

A computer virus is a program that replicates itself, attaches to other programs, and performs unsolicited or unwanted, if not malicious, actions when it executes. The two fundamental virus categories are “boot” and “file” viruses.

Boot viruses dwell in the [boot sector](#) of the hard or floppy disk that carries them. These execute as your computer starts. Once they copy themselves into your computer’s memory, they can then spread to other disks or other computers on a network, each time leaving copies of themselves that can repeat the cycle.

File viruses become active only when you execute the program that carries them. Typically, such viruses infect files with the extensions .EXE, .COM, or .DLL, and such other executable files as Microsoft Word or Excel data and template files. Once executed, the file virus also loads itself into your computer’s memory, then replicates and attaches itself to other executable programs.

The following list describes some of the characteristics of common viruses. Click an item to learn more.

- [Boot virus](#)
- [File virus](#)
- [Stealth virus](#)
- [Multi-partite virus](#)
- [Mutating virus](#)
- [Encrypted virus](#)
- [Polymorphic virus](#)
- [Macro virus](#)

 [Related Topics](#)

Boot Virus

A boot virus copies itself from the [boot sector](#) of one drive to that of another (e.g., from a floppy disk to a hard disk).

File Virus

A file virus attaches itself to an executable program. Whenever the program runs, the virus attaches itself to other executable programs.

Stealth Virus

A stealth virus hides itself to evade detection. A stealth virus may be either a [boot virus](#) or a [file virus](#).

Multi-partite Virus

A multi-partite virus acts like both a [boot virus](#) and a [file virus](#) by spreading through disk boot sectors and executable files.

Mutating Virus

Mutating viruses change their code signature to avoid detection. Many mutating viruses are also [encrypted viruses](#).

Encrypted Virus

Encrypted viruses encrypt part of their code signature to avoid detection. Many encrypted viruses are also [mutating viruses](#).

Polymorphic Virus

Polymorphic viruses act somewhat like mutating viruses, but each time a polymorphic virus copies itself, it changes its code signature slightly to avoid detection.

As the popularity of the Internet has grown in the last few years, website design has become much more sophisticated. Many sites now include interactive elements, such as forms, search engines, animations, and a host of other multimedia features that make web browsing more useful and more exciting. Much of the technology that makes these features possible comes from small, easily downloaded programs that interact with your browser software to exchange information, to display multimedia files, to formulate database queries, and to perform other tasks. Java and ActiveX are tools programmers use to write these types of programs.

Programmers use Sun Microsystems' Java programming language to write small, special-purpose applications, or "applets," that run on a Java "virtual machine" incorporated into your browser software, either directly or as a plug-in module. A Java "class" is a prewritten software module that programmers can modify for their own use.

Programmers use Microsoft's ActiveX technology for similar purposes. ActiveX differs from Java primarily in how it runs—where Java runs in a virtual machine built specifically to interpret Java applets, ActiveX serves as a sophisticated software bridge between existing programs, or between other programs and Windows itself. An ActiveX "control" is a software module that links programs and allows them to share data without either having to know anything about how the other operates.

Java classes and ActiveX controls are called, collectively, "objects."



[Related Topics](#)

Although both Java and ActiveX include safeguards designed to prevent harm to your computer system, determined programmers have developed objects that exploit arcane Java or ActiveX features to read data stored on your hard disk and pass it back to websites you visit, to forge offensive e-mail in your name and send it out to others, to corrupt or destroy your data, or to cause other damage to your system.

Dangerous objects such as these can often lurk on websites until you visit and download them to your system, usually without realizing that they exist. Most browser software includes a feature that allows you to block Java applets or ActiveX controls altogether, or to turn on security features that authenticate objects before downloading them to your system. But these approaches can deprive you of the interactive benefits of websites you visit by indiscriminately blocking all objects, dangerous or not.

WebScanX allows a more judicious approach. It uses an up-to-date database of objects known to cause harm to screen Java classes and ActiveX controls you encounter as you browse. Potentially harmful objects stay where they are, away from your system, while other objects continue to function.



[Related Topics](#)

Not so long ago, individual computer users could avoid virus infections without much thought or planning, simply because they rarely came in contact with likely virus sources. Today, however, most computer users send messages to each other, share data and transfer files constantly—whether through a modem, via diskettes, or over networks and the Internet. In this same span of time, viruses have come to number in the thousands and can spread more quickly and easily than ever.

In this environment, taking steps to protect yourself from a computer virus infection is no longer a luxury but a necessity. Consider the value of the data on your computer. It would probably require a significant investment of time and money to replace if it became corrupted or unusable because of a viral infection—it may even be irreplaceable. But whether your own data is important to you or not, neglecting to guard against viruses may mean that your computer could play unwitting host to a virus that can spread and attack the data on computers your co-workers and colleagues use.

Scheduling periodic virus scans with WebScanX and other McAfee virus scanning solutions significantly reduces your vulnerability to infection and prevents unnecessary loss of time, money and data.



[Related Topics](#)

WebScanX protects your computer from viruses by checking these possible sources for infection: message attachments you receive from the Internet via Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant client software; websites you visit with Netscape Navigator, Microsoft Internet Explorer, SPRY Mosaic or America Online Web Browser; files you download; and Java classes or ActiveX controls you encounter. WebScanX also makes it easy to keep your system safe by

- n Allowing you to decide whether it should look at all message attachments or only at designated files
- n Scanning compressed files, at your option
- n Notifying co-workers, your network administrator, and the person who sent you an infected e-mail attachment automatically whenever it detects infected files
- n Deleting or moving infected files to a “quarantine” directory
- n Logging actions it takes to identify and respond to viruses
- n Blocking Java classes and ActiveX controls known to cause harm from reaching your computer system
- n Preventing access to a specified list of dangerous websites or IP addresses
- n Protecting your settings from alteration with a password you supply
- n Allowing easy access to configuration options via a simple and intuitive dialog box

 **See Note**

 [Related Topics](#)

Founded in 1989, McAfee Associates, Inc. is the leading provider of productive computing tools for the DOS, OS/2, UNIX and Windows environments. More than 16,000 corporations worldwide use our anti-virus products. Our utility products provide data security, automated version updating, and system inspection and editing. McAfee also pioneered and has become the leading provider of electronically distributed software. All McAfee products may be purchased through dealers or downloaded from bulletin-board systems and online services around the world.

McAfee does not stop at developing the world's best anti-virus and utility products. We back them with a full-time staff of virus researchers, programmers and support professionals, who together provide the industry's best service and technical assistance. Contact McAfee directly, or contact McAfee through our worldwide network of authorized agents in more than 50 countries.

 [Related Topics](#)

McAfee maintains a support staff with expertise in the each of the areas listed below. Click any of these topics for more information:

{button ,JI('webscanx.hlp','Customer_Care')} [Customer Care](#)

{button ,JI('webscanx.hlp','Technical_Support')} [Technical Support](#)

{button ,JI('webscanx.hlp','McAfee_Training')} [Training](#)

 [Related Topics](#)


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

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

 [Related Topics](#)

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

 [Related Topics](#)

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 the latest news and information. Click the website address shown below to link directly to McAfee's site. To specify the web browser you want to use or to learn how to obtain web browsing software, click [here](#) .

World Wide Web <http://www.mcafee.com> Click [here](#) to link to the McAfee Web Site.

If you do not find what you need or do not have Web access, try one of McAfee's automated services:

Automated Voice and Fax Response System	(408) 988-3034
E-mail	support@mcafee.com
McAfee dial-up Bulletin Board System	(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 do not have the answer 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 software. Please have this information ready before you call:

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





 [Related Topics](#)


New viruses, along with harmful Java classes and ActiveX controls, appear at a rate of more than 200 per month. Often, WebScanX cannot use the information included in older data files to detect these new variations. To offer the best virus protection possible, McAfee continually updates the files WebScanX uses to detect viruses and harmful objects. After a certain time period, WebScanX will notify you that you should update its virus definition, or .DAT, file. For maximum protection, you should update these files on a regular basis—McAfee releases new data files monthly.

 **See Note**

Your purchase of WebScanX entitles you to free updates to your data files for as long as you use this version of WebScanX. You may not, however, update WebScanX evaluation copies. Please note also that McAfee cannot guarantee that future data file releases will remain compatible with earlier versions of its products.

To update your files regularly and conveniently, use any of these methods:

- n **SecureCast.** Install and use McAfee's automatic update service to take advantage of the latest "push" technology to update your data files automatically and invisibly. To learn more, click [here](#) .
- n **WebScanX One-button Electronic Updating.** Click **Update** in the WebScanX Old Virus Definitions dialog box, when it appears, in order to connect directly with one of McAfee's FTP sites. To learn more, click [here](#) .
- n **McAfee Electronic Services.** Connect to any of McAfee's electronic services, including the McAfee Web Site and the McAfee BBS to update your definition files. To learn more, click [here](#) .
- n **Major electronic services.** Connect to one of the major electronic services, including America Online, CompuServe or the Microsoft Network, to update your definition files. To learn more, click [here](#) .

