User's Guide

WebScanX for Windows 95 and Windows NT

McAfee Associates, Inc.
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 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, Inc.

TRADEMARK NOTICES

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

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

FEEDBACK

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

Issued June 1997/WebScanX v3.0.0

Table of Contents

Chapter 1. Introducing WebScanX 5

What is WebScanX? 5

WebScanX as online sentry 5

How To Contact Us 6

Customer service 6

Technical support 6

McAfee training 7

International contact information 8

Chapter 2. Installing WebScanX 9

Getting Started 9

Basic System Requirements 9

Installing WebScanX 10

Chapter 3. Using WebScanX 12

Getting Started 12

The WebScanX Icon 12

Accessing the WebScanX Main Window 13

Configuring WebScanX 14

Configuring WebScanX filtering 15

Configuring WebScanX action 17

Configuring WebScanX Centralized Alerting 17

Configuring WebScanX report logs 18

Configuring WebScanX Security 18

Exiting WebScanX 20

Accessing the WebScanX status window 21

Index 22

1 Introducing WebScanX

What is WebScanX?

WebScanX is a new addition to McAfee's family of security tools, and is designed to provide a safe computing environment for internet users, protecting systems running either Windows 95 or Windows NT.

WebScanX as online sentry

WebScanX functions as a sentry for your internet connections. It does this by keeping a list of Java classes, ActiveX controls, and IP addresses that are known to be potentially dangerous. Each time your browser attempts to connect to a website, or when you attempt to download something from the internet, WebScanX filters for a match against this list. When a match is made, WebScanX can alert the user or deny access to these banned objects and prevent the downloading of dangerous files. WebScanX helps protect one of your most important assets—the information on your computer.

WebScanX is an important element of a comprehensive security program that includes a variety of safety measures such as regular backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program.

How To Contact Us

Customer service

To order products or obtain product information, we invite you to contact our Customer Care department at (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. McAfee has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating McAfee software and obtaining the latest news and information. For technical support information and issues, we encourage you to visit our website first.

World Wide Web	http://www.mcafee.com

If you do not find what you need or do not have access to the Web, try one of McAfee's 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
Microsoft Network (MSN)	MCAFEE

If the automated services did not solve your problem, you may contact McAfee Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

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

To speed the process of helping you use our products, please note the following before you call:

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

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

178 Main Street

Unionville, Ontario

Canada L3R 2G9

Phone: (905) 479-4189

Fax: (905) 479-4540

McAfee Europe B.V.

Orlyplein 81 - Busitel 1

1043 DS Amsterdam

The Netherlands

Phone: (0) 31 20 6815500

Fax: (0) 31 20 6810229

McAfee France S.A.

50 rue de Londres

75008 Paris

France

Phone: 33 1 44 908733

Fax: 33 1 45 227554

McAfee Deutschland GmbH

Industriestrasse 1

D-82110 Germering

Germany

Phone: 49 89 8943560

Fax: 49 89 89435699

McAfee (UK) Ltd.

Hayley House, London Road

Bracknell, Berkshire

RG12 2TH

United Kingdom

Phone: 44 1344 304730

Fax: 44 1344 306902

McAfee Japan KK

4F Toranomon Mori Bldg. 33

3-8-21 Toranomon

Minato-Ku

Tokyo, 105

Japan

Phone: 81 3 3435 8246

Fax: 81 3 3435 1349

2 Installing WebScanX

Getting Started

This chapter details the WebScanX installation procedure. Before you begin the installation, however, be sure to review the Basic Sytstem Requirements outlined below.

Basic System Requirements

An IBM-compatible personal computer running one of the following operating systems:

- Windows 95
- Windows NT v3.5.1 or later

Operating system requirements for Windows 95:

- 486 with at least 8MB of memory
- 2MB of free hard drive space

Operating system requirements for Windows NT:

- CPU running Windows NT workstation v3.5.1 or later
- 2MB of free hard drive space

Installing WebScanX

To install WebScanX, complete the following procedure:

Step	Action

1. Start your computer and do one of the following:

- If installing from files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive.
- If installing from a compact disc, insert it into your CD-ROM drive.

