions in its own log file and it can report its actions via the Windows NT Event Viewer. The options you choose on the Log/Alert page tell WebShieldX Proxy which types of log files to set up and how to maintain them. To tell WebShieldX Proxy what information you want it to collect and record in each type of log file, you must activate the logging options in each of the other Console pages.

To see the information WebShieldX Proxy reports via the Windows NT Event Viewer, click Start in the Windows NT taskbar, point to Programs, then to Administrative Tools (Common). Next, choose Event Viewer to open the Windows NT Event Viewer window. Locate an event that lists WebShieldX in the Source column, then double-click it to see the detail window.

To see the information WebShieldX Proxy records in its own log file, use any text editor or any word processing software to open, view or print the file. By default, you'll find the log file in this path:

```
c:\Program Files\McAfee\WebShieldX\Log.txt
```

To use a different path or filename for your WebShieldX Proxy log file, first use a text editor to create and name a text file, then locate that file from the Log/Alert Console page. See Step 3 below for details.

Other options on this page allow you to determine when to discard existing log entries, which directory you want to use to quarantine infected files and what types of alert messages you want to send whenever WebShieldX Proxy

To tell WebShieldX Proxy to set up and maintain log files, follow these steps:

Step

Action

1. Start the Administration Console, then click the Log/Alert tab.

Response: The Log/Alert page (Figure 3-12) appears.

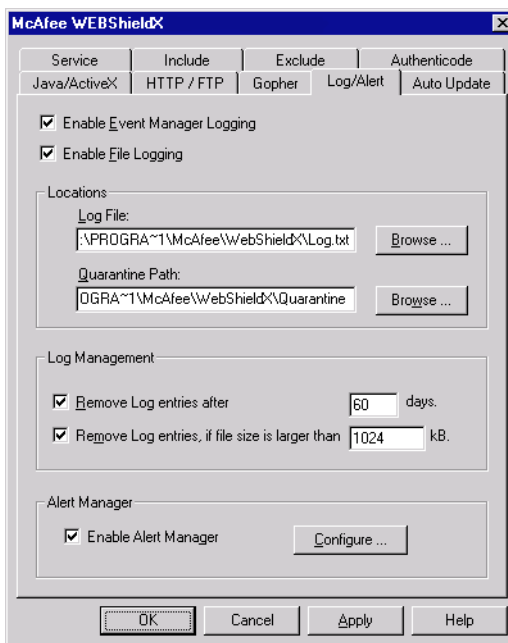



Figure 3-12. Administration Console—Log/Alert page

2. Select the Enable Event Manager Logging checkbox or the Enable File Logging checkbox, or both, to have WebShieldX Proxy record and report its actions.
3. Enter the path and filename you want to use for your log file in the text box provided in the Locations area. You can also click Browse to locate an existing file for your use.


4. To keep the log file size manageable, select the Remove Log Entries After ____ Days checkbox or the Remove Log Entries If File Size Is Larger than ____ KB checkbox, or both. Next, enter in the text boxes provided the number of days you want WebShieldX Proxy to wait before it discards old log entries and the maximum size, in kilobytes, to which you want your log file to grow.

 *By default, WebShieldX Proxy retains log entries for 60 days and allows your log file to grow to one megabyte in size. When it reaches the limits you set in the Log Management area, WebShieldX Proxy deletes all existing entries and starts the log file again.*

To choose a directory to serve as your quarantine area, enter the path and filename in the text box provided in the Locations area, or click Browse to locate a suitable directory.

To have WebShieldX Proxy send alert messages when it detects viruses or other harmful code, select the Enable Alert Manager checkbox. This activates whatever alert methods you have configured in the Alert Manager dialog box. To see and configure your Alert Manager options, click Configure, then see “Using Alert Manager” on page 50 to learn how to choose your options.

Click Apply to save the options you chose without leaving the Log/Alert page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Choosing Update options

WebShieldX Proxy includes AutoUpdate, a utility you can use to update the data files (.DAT) the program uses to detect viruses and other malicious code. You can use this same utility to upgrade the entire program, either by purchasing an upgrade, or by upgrading for free if your license permits. AutoUpdate connects with McAfee's website and locates any new data files stored there, either at scheduled intervals or when you want it to check for them. The options you choose in the AutoUpdate page tell WebShieldX Proxy when to schedule update requests.

To set your update options, follow these steps:

Step	Action
------	--------

- | | |
|----|--|
| 1. | Start the Administration Console, then click the AutoUpdate tab. |
|----|--|

Response: The AutoUpdate page (Figure 3-13) appears.

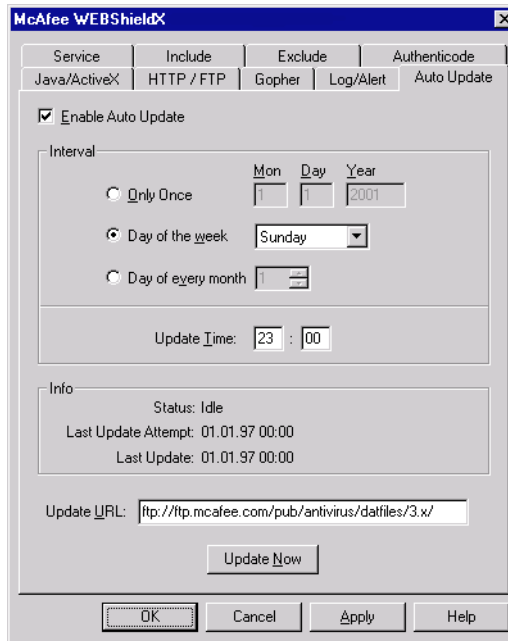


Figure 3-13. Administration Console–AutoUpdate page


- | | |
|----|--|
| 2. | Select the Enable AutoUpdate checkbox to have WebShieldX Proxy look for updated files according to the schedule you set in the following steps. |
| 3. | Select a time interval to schedule WebShieldX Proxy's next connection. You can choose one of these options from the Interval area: <ul style="list-style-type: none"> ■ Only Once. Select this to have WebShieldX Proxy check for updated files only once. Enter the month, day and year you want the program to perform this check in the text boxes provided, then enter a particular time (see Step 4 below). |

- **Day of the week.** Select this to have WebShieldX Proxy check once per week for updated files. Choose the day of the week during which the program should perform this check from the list to the right, then enter a particular time (see Step 4 below).
 - **Day of every month.** Select this to have WebShieldX Proxy check once per month for updated files. Choose the date on which the program should perform this check from the list to the right. Be sure to choose a date that occurs each month—choosing 31, for example, will skip updates for February and for months with only 30 days. Next, enter a particular time (see Step 4 below).
4. Enter the time, in hours and minutes, when WebShieldX Proxy should connect to the McAfee website to check for updated files. Enter the time using a 24-hour clock.
 5. Enter the website address WebShieldX Proxy should use to connect to the McAfee website in the text box labeled Update URL (Uniform Resource Locator). By default, the update address is:

`ftp://ftp.mcafee.com/pub/antivirus/datfiles/3.x/`

You can enter any address here to which you can connect via anonymous FTP. McAfee makes its software available on other electronic services, such as America Online and Compuserve. See “How To Contact McAfee” on page 15 for details.

6. To send an update request immediately, without waiting for the next update you’ve scheduled, click Update Now at the bottom of the AutoUpdate page. WebShieldX immediately connects with the McAfee website.
7. Check the Info area to learn when WebShieldX Proxy last connected to the McAfee website, when it last updated its data files, and its current update status.
8. Click Apply to save the options you chose without leaving the AutoUpdate page. To save your options and close the Console, click OK. To close the Console without saving any changes, click Cancel.

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

Using Alert Manager

WebShieldX Proxy uses McAfee's Alert Manager utility to notify you or others when it detects a virus or malicious code in files on your proxy server. Alert Manager gives you a wide variety of notification options that you can use individually or in combinations that suit your needs.

If you have Alert Manager installed on other computers on your network, you can also forward alert messages to computers in other domains, which can in turn notify the workstations that they host about infected files on your proxy server. Alert Manager supports McAfee's Centralized Alerting technology, available with products such as McAfee NetShield. For details, consult the *NetShield User's Guide*.

To open the Alert Manager dialog box and choose configuration options, follow these steps:

- | Step | Action |
|-------------|--|
| 1. | Start the Administration Console, then click the Log/Alert tab. To learn how to start the Administration Console, see "Starting the Administration Console" on page 27.

Response: The Log/Alert page (see Figure 3-12 on page 46) appears. |
| 2. | Select the Enable Alert Manager checkbox at the bottom of the page, then click Configure.

Response: WebShieldX Proxy opens the Alert Manager dialog box Figure 3-14 on page 51 with the Summary tab selected. |

The Alert Manager dialog box includes six different alert methods, each with configuration options shown in individual property pages. Click the tab corresponding to the alert method you want to configure to see the options available. When you have finished choosing your options, click OK to save your changes, close the Alert Manager dialog box, and return to the WebShieldX Proxy Administration Console. Click Cancel to close the Alert Manager dialog box without saving your changes.

The following sections describe the options available for each method.

Viewing the Summary page

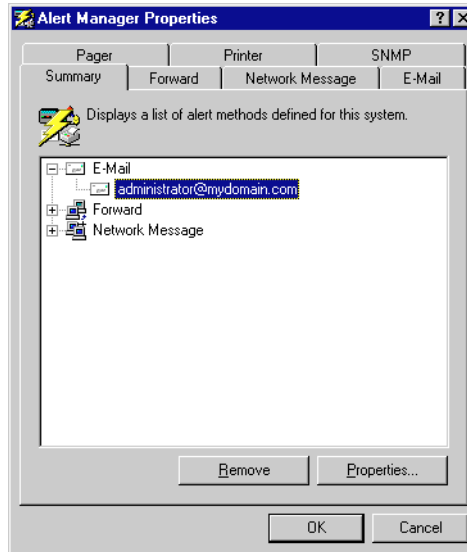


Figure 3-14. Alert Manager Properties dialog box (Summary page)

The Summary page lists all of the alert methods you've told WebShieldX Proxy to use to notify you when it finds a virus or other malicious code on your proxy server. In the example shown in Figure 3-14, the Alert Manager will send alerts to an e-mail address, to a network server, and to another computer. If you have not yet configured Alert Manager, the Summary Page will be blank.

Click **+** next to each listed alert method to display the computers, printers, phone numbers, or e-mail addresses that will receive alert messages from WebShieldX Proxy. To remove an alert method, select it, then click Remove. To change the configuration options for a listed method, select it, then click Properties. Alert Manager will open the same property page you used to configure your options for that alert method.

See the following sections to learn more about the options available for each alert method.

Forwarding alert messages to another computer

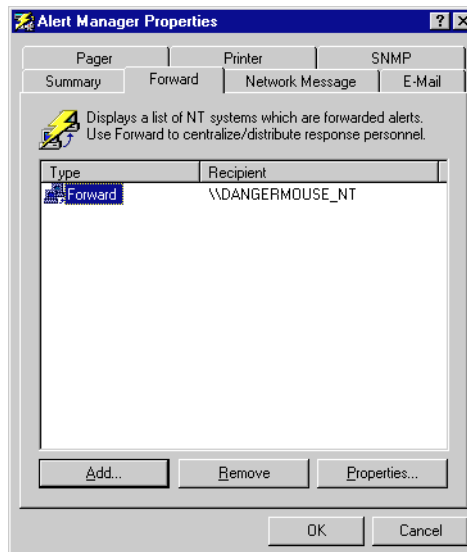
Alert Manager can forward the alert messages that WebShieldX Proxy generates to other computers on your network. If you have installed Alert Manager on each of the destination computers, they can in turn forward alert messages to the recipients listed in their Alert Manager Summary pages. You might use this feature to pass alert messages across network domains or to construct a hierarchical arrangement for passing alert messages.

To configure Alert Manager's Forwarding options, follow these steps:

Step	Action
------	--------

1. Open the Alert Manager Properties dialog box.
2. Click the Forward tab.

Response: The Forward page (Figure 3-15) appears with a list of all of the computers you have chosen to receive forwarded messages. If you have not yet chosen any destination computers, this list will be blank.



**Figure 3-15. Alert Manager Properties dialog box
(Forward page)**

3. To update this list, you can:

- **Remove a listed computer.** Select one of the destination computers listed, then click Remove.
- **Add a computer to the list.** Click Add to open the Forward Properties dialog box (Figure 3-16), then enter the name of the computer that will receive forwarded messages in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network. To choose additional options, continue with Step 4.
- **Change configuration options.** Select one of the destination computers listed, then click Properties. Alert Manager opens the Forward Properties dialog box (Figure 3-16). Change any of the information you want to change in the Computer text box, then continue with Step 4 to learn how to choose new or different configuration options.

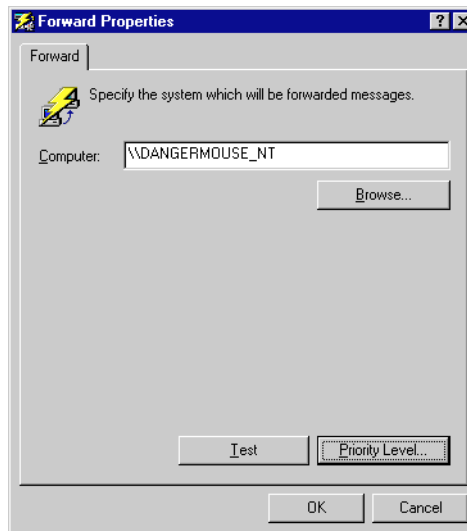


Figure 3-16. Forward Properties dialog box

4. Click Priority Level to specify which types of alert messages the destination computer will receive.

In the Priority Level dialog box that appears (Figure 3-17), drag the slider to the right to send the destination computer fewer, but higher priority, messages. Drag the slider to the left to send the destination computer more alert messages, including lower priority messages. Next, click OK to save your changes and return to the Forward Properties dialog box.