 [Related Topics](#)

McAfee's SecureCast gives you several options for keeping your WebScanX installation up-to-date, with varying levels of user interaction. One option, which uses BackWeb's Internet "push" technology, automatically updates your data files on a regular basis whenever you are connected to the Internet. If you do not connect long enough for a full download, the software will automatically piece out the work and notify you when a complete update package has arrived.

To use SecureCast, either install the client software from the CD-ROM that contains WebScanX, or download it from the McAfee Web Site <http://www.mcafee.com>. See the WHATSNEW.TXT file included with the WebScanX CD-ROM for installation instructions.

The McAfee Web Site contains its own instructions for downloading and installing SecureCast software. Please refer to the site for details.

 [Return to Previous Topic](#)

WebScanX periodically reminds you as you start your computer to update your virus definition files. You can download new definition files automatically by following these steps:

 **See Note**

- 1 Click **Update** in the Old Virus Definitions dialog box to connect automatically with the directory that contains current data files.
- 2 In the Update Files dialog that appears, choose the site from which you want to download your new definition files from the list shown. Choose the site closest to your location to shorten your download time.
- 3 Click **OK**.

WebScanX downloads the new files.

To prepare the new files for use with WebScanX, follow these steps:

- 1 Download the file to a new directory on your computer.
- 2 The file is compressed. Decompress it with any PKUNZIP-compatible decompression software. If you don't have decompression software, you can download PKUNZIP (shareware) from any of McAfee's electronic sites.
- 3 Locate the directories on your hard disk that contain WebScanX files. If you followed the recommended installation procedure, WebScanX installs itself here: `C:\Program Files\McAfee\WebScanX`.
- 4 Copy the new files into the directory or directories that contain your current WebScanX files. When Windows asks you whether you want to replace your old files with the new data files, click **Yes**.
- 5 Reboot your computer so that changes take place immediately.

 [Return to Previous Topic](#)

To update your WebScanX data files by downloading new files from the McAfee Web Site or the McAfee BBS, follow these steps:

- 1 Download the correct data file (for example, DAT-3007.ZIP) from one of McAfee's electronic services.


On most services, you'll find update files in a separate anti-virus section. Instructions for choosing correct data files appear on the McAfee Web Site. Click [here http://www.mcafee.com](http://www.mcafee.com) to connect.

 **See Note**

- 2 Download the file to a new directory.

The file is compressed. Decompress it with any PKUNZIP-compatible decompression software. If you don't have decompression software, you can also download PKUNZIP (shareware) from any of McAfee's electronic sites.

- 6 Locate the directories on your hard disk that contain WebScanX files. If you followed the recommended installation procedure, WebScanX installs itself here: C:\Program Files\McAfee\WebScanX.
- 7 Copy the new files into the directory or directories that contain your current WebScanX files. When Windows asks you whether you want to replace your old files with the new data files, click **Yes**.
- 8 Reboot your computer so that changes take place immediately.

 [Related Topics](#)

McAfee maintains a presence on most of the major online services, including America Online, CompuServe and the Microsoft Network (MSN). Each service includes a software download area where you can find up-to-date .DAT files and other McAfee software. Keywords to locate McAfee on each service appear below:

CompuServe	GO MCAFEE
America Online	Keyword MCAFEE
Microsoft Network (MSN)	MCAFEE

When you have located the McAfee software download area, follow these steps to update your WebScanX files:

- 1 Download the correct data file (for example, DAT-3007.ZIP).

On most services, you'll find update files in a separate anti-virus section. Instructions for choosing correct data files appear in the same area.

 **See Note**

- 2 Download the file to a new directory.

The file is compressed. Decompress the file using any PKUNZIP-compatible decompression software. If you don't have decompression software, you can also download PKUNZIP (shareware) from the same electronic site.

- 3 Locate the directories on your hard disk that contain WebScanX files. If you followed the recommended installation procedure, WebScanX installs itself here: C:\Program Files\McAfee\WebScanX.
- 4 Copy the new files into the directory or directories that contain your current WebScanX files. When Windows asks you whether you want to replace your old files with the new data files, click **Yes**.
- 5 Reboot your computer so that changes take place immediately.

 [Related Topics](#)

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

ResearchX@McAfee.com

Use this address to report harmful ActiveX controls and Java classes, or dangerous Internet sites.

AVResearch@McAfee.com

Use this address to report new virus strains.



[Related Topics](#)

To choose a web browser to use when linking to McAfee's Web Site from the WebScanX help system, click [here](#) 


■ **See Note**

If you have Internet access, but do not have one of the supported browsers, you may download software from one of these sites:

Netscape website: <http://www.netscape.com>

Microsoft website: <http://www.microsoft.com>

■ **See Note**

 [Return to Previous Topic](#)

During installation, WebScanX sets itself to start automatically each time you start your computer. Once started, WebScanX remains active in your computer's memory, automatically checking for viruses and harmful objects using the configuration options you choose. To **disable** this "autoload" feature

1 Click any of the WebScanX activity icons—.




or



 **See Note**

2 Choose **Properties** from the shortcut menu that appears.

The WebScanX Properties dialog box opens.

3 Click the switch  beside **Load at startup** to turn it off



This tells WebScanX not to start automatically. Clicking the switch again reactivates the autoload feature.

4 Click **OK** to close the WebScanX Properties dialog box.



[Related Topics](#)

If you disable WebScanX's autoload feature, then [quit WebScanX](#), restart the program using one of the methods below. Please note that Windows NT 3.51 does not support the first method listed. Click an item to learn more:

{button ,JI(`webscanx.HLP`, `Starting_WebScanX_from_the_Start_Menu`)} [Choose **WebScanX** from the **Start** menu](#)

{button ,JI(`webscanx.HLP`, `Starting_WebScanX_from_its_Program_Icon`)} [Double-click the WebScanX program icon](#)

{button ,JI(`webscanx.HLP`, `Running_WebScanX.exe`)} [Run webscanx.exe](#)

If you have disabled all of the WebScanX activity icons and want to open the WebScanX Properties dialog box, use one of the methods below. Please note that Windows NT 3.51 does not support the first method listed. Click an item to learn more:

{button ,JI(`webscanx.HLP`, `Opening_the_WebScanX_Properties_Dialog_Box_from_the_Start_Menu`)} [Choose **Configure WebScanX** from the **Start** menu](#)

{button ,JI(`webscanx.HLP`, `Opening_the_WebScanX_Properties_Dialog_Box_Using_the_Program_Icon`)} [Double-click the Configure WebScanX program icon](#)

{button ,JI(`webscanx.HLP`, `Running_Webcfg32.exe`)} [Run webcfg32.exe](#)



[Related Topics](#)

Follow these steps:

- 1 Locate the folder named McAfee on your hard disk, then double-click it. If you followed the recommended installation instructions, you should find the folder in this path—`c:\Program Files\McAfee`—on Windows 95 and Windows NT 4.0 systems. On Windows NT 3.51 systems, the default path is `c:\mcafee`.
- 2 Double-click the WebScanX folder.
- 3 Double-click the WebScanX.exe icon.
- 4 Choose your [user profile](#) from the list beside **Profile Name** in the Choose Profile dialog box that appears.
- 5 Click **OK**.

WebScanX starts and begins scanning with the most recent configuration options you have chosen. If you have disabled all of the WebScanX program icons, WebScanX runs without any visual interface.

 [Return to Previous Topic](#)

Follow these steps:

- 1 Click **Start** in the Windows taskbar.
- 2 Point to **Programs**.
- 3 Point to the **McAfee WebScanX** folder.
- 4 Choose **WebScanX**.
- 5 Choose your [user profile](#) from the **Profile Name** list in the Choose Profile dialog box that appears.
- 6 Click **OK**.


WebScanX starts and begins scanning with the most recent configuration options you have chosen. If you have disabled all of the WebScanX program icons, WebScanX runs without any visual interface.

■ [Return to Previous Topic](#)

Follow these steps:


- 1 Choose **Run...** from the Windows 95 or Windows NT 4.0 **Start** menu. If you use Windows NT 3.51, choose **Run...** from the **File** menu in the Program Manager.
- 2 Type the path for `webscan.exe` in the text box provided, or click **Browse** to locate the file on your hard disk.
The default path on Windows 95 and Windows NT 4.0 systems is `c:\Program files\McAfee\WebScanX\webscanx.exe`
The default path on Windows NT 3.51 systems is `c:\mcafee\webscanx\webscanx.exe`.
- 3 Click **OK**.
- 4 Choose your [user profile](#) from the list beside **Profile Name** in the Choose Profile dialog box that appears.
- 5 Click **OK**.

WebScanX starts and begins scanning with the most recent configuration options you have chosen. If you have disabled all of the WebScanX program icons, WebScanX runs without any visual interface.