  ✍ *You will be prompted to choose which software you wish to install. If you click Install WebScanX, skip to step 3.*

2. Select Run from the Start menu.

- If you are running Windows 95, type the following:

  `x:\WebScanX\win95\setup.exe`

  where `x` is the drive that contains the CD-ROM. Click OK.
- If you are running Windows NT, type the following:

  `x:\WebScanX\WinNT\setup.exe`

  where `x` is the drive that contains the CD-ROM. Click OK.
- If installing from downloaded files, type:

  `x:\path\setup.exe`

  where `x:\path` is the location of the files. Click OK.

Response: The Welcome screen is displayed. Click Next to continue.

3. Select a destination directory for your WebScanX files. Enter the directory in the text box provided, or click Browse to navigate to a specific directory. Click Next to continue.

4. When prompted, review your settings and click Next to continue.

   Response: WebScanX files are copied to the hard drive.

5. Click Yes to review the What's New text file for information on WebScanX.

6. Review the modifications made to files on your system and click Next. A screen appears indicating that the installation is now complete, and that the configurations are finalizing.

7. Select Yes to restart your computer. Click Finish.

   Response: The system restarts. WebScanX is now running.

3 Using WebScanX

Getting Started

This chapter takes you through the step-by-step process of configuring WebScanX to suit your needs. Most of the configuration for WebScanX is done on the Internet Filter property page from the Main Window. This is where you will determine what WebScanX will filter, what action to take, where any network alert messages should be sent, and where to log activity. The Security Page is where you can designate password protection to lock down the filtering for Java classes, ActiveX and IP addresses.

The WebScanX Main Window, Internet Filter property page, and Security page are easily accessed from the WebScanX icon on your computer screen.

The WebScanX Icon

Once the WebScanX installation is complete, the WebScanX icon (the image at far right) will appear on your computer screen (Figure 3-1).

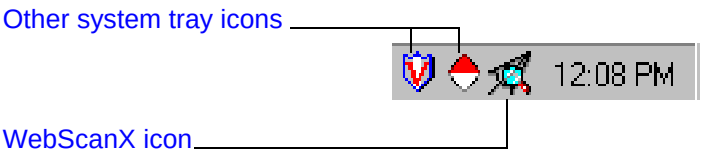

Figure 3-1. The WebScanX Icon

- For Windows 95 and Windows NT 4.0, the WebScanX icon will appear in the taskbar system tray as shown in Figure 3-1.

- For Windows NT 3.5.1, a minimized icon will appear on the bottom left corner of your computer screen.

Accessing the WebScanX Main Window

To access the WebScanX Main Window, simply right-click once on the Web-ScanX icon and select Properties from the pop-up menu. The WebScanX Main Window is displayed with the Internet Filter page on top (Figure 3-2 on page 14).

You are now ready to configure WebScanX.

Configuring WebScanX

Configuring what WebScanX will filter and what action will be taken is both simple and efficient. Most of the functions can be configured on the Internet Filter Page (Figure 3-2).

Figure 3-2. WebScanX Main Window (Internet Filter Property Page)

Take a few moments to look at the Internet Filter Property Page. You'll notice that there are four separate sections on the screen. Each has its own functionality:

Look at the two checkboxes at the top of the window and do the following:

Step	Action
1.	Select Enable Java & ActiveX Filter to activate. When the check box is blank, it means that this feature has been disabled. ("Configuring WebScanX Security" on page 18).

2. Select Load at startup. This ensures that WebScanX is working silently in the background each time you start your computer.

Configuring WebScanX filtering

Determine exactly what WebScanX will filter:

Step	Action

1. Under the Applets area of the Filters section, select the items to be filtered:
   - ActiveX Controls
   - Java Classes
2. Select IP Addresses if you want WebScanX to filter these.

   ✍ *For maximum protection, McAfee recommends filtering all of the above.*

Adding IP addresses and networks

An IP address or network can be added to the .DAT file by the following method, using a plain text editor such as Notepad. The .DAT file tells WebScanX what to filter.

1. Use Notepad to open the file WebScanX.DAT (default location: C:\Program Files\McAfee\WebScanX\WebScanX.DAT).

2. Enter a new line beginning with I, (where the upper case letter I is the identifier for a new IP address), followed by the actual IP address, a forward slash, and the net mask. The net mask defines the range of IP addresses that are within a local network.