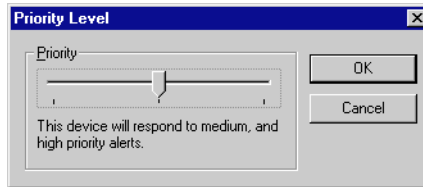


Figure 3-17. Priority Level dialog box

5. Click Test to send the destination computer a test message. The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer for an error message.
6. Click OK to return to the Alert Manager dialog box.
7. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click OK. To close the Alert Manager dialog box without saving changes, click Cancel.

Sending network messages

Alert Manager can send the alert messages that WebShieldX Proxy generates to other computers on your network using a standard Windows NT network message. The alert message appears on the destination computer's screen and requires the recipient to acknowledge it.

To send alerts via network messages, your proxy server must have the Alerter and Messenger Windows NT services running. The destination computers running Windows NT must have the Messenger service running to receive alert messages. Those running Windows 95 or Windows 3.1x must also be running the WinPopup utility to receive network messages. WinPopup comes with some Windows versions. See your Windows documentation for details.

To configure Alert Manager's Network Message options, follow these steps:

Step	Action
------	--------

- | | |
|----|---|
| 1. | Open the Alert Manager Properties dialog box. |
| 2. | Click the Network Message tab. |

Response: The Network Message page (Figure 3-18) appears with a list of all of the computers you have chosen to receive network messages. If you have not yet chosen any destination computers, this list will be blank.

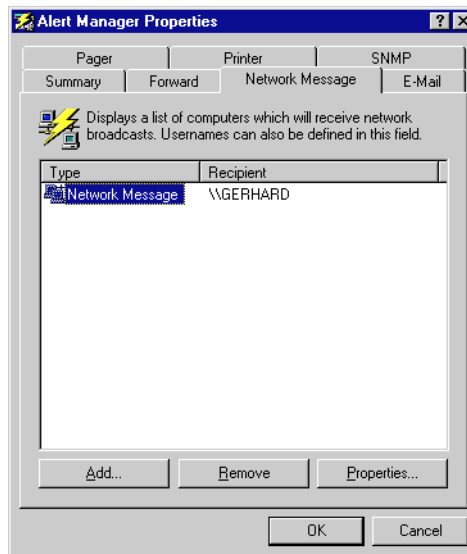


Figure 3-18. Alert Manager Properties dialog box (Network Message page)

- | | |
|----|---|
| 3. | To update this list, you can: <ul style="list-style-type: none"> ▪ Remove a listed computer. Select one of the destination computers listed, then click Remove. |
|----|---|

- **Add a computer to the list.** Click Add to open the Network Message Properties dialog box (Figure 3-19), then enter the name of the destination computer in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the computer on the network. To choose additional options, continue with Step 4.
- **Change configuration options.** Select one of the destination computers listed, then click Properties. Alert Manager opens the Network Message Properties dialog box (Figure 3-19). Change any of the information you want to change in the Computer text box, then continue with Step 4 to learn how to choose new or different configuration options.

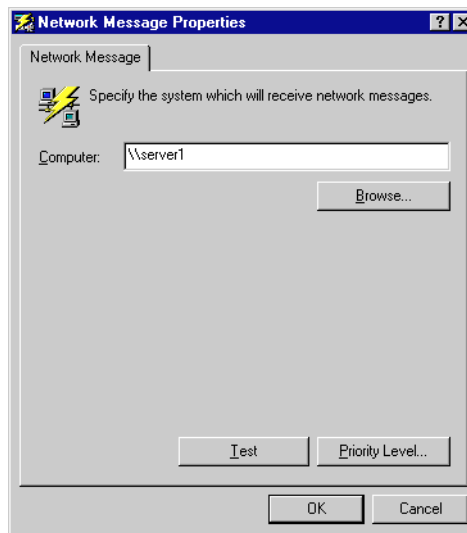


Figure 3-19. Network Message Properties dialog box

4. Click Priority Level to specify which types of alert messages the destination computer will receive.

In the Priority Level dialog box (see Figure 3-17 on page 54), drag the slider to the right to send the destination computer fewer, but higher priority, messages. Drag the slider to the left to send the destination computer more network messages, including lower priority messages. Next, click OK to save your changes and return to the Network Message Properties dialog box.

5. Click Test to send the destination computer a test message.

The message will appear instantly on the destination computer's screen and the recipient will need to click OK to acknowledge it. If your recipient does not receive the message, check the Windows NT Event Viewer for an error message.

6. Click OK to return to the Alert Manager Properties dialog box.
7. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click OK. To close the Alert Manager dialog box without saving changes, click Cancel.

Sending alert messages to e-mail addresses

Alert Manager can send the alert messages that WebShieldX Proxy generates to a recipient's e-mail address using standard Internet mail. The alert message appears in the recipient's mail box. If your message is particularly urgent, you might want to supplement an e-mail message with other methods to ensure that your recipient sees the alert in time to take appropriate action.

To configure Alert Manager's E-mail options, follow these steps:

Step	Action
------	--------

- | | |
|----|---|
| 1. | Open the Alert Manager Properties dialog box. |
| 2. | Click the E-Mail tab. |

Response: The E-Mail page (Figure 3-18 on page 55) appears with a list of the e-mail addresses to which you want to send alert messages. If you have not yet chosen any e-mail addresses, this list will be blank.

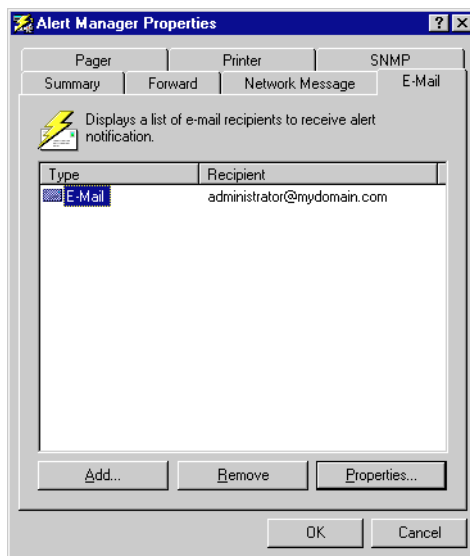


Figure 3-20. Alert Manager Properties dialog box (E-Mail page)

3. To update this list, you can:
 - **Remove a listed address.** Select one of the e-mail addresses listed, then click Remove.
 - **Add an e-mail address to the list.** Click Add to open the E-Mail Properties dialog box (see [Figure 3-21 on page 59](#)). Enter the e-mail address for your alert recipient in the Address text box, enter a subject in the Subject text box, then enter your e-mail address in the From text box. Use the standard Internet address format `<username>@<domain>`—`administrator@mydomain.com`, for example. To choose additional options, continue with [Step 4](#).

- **Change configuration options.** Select one of the e-mail addresses listed, then click Properties. Alert Manager opens the E-Mail Properties dialog box (Figure 3-21). Change any of the information you want to change in the text boxes shown, then continue with [Step 4](#) to learn how to choose new or different configuration options.

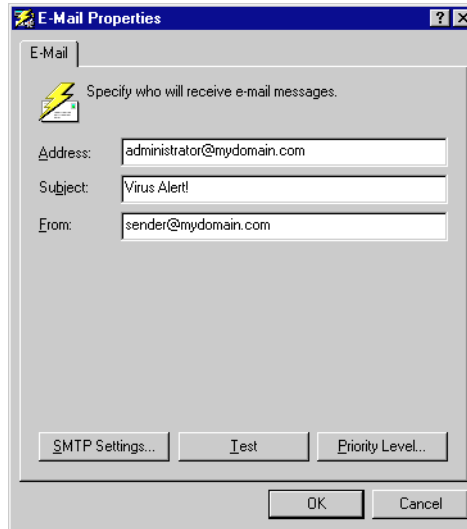


Figure 3-21. E-Mail Properties dialog box

4. Click Priority Level to specify which types of alert messages your recipient will receive.

In the Priority Level dialog box (see [Figure 3-17 on page 54](#)), drag the slider to the right to send the recipient fewer, but higher priority, messages. Drag the slider to the left to send the recipient more messages, including lower priority messages. Next, click OK to save your changes and return to the E-Mail Properties dialog box.

5. Click SMTP Settings to specify the network server you use to send Internet mail via Simple Mail Transfer Protocol. In the dialog box that appears (Figure 3-22), enter the server name in the Server text box and a username for an active mail account that WebShieldX Proxy can use to log on to the server in the Login text box.

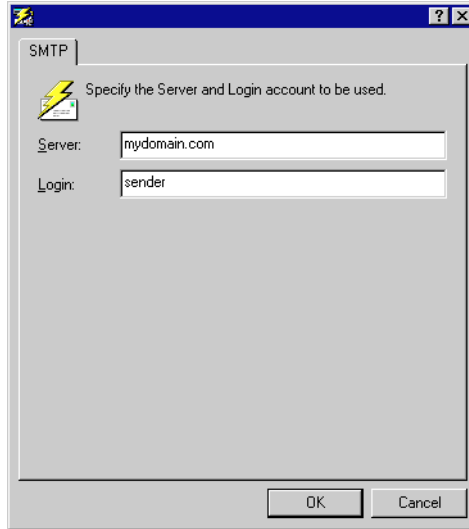


Figure 3-22. SMTP dialog box

You can enter the server name as an Internet Protocol (IP) address, as a name your local domain name server can recognize, or in Universal Naming Convention (UNC) notation. Click OK to save your changes and return to the E-Mail Properties dialog box.

6. Click Test to send a test message to the e-mail address you entered. The message will appear in your recipient's mailbox.
7. Click OK to return to the Alert Manager Properties dialog box.
8. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click OK. To close the Alert Manager dialog box without saving changes, click Cancel.

Sending alert messages to pagers

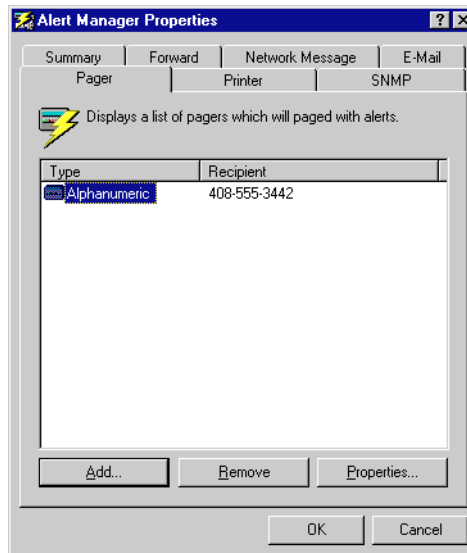
Alert Manager can send the alert messages that WebShieldX Proxy generates to a recipient's pager, provided that you have a modem and telephone line connected to your proxy server. Alert Manager supports both alphanumeric pagers and pagers that receive only numeric messages. Depending on how your recipient's paging service operates, you might need to write a custom script to dial and select the correct menu options before WebShieldX Proxy can deliver its message.

To configure Alert Manager's Pager options, follow these steps:

Step	Action
------	--------

- | | |
|----|---|
| 1. | Open the Alert Manager Properties dialog box. |
| 2. | Click the Pager tab. |

Response: The Pager page (Figure 3-23) appears with a list of the pager numbers to which you want to send alert messages. If you have not yet chosen any pager numbers, this list will be blank.



**Figure 3-23. Alert Manager Properties dialog box
(Pager page)**

3. To update this list, you can:

- **Remove a listed pager number.** Select one of the pager numbers listed, then click Remove.
- **Add a pager number to the list.** Click Add to open the Pager Properties dialog box (see [Figure 3-24 on page 63](#)). Choose the type of pager your recipient uses from the list at the top of the page, then enter the information for that pager type in the text boxes provided.
 - If your recipient uses an alphanumeric pager, enter the pager number and, if necessary, the recipient's ID and password in the text boxes provided. Next, select the Use Alert Message button to send WebShieldX Proxy's standard alert message, or select the Use Custom Message button, then enter your custom message in the text box below.
 - If your recipient uses a numeric pager, enter the pager number and the numeric message you want to send in the text boxes provided. Next, enter in the Delay box the number of seconds Alert Manager should wait before transmitting its message.

Give Alert Manager enough time to get past the initial greeting and any other preliminary messages the paging service plays before it accepts messages. If the service requires touch tones to activate menu options, you might need to write a login script for use with your modem.

To choose additional options, continue with [Step 4](#).

- **Change configuration options.** Select one of the pager numbers listed, then click Properties. Alert Manager opens the Pager Properties dialog box (see [Figure 3-24 on page 63](#)). Change any of the information you want to change in the text boxes shown, then continue with [Step 4](#) to learn how to choose new or different configuration options.

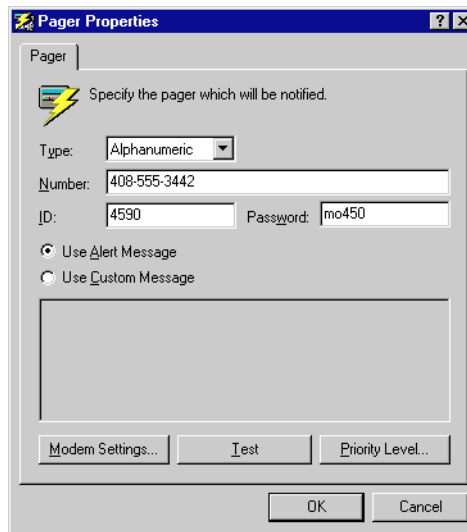


Figure 3-24. Pager Properties dialog box

4. Click Priority Level to specify which types of alert messages your recipient will receive.

In the Priority Level dialog box (see [Figure 3-17 on page 54](#)), drag the slider to the right to send the recipient fewer, but higher priority, messages. Drag the slider to the left to send the recipient more messages, including lower priority messages. Next, click OK to save your changes and return to the Pager Properties dialog box.

5. Click Modem Settings to configure your modem to send pager messages. In the dialog box that appears (see [Figure 3-25 on page 64](#)), choose the type of modem connected to your server from the Modem list, the COM port it uses from the Port list, and the rate at which it can transmit data from the Baud list. Next, enter in the text boxes provided any dialing prefixes or suffixes the modem must dial to reach outside lines, use particular long-distance carriers, enter personal identification numbers or perform similar tasks.