 [Return to Previous Topic](#)


Follow these steps:

- 1 Click **Start** in the Windows taskbar.
- 2 Point to **Programs**.
- 3 Point to the **McAfee WebScanX** folder.
- 4 Choose **Configure WebScanX**.

The WebScanX Properties dialog box appears. To open this dialog box from the taskbar in Windows 95 or Windows NT 4.0, or from the desktop in Windows NT 3.51, click the **Show Icon** checkbox in any property page to display the WebScanX activity icons—,


 or

. Choose **Properties** from the shortcut menus associated with these icons to open the WebScanX Properties dialog box.

 [Return to Previous Topic](#)

Follow these steps:

- 1 Locate the folder named McAfee on your hard disk, then double-click it. If you followed the recommended installation instructions, you should find the folder in this path—`c:\Program Files\McAfee`—on Windows 95 and Windows NT 4.0 systems. On Windows NT 3.51 systems, the default path is `c:\mcafee`.
- 2 Double-click the WebScanX folder.
- 3 Double-click the WebCfg32.exe icon.


The WebScanX Properties dialog box appears. To open this dialog box from the taskbar in Windows 95 or Windows NT 4.0, or from the desktop in Windows NT 3.51, click the **Show Icon** checkbox in any property page to display the WebScanX activity icons—,



or




Choose **Properties** from the shortcut menus associated with these icons to open the WebScanX Properties dialog box.


 [Return to Previous Topic](#)

Follow these steps:

- 1 Choose **Run...** from the Windows 95 or Windows NT 4.0 **Start** menu. If you use Windows NT 3.51, choose **Run...** from the **File** menu in the Program Manager.
- 2 Type the path for webcfg32.exe in the text box provided, or click **Browse** to locate the file on your hard disk.
The default path on Windows 95 and Windows NT 4.0 systems is `c:\Program files\McAfee\WebScanX\webcfg32.exe`
The default path on Windows NT 3.51 systems is `c:\mcafee\webscanx\webcfg32.exe`.
- 3 Click **OK**.


The WebScanX Properties dialog box appears. To open this dialog box from the taskbar in Windows 95 or Windows NT 4.0, or from the desktop in Windows NT 3.51, click the **Show Icon** checkbox in any property page to display the WebScanX activity icons—,

 or

-  Choose **Properties** from the shortcut menus associated with these icons to open the WebScanX Properties dialog box.

 [Return to Previous Topic](#)

To quit WebScanX

1 Press and hold **Shift** on your keyboard, then click a WebScanX activity icon—,





 **See Note**

2 Choose **Exit All**.


WebScanX immediately stops all virus scanning and quits.

 **See Note**

 [Related Topics](#)

WebScanX groups several of its common commands in shortcut menus associated with these activity icons: 

 or

. Each icon corresponds to one of WebScanX's program components—E-mail Scan, Download Scan and Internet Filter, respectively—and each has its own menu. Click any of these icons to display these commands:


 **See Note**

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

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

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

 **See Note**

 [Related Topics](#)

To configure WebScanX to look for viruses attached to e-mail messages you receive from the Internet via Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant e-mail client

1 Click any of the WebScanX activity icons—

 or




See Note

3 Choose **Properties** from the shortcut menu that appears.

The WebScanX Properties dialog box opens.

3 Click the **E-mail Scan** tab to display the correct property page.

4 Select the **Enable Scanning of e-mail attachments** checkbox. The options in the rest of the property page activate.

5 Select the **Show Icon** checkbox to display the activity icon for this program component .

The icon is animated and runs whenever WebScanX scans e-mail attachments. Depending on the options you choose in other property pages, it may appear along with other WebScanX icons.

6 Click the button that corresponds to the e-mail software—Lotus cc:Mail or Microsoft Mail—that you use. Clicking **Microsoft Mail (MAPI)** also tells WebScanX to scan e-mail you receive through any [MAPI-compliant](#) client software.

WebScanX can protect your computer from viruses that accompany e-mail messages with a combination of actions. Click any of the topics below to learn how to tell WebScanX to

{button ,JI('webscanx.hlp','Detecting_Viruses_Carried_in_E_Mail_Attachments')} [Detect Viruses Carried in E-mail Attachments](#)

{button ,JI('webscanx.hlp','Responding_to_Viruses_Detected_in_E_mail_Attachments')} [Respond to viruses it detects](#)

{button ,JI('webscanx.hlp','Displaying_and_Sending_Alert_Messages')} [Alert you or others when it detects a virus](#)


{button ,JI('webscanx.hlp','Logging_WebScanX_Responses_to_E_mail_Viruses')} [Save a log showing the actions it took](#)

Related Topics

The virus “signatures,” or characteristic code sequences, that WebScanX searches for generally appear only in files attached to e-mail messages, rather than in the messages themselves. Although code for a virus could appear in the text of an e-mail message, perhaps because of a mail transmission error, such a virus could not infect your computer system because e-mail software transmits messages as text. To function as a virus, the code sequence must be able to run as a program or as [part of another program](#).

To detect viruses attached to your e-mail, locate the area labeled **Detection** in the **E-mail Scan** property page, then

1 Tell WebScanX where to look. If you use Microsoft Mail or any MAPI-compliant client software you have these options:


- u **All new mail**. Click this button to have WebScanX search for viruses in all e-mail message attachments as they reach your mailbox; or
- u **Select Folder**. Click this button to tell WebScanX to look for all message attachments in a specific location. Next, click  to choose the folder WebScanX should search.

 **See Note**

If you use Lotus cc:Mail, simply tell WebScanX how often it should scan incoming e-mail attachments for viruses. In the text box provided, enter the number of seconds WebScanX should wait before performing a scan.

2 Tell WebScanX what to look for.

- u Choose **All attachments** from the **Attachments** list to have WebScanX search for viruses in all files attached to e-mail messages. Although searching all incoming message attachments serves as your best protection against infection, doing so may have an impact on your computer’s performance if WebScanX must scan and process a large volume of e-mail.
- u Choose **Program files only** from the **Attachments** list to have WebScanX search only for those attachments most susceptible to virus infection. By default, WebScanX uses these common extensions to identify susceptible files: .COM, .EXE, .SYS, .RTF, .DO?, and .XL?. It uses .RTF, .DO?, and .XL? to identify Microsoft Word and Microsoft Excel data files, whose macros can contain viruses. The ? character is a wildcard.

To change the list of file extensions WebScanX uses, click . Click [here](#)

 to learn more.


3 Tell WebScanX whether to examine compressed files.

Select the **Compressed files** checkbox to have WebScanX search compressed files created with LHA, LZEXE, PKLite, PkZip, or WinZip. Because WebScanX decompresses each such file in memory, then checks for virus signatures, selecting this option can lengthen the time it takes to scan your e-mail.

 **See Note**

4 Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**


 [Related Topics](#)

To tell WebScanX what to do about viruses it finds attached to your e-mail, choose a response from the **Action** list in the **E-mail Scan** property page.

 **See Note**

You can

- u Tell WebScanX to ask you what to do when it finds a virus.

Choose **Prompt for user action**. Next, click  to open the Action dialog box, then select possible responses from the checkboxes shown. When WebScanX finds an infected file during a scan, it displays an alert dialog box that offers you each of the response options you choose here.

The options are:

Delete file. This tells WebScanX to immediately delete the infected file from your system and move the e-mail message to your e-mail client application's trash folder.


Move file. This tells WebScanX to move the infected file to a particular "quarantine" directory (see below to learn how to choose a directory).

Continue scan. This tells WebScanX to ignore the infected file completely and continue searching.

Stop scan. This tells WebScanX to stop scanning for any other infected files.


Select the **Sound audible alert** checkbox to tell WebScanX to beep when it finds infected files. Select the **Display custom message** checkbox to tell WebScanX to alert you with your own custom message when it finds infected files. Next, enter the message you want to see in the text box below.


- u Tell WebScanX to move infected files to a particular directory.


Choose **Move infected files to a folder**, then click  to open a dialog box where you can choose a quarantine folder to store infected files. By default, WebScanX creates a folder called Infected in its program directory and stores infected files there. Click

 to choose or create a different folder.

 **See Note**

Click  to open a folder or other icon shown in the Choose Folder dialog box. Click

 to choose the folder you want to use; the icon for the folder you select changes to

. Click **OK** to return to the Action dialog box—the pathname for the folder you chose appears in the text box beside



- u Delete the infected file immediately.

Choose **Delete infected files**. WebScanX deletes infected files from your system automatically, as it finds them, and moves the messages that carry them to your e-mail client program's trash folder.

 **See Note**

- u Tell WebScanX to keep scanning.

Choose **Continue scanning**. WebScanX ignores any infected files it finds and completes its scan.