- If you are blocking a single host, your new entry should look like this:

  I 192 187 128 17 / 255 255 255 255

- If you are blocking an entire network, your new entry will look like one of these:

  Class C user
  I 205 227 131 0 / 255 255 255 255

  Class B user
  I 125 32 0 0 / 255 255 255 255

  Class A user
  I 15 0 0 0 / 255 255 255 255

✍ *Your net mask will differ from the examples used above.*

3. Save the file. You have now added another IP address that WebScanX will automatically filter.

Configuring WebScanX action

Decide what action WebScanX should take when it detects a banned object you have configured it to filter:

Step	Action

1. From the Action section of the screen, choose one of the following options from the pull down menu:

   - Prompt user
   - Deny access to banned objects

   ✍ *McAfee strongly recommends that you select Deny access to banned objects. This selection allows for no user options, but is the safest choice because it automatically denies access to banned objects and dangerous sites.*

Configuring WebScanX Centralized Alerting

This option is for users who are part of a network that is protected by NetShield, McAfee's server anti-virus solution. Users will always have the option to log activity to a local file. (See "Configuring WebScanX report logs" on page 18).

If you want WebScanX to send a network alert, complete the following procedure:

Step	Action

1. Click in the Send Network Alert To checkbox under Alert.

2. Direct WebScanX where to send the Network alert:

   - Specify the path to the alert file by entering the name of the folder in the text box, or click Browse and navigate to the folder you want.

     ✍ *This path should be to a folder containing the Centralized Alerting file, CENTALERT.TXT. For more information on Centralized Alerting, see the NetShield documentation.*

Configuring WebScanX report logs

WebScanX automatically records its activity in a file of your choice. To define where WebScanX will log its activity, do the following:

Step	Action

1. Click in the Log to File checkbox under Report.

2. Enter the path for the log file in the text box or click Browse and navigate to another existing file.

Configuring WebScanX Security

WebScanX can be password-protected to prevent accidental changes from being made to the configuration. To use password protection, complete the following procedure:

Step	Action

1. Select the Security tab from the WebScanX Main Window.

   Response: The Security property page is displayed on top (Figure 3-3 on page 19)

.

Figure 3-3. WebScanX Main Window (Security Property Page)

2. Select the item(s) to be password-protected, as shown in Figure 3-3.

3. Click the Password button to enter a password. You will be asked to confirm your password.

4. Clilck OK to save your changes and exit the dialogue box. To exit the Password dialogue box without saving your changes, click Cancel.

✍ *Notice the padlock in the locked position next to the item that has been designated for password protection. Conversely, a padlock in the unlocked position indicates that password protection has been disabled.*

Exiting WebScanX

To exit WebScanX at any time, do the following:

Step	Action
1.	Hold down the Shift key and right-click on the WebScanX icon.
2.	Select Exit from the pop-up menu.

✍ *Selecting Exit from the pop-up menu will disable WebScanX and unload it from memory.*

Accessing the WebScanX status window

The WebScanX Status window lists how many Java Classes and ActiveX Controls were filtered, and which IP addresses, if any, were blocked. To access the status window, simply double-click on the WebScanX icon. The WebScanX status window will be displayed on your screen. Click anywhere to exit.

Index

A

ActiveX controls 15
Activity logging 18
America Online 7

B

Banned object 17
BBS 6
Bulletin Board System 6

C

Centralized alerting 17
CompuServe 7
Configuring WebScanX
- action 17
- Network Alerting 17
- report logs 18
- security 18

Customer care 6
Customer service 6

E

Exiting WebScanX 20

F

Filtering
- internet 14
- IP addresses 15

I

Installing 9
Installing WebScanX 9
- Windows NT 10
- Windows 95 10

Internet filter 14
Internet support 6

J

Java classes 15

L

Load at startup 15

M

McAfee
- BBS 6
- international locations 8
- support 6

Microsoft Network (MSN) 7

O

Online support 6
Operating system requirements
- Windows NT 9
- Windows 95 9

P

Password protection 18

R

Report logs 18

S

Security 18
Status window 21
Support
- international 8
- technical 6

System requirements 9

T

Technical support
- contacting 6
- international 8

Training
scheduling 7

W

WebScanX 12
introducing 5
using 12
What is WebScanX? 5
What's new text file 11