Choose the dialing method—Tone or Pulse—that you want the modem to use and click the Speaker Off checkbox to have the modem dial and connect silently. Click OK to save your settings and return to the Pager Properties dialog box.

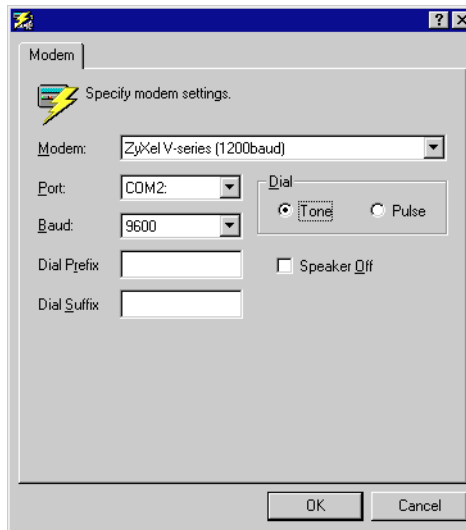


Figure 3-25. Modem dialog box

6. Click Test to send a test message to the pager number you entered. If your recipient uses an alphanumeric pager, he or she will receive a text message from Alert Manager. If your recipient uses a numeric pager, he or she will see the telephone number or other message you specified in the Pager Properties dialog box.
7. Click OK to return to the Alert Manager Properties dialog box.
8. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click OK. To close the Alert Manager dialog box without saving changes, click Cancel.

Sending alert messages to printers

Alert Manager can send the alert messages that WebShieldX Proxy generates as a print job for your network print server to process. To use this option, you must first set up your printer with the Windows Print Manager and choose the correct printer driver for your target printer. See your Windows documentation for details.

To configure Alert Manager's Printer options, follow these steps:

Step	Action
------	--------

- | | |
|----|---|
| 1. | Open the Alert Manager Properties dialog box. |
| 2. | Click the Printer tab. |

Response: The Printer page (Figure 3-26) appears with a list of all of the network printers you have chosen to receive alert messages. If you have not yet chosen any printers, this list will be blank.

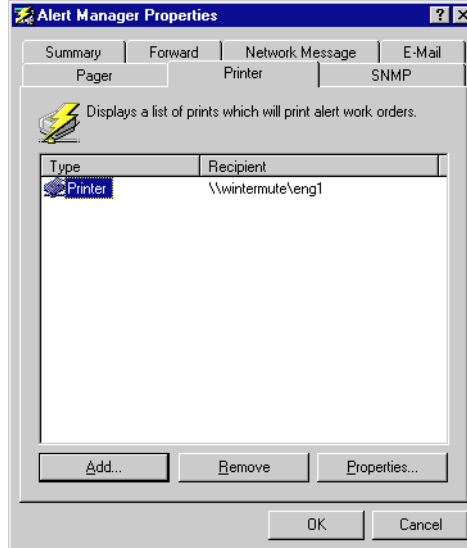


Figure 3-26. Alert Manager Properties dialog box (Printer page)

3. To update this list, you can:

- **Remove a listed printer.** Select one of the printers listed, then click Remove.
- **Add a printer to the list.** Click Add to open the Printer Properties dialog box (Figure 3-27), then enter the name of the target printer in the text box provided. You can enter the printer name in Universal Naming Convention (UNC) notation, or you can click Browse to locate the printer on the network. To choose additional options, continue with Step 4.
- **Change configuration options.** Select one of the target printers listed, then click Properties. Alert Manager opens the Printer Properties dialog box (Figure 3-27). Change any of the information you want to change in the Computer text box, then continue with Step 4 to learn how to choose new or different configuration options.



Figure 3-27. Network Message Properties dialog box

4. Click Priority Level to specify which types of alert messages the destination printer will receive.

In the Priority Level dialog box (see [Figure 3-17 on page 54](#)), drag the slider to the right to send the destination printer fewer, but higher priority, messages. Drag the slider to the left to send the destination printer more network messages, including lower priority messages. Next, click OK to save your changes and return to the Printer Properties dialog box.

5. Click Test to send the destination printer a test message. The message will print as a simple, unformatted line of text.
6. Click OK to return to the Alert Manager Properties dialog box.
7. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click OK. To close the Alert Manager dialog box without saving changes, click Cancel.

Sending alert messages via SNMP

Alert Manager can send the alert messages that WebShieldX Proxy generates to other computers via the Simple Network Management Protocol (SNMP). To see the alert messages that WebShieldX Proxy sends, you must have an SNMP management system configured with an SNMP viewer, such as Hewlett-Packard's OpenView. To learn how to set up and configure your SNMP management system, see the documentation for your SNMP viewer software.

To configure WebShieldX Proxy to send alert messages via SNMP, follow these steps:

- | Step | Action |
|------|---|
| 1. | Open the Alert Manager Properties dialog box. |
| 2. | Click the SNMP tab. |

Response: The SNMP page (Figure 3-26) appears.

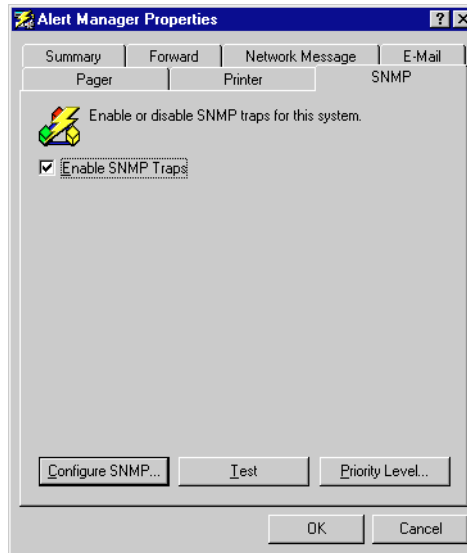


Figure 3-28. Alert Manager Properties dialog box (SNMP page)

3. Select the Enable SNMP Traps checkbox.
4. Click Priority Level to specify which types of alert messages your SNMP management computer will receive.

In the Priority Level dialog box (see [Figure 3-17 on page 54](#)), drag the slider to the right to send the SNMP management computer fewer, but higher priority, messages. Drag the slider to the left to send the SNMP management computer more messages, including lower priority messages. Next, click OK to save your changes and return to the Printer Properties dialog box.

To use this option, you must also install and activate the Windows NT SNMP service on the same machine that runs WebShieldX Proxy. If you have not yet done so, follow these steps:

Step	Action
------	--------

- | | |
|----|-----------------------|
| 1. | Click Configure SNMP. |
|----|-----------------------|

Response: The Windows NT Network control panel dialog box appears. Click the Services tab to open the Services property page (Figure 3-29).

Figure 3-29. The Network control panel dialog box (Service page)

- | | |
|----|---|
| 2. | Click Add to install the Windows NT SNMP service, then follow the Microsoft installation instructions to complete your setup. You can find complete details in the Microsoft TCP/IP Help file included with Windows NT. |
| 3. | When you have finished installing the service, return to the Alert Manager's SNMP page. |

4. Click Test to send the SNMP management computer a test message. To see the message you sent, start your SNMP viewer software.
5. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click OK. To close the Alert Manager dialog box without saving changes, click Cancel.

4

Using a Web Browser to Configure WebShieldX

Displaying the Configuration Pages


WebShieldX Proxy offers you two ways to configure and manage its scanning operations. One method allows you to use the WebShield X Proxy Administration Console to see and change configuration options. To learn how to set up and use that method, see [Chapter 3, “Using the Administration Console.”](#) The method outlined in this chapter uses a web browser to connect to the server running WebShieldX Proxy. To use this method, you must also install and configure Microsoft’s Internet Information Server. See your Windows NT Server documentation for more details.

To use your web browser to configure WebShieldX Proxy, follow these steps:

- | Step | Action |
|------|--|
| 1. | Verify that you have installed and started both WebShieldX Proxy and Microsoft’s Internet Information Server on your proxy server. |
| 2. | Start your web browser software on the computer you want to use to administer WebShieldX Proxy. You can use any computer on your network that can connect to your proxy server. |
| 3. | Enter the Uniform Resource Locator (URL) for your proxy server in the Address or the Location text box, then append the path to wscancfg.dll, WebShieldX Proxy’s administration application. The complete URL should look like this: |

`http://<computer>/webshieldx/wscancfg.dll?`

You can enter the computer name as an IP address or as a name that your network’s domain name server can recognize.

 *Not all browsers require you to add the final ? to the path and filename.*

4. To see the WebShieldX Proxy configuration pages, you must log onto your proxy server with administrator rights. Enter your username and password when prompted, then click OK to continue.

Response: The first WebShieldX Proxy configuration page (Figure 4-1) appears in your browser window.

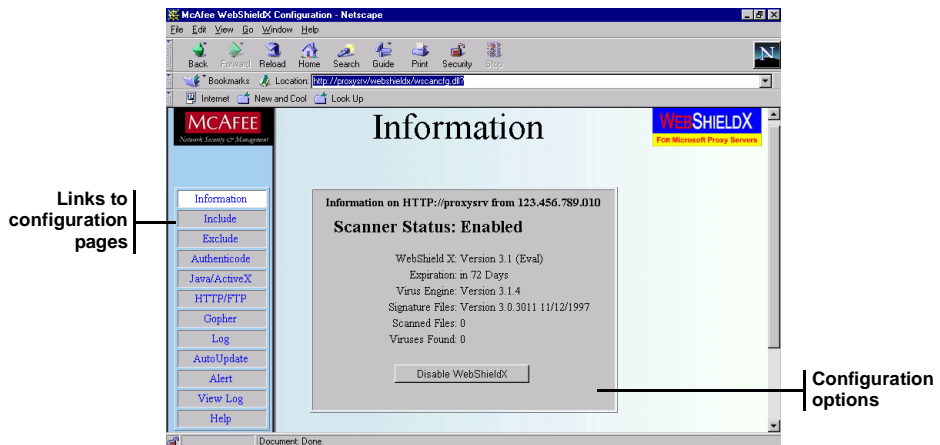


Figure 4-1. WebShieldX Proxy Configuration Pages

WebShieldX Proxy's configuration options appear in your browser's main window. A separate frame along the left side of the browser window lists each of the configuration pages available. Click each listed name to link to the corresponding page and see each set of options.

Once you have chosen your options on a configuration page, click Submit to save your changes and send your commands to WebShieldX Proxy's administration application. Be sure to do so before you move to another configuration page—WebShieldX Proxy does **not** save any options you choose after you leave a configuration page unless you first click Submit.

Once you have finished configuring WebShieldX Proxy, you may use your web browser for other tasks, or quit to disconnect from the WebShieldX Proxy administration application.

Configuring WebShieldX Proxy

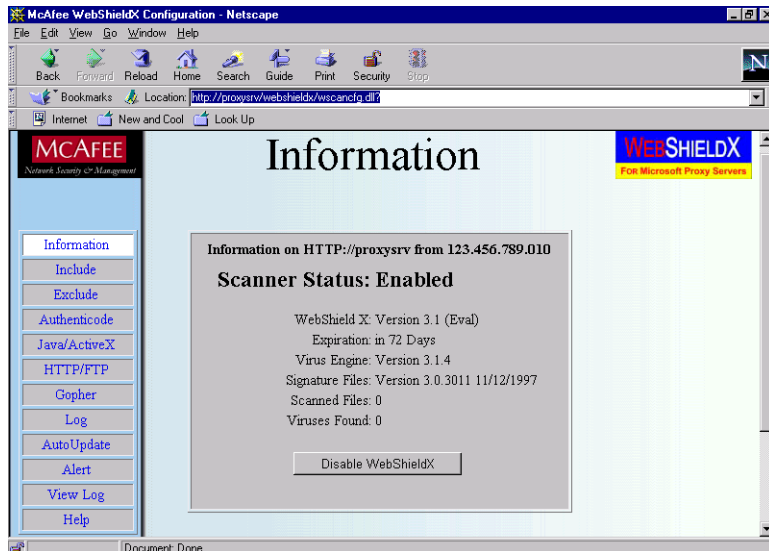
You can use your browser software to configure and manage WebShieldX Proxy from any computer on your network that can connect to your proxy server. The following summary describes the available configuration pages:

- **Information.** This page lists WebShieldX Proxy's anti-virus engine and data file specifications, reports the number of files it scanned and the number of viruses it found, and allows you to disable WebShieldX Proxy.
- **Include.** Use this page to specify which file types WebShieldX Proxy should scan for viruses or other malicious code.
- **Exclude.** Use this page to specify which Multipurpose Internet Mail Extension (MIME) types WebShieldX Proxy should skip during scanning operations—audio files, image files or video files, for example. Most MIME files in these categories are not susceptible to virus infection.
- **Authenticode.** Use this page to check incoming files for authentication certificates and to block those without valid certificates. You can check executable files, Java applets and .CAB files. To learn more about Microsoft Authenticode™, see <http://microsoft.com/security>.
- **Java/ActiveX.** Use this page to tell WebShieldX Proxy how to respond when it detects potentially harmful Java or ActiveX objects, or malicious script code, such as JavaScript or VBScript. You can block all objects and scripts, block only objects known to cause harm, or allow all objects and scripts to pass through the proxy server. This page also includes options for logging WebShieldX Proxy actions and sending alert messages.
- **HTTP/FTP.** Use this page to tell WebShieldX Proxy to look for viruses in Internet traffic sent via either or both of these protocols. You can configure WebShieldX Proxy to clean, reject, quarantine, or ignore infected files that it finds. This page also includes options for logging WebShieldX Proxy actions and sending alert messages.
- **Gopher.** Use this page tell WebShieldX Proxy to scan Gopher traffic. This page has the same response options as those for HTTP/FTP scanning.
- **Log.** Use this page to activate the WebShieldX Proxy activity logs. You can have the program save activity information to a log file or to the Windows NT Event Viewer. Use this page also to specify your quarantine directory.
- **AutoUpdate.** Use this page to schedule data file updates for WebShieldX Proxy. You can update automatically or on demand.