 **See Note**

Click **Apply** to save the response options you chose without leaving the **E-mail Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**

 [Related Topics](#)

WebScanX offers you three ways to alert others about infected files you have found in your e-mail. Click any of the topics below to learn how to


{button ,JI('webscanx.hlp','Alerting_an_E_mail_Correspondent_About_Infected_Files')}} [Reply to the person who sent you a message with an infected attachment](#)

{button ,JI('webscanx.hlp','Warning_Others_About_Infected_Files_via_E_mail')}} [Send e-mail to warn others about an infected attachment](#)

{button ,JI('webscanx.hlp','Notifying_Your_Network_Administrator_About_Infected_Files')}} [Alert your network administrator about an infected attachment](#)

 [Related Topics](#)

To compose a standard reply to the person who sent you a message with an infected attachment, locate the area labeled **Alert** in the **E-mail Scan** property page, then

- 1 Select the **Return reply mail to sender** checkbox.
- 2 Click  to open a standard mail message form.
- 3 Fill in the subject line, then add any comments you want to make in the body of the message below the infection notice. You may add up to 1024 characters of text.

To send a copy of this message to someone else, enter an e-mail address in the text box labeled **Cc:**, or click **Cc:** to choose a recipient from your mail system's user directory or address book.


 **See Note**

- 4 Click **OK** to save the message.

Whenever it detects a virus, WebScanX sends a copy of this message to each person who sends you e-mail with an infected attachment. It fills in the recipient's address with information found in the original message header, and identifies the virus and the affected file in the area immediately below the subject line. If you have activated its logging feature, WebScanX also logs each instance when it sends an alert message.

 [Related Topics](#)

To send an e-mail message to warn others about an infected attachment, locate the area labeled **Alert** in the **E-mail Scan** property page, then

- 1 Select the **Send mail to user** checkbox.
- 2 Click  to open a standard mail message form.
- 3 Enter an e-mail address in the text box labeled **To:**, or click **To:** to choose a recipient from your mail system's user directory or address book. Repeat the process in the text box labeled **Cc:** to send a copy of the message to someone else.

 **See Note**


- 4 Fill in the subject line, then add any comments you want to make in the body of the message below the infection notice. You may add up to 1024 characters of text.
- 5 Click **OK** to save the message.

Whenever it detects a virus, WebScanX sends a copy of this message to each of the addresses that you entered in Step 3. It adds information to identify the virus and the affected file in the area immediately below the subject line. If you have activated its [logging feature](#), WebScanX also logs each instance when it sends an alert message.




 [Related Topics](#)


WebScanX works in conjunction with a network server running McAfee's [NetShield](#) to notify your network system administrator whenever it detects a virus. The notification consists of a report form, or "network alert," that WebScanX generates automatically and sends to a specific location for NetShield to read.

To tell WebScanX to generate and send a network alert, locate the area labeled **Alert** in the **E-mail Scan** property page, then

- 1 Select the **Send network alert to** checkbox.
- 2 Click  to open a dialog box where you can choose the folder that receives WebScanX's report.

 **See Note**

- 3 Click  to open a disk, folder, or other icon shown in the dialog box. Next, click  to choose the folder you want to use; the icon for the folder you select changes to .

- 4 Click **OK** to close the Browse for Folder dialog box. The pathname for the folder you chose appears in the text box beside .



- 5 Click **Apply** to save the alert options you chose without leaving the **E-mail Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**



 [Related Topics](#)

WebScanX can record the actions it takes when it scans for infected attachments, along with other information useful for tracking infections, and save the information to a text file that you can open in any standard word processing software. Tracking information in a log file enables you to see the number of files WebScanX examined, determine which files carried viruses, and note the WebScanX settings you used to detect and respond to them. You should, therefore, activate this function.

To log WebScanX actions, locate the area labeled **Reports** in the **E-mail Scan** property page, then

- 1 Select the **Log to file** checkbox.
- 2 Click  to open the Activity Logging dialog box.
- 3 Type the filename and path you want to use to save your log file, or click  to open the Activity Log Filename dialog box.
 - § Type the filename you want to use in the text box provided, then click **Open**.
 - § WebScanX asks you if you want to create a log file in this location with the name you've chosen. Click **Yes**.
 - § WebScanX creates a log file with your filename. When WebScanX stores data from a scanning operation in the log file, the file appears in the location to which you saved it. To view the log file, open it in any standard text editor, such as Notepad or WordPad.
- 4 To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

 **See Note**

- 5 Select the checkboxes beside each set of data you want WebScanX to collect and log. Click [here](#)  to learn more about what each data set includes.
- 6 Click **OK** to close the Activity Logging dialog box. The pathname for your log file appears in the text box beside .
- 7 Click **Apply** to save the log options you chose without leaving the **E-mail Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**

 [Related Topics](#)

To configure WebScanX to look for viruses attached to files, including e-mail attachments, that you download or receive from the Internet via one of the [supported web browsers](#) or with another e-mail client

1 Click any of the WebScanX activity icons—.



or




See Note

4 Choose **Properties** from the shortcut menu that appears.

The WebScanX Properties dialog box opens.

3 Click the **Download Scan** tab to display the correct property page.

4 Select the **Enable Internet download scanning** checkbox. The options in the rest of the property page activate.

5 Select the **Show Icon** checkbox to display the activity icon for this program component .

The icon is animated and runs whenever WebScanX scans files that you download. Depending on the options you choose in other property pages, it may appear along with other WebScanX icons.

WebScanX can protect your computer from viruses that accompany downloaded files or e-mail attachments with a combination of actions. Click any of the topics below to learn how to tell WebScanX to

{button ,JI('webscanx.hlp','Detecting_Viruses_Carried_in_Internet_Downloads_or_E_mail_Attachments')} [Detect viruses carried in Internet downloads or e-mail attachments](#)

{button ,JI('webscanx.hlp','Responding_to_Viruses_Detected_in_Internet_File_Downloads')} [Respond to viruses it detects](#)

{button ,JI('webscanx.hlp','Notifying_Your_Network_Administrator_About_Infected_Downloads')} [Alert your network administrator when it detects a virus](#)

{button ,JI('webscanx.hlp','Logging_WebScanX_Responses_to_Infected_Internet_Downloads')} [Save a log showing the actions it took](#)




[Related Topics](#)


The virus “signatures,” or characteristic code sequences, that WebScanX searches for generally appear only in executable files, whether stand-alone or attached to e-mail messages. Although code for a virus could appear in the text of an e-mail message, perhaps because of a mail transmission error, such a virus could not infect your computer system because Internet mail systems transmit messages as plain text. To function as a virus, the code sequence must be able to run as a program or as [part of another program](#).

To detect viruses attached to files or to e-mail attachments downloaded from the Internet, locate the area labeled **Detection** in the **Download Scan** property page, then

1 Tell WebScanX which files to scan. You have these options:

- u **All files**. Click this button to have WebScanX search for viruses in all files and e-mail message attachments as you receive them; or
- u **Program files only**. Click this button to have WebScanX search only for those attachments most susceptible to virus infection. By default, WebScanX uses these common extensions to identify susceptible files: .COM, .EXE, .SYS, .RTF, .DO?, and .XL?. It uses .RTF, .DO?, and .XL? to identify Microsoft Word and Microsoft Excel data files, whose macros can contain viruses. The ? character is a wildcard.

To change the list of file extensions WebScanX uses, click . Click [here](#)

 to learn more.


2 Tell WebScanX whether to examine compressed files.

Select the **Compressed files** checkbox to have WebScanX search compressed files created with LHA, LZEXE, PKLite, PKZip or WinZip. Because WebScanX decompresses each such file in memory, then checks for virus signatures, selecting this option can lengthen the time it takes to scan your e-mail.


 **See Note**

3 Click **Apply** to save the detection options you chose without leaving the **Download Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**


 [Related Topics](#)

To tell WebScanX what to do about viruses it finds incorporated in files or e-mail attachments you download from the Internet, choose a response from the **Action** list in the **Download Scan** property page.

 **See Note**

You can

- u Tell WebScanX to ask you what to do when it finds a virus.

Choose **Prompt for user action**. Next, click  to open the Action dialog box, then select possible responses from the checkboxes shown. When WebScanX finds an infected file during a scan, it displays an alert dialog box that offers you each of the response options you choose here.

The options are:

Delete file. This tells WebScanX to immediately delete the infected file from your system and move any associated e-mail message to your e-mail client application's trash folder.


Move file. This tells WebScanX to move the infected file to a particular "quarantine" directory (see below to learn how to choose a directory).

Continue scan. This tells WebScanX to ignore the infected file completely and continue searching.


Stop scan. This tells WebScanX to stop scanning for any other infected files.


Select the **Sound audible alert** checkbox to tell WebScanX to beep when it finds infected files. Select the **Display custom message** checkbox to tell WebScanX to alert you with your own custom message when it finds infected files. Next, enter the message you want to see in the text box below.


- u Tell WebScanX to move infected files to a particular folder.

Choose **Move infected files to a directory** then click  to open a dialog box where you can choose a quarantine folder to store infected files. Click

 to locate the folder you want to use.

Click  to open a disk, folder, or other icon shown in the dialog box. Click

 to choose the folder you want to use; the icon for the folder you select changes to

 Click **OK** to return to the Action dialog box—the pathname for the folder you chose appears in the text box beside



- u Delete the infected file immediately.

Choose **Delete infected file**. WebScanX deletes infected files from your system automatically, as it finds them, and moves the messages that carry them to your e-mail client program's trash folder.

 **See Note**


- u Tell WebScanX to keep scanning.

Choose **Continue scanning**. WebScanX ignores any infected files it finds and completes its scan.

 **See Note**


Click **Apply** to save the response options you chose without leaving the **Download Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**


 [Related Topics](#)


WebScanX works in conjunction with a network server running McAfee's [NetShield](#) to notify your network system administrator whenever it detects a virus. The notification consists of a report form, or "network alert," that WebScanX generates automatically and sends to a specific location for NetShield to read.

To tell WebScanX to generate and send a network alert, locate the area labeled **Alert** in the **Download Scan** property page, then


- 1 Select the **Send network alert to** checkbox.
- 2 Click  to open a dialog box where you can choose the folder that receives WebScanX's report.

 **See Note**

- 3 Click  to open a disk, folder, or other icon shown in the dialog box. Next, click

 to choose the folder you want to use; the icon for the folder you select changes to



- 4 Click **OK** to close the Browse for Folder dialog box. The pathname for the folder you chose appears in the text box beside .



- 5 Click **Apply** to save the alert options you chose without leaving the **Download Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**


 [Related Topics](#)

WebScanX can record the actions it takes when it scans for infected attachments, along with other information useful for tracking infections, and save the information to a text file that you can open in any standard word processing software. Tracking information in a log file enables you to see the number of files WebScanX examined, determine which files carried viruses, and note the WebScanX settings you used to detect and respond to them. You should, therefore, activate this function.

To log WebScanX actions, locate the area labeled **Report** in the **Download Scan** property page, then

- 1 Select the **Log to file** checkbox.
- 2 Click  to open the Activity Logging dialog box.
- 3 Type the filename and path you want to use to save your log file, or click  to open the Activity Log Filename dialog box.
 - § Type the filename you want to use in the text box provided, then click **Open**.
 - § WebScanX asks you if you want to create a log file in this location with the name you've chosen. Click **Yes**.
 - § WebScanX creates a log file with your filename. When WebScanX stores data from a scanning operation in the log file, the file appears in the location to which you saved it. To view the log file, open it in any standard text editor, such as Notepad or WordPad.
- 4 To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

 **See Note**

- 5 Select the checkboxes beside each set of data you want WebScanX to collect and log. Click [here](#)  to learn more about what each data set includes.
- 6 Click **OK** to close the Activity Logging dialog box.
- 7 Click **Apply** to save the log options you chose without leaving the **Download Scan** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**

 [Related Topics](#)

To configure WebScanX to scan for harmful [Java or ActiveX objects](#) you encounter on websites you visit

1 Click any of the WebScanX activity icons—.

 or

.

 **See Note**

2 Choose **Properties** from the shortcut menu that appears.

The WebScanX Properties dialog box opens.

3 Click the **Internet Filter** tab to display the correct property page.

4 Select the **Enable Java & ActiveX filter** checkbox. The options in the rest of the dialog box activate.

5 Select the **Show Icon** checkbox to display the icon for this program component .

The icon is animated and runs whenever WebScanX scans Java classes or ActiveX controls. Depending on the options you choose in other property pages, it may appear along with other WebScanX icons.

WebScanX can protect your computer from potential harm with a combination of actions. Click any of the topics below to learn how to tell WebScanX to

{button ,JI('webscanx.hlp',`Scanning_Java_Classes_and_ActiveX_Controls')} [Scan Java and ActiveX Applets](#)

{button ,JI('webscanx.hlp',`Preventing_Access_to_Specific_Internet_Addresses')} [Prevent Access to Internet Addresses You Specify](#)

{button ,JI('webscanx.hlp',`Responding_to_Harmful_Java_or_ActiveX_Objects')} [Respond to Harmful Java or ActiveX Applets](#)

{button ,JI('webscanx.hlp',`Notifying_Your_Network_Administrator_About_Harmful_Objects')} [Notify Your Network Administrator About Harmful Applets](#)

{button ,JI('webscanx.hlp',`Logging_WebScanX_Responses_to_Harmful_Objects')} [Log WebScanX Responses to Harmful Applets](#)

 [Related Topics](#)

To scan [Java or ActiveX objects](#) you encounter when visiting a website, locate the area labeled **Applets** in the **Internet Filters** property page, then

1 Tell WebScanX which objects to scan.

- u Select the **ActiveX Controls** checkbox to have it scan for harmful ActiveX or [.OCX](#) controls.
- u Select the **Java Classes** checkbox to have it scan Java classes, or applets written in Java.

WebScanX compares the objects you encounter with an internal database that lists the characteristics of objects known to cause harm. When it finds a match, it can alert you and let you decide what to do, or it can block access to the object automatically. See [Responding to Harmful Java or ActiveX Objects](#) for more details.

2 Click **Apply** to save the scanning options you chose without leaving the **Internet Filters** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.



See Note



[Related Topics](#)

To block all access to websites or to other Internet addresses that you know contain harmful objects, locate the area labeled **Sites** in the **Internet Filters** property page. You can enter a list of “forbidden” websites in either of two ways:



See Note

- u Select the **IP Addresses** checkbox to block dangerous sites using numeric [IP addresses](#). To learn how to add IP addresses to the list WebScanX uses, click [here](#)
- u Select the **Host Names** checkbox to block dangerous sites using [Uniform Resource Locator \(URL\)](#) designations. To learn how to add URLs to the list WebScanX uses, click [here](#)


Click **Apply** to save the blocking options you chose without leaving the **Internet Filters** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.



See Note




[Related Topics](#)

- 1 Click  to open the Banned IP Addresses dialog box.
- 2 Click **Add** to add an IP address to the list.
- 3 Enter an IP address in the Add IP Address dialog box. Be sure to use the [correct format](#) and check the numbers you enter carefully. If you know the subnet mask value for the site you want to avoid, enter it in the text box below. Otherwise, leave the default value shown.
- 4 Click **OK** to close the Add IP Address dialog box.

To add another IP address to the list, repeat steps 2 through 4. To delete an existing IP address, select it in the list, then click **Delete**.

When you have finished entering your list of IP addresses, click **OK** to close the Banned IP Addresses dialog box and return to the Internet Filter property page.

 [Return to Previous Topic](#)

- 1 Click  to open the Banned Domain Addresses dialog box.
- 2 Click **Add**.
- 3 Enter a URL in the Add Domain Address dialog box. Be sure to use the [correct format](#) and check the name you enter carefully.
- 4 Click **OK** to close the Add Domain Address dialog box.

To add another IP address to the list, repeat steps 2 through 4. To delete an existing domain address, select it in the list, then click **Delete**.

When you have finished entering your list of domain addresses, click **OK** to close the Banned Domain Addresses dialog box and return to the Internet Filter property page.

 [Return to Previous Topic](#)

WebScanX gives you the choice to respond to potentially harmful objects either by

- n Asking you whether it should block or allow you access to such applets; or
- n Automatically denying access to them.

Choose which action you want WebScanX to take when it finds a suspicious object from the **Action** list in the **Internet Filters** property page.

Click **Apply** to save your settings without leaving the **Internet Filters** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.




See Note




[Related Topics](#)



WebScanX works in conjunction with a network server running McAfee's [NetShield](#) to notify your network system administrator whenever it encounters a potentially harmful Java class or ActiveX control. The notification consists of a report form, or "network alert," that WebScanX generates automatically and sends to a specific location for NetShield to read.


To tell WebScanX to generate and send a network alert, locate the area labeled **Alert** in the **Internet Filters** property page, then

- 1 Select the **Send network alert to** checkbox.
- 2 Click  to open a dialog box where you can choose the folder that receives WebScanX's report.

 **See Note**

- 3 Click  to open a disk, folder, or other icon shown in the dialog box. Click

 to choose the folder you want to use; the icon for the folder you select changes to .



- 4 Click **OK** to close the Browse for Folder dialog box. The pathname for the folder you chose appears in the text box beside .
- 5 Click **Apply** to save the alert options you chose without leaving the **Internet Filters** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**

 [Related Topics](#)

WebScanX can record whether it blocks or allows potentially harmful Java and ActiveX applets onto your hard disk, along with other useful information, and save the information to a text file that you can open in any standard word processing software. Tracking information in a log file enables you to locate the source of the Java or ActiveX objects, note their names and remember the WebScanX settings you used to respond to them. You should, therefore, activate this function.