- **Alert.** This link takes you to another set of configuration pages for the web-based version of McAfee's Alert Manager. Each configuration page has its own link in a frame along the left side of the browser window. Use these pages to send alert messages to other computers, printers, e-mail addresses, and pagers.
- **View Log.** Use this page to open and view WebShieldX Proxy's log file. To see log entries recorded with the Windows NT Event Manager, start the Event Viewer.
- **Help.** Use this page to read WebShieldX Proxy's online help files.

Viewing the WebShieldX Proxy Information page


When you use your browser to connect to WebShieldX Proxy's administration application, the Information page appears first (Figure 4-2). If you have already opened the configuration pages in your web browser and chosen a different page, click the Information link to return to this page.



**Figure 4-2. WebShieldX Proxy Configuration
(Information page)**

This page tells you which versions of WebShieldX Proxy's scanning engine and data files you have installed. The page also shows you the number of files that WebShieldX Proxy has scanned and how many viruses it has found.

To prevent WebShieldX Proxy from scanning your proxy server's cache, click Disable WebShieldX.

 Click *Refresh* (or *Reload* on some browsers) to update the figures shown. WebShieldX Proxy displays usage information when you first connect. After that, you must request updates.

Choosing Include options

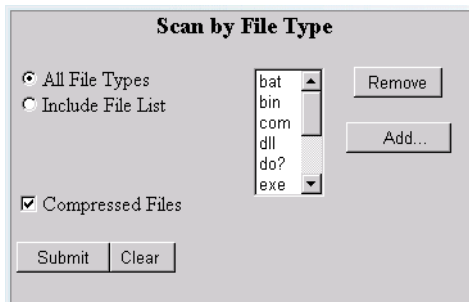
WebShieldX Proxy can look for viruses or identify harmful agents either in all files on your proxy server, or in those files most likely to contain malicious code. Scanning all traffic that passes through your proxy server provides the best protection for your network, but narrowing the scope of WebShieldX Proxy's scan operations improves its performance. To choose the options you want WebShieldX Proxy to use, follow these steps:

Step

Action

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the Include link at the left of your browser window.

Response: The Include configuration options appear in your web browser window (Figure 4-3).




The image shows a web-based configuration window titled "Scan by File Type". It contains two radio buttons: "All File Types" (selected) and "Include File List". Below these is a checked checkbox for "Compressed Files". To the right of the radio buttons is a list box containing file extensions: bat, bin, com, dll, do?, and exe. Above the list box is a "Remove" button, and below it is an "Add..." button. At the bottom of the window are "Submit" and "Clear" buttons.

**Figure 4-3. WebShieldX Proxy Configuration
(Include options)**

2. Choose which files you want WebShieldX Proxy to scan for viruses or malicious code by selecting one of these options:
 - **All File Types.** Select this to tell WebShieldX Proxy to examine all traffic that passes through your proxy server.
 - **Include File List.** Select this to tell WebShieldX Proxy to examine only those files most susceptible to virus infection or most likely to contain harmful agents.
3. Select the Compressed Files checkbox to have WebShieldX Proxy look for viruses in files compressed in .ZIP, .LHA or .CAB formats.

To determine which filename extensions WebShieldX Proxy uses to identify files likely to contain malicious code, continue with [Step 4](#). Otherwise, skip to [Step 7](#).

 *By default, WebShieldX Proxy identifies files with the extensions .BAT, .BIN, .COM, .DLL, .EXE, .DO?, .OCX, .SCR, .VBX, .VXD, and .XL? as those most likely to harbor malicious code, which includes viruses, harmful Java or ActiveX objects, and dangerous JavaScript or VBScript. 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.*

4. To remove a filename extension from the default list, select it, then click Remove.
5. To add a filename extension to the default list, click Add.

Response: The Add File Type to Include dialog box (Figure 4-4) appears.

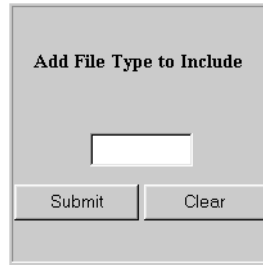


Figure 4-4. Add File Type to Include dialog box

6. Type the filename extension you want to add in the text box provided, then click Submit to send your command to WebShieldX Proxy.

Response: Your web browser returns to the Include options page and the filename extension appears in the default file list.

✍ WebShieldX Proxy adds new filename extensions to the bottom of the list, not in alphabetical order.

7. Click Submit to save the options you chose without leaving the Include page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

✍ Clicking Clear will not undo any changes you already saved by clicking Submit.

Choosing Exclude options

Files that contain no executable code—video, audio, and image data, for example—cannot contain viruses or other malicious agents. Because data files of this sort make up a large part of the file attachments that network users receive via e-mail or download from the Internet, excluding them from WebShieldX Proxy scanning operations can improve the program's performance considerably.

WebShieldX Proxy can exclude MIME file attachments—files encoded with the widely supported Multipurpose Internet Mail Extension standard—from its scanning operations by looking at their content-type headers. The content-type header is a portion of a MIME-encoded e-mail message that identifies what sort of file attachment it carries. E-mail software and associated programs use the header information to decide which applications can open and work with the data contained in the file attachment.

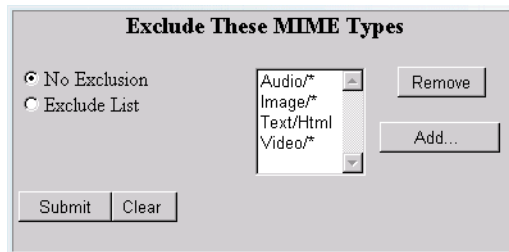
The content-type header consists of two parts: a “type” designation chosen from a standard list of content type names—“video,” “audio,” or “text,” for example; and a “subtype” designation chosen from a central registry of subtype names. E-mail software and other programs that support the MIME standard can read and interpret these headers, then locate and open the correct application. See RFC 2046 at <http://ds.internic.net/ds/dspg1intdoc.html> for a thorough discussion of MIME content-type headers. See <http://www.iana.org> for a list of registered MIME types and subtypes.

To determine which files WebShieldX Proxy should not scan, follow these steps:

Step**Action**

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the Exclude link at the left of your browser window.

Response: The Exclude configuration options appear in your web browser window (Figure 4-5).



Exclude These MIME Types

☒ No Exclusion
☐ Exclude List

Audio/*
Image/*
Text/Html
Video/*


Remove
Add...

Submit Clear

**Figure 4-5. WebShieldX Proxy Configuration
(Include options)**

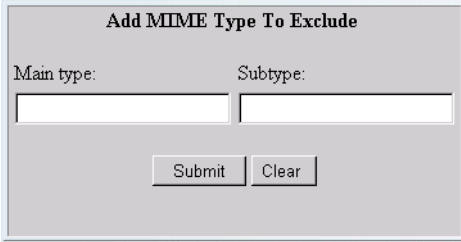
2. Choose which MIME-encoded files you want WebShieldX Proxy to exclude from its scanning operations by selecting one of these options:
 - **No Exclusion.** Select this to tell WebShieldX Proxy to scan all MIME-encoded files.
 - **Exclude List.** Select this to tell WebShieldX Proxy to exclude files with the content-type headers specified in the exclusion list shown at the center of the page.

To designate the MIME-encoded files that the program will not scan, continue with [Step 3](#). Otherwise, skip to [Step 6](#).

 *By default, WebShieldX Proxy does not scan files with these content-type headers: Audio/*, Image/*, Text/*, and Video/*.*

3. To remove a MIME content-type header from the exclusion list, select it, then click Remove. WebShieldX Proxy will now scan this file type.
4. To add a MIME content-type header to the default list, click Add. WebShieldX Proxy will not scan files that have the content-type headers you add to the list.


Response: The Add MIME Type to Exclude page appears ([Figure 4-6](#)).




The dialog box is titled "Add MIME Type To Exclude". It contains two text input fields: "Main type:" and "Subtype:". Below these fields are two buttons: "Submit" and "Clear".

Figure 4-6. Add MIME Type to Exclude dialog box


5. Enter the content-type header and the subtype you want to add to the exclusion list in the text boxes provided, then click Submit.

 *WebShieldX Proxy allows you to specify * as a wildcard designation for all subtypes.*

Response: Your web browser returns to the Exclude options page and the MIME content-type header you entered appears at the bottom of the exclusion list.


 *MIME content-type headers appear in the order you add them to the exclusion list, not in alphabetical order.*

6. Click Submit to save the options you chose without leaving the Exclude page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Choosing Authenticode options

WebShieldX Proxy can look for valid Microsoft Authenticode certificates in file attachments and block those with invalid or missing certificates from access to your proxy server. Authenticode is a Microsoft security standard built into Internet Explorer 3.0 and later that allows software developers to “sign” their products with a tamper-proof digital certificate. WebShieldX Proxy can read and verify these certificates—you can decide whether to allow those with invalid certificates to have access to your proxy server.

 *Authenticode support extends only to certain platforms and development environments. Consult <http://www.microsoft.com/security> for details.*

To configure WebShieldX Proxy to look for Authenticode certificates, follow these steps:

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the Authenticode link at the left of your browser window.

Response: The Authenticode/Signing configuration options appear in your web browser window (Figure 4-7)




The image shows a web browser window titled "Check for Authenticode/Signing". It contains three checkboxes: "Executables", "Java Applets", and "CAB Files". Below these is a checkbox labeled "Reject, if file is not signed". Underneath is a section titled "Reports" with two checkboxes: "Enable Logging" and "Enable Alerting". At the bottom are two buttons: "Submit" and "Clear".

**Figure 4-7. WebShieldX Proxy Configuration
(Authenticode/Signing options)**

2. In the Check For Authenticode/Signing area, select the items you want WebShieldX Proxy to verify. Clear the checkboxes beside items you do not want verified. You may choose all, any, or none of these items:
 - **Executables.** Select this to have WebShieldX Proxy verify certificates for ActiveX controls and other executable files.
 - **Java Applets.** Select this to have WebShieldX Proxy verify certificates for Java classes and applets.
 - **CAB Files.** Select this to have WebShieldX Proxy verify certificates for files archived in the compressed application binary (.CAB) format.

3. Select the Reject If File Is Not Signed checkbox to tell WebShieldX Proxy to block any files that do not have valid Authenticode certificates. Clearing this checkbox allows unverified files to pass through to your proxy server.
4. To have WebShieldX Proxy generate alert messages when it detects invalid or missing Authenticode certificates and to log its actions, select either or both of these checkboxes:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked, how many had valid Authenticode certificates and how many files it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which Log options you choose. See “Choosing Log options” on page 90 for details.
 - **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected a file with an invalid Authenticode certificate. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy’s Alert options. See “Configuring Alert Options” on page 97 for details.
5. Click Submit to save the options you chose without leaving the Authenticode page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Choosing Java/ActiveX options

WebShieldX Proxy can examine any Java classes, ActiveX controls or JavaScript code on your proxy server for potential danger. You can choose to filter Java classes and ActiveX controls by comparing them with an internal database of classes and controls known to cause harm. You can also choose to block all harmful objects and script code—such as JavaScript or VBScript—or let it all pass through your proxy server unimpeded. With WebShieldX Proxy’s scanning features, your network users benefit from the interactive features available at some websites without your having to worry about possible harm to the network, and without needing to turn off Java or ActiveX access in each user’s browser software.

To configure WebShieldX Proxy to examine Java and ActiveX objects and script code, follow these steps:

- | Step | Action |
|------|--|
| 1. | Use your web browser to connect to the WebShieldX Proxy administration application, then click the Java/ActiveX link at the left of your browser window. |

Response: The Java/ActiveX configuration options appear in your web browser window (Figure 4-8).

The screenshot shows a web browser window titled "Java/ActiveX". It contains three sections: "Java", "Scripts", and "ActiveX". Each section has radio buttons for "Block", "Filter", and "Pass Through". The "Filter" option is selected in all three sections. In the "Scripts" section, there are also checkboxes for "Enable Logging" (checked) and "Enable Alerting" (unchecked). At the bottom, there are "Submit" and "Clear" buttons.


Java/ActiveX	
Java	
<input type="radio"/> Block	
<input checked="" type="radio"/> Filter	
<input type="radio"/> Pass Through	
Scripts	
<input type="radio"/> Block	<input checked="" type="checkbox"/> Enable Logging
<input checked="" type="radio"/> Pass Through	<input type="checkbox"/> Enable Alerting
ActiveX	
<input type="radio"/> Block	
<input checked="" type="radio"/> Filter	
<input type="radio"/> Pass Through	
<input type="button" value="Submit"/>	<input type="button" value="Clear"/>

**Figure 4-8. WebShieldX Proxy Configuration
(Java/ActiveX options)**

2. Select the actions you want WebShieldX Proxy to take when it finds potentially harmful objects or malicious code. You can have WebShieldX Proxy respond in different ways to each element.
 - To respond to harmful Java classes or ActiveX controls, select one of the following actions:
 - **Block.** Select this to deny all Java and ActiveX objects access to your proxy server.
 - **Filter.** Select this to compare Java and ActiveX objects to a database of objects known to cause harm. WebShieldX Proxy then allows only those objects not likely to cause harm on to your proxy server.
 - **Pass Through.** Select this to allow Java and ActiveX objects access to your proxy server whether they could cause harm or not. Depending on how you have configured its logging and alert options, WebShieldX Proxy can still log its actions and can send alert messages when it discovers a harmful object. (See Step 3, below.)
 - To respond to harmful script code, select one of the following actions:
 - **Block.** Select this to deny all script code access to your proxy server.
 - **Pass Through.** Select this to allow script code to remain on your proxy server whether it could cause harm or not. This option could expose your network users to harm from malicious code.

Depending on how you have configured its logging and alert options, WebShieldX Proxy can still log its actions and can send alert messages when it discovers a harmful Java object. (See Step 3, below.)