To log WebScanX Internet Filter actions, locate the area labeled **Report** in the **Internet Filter** property page, then

- 1 Select the **Log to file** checkbox.
- 2 Click  to open the Activity Logging dialog box.
- 3 Type the filename and path you want to use to save your log file, or click  to open the Activity Log Filename dialog box.
 - § Type the filename you want to use in the text box provided, then click **Open**.
 - § WebScanX asks you if you want to create a log file in this location with the name you've chosen. Click **Yes**.
 - § WebScanX creates a log file with your filename. When WebScanX stores data from a scanning operation in the log file, the file appears in the location to which you saved it. To view the log file, open it in any standard text editor, such as Notepad or WordPad.
- 4 To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

 **See Note**

- 5 Click **OK** to close the Activity Logging dialog box.
- 6 Click **Apply** to save the log options you chose without leaving the **Internet Filtering** property page. Click **OK** to save any changes you made in this or any other property page and close the WebScanX Properties dialog box. Click **Cancel** to close the dialog box without saving any changes.

 **See Note**

 [Related Topics](#)

Java classes and ActiveX controls are small, special-purpose programs written in the Java programming language developed by Sun Microsystems or developed using Microsoft ActiveX technology. These programs, or "objects," often work as building blocks for constructing larger programs, or serve to add capabilities to existing programs. Many websites use Java classes or ActiveX controls to display animations or forms, run queries, and manipulate data.

Although both technologies include safeguards designed to protect you from data loss or other types of harm, determined programmers can create objects that exploit some Java or ActiveX features to learn about the contents of your hard disk or corrupt your data. WebScanX includes a database of classes and controls known to cause harm and can block their actions.

To keep the settings you choose for WebScanX safe from unauthorized changes, you can protect any or all of the WebScanX property pages with a password. To choose which pages to protect and to assign a password

1 Click any of the WebScanX activity icons—.



or




See Note

2 Choose **Properties** from the shortcut menu that appears.

The WebScanX Properties dialog box opens.

3 Click the **Security** tab to display the correct property page.

5 Click  beside each setting you want to protect from tampering. Protected settings display this icon



to their left. To remove password protection from settings, click



6 Click **Password** to open the Specify Password dialog box.

7 Enter a password in the first text box shown, then enter the same password to confirm your choice in the text box below.



See Note

7 Click **OK** to close the Specify Password dialog box.

WebScanX asks for a password whenever anybody tries to change the settings you chose or disable the WebScanX autoload feature. To disable password protection, return to the Security property page, enter your password, then unlock each of the settings you no longer want to protect.



[Related Topics](#)

Once activated and configured, WebScanX operates continuously in the background, watching for and then scanning e-mail you receive, files you download or Java and ActiveX objects you encounter. To enable or disable its scanning activity, or to see a summary of its progress

1 Double-click any of the WebScanX activity icons—,



or



to open the WebScanX Status dialog box.

2 Click the tab that corresponds to the program component you want to enable or disable, or whose progress you want to check.

WebScanX reports the number of files it has scanned, moved or deleted and the number of infected files it has found for the E-mail Scan and Download Scan program components. For Java and ActiveX applets or Internet sites, WebScanX reports the number of items it has scanned and the number it has “banned,” or kept you from encountering. If you have activated its logging feature, WebScanX also records the same information in the log file for each program component.

3 Click **Enable** to start the program component. To disable it, click **Disable**.



See Note

4 Click **Properties** to open the WebScanX Properties dialog box, where you can set options that tell WebScanX how to perform each type of scan.

5 Click **Close** to close the WebScanX Status dialog box.



See Note



[Related Topics](#)

Macro Virus

A virus written in a macro language or attached to macros included in a program's data files. Microsoft Word and Microsoft Excel data files and template files, for example, can include such viruses.

Messaging Application Programming Interface (MAPI)

A Microsoft standard that governs how communications applications pass data back and forth between themselves. To install and work with MAPI-compliant applications, you must first set up Microsoft Messaging, a standard Windows component. To learn more, consult the documentation for Microsoft Exchange.

To add a new extension

- 1 Click **Add...** in the Program Extensions dialog box, then enter any extension between one and three characters long in the dialog box that appears next.

WebScanX does not accept reserved characters—usually punctuation and certain symbols—but you may use * and ? as wildcards. Do not include the period that separates the extension from the filename.

- 2 Click **OK** to add this new extension to the list that WebScanX uses to look for infected files.

To delete an extension

- 1 Select one of the extensions shown in the Program Extensions dialog box.
- 2 Click **Delete** to remove it from the list that WebScanX uses to look for infected files.

 **See Note**

When you have changed the list to suit your needs, click **OK** to save your changes and close the Program Extensions dialog box. Click **Cancel** to close the dialog box without changing the extension list.

Choosing Log Data for E-mail Scanning

- n **Virus detection.** Select this checkbox to tell WebScanX to note the number of infected files it found during this scanning session.
- n **Infected file deletion.** Select this checkbox to tell WebScanX to note the number of infected files it deleted from your system.
- n **Infected file move.** Select this checkbox to tell WebScanX to note the number of infected files it moved to your quarantine directory.
- n **Session settings.** Click this checkbox to tell WebScanX to list the options you choose in the WebScanX Properties dialog box for each scanning session.
- n **Session summary.** Click this checkbox to tell WebScanX to summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information. A scanning session is the period of time WebScanX remained active in your computer's memory. It ends when you either quit WebScanX or restart your computer.

Choosing Log Data for Download Scanning

- n **Virus detection.** Select this checkbox to tell WebScanX to note the number of infected files it found during this scanning session.
- n **Infected file deletion.** Select this checkbox to tell WebScanX to note the number of infected files it deleted from your system.
- n **Infected file move.** Select this checkbox to tell WebScanX to note the number of infected files it moved to your quarantine directory.
- n **Session settings.** Click this checkbox to tell WebScanX to list the options you choose in the WebScanX Properties dialog box for each scanning session.
- n **Session summary.** Click this checkbox to tell WebScanX to summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information. A scanning session is the period of time WebScanX remained active in your computer's memory. It ends when you either quit WebScanX or restart your computer.

Boot sector

The first logical division of a hard or floppy disk. Your computer's BIOS looks here soon after you turn it on to find the files and programs it needs to start operations.

IP Addresses

Internet Protocol addresses use a cluster of up to 12 numbers formatted in this manner:

123.456.789.101

to locate a specific computer or network of computers on the Internet. The status bar in your browser should tell you the IP address for sites you visit when you first connect.

A “subnet mask” is a way to “remap” a range of computer addresses within an internal network. WebScanX uses a default subnet mask of **255.255.255.255**. In most circumstances, you will not need to change this number, but if you know that a particular network node at the site you visit is the source of danger, you might need to enter a subnet mask to preserve your access to other machines at this site.

URL Designations

Do **not** include the transport protocol when entering URLs for use with WebScanX—identify a site you want to avoid with the domain name only. For example, WebScanX reads a domain name like this:

www.mydomain.com

correctly, but does not read the name correctly if you precede it with “http://.”

Uniform Resource Locator (URL)

Sometimes used interchangeably with “domain name” or “host name,” a URL specifies the name and location of a computer on the Internet, usually together with the “transport protocol” you want to use to request a resource from that computer. A complete URL for a website, for instance, would look like:

`http://www.mydomain.com`

The complete URL tells your browser to request the resource via the Hyper Text Transport Protocol (“http://”) from a computer named “www” on a network named “mydomain.com.” Other transport protocols include “ftp://” and “gopher://.” The Internet’s Domain Name Server system translates URLs into correct IP addresses using an up-to-date, centralized, and cross-referenced database.

To enter URLs for WebScanX, use only the domain name—leave the transport protocol off.

Note

WebScanX does not have the ability to "clean," or remove virus code, from infected files. To clean infected files, move them to a quarantine directory, then run McAfee VirusScan.

Note

You must have a dial-up or direct-access Internet account with a service provider in order to link to the McAfee Web Site. Contact an Internet service provider to obtain account information.

Note

Contact each vendor directly to learn more about access options using file transfer protocol (FTP) client software or other ways to obtain browser software.

Note

Disabling all virus scanning—by clearing all checkboxes in either the WebScanX [Status dialog box](#) or in all of the [property pages](#)—also causes WebScanX to quit. For WebScanX to remain active, you must enable at least one type of virus scanning.

Note

If a compressed file includes a validation code, WebScanX routinely checks for modifications to that code whether you choose this option or not. Changes in the validation code, however, do not necessarily mean that the compressed file contains a virus.

Note

Clicking **Cancel** does not undo any changes you save when you click **Apply**.

To choose options for other types of scans, click a different tab in the WebScanX Properties dialog box.

Note

Setting WebScanX's log feature ensures that you can identify deleted files so that you can find or request uninfected copies.

Note

If you have activated its logging feature, the name and location of each infected file appears in the report WebScanX generates and saves. That way, you can later move, delete or otherwise dispose of the infected files that WebScanX finds.