3. To tell WebShieldX Proxy to send alert messages and log its actions when it detects potentially harmful objects or malicious code, select either or both of these checkboxes:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked and how many files it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which Log options you choose. See “Choosing Log options” on page 90 for details.
 - **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected a potentially harmful object or malicious code. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy’s Alert options. See “Configuring Alert Options” on page 97 for details.
4. Click Submit to save the options you chose without leaving the Java/ActiveX page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Choosing HTTP/FTP options

WebShieldX Proxy can look for viruses in all network traffic sent via Hyper Text Transfer Protocol (HTTP) or File Transfer Protocol (FTP), then respond with the actions you specify here when it finds a virus. You can configure scanning operations for each protocol separately, telling WebShieldX Proxy to block infected files from access to your proxy server, to allow files to pass through the server unimpeded, to quarantine infected files in a particular directory, or to remove viruses from infected files before allowing them onto your server.

To configure WebShieldX Proxy to look for viruses in HTTP and FTP traffic, follow these steps:

Step**Action**

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the HTTP/FTP link at the left of your browser window.

Response: The HTTP/FTP configuration options appear in your web browser window (Figure 4-9).

The image shows a web-based configuration window for WebShieldX Proxy. It has a light gray background and a thin border. At the top, there is a checkbox labeled "Enable HTTP Scanning" which is checked. Below this is a section titled "If Virus Found:" containing three radio buttons: "Clean Files" (selected), "Reject Files", and "Pass Through". To the right of these radio buttons are two checkboxes: "Enable Logging" (checked) and "Enable Alerting" (unchecked). Below the "If Virus Found:" section is another checkbox labeled "Quarantine Infected Files" which is checked. This entire section is enclosed in a box. Below this box is another identical section for "Enable FTP Scanning", also with the "Clean Files" radio button selected and "Quarantine Infected Files" checked. At the bottom of the window are two buttons: "Submit" and "Clear".


**Figure 4-9. WebShieldX Proxy Configuration
(HTTP/FTP options)**

2. Select the Enable HTTP Scanning checkbox or the Enable FTP Scanning checkbox, or both, to have WebShieldX Proxy monitor each type of traffic.
3. Select the actions you want WebShieldX Proxy to take when it finds infected files—you can tell the program to respond in different ways for each protocol. Your options are:
 - ❑ **Clean Files.** Select this to have WebShieldX Proxy remove virus code from infected files. The cleaned files remain on your proxy server.

- ❑ **Reject Files.** Select this to deny infected files access to your proxy server. The rejected files do not remain on your server.
- ❑ **Pass Through.** Select this to allow infected files to remain on your proxy server whether they could cause harm or not. Although this can expose your network users to the risk of virus infection, you can quarantine infected files (see Step 4 below) and keep them in a directory separate from your proxy cache.

Depending on how you have configured its logging and alert options, WebShieldX Proxy can also log its actions and can send alert messages when it discovers a harmful object. (See Step 5, below.)

4. Select either or both of the Quarantine Infected Files checkboxes to have WebShieldX Proxy preserve copies of infected files found in each type of traffic. The program can quarantine files regardless of how else you ask it to respond when it finds infections.
5. To have WebShieldX Proxy send alert messages and log its actions, select either or both of these checkboxes for each type of traffic:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked, how many infected files it found, how many it cleaned, and how many it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which Log options you choose. See “Choosing Log options” on page 90 for details.
 - **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected an infected file. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy’s Alert options. See “Configuring Alert Options” on page 97 for details.
6. Click Submit to save the options you chose without leaving the HTTP/FTP page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

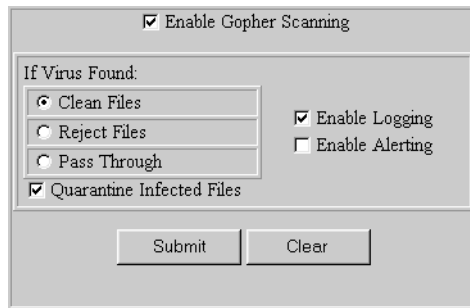
Choosing Gopher options

WebShieldX Proxy can look for viruses in all network traffic sent to your proxy server from Gopher servers, then respond with the actions you specify here when it finds a virus. You can tell WebShieldX Proxy to block infected files from access to your proxy server, to allow files to pass through the server unimpeded, to quarantine infected files in a particular directory, or to remove viruses from the infected files before allowing them onto your server.

To configure WebShieldX Proxy to look for viruses in Gopher traffic, follow these steps:

- | Step | Action |
|-------------|--|
| 1. | Use your web browser to connect to the WebShieldX Proxy administration application, then click the Gopher link at the left of your browser window. |

Response: The Gopher configuration options appear in your web browser window (Figure 4-10).

A screenshot of a web-based configuration window titled "WebShieldX Proxy Configuration (Gopher options)". At the top, there is a checkbox labeled "Enable Gopher Scanning" which is checked. Below this is a section titled "If Virus Found:" containing three radio buttons: "Clean Files" (selected), "Reject Files", and "Pass Through". To the right of these radio buttons are two checkboxes: "Enable Logging" (checked) and "Enable Alerting" (unchecked). At the bottom of the form, there is a checkbox labeled "Quarantine Infected Files" which is checked. Below the checkboxes are two buttons: "Submit" and "Clear".

**Figure 4-10. WebShieldX Proxy Configuration
(Gopher options)**


2. Select the Enable Gopher Scanning checkbox to have WebShieldX Proxy monitor Gopher traffic on your proxy server.
3. Select the actions you want WebShieldX Proxy to take when it finds infected files. The program can respond in any of these ways:

- ❑ **Clean Files.** Select this to have WebShieldX Proxy remove virus code from infected files. The cleaned files remain on your proxy server.
- ❑ **Reject Files.** Select this to deny infected files access to your proxy server. The rejected files do not remain on your server.
- ❑ **Pass Through.** Select this to allow infected files to remain on your proxy server whether they could cause harm or not. Although this can expose your network users to the risk of virus infection, you can quarantine infected files (see Step 4 below) and keep them in a directory separate from your proxy cache.

Depending on how you have configured its logging and alert options, WebShieldX Proxy can also log its actions and can send alert messages when it discovers a harmful object. (See Step 5, below.)

4. Select the Quarantine Infected Files checkbox to have WebShieldX Proxy preserve copies of infected files found in Gopher traffic. The program can quarantine files regardless of how else you ask it to respond when it finds infections.
5. To have WebShieldX Proxy send alert messages and log its actions, select either or both of these checkboxes:
 - **Enable Logging.** Select this to have WebShieldX Proxy record how many files it checked, how many infected files it found, how many it cleaned, and how many it rejected. The program records this information in its own log file, in the Windows NT Event Viewer, or both, depending on which Log options you choose. See “Choosing Log options” on page 90 for details.
 - **Enable Alerting.** Select this to have WebShieldX Proxy tell you or others when it has detected an infected file. The program sends alert messages via the methods you choose when you configure WebShieldX Proxy’s Alert options. See “Configuring Alert Options” on page 97 for details.

6. Click Submit to save the options you chose without leaving the Gopher page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Choosing Log options

WebShieldX Proxy can record its actions in its own log file and it can report its actions via the Windows NT Event Viewer. The options you choose on the Log configuration page tell WebShieldX Proxy which types of log files to set up and how to maintain them. To tell WebShieldX Proxy what information you want it to collect and record in each type of log file, you must activate the logging options in each of the other configuration pages.

To see the information WebShieldX Proxy reports via the Windows NT Event Viewer, click Start in the Windows NT taskbar, point to Programs, then to Administrative Tools (Common). Next, choose Event Viewer to open the Windows NT Event Viewer window. Locate an event that lists WebShieldX in the Source column, then double-click it to see the detail window.

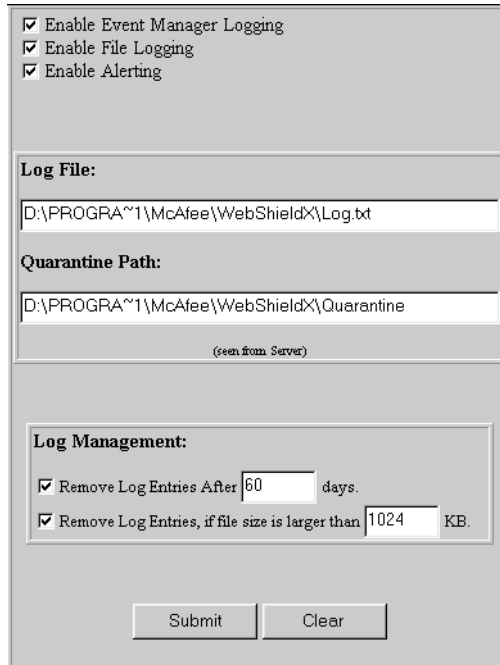
To see the information WebShieldX Proxy records in its own log file, click the View Log File link at the left of the browser window. You can also use any text editor or any word processing software to open, view or print the file. To use a different path or filename for your WebShieldX Proxy log file, first use a text editor to create and name a text file, then enter the filename and path in the Log File text box in the middle of the page. See Step 3 below for details.

Other options on this page allow you to determine when to discard existing log entries and which directory you want to use to quarantine infected files.

To tell WebShieldX Proxy to set up and maintain log files, follow these steps:

Step	Action
1.	Use your web browser to connect to the WebShieldX Proxy administration application, then click the Log link at the left of your browser window.

Response: The Log configuration options appear in your web browser window (Figure 4-11).




The screenshot shows a web browser window displaying the WebShieldX Proxy configuration page for log options. At the top, there are three checked checkboxes: 'Enable Event Manager Logging', 'Enable File Logging', and 'Enable Alerting'. Below these is a section titled 'Log File:' with a text box containing the path 'D:\PROGRA~1\McAfee\WebShieldX\Log.txt'. Underneath is a section titled 'Quarantine Path:' with a text box containing the path 'D:\PROGRA~1\McAfee\WebShieldX\Quarantine'. Below the text boxes is a small text '(seen from Server)'. At the bottom of the form is a 'Log Management:' section with two checked checkboxes: 'Remove Log Entries After' followed by a text box with '60' and the word 'days', and 'Remove Log Entries, if file size is larger than' followed by a text box with '1024' and the label 'KB'. At the very bottom are two buttons: 'Submit' and 'Clear'.


Figure 4-11. WebShieldX Proxy Configuration (Log options)

2. Select the Enable Event Manager Logging checkbox or the Enable File Logging checkbox, or both, to have WebShieldX Proxy record and report its actions.
3. Enter the path and filename you want to use for your log file in the Log File text box. By default, you'll find the log file in this path on the proxy server:

`c:\Program Files\McAfee\WebShieldX\Log.txt`


 *The path you enter here will tell WebShieldX Proxy where on the proxy server to store its log file. You may enter a filename and a path to a different computer on the network, but you must enter the path as you would see it if you were working from the proxy server and the file must already exist on the other computer.*

4. To keep the log file size manageable, select the Remove Log Entries After ____ Days checkbox or the Remove Log Entries If File Size Is Larger than ____ KB checkbox, or both. Next, enter in the text boxes provided the number of days you want WebShieldX Proxy to wait before it discards old log entries and the maximum size, in kilobytes, to which you want your log file to grow.

 *By default, WebShieldX Proxy retains log entries for 60 days and allows your log file to grow to one megabyte in size. When it reaches the limits you set in the Log Management area, WebShieldX Proxy deletes all existing entries and starts the log file again.*


To choose a directory to serve as your quarantine area, enter the path and filename in the Quarantine Path text box. By default, WebShieldX Proxy moves infected files to this directory on the proxy server:

`c:\Program Files\McAfee\WebShieldX\Quarantine`

 *The path you enter here will tell WebShieldX Proxy where on the proxy server to store infected files. You may enter a path to a different computer on the network, but you must enter the path as you would see it if you were working from the proxy server.*

To have WebShieldX Proxy send alert messages when it detects viruses or other harmful code, select the Enable Alerting checkbox. This activates whatever alert methods you have configured in the Alert configuration pages. To see and configure your Alert options, click Submit to save your log options, then click the Alert link at the left of the browser window. See [“Configuring Alert Options” on page 97](#) to learn how to choose your Alert options.

Click Submit to save the options you chose without leaving the Log page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Choosing AutoUpdate options

WebShieldX Proxy includes AutoUpdate, a utility you can use to update the data files (.DAT) the program uses to detect viruses and other malicious code. You can use this same utility to upgrade the entire program, either by purchasing an upgrade, or by upgrading for free if your license permits. AutoUpdate connects with McAfee's website and locates any new data files stored there, either at scheduled intervals or when you want it to check for them. The options you choose in the AutoUpdate page tell WebShieldX Proxy when to schedule update requests.


To set your AutoUpdate options, follow these steps:

- | Step | Action |
|------|--|
| 1. | Use your web browser to connect to the WebShieldX Proxy administration application, then click the AutoUpdate link at the left of your browser window. |

Response: The AutoUpdate configuration options appear in your web browser window (Figure 4-12).

**Figure 4-12. WebShieldX Proxy Configuration
(AutoUpdate options)**

2. Select the Enable AutoUpdate checkbox to have WebShieldX Proxy look for updated files according to the schedule you set in the following steps.
3. Select a time interval to schedule WebShieldX Proxy's next connection. You can choose one of these options from the Interval area:
 - **Only Once.** Select this to have WebShieldX Proxy check for updated files only once. Enter the month, day and year you want the program to perform this check in the text boxes provided, then enter a particular time (see Step 4 below).


 *You must enter the year using four digits—WebShieldX Proxy is Year 2000—compliant*

 - **Day of the week.** Select this to have WebShieldX Proxy check once per week for updated files. Choose the day of the week during which the program should perform this check from the list to the right, then enter a particular time (see Step 4 below).
 - **Day of every month.** Select this to have WebShieldX Proxy check once per month for updated files. Choose the date on which the program should perform this check from the list to the right. Be sure to choose a date that occurs each month—choosing 31, for example, will skip updates for February and for months with only 30 days. Next, enter a particular time (see Step 4 below).
4. Enter the time, in hours and minutes, when WebShieldX Proxy should connect to the McAfee website to check for updated files. Enter the time using a 24-hour clock in the text box labeled Update Time.
5. Enter the website address WebShieldX Proxy should use to connect to the McAfee website in the text box labeled Update URL (Uniform Resource Locator). By default, the update address is:

`ftp://ftp.mcafee.com/pub/antivirus/datfiles/3.x/`

You can enter any address here to which you can connect via anonymous FTP. McAfee makes its software available on other electronic services, such as America Online and Compuserve. See “How To Contact McAfee” on page 15 for details.

6. To send an update request immediately, without waiting for the next update you've scheduled, click Update Now at the bottom of the AutoUpdate page. WebShieldX Proxy immediately connects with the McAfee website.
7. Check the Info area to learn when WebShieldX Proxy last connected to the McAfee website, when it last updated its data files, and its current update status.
8. Click Submit to save the options you chose without leaving the Log page. To configure other WebShieldX Proxy options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Choosing Alert options

The Alert link takes you to a different set of configuration pages for WebShieldX Proxy's Alert Manager. You can also link to the Alert Manager configuration pages by clicking Start in the Windows taskbar, pointing to Programs, then to McAfee WebShieldX before choosing Web-based Alert Manager Configuration.

Response: The Summary configuration page appears (see Figure 4-14 on page 98).

Descriptions of Alert configuring procedures and management begin with "Configuring Alert Options" on page 97.

Viewing the WebShieldX Proxy log file

Click the View Log link to view WebShieldX Proxy's log file in a separate browser window. To see this log file, you must have selected the Enable File Logging checkbox in the Log page and the various log options in other configuration pages. To return to the WebShieldX Proxy configuration pages after you see the log, click your browser's Back button. To see log information from the Windows NT Event Viewer, start the event viewer, then look for any event that lists WebShieldX as its source. See "Choosing Log options" on page 90 for details.

Getting help

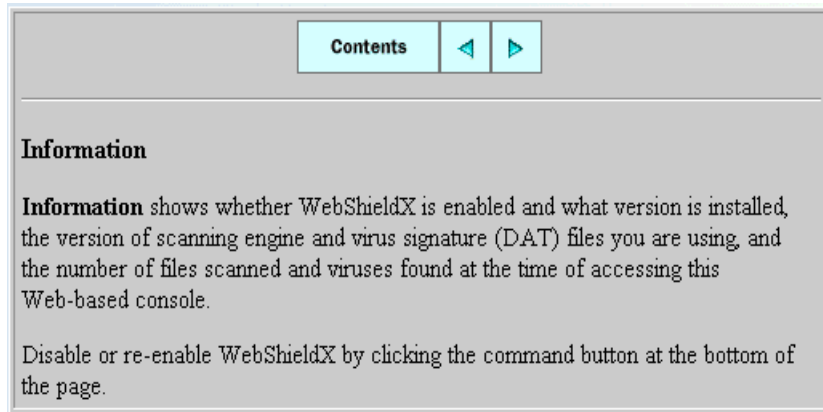
WebShieldX Proxy includes online help that you can view with the aid of your web browser.

Step

Action

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the Help link at the left of your browser window.

Response: The Help window appears in your browser window. WebShieldX Proxy shows you the help page that corresponds to the last configuration page you visited. If you clicked the Information link then the Help link, for example, you'd see the page shown in Figure 4-13.



**Figure 4-13. WebShieldX Proxy Configuration
(Help page)**

2. Click Contents at the top of the Help page to see a list of Help topics. Click a topic to view its Help page.
3. Click the left or right arrow at the top of the help page to see the previous or the next help topic in the series.

Configuring Alert Options

For the configuration pages available through your web browser, WebShieldX Proxy uses a different version of McAfee's Alert Manager utility to notify you or others when it detects a virus or malicious code in files on your proxy server. This version of Alert Manager gives you the same set of notification options available through the WebShieldX Proxy Administration Console. You can use these options individually or in combinations that suit your needs.

If you have McAfee's Alert Manager utility installed on other computers on your network, you can also forward alert messages to computers in other domains, which can in turn notify the workstations that they host about infected files on your proxy server. Alert Manager supports McAfee's Centralized Alerting technology, available with products such as McAfee NetShield. For details, consult the NetShield *User's Guide*.

To see the Alert Manager configuration pages and choose configuration options, follow these steps:

Step

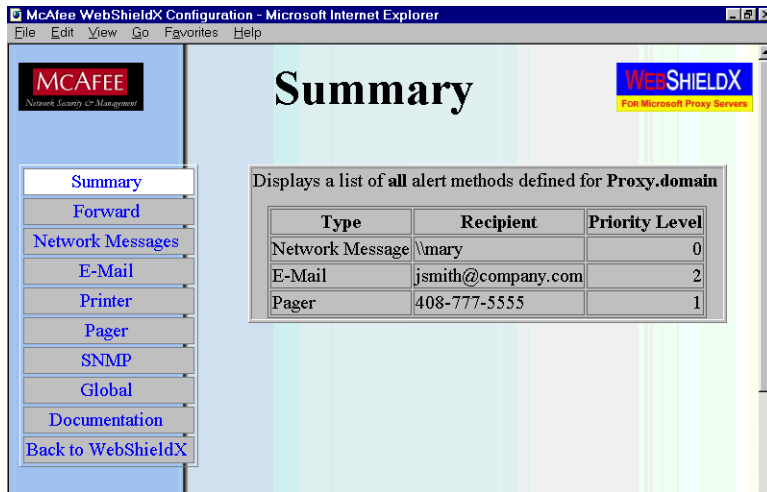
Action

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window.

Response: The first Alert Manager configuration page appears in your web browser window (see [Figure 4-14 on page 98](#)). A separate frame along the left side of the browser window lists each of the other Alert Manager configuration pages available.

2. Click each listed name to link to the corresponding page and see each set of options.

Once you have chosen your options on an Alert Manager configuration page, click Submit to save your changes and send your commands to WebShieldX Proxy's administration application. Be sure to do so before you move to another configuration page—WebShieldX Proxy does **not** save any options you choose after you leave a configuration page unless you first click Submit.



**Figure 4-14. WebShieldX Proxy Alert Manager
(Summary page)**

The Alert Manager dialog box includes six different alert methods, each with configuration options shown in individual property pages. Other configuration pages have different options that correspond to one or more of these alert methods.

Click the tab corresponding to the alert method you want to configure to see the options available. When you have finished choosing your options, click the Back to WebShieldX link to return to the WebShieldX Proxy configuration pages or use your web browser for other tasks. You can also quit your browser software to disconnect from the WebShieldX Proxy administration application.

The following sections describe the options available for each method.

Viewing the Summary Page

The Summary page lists all of the alert methods you've told WebShieldX Proxy to use to notify you when it finds a virus or other malicious code on your proxy server. In the example shown in Figure 4-15, the Alert Manager will send alerts to an e-mail address, to a network server, and to another computer. If you have not yet configured Alert Manager, the Summary Page will be blank.

Displays a list of all alert methods defined for gerhard		
Type	Recipient	Priority Level
Network Message	\\dangermouse_nt	0
E-Mail	administrator@mydomain.com	0
Forward	\\nervecenter\\centalrt	0

**Figure 4-15. WebShieldX Proxy Alert Manager
(Summary page detail)**

To change what you see in this page, you must choose options from each of the other Alert Manager configuration pages. Click the link that corresponds to the alert method shown in the Type column to change your settings. When you return to the summary page, WebShieldX Proxy updates the information you see here.

See the following sections to learn more about the options available for each alert method.

Forwarding alert messages to other computers

Alert Manager can forward the alert messages that WebShieldX Proxy generates to other computers on your network. If you have installed the console version of Alert Manager on each of the destination computers, they can in turn forward alert messages to the recipients listed in their Alert Manager Summary pages. You might use this feature to pass alert messages across network domains or to construct a hierarchical arrangement for passing alert messages.

To configure Alert Manager's Forwarding options, follow these steps:

Step**Action**

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window.
2. Click the Forward link.

Response: The Forward page (Figure 4-16) appears with a list of all of the computers you have chosen to receive forwarded messages. If you have not yet chosen any destination computers, this list will be blank.

Displays a list of all alert methods defined for gerhard			
Type	Recipient	Priority Level	Action
Forward	\\nervecenter\centalrt	0	Edit... Remove
			Add...

**Figure 4-16. WebShieldX Proxy Alert Manager
(Forward page detail)**

3. To update this list, you can:
 - **Remove a listed computer.** Click Remove in the Action column beside one of the destination computers listed.
 - **Add a computer to the list.** Click Add to link to the Forward properties configuration page (Figure 4-17), then enter the name of the computer that will receive forwarded messages in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation. To choose additional options, continue with Step 4.
 - **Change configuration options.** Click Edit in the Action column beside one of the destination computers listed to link to the Forward properties configuration page (Figure 4-17). Change any of the information you want to change in the Computer text box, then continue with Step 4 to learn how to choose new or different configuration options

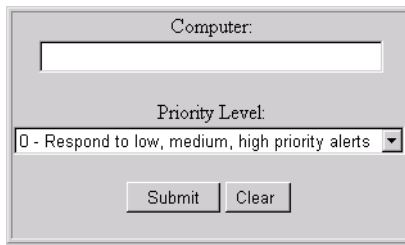



Figure 4-17. Forward properties configuration page (detail)


4. Choose a priority level from the list to specify which types of alert messages the destination computer will receive.

Set the Priority Level at zero to send the destination computer all alert messages, no matter what their priority. Set the priority level at 1 to send the destination computer fewer, but higher priority, messages—it will receive only those designated medium or high priority. Set the priority level to 2 to send the destination computer only messages with high priority.

Next, click Submit to save your changes and return to the Forward configuration page. Click Clear to discard your changes and start again.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

5. Click Submit to save the options you chose without leaving the Forward page. To configure other Alert Manager options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Sending network messages

Alert Manager can send the alert messages that WebShieldX Proxy generates to other computers on your network using a standard Windows NT network message. The alert message appears on the destination computer's screen and requires the recipient to acknowledge it.

To send alerts via network messages, your proxy server must have the Alerter and Messenger Windows NT services running. The destination computers running Windows NT must have the Messenger service running to receive alert messages. Those running Windows 95 or Windows 3.1x must also be running the WinPopup utility to receive network messages. WinPopup comes with some Windows versions. See your Windows documentation for details.

To configure Alert Manager's Network Message options, follow these steps:

- | Step | Action |
|------|---|
| 1. | Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window. |
| 2. | Click the Network Messages link. |

Response: The Network Messages page (Figure 4-18) appears with a list of all of the computers you have chosen to receive network messages. If you have not yet chosen any destination computers, this list will be blank.

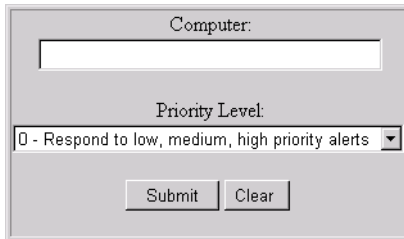
Displays a list of **all** alert methods defined for **gerhard**

Type	Recipient	Priority Level	Action
Network Message	\\dangermouse_nt	0	Edit... Remove
			Add...

**Figure 4-18. WebShieldX Proxy Alert Manager
(Network Messages page detail)**

3. To update this list, you can:

- **Remove a listed computer.** Click Remove in the Action column beside one of the destination computers listed.
- **Add a computer to the list.** Click Add to link to the Network Message properties configuration page (Figure 4-19), then enter the name of the computer that will receive forwarded messages in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation. To choose additional options, continue with Step 4.
- **Change configuration options.** Click Edit in the Action column beside one of the destination computers listed to link to the Network Message properties configuration page (Figure 4-19). Change any of the information you want to change in the Computer text box, then continue with Step 4 to learn how to choose new or different configuration options.



Computer:

Priority Level:

0 - Respond to low, medium, high priority alerts ▼


Submit Clear

Figure 4-19. Network Message properties configuration page (detail)


4. Choose a priority level from the list to specify which types of alert messages the destination computer will receive.

Set the Priority Level at zero to send the destination computer all alert messages, no matter what their priority. Set the priority level at 1 to send the destination computer fewer, but higher priority, messages—it will receive only those designated medium or high priority. Set the priority level to 2 to send the destination computer only messages with high priority.

Next, click Submit to save your changes and return to the Network Messages configuration page. Click Clear to discard your changes and start again.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

5. Click Submit to save the options you chose without leaving the Network Messages page. To configure other Alert Manager options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Sending alert messages to e-mail addresses

Alert Manager can send the alert messages that WebShieldX Proxy generates to a recipient's e-mail address using standard Internet mail. The alert message appears in the recipient's mail box. If your message is particularly urgent, you might want to supplement an e-mail message with other methods to ensure that your recipient sees the alert in time to take appropriate action.

To send alerts via e-mail, you must also specify the network server and an account name you use to send Internet mail via Simple Mail Transfer Protocol. To learn how to configure these settings, see [“Choosing Global options” on page 114](#).

To configure Alert Manager's E-mail options, follow these steps:

Step	Action
1.	Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window.
2.	Click the E-Mail link.

Response: The E-Mail page ([Figure 4-20 on page 105](#)) appears with a list of the e-mail addresses to which you want to send alert messages. If you have not yet chosen any e-mail addresses, this list will be blank.

Displays a list of **all** alert methods defined for **gerhard**

Type	Recipient	Priority Level	Action
E-Mail	administrator@mydomain.com	0	Edit... Remove
			Add...

**Figure 4-20. WebShieldX Proxy Alert Manager
(E-Mail page detail)**

3. To update this list, you can:

- **Remove an e-mail address.** Click Remove in the Action column beside one of the e-mail addresses listed.
- **Add an e-mail address to the list.** Click Add to link to the E-Mail Properties configuration page (Figure 4-21). Enter the e-mail address for your alert recipient in the Address text box, enter a subject in the Subject text box, then enter your e-mail address in the From text box. Use the standard Internet address format `<username>@<domain>`—`administrator@mydomain.com`, for example. To choose additional options, continue with [Step 4](#).
- **Change configuration options.** Click Edit in the Action column beside one of the e-mail addresses listed to link to the E-Mail properties configuration page (Figure 4-21). Change any of the information you want to change in the text boxes shown, then continue with [Step 4](#) to learn how to choose new or different configuration options.