Note

To find an e-mail address in this way, you must store address information in a [MAPI-compliant](#) user directory, database or address book or in an equivalent Lotus cc:Mail directory. If you have not yet logged onto your e-mail system, WebScanX asks you either to choose a [user profile](#) it can use to log onto MAPI-compliant mail systems, or to supply a user name, password and path to your Lotus cc:Mail mailbox. Enter the requested information, then click **OK** to continue.

Note

If necessary, check with your network administrator to determine which folder to use. The folder you choose should contain the file CENTALRT.TXT.

Note

Enter a value between 10KB and 999KB. By default, WebScanX limits the file size to 100KB. If the data in the log exceeds this file size, WebScanX deletes the existing log and begins again from the point at which it left off.

WebScanX logs all information about e-mail scanning activity in one file—log files for other program components record data for those types of scans.

Note

If a compressed file includes a validation code, WebScanX routinely checks for modifications to that code whether you choose this option or not. Changes in the validation code, however, do not necessarily mean that the compressed file contains a virus.

Note

Enter a value between 10KB and 999KB. By default, WebScanX limits the file size to 100KB. If the data in the log exceeds this file size, WebScanX deletes the existing log and begins again from the point at which it left off.

WebScanX logs all information about download scanning activity in one file—log files for other program components record data for those types of scans.

Note


WebScanX does not distinguish between upper- and lower-case characters in passwords. You may enter the password "lockup," for example, as "Lockup," "lockup," or "LOCKUP."

Note

If the program component is active, the button reads **Disable**. If the program component is inactive, the same button reads **Enable**.

Using the button to enable or disable a program component is equivalent to selecting or clearing the Enable checkbox in the appropriate component's property page.

Note

Closing the WebScanX Status dialog box does not quit WebScanX. To learn how to quit, click [here](#) .

Note


Click **Default** to return the list of extensions to its original configuration.

Note


Enter a value between 10KB and 999KB. By default, WebScanX limits the file size to 100KB. If the data in the log exceeds this file size, WebScanX deletes the existing log and begins again from the point at which it left off.

WebScanX logs all information about Internet filtering activity in one file—log files for other program components record data for those types of scans.

Note

WebScanX activity icons—

 or


 appear in these locations:


- n In the taskbar's system tray, to the left of the clock, if you run WebScanX on Windows 95 or Windows NT 4.0 systems. Right-click any of these icons to display its associated shortcut menu.
- n On the desktop, at the bottom left corner of your screen, if you run WebScanX on Windows NT 3.51 systems. Click any of these icons to display its associated shortcut menu.


Double-clicking any activity icon opens the WebScanX Status dialog box. Click **Properties** to open the WebScanX Properties dialog box.

Note

If you have not yet logged on to your e-mail system, WebScanX may ask you to choose or specify a [user profile](#) it can use to log on to your e-mail system. If you see your user profile listed, choose it, then click **OK** to close the Choose Profile dialog box. WebScanX then allows you to choose or create a new quarantine directory. Follow these steps:


3 Click  to open a disk, folder, or other icon shown in the dialog box.

4 Click  to choose the folder you want to use, or click **New Folder** to create a new quarantine folder.

The icon for the folder you select changes to .

5 Select the **Include subfolders** checkbox to tell WebScanX to look for new mail in all folders contained within the folder you choose.

6 Click **OK** to return to the Action dialog box.

The pathname for the folder you chose appears in the text box beside .

Note

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

Note


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


Note


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.

Note

If you have not yet logged on to your e-mail system, WebScanX may ask you to choose or specify a [user profile](#) it can use to log on to your e-mail system. If you see your user profile listed, choose it, then click **OK** to close the Choose Profile dialog box. WebScanX then allows you to choose or create a new quarantine directory. Follow these steps:


1 Click  to open a disk, folder, or other icon shown in the dialog box.

2 Click  to choose the folder you want to use.

The icon for the folder you select changes to .

3 Select the **Include subfolders** checkbox to tell WebScanX to look for new mail in all folders contained within the folder you choose.

4 Click **OK** to return to the Action dialog box.

The pathname for the folder you chose appears in the text box beside .

User Profile

A user profile is a group of settings that defines how you want WebScanX and other Windows software to interact with MAPI-compliant information services that you use. Examples of such information services include: Lotus cc:Mail version 7 or later; Microsoft Mail or other MAPI-compliant e-mail systems; and Internet mail or World Wide Web browsing with Microsoft Internet Explorer. The user profile specifies how you log on to these services, where you store incoming mail, which address books or directories you use, and other preferences. WebScanX needs to know this information so that it can perform its scanning operations properly.

Normally you have only one user profile to choose from, but if more than one person uses the computer you use, or if you need different settings for different tasks, you can create additional user profiles. Consult the documentation for Windows Messaging for more details.

McAfee NetShield

NetShield is McAfee's server anti-virus solution. It permits a network administrator to set up Centralized Alerting, a client-server arrangement for detecting and responding to virus infections on a consistent, regular, network-wide basis. NetShield collects alert messages from client programs such as WebScanX in a text file, CENTALRT.TXT, and makes them available to the network administrator. To tell WebScanX to route its network alert messages properly, specify the path to the folder than contains CENTALRT.TXT. For more information, see the NetShield User's Guide.

WebScanX Supported Browsers

WebScanX scans e-mail messages and files you download or receive with these browsers:

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

WebScanX also scans e-mail you receive via standard POP-3 or SMTP Internet Mail protocols using client software such as Qualcomm's Eudora.

.OCX file

An ActiveX control that incorporates a user interface.

This is the activity icon for WebScanX's **E-mail Scan** program component.

This is the activity icon for WebScanX's **Download Scan** program component.


This is the activity icon for WebScanX's **Internet Filter** program component.

This is a context-sensitive Help file that is called from an application.


▶ Click this button to close this dialog box.


▶ Click this button to ignore infected files and continue scanning.


▶ Click this button to delete the infected file from your system.


 Click this button to move the infected file to a quarantine directory.


To create or designate a quarantine directory, open the WebScanX Properties dialog box.


 This shows the name of the file or object WebScanX scanned.


 This shows the name of the virus carried in the infected file.

 Click this button to stop scanning immediately.


 Click this button to deny the Java class or ActiveX control access to your system.

 This shows the name of the file or object WebScanX scanned.


 Click any of the buttons shown in this dialog box to respond when WebScanX detects a virus or encounters a harmful Java or ActiveX object.

To determine which options appear here, open the WebScanX Properties dialog box, click one of the tabs to display the property page for the scan type whose options you want to change, then choose **Prompt for user action** from the Action list. Next, click  to open the Action dialog box.


 This shows the last action you asked WebScanX to take to respond to an infected file.

 Type your cc:Mail user name here.


WebScanX logs on to your cc:Mail account with your user name in order to scan incoming mail for viruses.


 Type your cc:Mail account password here.


WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Type the path to your cc:Mail post office or server in the text box.

WebScanX uses this path to locate your cc:Mail Inbox and check it periodically for new e-mail.


 Click this button to have WebScanX log on to your cc:Mail account and scan your e-mail for viruses.


 Click this button to close this dialog box without logging on to your cc:Mail account.

 Enter the password you use to log on to your cc:Mail system here.


WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Click this button to have WebScanX log on to your cc:Mail system with this password.


 Click this button to close this dialog box without entering a password.

 Click this button to enable or disable this program component.


If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.


 This shows the name of the last Java class or ActiveX control that WebScanX examined.


 This shows the IP address for the last web or Internet site that WebScanX examined.


 This number shows how many Java classes or applets WebScanX examined.

 This number shows how many ActiveX controls WebScanX examined.


 This number shows how many Internet sites WebScanX examined.


 This number shows how many harmful Java applets or classes WebScanX found.

 This number shows how many harmful ActiveX controls WebScanX found.


 This number shows how many harmful Internet sites WebScanX blocked your browser software from visiting.


 Click this button to open the WebScanX Properties dialog box.

 Click this button to close the WebScanX Status dialog box.


 This area summarizes


- The number of Java classes or applets, ActiveX controls and Internet sites WebScanX examined
- The number of harmful sites or objects it blocked from your system


 This shows the name of the last Java class or ActiveX control that WebScanX examined.

 The numbers in this row show how many Java applets or classes WebScanX examined and how many it blocked from your system.


 The numbers in this row show how many ActiveX controls WebScanX examined and how many it blocked from your system.

 The numbers in this row show how many Internet sites WebScanX examined and how many it blocked your browser software from visiting.


 The numbers in this column show how many objects and Internet sites WebScanX blocked.


 The numbers in this column show how many objects and Internet sites WebScanX examined.


 This shows the IP address for the last web or Internet site that WebScanX examined.

 Click this button to enable or disable this program component.


If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.

 This shows the path and filename for the most recent item that WebScanX examined.


 This number shows how many files WebScanX examined.