Address:

Subject:

From:


Priority Level:
 ▼

**Figure 4-21. E-Mail properties
configuration page (detail)**


4. Choose a priority level from the list to specify which types of alert messages your e-mail recipient will receive.

Set the Priority Level at zero to send your recipient all alert messages, no matter what their priority. Set the priority level at 1 to send the recipient fewer, but higher priority, messages—he or she will receive only those designated medium or high priority. Set the priority level to 2 to send the recipient only messages with high priority.

Next, click Submit to save your changes and return to the E-Mail configuration page. Click Clear to discard your changes and start again.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

5. Click Submit to save the options you chose without leaving the E-Mail page. To configure other Alert Manager options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Sending alert messages to printers

Alert Manager can send the alert messages that WebShieldX Proxy generates as a print job for your network print server to process. To use this option, you must first set up your printer with the Windows Print Manager and choose the correct printer driver for your target printer, either from your proxy server or from the print server you intend to use. See your Windows documentation for details.

To configure Alert Manager's Printer options, follow these steps:

Step	Action
1.	Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window.
2.	Click the Printer link.

Response: The Printer page (Figure 4-22) appears with a list of all of the network printers you have chosen to receive alert messages. If you have not yet chosen any printers, this list will be blank.

Displays a list of **all** alert methods defined for **gerhard**

Type	Recipient	Priority Level	Action
Printer	\\wintermute\eng_3	2	Edit... Remove Add...

Figure 4-22. WebShieldX Proxy Alert Manager (Printer page detail)

3. To update this list, you can:
 - **Remove a listed printer.** Click Remove in the Action column beside one of the printers listed.
 - **Add a printer to the list.** Click Add to link to the Printer properties configuration page (Figure 4-23), then enter the name of the printer that will receive alert messages in the text box provided. You can enter the printer name in Universal Naming Convention (UNC) notation. To choose additional options, continue with Step 4.
 - **Change configuration options.** Click Edit in the Action column beside one of the printers listed to link to the Printer properties configuration page (Figure 4-23). Change any of the information you want to change in the Printer text box, then continue with Step 4 to learn how to choose new or different configuration options.

Printer:

\\wintermute\eng_3

Priority Level:

0 - Respond to low, medium, high priority alerts ▼


Submit Clear

Figure 4-23. Network Message properties configuration page (detail)


4. Choose a priority level from the list to specify which types of alert messages the printer will receive.

Set the Priority Level at zero to send the printer all alert messages, no matter what their priority. Set the priority level at 1 to send the printer fewer, but higher priority, messages—it will receive only those designated medium or high priority. Set the priority level to 2 to send the printer only messages with high priority.

Next, click Submit to save your changes and return to the Printer configuration page. Click Clear to discard your changes and start again.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

5. Click Submit to save the options you chose without leaving the Printer page. To configure other Alert Manager options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

Sending alert messages to pagers

Alert Manager can send the alert messages that WebShieldX Proxy generates to a recipient's pager, provided that you have a modem and telephone line connected to your proxy server. Alert Manager supports both alphanumeric pagers and pagers that receive only numeric messages. Depending on how your recipient's paging service operates, you might need to write a custom script to dial and select the correct menu options before WebShieldX Proxy can deliver its message.

To send alerts to pagers, you must also specify settings for the modem attached to your proxy server¹. To learn how to configure these settings, see “Choosing Global options” on page 114.

To configure Alert Manager's Pager options, follow these steps:

- | Step | Action |
|------|---|
| 1. | Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window. |
| 2. | Click the Pager link. |

Response: The Pager page (Figure 4-24) appears with a list of the pager numbers to which you want to send alert messages. If you have not yet chosen any pager numbers, this list will be blank.

Displays a list of **all** alert methods defined for **gerhard**

Type	Recipient	Priority Level	Action
Pager	(888) 555-2910	0	Edit... Remove Add...

Figure 4-24. WebShieldX Proxy Alert Manager (Pager page detail)

3. To update this list, you can:
 - **Remove a listed pager number.** Click Remove in the Action column beside one of the pager numbers listed.
 - **Add a pager number to the list.** Click Add to link to the Pager properties configuration page (see Figure 4-25 on page 110). Choose the type of pager your recipient uses from the list at the top of the page, then enter the information for that pager type in the text boxes provided.
 - If your recipient uses an alphanumeric pager, enter the pager number and, if necessary, the recipient's ID and password in the text boxes provided. Next, select the Use Alert Message button to send WebShieldX Proxy's standard alert message, or select the Use Custom Message button, then enter your custom message in the text box below.

- ❑ If your recipient uses a numeric pager, enter the pager number, then select the Custom Message button. Next, enter the numeric message you want to send in the Custom Message text box. You can ignore the ID and Password text boxes for most numeric pager services. If, however, the service requires touch tones to activate menu options, you might need to write a login script for use with your modem.

To choose additional options, continue with [Step 4](#).

- **Change configuration options.** Click Edit in the Action column beside one of the pager numbers listed to link to the Pager properties configuration page ([Figure 4-25](#)). Change any of the information you want to change in the text boxes shown, then continue with [Step 4](#) to learn how to choose new or different configuration options.

Type: Alphanumeric

Number: (888) 555-2910

ID: jitterbug Password: fiji2178

☐ Use Alert Message
☒ Use Custom Message

Virus Alert!

Priority Level:
0 - Respond to low, medium, high priority alerts


Submit Clear

Figure 4-25. Pager properties configuration page (detail)


4. Choose a priority level from the list to specify which types of alert messages your recipient will receive.

Set the Priority Level at zero to send your recipient all alert messages, no matter what their priority. Set the priority level at 1 to send your recipient fewer, but higher priority, messages—he or she will receive only those designated medium or high priority. Set the priority level to 2 to send your recipient only messages with high priority.

Next, click Submit to save your changes and return to the Pager configuration page. Click Clear to discard your changes and start again.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

5. Click Submit to save the options you chose without leaving the Pager page. To configure other Alert Manager options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

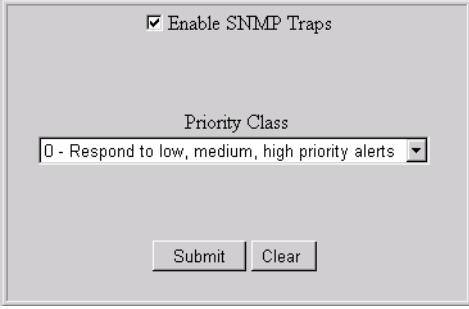
Sending alert messages via SNMP

Alert Manager can send the alert messages that WebShieldX Proxy generates to other computers via the Simple Network Management Protocol (SNMP). To see the alert messages that WebShieldX Proxy sends, you must have an SNMP management system configured with an SNMP viewer, such as Hewlett-Packard's OpenView. To learn how to set up and configure your SNMP management system, see the documentation for your SNMP viewer software.

To configure WebShieldX Proxy to send alert messages via SNMP, follow these steps:

- | Step | Action |
|------|---|
| 1. | Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window. |
| 2. | Click the SNMP link. |

Response: The SNMP page (Figure 4-26) appears.


A screenshot of a web form titled "WebShieldX Proxy Alert Manager (SNMP page detail)". The form has a light gray background and a thin border. At the top, there is a checkbox labeled "Enable SNMP Traps" which is checked. Below this, there is a section titled "Priority Class" containing a dropdown menu. The dropdown menu is open, showing the text "0 - Respond to low, medium, high priority alerts" and a downward-pointing arrow. At the bottom of the form, there are two buttons: "Submit" and "Clear".

**Figure 4-26. WebShieldX Proxy Alert Manager
(SNMP page detail)**

3. Select the Enable SNMP Traps checkbox.
4. Choose a priority level from the Priority Class list to specify which types of alert messages your SNMP management computer will receive.

Set the Priority Level at zero to send the SNMP management computer all alert messages, no matter what their priority. Set the priority level at 1 to send the SNMP management computer fewer, but higher priority, messages—it will receive only those designated medium or high priority. Set the priority level to 2 to send the SNMP management computer only messages with high priority.

5. Click Submit to save the options you chose without leaving the SNMP page. To configure other Alert Manager options, click a different link. To discard the changes you made, click Clear.

 *Clicking Clear will not undo any changes you already saved by clicking Submit.*

To send alert messages via SNMP, you must also install and activate the Windows NT SNMP service on the same machine that runs WebShieldX Proxy. If you have not yet done so, follow these steps:

- | Step | Action |
|-------------|---|
| 1. | Log in to your proxy server using an account with administrator rights. Unless you have remote management software installed, you must log in to the computer you use as your proxy server. |
| 2. | Click Start in the Windows taskbar, point to Settings, then choose Control Panel. |
| 3. | Locate, then double-click the Network control panel. |

Response: The Windows NT Network control panel dialog box appears. Click the Services tab to open the Services property page (Figure 4-27).

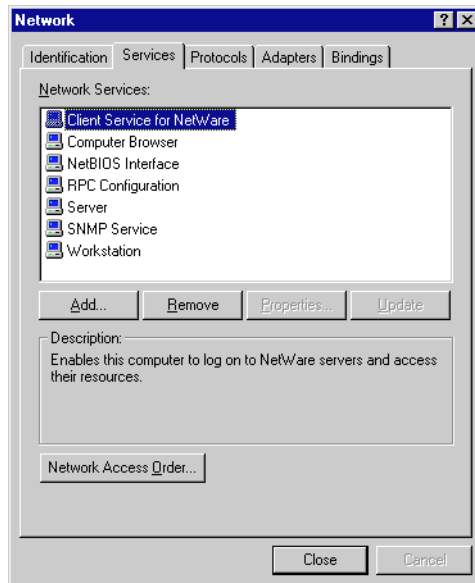


Figure 4-27. The Network control panel dialog box (Service page)

4. Click Add to install the Windows NT SNMP service, then follow the Microsoft installation instructions to complete your setup. You can find complete details in the Microsoft TCP/IP Help file included with Windows NT.

Choosing Global options

Alert Manager's Global configuration page stores the settings that direct e-mail alert messages to the proper SMTP server for delivery and that configure the modem attached to your proxy server.

To configure these settings, follow these steps:

- | Step | Action |
|------|---|
| 1. | Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window. |
| 2. | Click the Global link. |

Response: The Global page appears (Figure 4-28).

E-Mail Account

Server:

Login Account:

Modem Settings

Modem:

Port:

Baud:

Dial Tone:

Dial Prefix:

Dial Suffix:

☐ Speaker Off

**Figure 4-28. WebShieldX Proxy Alert Manager
(Global page detail)**

3. Specify the network server you use to send Internet mail via Simple Mail Transfer Protocol in the Server text box. In the Login Account text box, enter a username for an active mail account that WebShieldX Proxy can use to log on to the server.
4. Specify the settings for the modem connected to your proxy server in the Modem Settings area. Your options are:
 - **Modem.** Choose the type of modem connected to your server from the Modem list. If you do not see your modem model listed, try using one of the Generic High Speed choices, or contact your modem vendor to find out which modem command set to use.
 - **Port.** Choose the COM port your modem uses from the Port list.
 - **Baud.** Choose the rate at which your modem can transmit data from the Baud list.
 - **Dial Tone.** Choose the dialing method—Tone or Pulse—that you want the modem to use.
 - **Dial Prefix.** Enter any dialing prefixes the modem must dial to reach outside lines, use particular long-distance carriers, enter personal identification numbers or perform similar tasks.
 - **Dial Suffix.** Enter any dialing suffixes you want the modem to dial to specify accounting codes, enter Touch Tone ID numbers or passwords, or perform similar tasks.
5. Select the Speaker Off checkbox to have the modem dial and connect silently.
6. Click Submit to save the options you chose without leaving the Global page. To configure other Alert Manager options, click a different link. To discard the changes you made, click Clear.



Clicking Clear will not undo any changes you already saved by clicking Submit.

Viewing online documentation

WebShieldX Proxy includes online help you can use to get a quick overview of the options available in each of the Alert Manager configuration pages. To use the help system, follow these steps:

Step

Action

1. Use your web browser to connect to the WebShieldX Proxy administration application, then click the Alert link at the left of your browser window.
2. Click the Documentation link.

Response: The Documentation window appears in your browser window. WebShieldX Proxy shows you the documentation page that corresponds to the last Alert Manager configuration page you visited. If you clicked the Global link then the Documentation link, for example, you'd see the page shown in Figure 4-29.

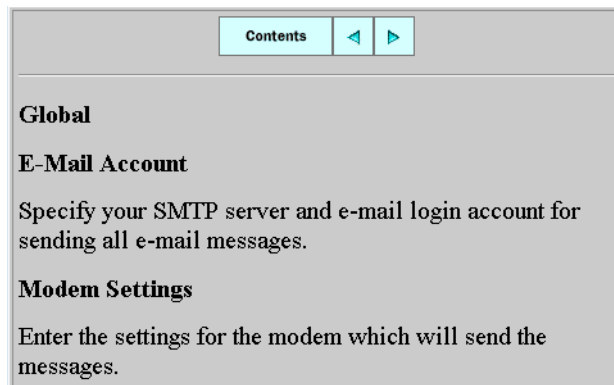


Figure 4-29. WebShieldX Proxy Configuration (Help page)

3. Click Contents at the top of the Documentation page to see a list of help topics. Click a topic to view the corresponding online documentation.
4. Click the left or right arrow at the top of the documentation page to see the previous or the next help topic in the series.

5. To configure other Alert Manager options, click a different link from the list at the left of the browser window.

Returning to WebShieldX Proxy

Click the Back to WebShieldX Proxy link to leave the Alert Manager and return to the WebShieldX Proxy Information configuration page.

A

Preventing Virus Infection

Keys to a Secure System Environment

WebShieldX Proxy is an effective tool for preventing virus infections and harm from Java classes, ActiveX controls, and dangerous script code. 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 WebShieldX Proxy and other McAfee anti-virus software
- Make frequent backups of important files. Even with WebShieldX Proxy 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

Although WebShieldX Proxy uses McAfee's advanced Hunter scanning technology and has sophisticated detection capability that can find previously unknown viruses, the best way to ensure that you have the maximum protection available is to update your WebShieldX Proxy data files. McAfee continually updates the files WebShieldX Proxy uses to detect viruses and harmful applets. For maximum protection, you should download these files on a regular basis. See ["Choosing Update options"](#) on page 47 or ["Choosing AutoUpdate options"](#) on page 93 to learn how to schedule updates for your copy of WebShieldX Proxy.

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 WebShieldX Proxy in detecting these new variations. The data files that came with your copy of WebShieldX Proxy, 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.

 *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. McAfee cannot guarantee that the WebShieldX Proxy .DAT files included with this release will work with previous WebShieldX Proxy versions.*


Updating data files on demand

To connect directly to the McAfee website and update your data files, follow these steps:

- | Step | Action |
|------|--|
| 1. | Download the data file (for example, DAT-3011.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 WebShieldX Proxy is currently installed. Typically, the files are stored in |

C:\Program Files\McAfee\WebShieldX

5. Copy the new files into the appropriate directory or directories, overwriting the old data files.

 *There might be part of the software in more than one directory. If so, place each updated file in the appropriate directory.*

6. Reboot your computer so that changes take place immediately.

Reporting new items for WebShieldX Proxy 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 WebShieldX Proxy 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 WebShieldX support program

All registered owners of single-node (one computer) WebShieldX products 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
 - 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 WebShieldX Deluxe support program

All registered owners of single-node (one computer) WebShieldX Deluxe products 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
 - 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
 - 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

- ActiveX and Java objects
 - allowing through 39, 84
 - blocking 39, 84
 - detecting harmful 38, 82
 - filtering 39, 84
- administration application
 - configuring WebShieldX Proxy via 71
- Administration Console
 - Authenticode page 36
 - AutoUpdate page 47
 - Exclude page 33
 - Gopher page 43
 - HTTP/FTP page 40
 - Include page 31
 - Java/ActiveX page 38
 - Log/Alert page 45
 - Service page 30
 - starting 27
 - what it is 27

- Alert Manager
 - Documentation page 116
 - E-Mail page 57, 104
 - Forward page 52, 99
 - Global page 114
 - Network Message page 54, 102
 - Pager page 61, 108
 - Printer page 65, 106
 - returning to WebShieldX Proxy from 117
 - SNMP page 67, 111
 - Summary page 51, 99
 - using to send alerts to other domains 50, 97
 - version used with Administration Console 50
 - version used with web browser 97

- alert messages
 - enabling for Authenticode verification 37, 82
 - enabling for Gopher scanning 45, 89
 - enabling for HTTP/FTP scanning 42, 87
 - enabling for Java/ActiveX scanning 40, 85
 - sending as network messages 54, 102
 - sending to another computer 52, 99
 - sending to pager numbers 61, 108
 - sending to printers 65, 106
 - sending via e-mail 57, 104
 - sending via Simple Network Management Protocol (SNMP) 67, 111
 - setting global options for using your web browser 114
 - testing 54, 57, 60, 64, 67, 70
- alert methods
 - summary of those in use 51, 99

- alert options
 - configuring 97
- Alert page
 - configuring 95
- Alerter
 - running as Windows NT service 54, 102
- alphanumeric pagers
 - options for sending alert messages to 62, 109
 - support for in Alert Manager 61, 108
- audio content-type header 35
- Authenticode
 - getting more information 36, 80
 - what it is 36, 80
- Authenticode page
 - configuring 36, 80
- AutoUpdate page
 - configuring 47, 93

B

- backups, use of in security program 118
- BAT files 32, 76
- baud rate
 - setting for modem 63, 115
- BIN files 32, 76
- blocking harmful Java and ActiveX objects 39, 84
- Bulletin Board System (BBS)
 - contacting 15

C

- CAB files
 - verifying Authenticode certificates for 37, 81
- Centralized Alerting 50, 97
- certificates, Microsoft Authenticode 36, 80
- cleaning Gopher traffic 44, 89
- cleaning HTTP and FTP traffic 41, 86
- COM files 32, 76
- COM port
 - setting for modem 63, 115
- Comment text box in service page 31
- Compressed Application Binary (CAB) files
 - verifying Authenticode certificates for 37, 81
- compressed files, scanning 32, 76

- configuration options
 - using Administration Console
 - Authenticode page 36
 - AutoUpdate page 47
 - Exclude page 33
 - Gopher page 43
 - HTTP/FTP page 40
 - Include page 31
 - Java/ActiveX page 38
 - Log/Alert page 45
 - Service page 30
 - using your web browser
 - Alert page 95
 - Authenticode page 80
 - AutoUpdate page 93
 - Gopher page 88
 - HTTP/FTP page 85
 - Include page 75
 - Java/ActiveX page 82
 - Log page 90
- configuration pages
 - displaying with your web browser 71
- configuring alert options 97
- console
 - starting the WebShieldX Proxy Administration 27
- contacting McAfee 15

content-type headers
 adding to exclusion list 35
 in MIME files 33, 78
 more information about 33, 78
Customer Care
 contacting 15
 programs 122

D

data files (.DAT)
 updating via AutoUpdate 47, 93
 URL for updates 49
 version number for 30, 74
Disable WebShieldX button
 in Information page 75
DLL files 32, 76
DO? files 32, 76
Documentation page
 in Alert Manager 116

E

e-mail
 address for technical support 15
 contacting McAfee virus researchers via 18
E-Mail page
 in Alert Manager 57, 104
Enable Alert Manager
 checkbox 47, 50
Enable Alerting checkbox 92

Enable AutoUpdate
 checkbox 48, 94
Enable Event Manager
 checkbox 46, 91
Enable File Logging
 checkbox 46, 91, 95
Enable FTP Scanning
 checkbox 41, 86
Enable Gopher Scanning
 checkbox 44, 88
Enable HTTP Scanning
 checkbox 41, 86
Enable SNMP Traps
 checkbox 68, 112
enterprise support 127
Event Viewer
 logging WebShieldX Proxy actions in 45, 90
Exclude page
 configuring 33
EXE files 32, 76
executable files
 verifying Authenticode certificates for 37, 81
extensions
 for susceptible files 32, 76

F

fax-on-demand system 15
features of WebShieldX Proxy 14
File Transfer Protocol (FTP)
 scanning traffic sent via 40, 85
files not susceptible to infection
 excluding 33

files susceptible to infection
 including extensions for 32, 76
filtering harmful Java and ActiveX objects 39, 84
Forward page
 in Alert Manager 52, 99
frequency of updates 48, 94

G

Global page
 in Alert Manager 114
Gopher page
 configuring 43, 88

H

help
 for Alert Manager 116
 viewing 96
Hewlett-Packard OpenView
 as example of SNMP viewer 67, 111
HTTP/FTP page
 configuring 40, 85
Hyper Text Transfer Protocol
 scanning traffic sent via 40, 85

I

image content-type header 35
immediate scan, starting 30

Include page

- Compressed Files
checkbox 32, 76
- configuring 31, 75
- list of files susceptible to
infection 32, 76

Information page

- Disable WebShieldX
button 75

installing WebShieldX Proxy 19

international McAfee offices contacting 17

Internet mail

- address format used for
alert messages 58,
105

Internet Protocol (IP)

address

- as format to enter
WebShieldX Proxy
server address 71
- entering mail server
name as 60

J

Java and ActiveX objects

- allowing through 39, 84
- blocking 39, 84
- detecting harmful 38, 82
- filtering 39, 84
- reporting new items 18

Java applets

- verifying Authenticode
certificates for 37, 81

Java/ActiveX page

- configuring 38, 82

JavaScript

- allowing through 39, 84
- blocking 39, 84
- detecting malicious 38,
82

L

Log page

- configuring 90

Log/Alert page

- configuring 45

logfile

- managing size of 47, 92
- path and filename for
45, 91
- viewing with your web
browser 95

logging

- enabling for
Authenticode
verification 37, 82
- enabling for Gopher
scanning 44, 89
- enabling for HTTP/FTP
scanning 42, 87
- enabling for Java/
ActiveX scanning 40,
85
- using WebShieldX
Proxy logfile for 45, 90
- using Windows NT
Event viewer for 45,
90

M

McAfee

- consulting services 126
- contacting 15
 - BBS 15
 - Customer Care 15
 - outside the United
States 17
 - via America Online
15
 - via CompuServe 15
 - within the United
States 16
- enterprise support 127
- jump start program 127
- support services 121
- training 16, 126

McAfee NetShield

- using to collect alert
messages 50, 97

Messenger

- running as Windows NT
service 54, 102

Microsoft Authenticode

- certificates 36, 80
- getting more information
36, 80
- what it is 36, 80

MIME Extensions dialog box 35

modem

- configuring for alert
messaging 63, 115

Multipurpose Internet Mail Extensions (MIME)

- content-type headers in
33, 78
- excluding from scans 33

N

- NetShield
 - using to collect alert messages 50, 97
- Network control panel 69, 113
- Network Message page
 - in Alert Manager 54, 102
- network messages
 - requirements for sending and receiving 54, 102
- numeric pagers
 - options for sending alert messages to 62, 110
 - support for in Alert Manager 61, 108

O

- OCX files 32, 76
- online help
 - for Alert Manager 116
 - viewing 96
- OpenView
 - as example of SNMP viewer 67, 111

P

- Pager page
 - in Alert Manager 61, 108

Pass Through

- allowing infected files in Gopher traffic onto your server 44, 89
- allowing infected files in HTTP and FTP traffic onto your server 42, 87
- allowing Java and ActiveX objects on to your server 39, 84
- personal support plan 125
- Print Manager
 - setting up printers via 65, 106
- Printer page
 - in Alert Manager 65, 106
- Priority Level
 - setting 53, 56, 59, 63, 67, 68, 101, 103, 106, 108, 111, 112
- professional services
 - consulting 126
 - enterprise support 127
 - jump start program 127
 - training 126
- pulse or tone dialing
 - setting for modem 63, 115

Q

- Quarantine Infected Files checkbox 42, 44, 87, 89

R

- receiving network messages
 - requirements for 54, 102
- Reject If File Is Not Signed checkbox 37, 82
- rejecting infected files
 - in Gopher traffic 44, 89
 - in HTTP and FTP traffic 41, 87
- Remove Log Entries After __ Days checkbox 47, 92
- Remove Log Entries if File Size Is Larger Than __ KB checkbox 47, 92
- reporting items WebShieldX does not detect 18

S

- Scan button
 - in Service page 30
- scan engine
 - version number for 30, 74
- scanning
 - compressed files 32, 76
 - proxy server cache immediately 30
- SCR files 32, 76
- script code
 - allowing through 39, 84
 - blocking 39, 84
- securing your system environment 118

sending alert messages 50, 97

as network messages 54, 102

setting global options for using your web browser 114

to another computer 52, 99

to pager numbers 61, 108

to printers 65, 106

via e-mail 57, 104

via Simple Network Management Protocol (SNMP) 67, 111

sending network messages requirements for 54, 102

Service page

Comment text box 31

configuring 30

information shown 30

Scan button 30

services

Windows NT Alerter 54, 102

Windows NT Messenger 54, 102

Simple Mail Transfer Protocol (SMTP)

sending e-mail alert messages via 60, 115

Simple Network Management Protocol (SNMP)

sending alert messages via 67, 111

SNMP page

in Alert Manager 67, 111

Speaker Off checkbox 63, 115

Submit button

sending commands to WebShieldX Proxy with 72

subscription maintenance program 124

subtype (MIME files) what it is 33, 78

Summary page

in Alert Manager 51, 99

support

fax response 15

programs 122

via e-mail 15

susceptible files

filename extensions for 32, 76

T

technical support

automated voice system 15

contacting 15

fax response system 15

free support policies 122

information needed from user 16

McAfee Bulletin Board System (BBS) 15

online 15, 122

programs 121

via e-mail 15

testing alert messages 54, 57, 60, 64, 67, 70

text content-type header 35

time interval for updates 48, 94

tone or pulse dialing

setting for modem 63, 115

Training

scheduling 16

training for McAfee products 16

U

Uniform Resource Locator (URL)

for data file updates 49

for the WebShieldX Proxy administration application 71

Universal Naming Convention (UNC)

entering mail server name as 60

use of in Alert Manager 53, 56, 66, 100, 103, 107

update, definition of 121

updating

frequency 48, 94

via AutoUpdate 47, 93

updating WebShieldX Proxy 118

upgrade, definition of 121

V

VBScript

- allowing through 39, 84
- blocking 39, 84
- detecting malicious 38, 82

VBX files 32, 76

version numbers for data files and scan engine 30, 74

video content-type header 35

View Log link 95

virus research

- contacting McAfee teams 18

Viruses

- preventing infection 118
- reporting new and unknown 118

viruses

- macro viruses viii
- origins and history vi
- reporting new strains 18
- responding to in Gopher traffic 44, 89
- responding to in HTTP or FTP traffic 41, 86
- similarity with biological viruses vii
- what they are vii
- where they come from vi
- who writes them viii

VXD files 32, 76

W

WebShieldX Proxy

Administration Console

starting 27

as a part of security program 118

benefits of 14

configuring with your web browser 71

disabling from web browser 75

features of 14

installing 19

reporting items not detected by 18, 120

returning to from Alert Manager 117

updating 118

version numbers for data files and scan engine 30, 74

what it does 14

what it is 12

why use it 12

wildcards

using in filename

extensions 32, 76

using in MIME content-type headers 35

Windows 95 and 3.1x

receiving network messages with 54, 102

Windows NT Event Viewer

logging WebShieldX

Proxy actions in 45, 90

Windows NT Server

network messages sent via 54, 102

SNMP service

activating 69, 113

needed to receive SNMP alerts 69, 113

WinPopup

receiving network messages via 54, 102

wscancfg.dll

configuring WebShieldX Proxy with 71

X

XL? files 32, 76