 This number shows how many infected files WebScanX found.

 This number shows how many infected files WebScanX moved to a quarantine directory.

 This number shows how many infected files WebScanX deleted from your system.

 Click this button to open the WebScanX Properties dialog box.

 Click this button to close this dialog box.

 This shows the path and filename for the most recent item that WebScanX examined.


>> This area summarizes


>> The number of files that WebScanX examined for viruses

>> The number of infected files it found


>> The number of infected files it moved to a quarantine directory

>> The number of infected files it deleted from your system


 This number shows how many files WebScanX examined.


 This number shows how many infected files WebScanX found.

 This number shows how many infected files WebScanX moved to a quarantine directory.


 This number shows how many infected files WebScanX deleted from your system.


 Click this button to open the WebScanX Properties dialog box.


 Click this button to close the WebScanX Status dialog box.

 Click this button to enable or disable this program component.


If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.


 This shows the path and filename for the most recent item WebScanX examined.

 This shows how many files WebScanX examined.

 This shows how many infected files WebScanX found.

 This shows how many infected files WebScanX moved to a quarantine directory.

 This shows how many infected files WebScanX deleted from your system.

 This shows the path and filename for the most recent item that WebScanX examined for viruses.


>> This area summarizes


>> The number of files that WebScanX examined for viruses

>> The number of infected files it found

>> The number of infected files it moved to a quarantine directory


>> The number of infected files it deleted from your system


 This shows how many files WebScanX examined.


 This shows how many infected files WebScanX found.

 This shows how many infected files WebScanX moved to a quarantine directory.


 This shows how many infected files WebScanX deleted from your system.


 Click this button to ignore infected files and continue scanning.


 Click this button to delete the infected file from your system.


 Click this button to move the infected file to a quarantine directory.


To create or designate a quarantine directory, open the WebScanX Properties dialog box.


 This shows the name of the file or object WebScanX scanned.


 This shows the name of the virus carried in the infected file.


 Click this button to stop scanning immediately.

 Click this button to deny the Java class or ActiveX control access to your system.

 This shows the name of the file or object WebScanX scanned.

 Click any of the buttons shown in this dialog box to respond when WebScanX detects a virus or encounters a harmful Java or ActiveX object.

To determine which options appear here, open the WebScanX Properties dialog box, click one of the tabs to display the property page for the scan type whose options you want to change, then choose **Prompt for user action** from the Action list. Next, click  to open the Action dialog box.

 This message tells you that you might need to update your WebScanX virus definition (.DAT) files or upgrade your WebScanX software.


Because as many as 200 new viruses and harmful Java and ActiveX objects emerge each month, the definition files included with your copy of WebScanX can become out of date within a couple of months. Updates to your .DAT files are free from the McAfee Web Site for the life of your product. Please note that McAfee cannot guarantee that updated .DAT files will continue to work with older versions of the scanning software.

 Click this button to connect directly with the McAfee Web Site to **upgrade** your copy of WebScanX.


Upgrade means a new version of the entire product, or its executable files and definition files. *Update* means revisions only to the virus definition files.

 Click this button to connect directly with the McAfee Web Site to **update** your copy of WebScanX.

Upgrade means a new version of the entire product, or its executable files and definition files. *Update* means revisions only to the virus definition files.

 Click this button to close this dialog box without connecting to the McAfee Web Site.



Select this checkbox to tell WebScanX to show this same message in 30 days.

 This message tells you that you might need to update your WebScanX virus definition (.DAT) files or upgrade your WebScanX software.

Because as many as 200 new viruses and harmful Java and ActiveX objects emerge each month, the definition files included with your copy of WebScanX can become out of date within a couple of months. Updates to your .DAT files are free from the McAfee Web Site for the life of your product. Please note that McAfee cannot guarantee that updated .DAT files will continue to work with older versions of the scanning software.


Select this checkbox to scan for viruses in e-mail files you receive from the Internet via Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant e-mail client.

Clear this checkbox to disable this program component.


 Select this checkbox to display the icon
 for this program component.

The icon appears in the toolbar's system tray, to the left of the clock, in systems running Windows 95 and Windows NT 4.0. Right-click it to display a shortcut menu.


The icon appears on the desktop at the bottom left corner of the screen on systems running Windows NT 3.51. Click it to display a shortcut menu.


 Select this button to scan for viruses in e-mail you receive from the Internet via Microsoft Mail or any MAPI-compliant e-mail client.


Next, in the Detection area, choose whether you want WebScanX to examine all e-mail you receive for viruses, or only those attachments most susceptible to virus infection.


 Select this button to scan for viruses in e-mail you receive from the Internet via Lotus cc:Mail.

Next, in the Detection area, specify how frequently WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.


 Select this button to tell WebScanX to look for viruses in all new e-mail you receive from the Internet via Microsoft Mail or any MAPI-compliant e-mail client.


 Select this button to tell WebScanX to look for new e-mail in a particular folder.


Next, click  to designate the folder WebScanX should watch.


 Click this button to designate the folder WebScanX should check for new e-mail.


If you have not yet logged on to your e-mail system, WebScanX asks you to choose or create a user profile for use with Microsoft Mail or a MAPI-compliant mail system. See the documentation for Microsoft Messaging for more details.


 In the text box, enter how often, in seconds, WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.


 In the text box, enter how often, in seconds, WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.

 Choose which files you want to examine from among those you receive from the Internet via your e-mail client software.

Choose **All attachments** to examine every message you receive. Choose **Program files only** to examine only those files most susceptible to infection. To see the list WebScanX uses to identify susceptible files, click . You can also tell WebScanX to examine compressed files.

 Choose which files you want to examine from among those you receive from the Internet via your e-mail client software.


Choose **All attachments** to examine every message you receive. Choose **Program files only** to examine only those files most susceptible to infection. To see the list WebScanX uses to identify susceptible files, click .

 Click this button to see the list WebScanX uses to identify those files most susceptible to virus infection.


Select this checkbox to scan for viruses in files compressed with LHA, LZEXE, PkLite, PkZip, or WinZip.


 Choose from this list how you want WebScanX to respond when it finds an infected file.


You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.


 Choose here how you want WebScanX to respond when it finds an infected file.


You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.


 If you choose **Prompt for user action** from the list to the left, click this button to tell WebScanX which response options you want to see when it finds a virus.


 If you have chosen **Move infected files to a folder** from the list to the left, click this button to choose a quarantine folder into which WebScanX can move infected files.


 Select this checkbox to send an alert message to the person who sent you e-mail that carried a virus.

WebScanX sends a standard alert message each time it detects a virus. To see or compose the message WebScanX sends, click .

 Click this button to see or compose the alert message that WebScanX sends to the person who sent you an infected e-mail message.



 Select this checkbox to send a message to other people to alert them about infected e-mail.

WebScanX sends a standard alert message each time it detects a virus. To see or compose the message WebScanX sends, click .


 Click this button to see or compose the message that WebScanX sends to alert others about infected e-mail.

Select this checkbox to alert your network administrator via NetShield when WebScanX finds an infected file.

NetShield is McAfee's server anti-virus solution.



 Enter the path to the NetShield directory that contains the file CENTALRT.TXT here, or click
 to browse for the correct directory.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


 Click this button to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box to the left.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


- Select this checkbox to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings

 Enter the path to your log file here or click
 to create or locate a log file.


 Click this button to create or locate a WebScanX log file, or enter the name and path of an existing log file in the text box to the left.

 In the text box, enter how often, in seconds, WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.

 Use this property page to tell WebScanX how to scan for viruses in files you download or receive from the Internet via Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant e-mail client software.


 Choose which files you want WebScanX to examine for viruses by clicking these buttons.


You may choose to scan all files you download or receive from the Internet via your client software, or only those files most susceptible to infection. You may also choose to scan compressed files.


 Select the checkboxes below to specify who WebScanX should alert when it detects a virus.


- Select the checkbox below to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings


Next, enter the path to your log file in the text box below, or click to create a new file or locate an existing file.

 In the text box below, enter the password you want to use to protect your property page settings from unauthorized changes.


 In this text box, enter the password you want to use to protect your property page settings from unauthorized changes.

 In the text box below, reenter the password you want to use in order to confirm your choice.

 In this text box, reenter the password you want to use in order to confirm your choice.


 Click this button to use the password you entered and close this dialog box.


 Click this button to close this dialog box without designating a password or changing an existing password.


 Type the numeric IP address you want to add to WebScanX's "banned" list here.

IP addresses consist of up to 12 numbers in groups of three separated by periods: 123.456.789.101, for example. To determine the IP address for a particular site, see the status bar in your browser software as you connect.

Because the IP address for a particular site can change without notice, McAfee recommends that you enter most addresses using their domain names instead.


 Click this button to add the IP address you entered to WebScanX's "banned" list and close this dialog box.


 Click this button to close this dialog box without adding an IP address to WebScanX's "banned" list.


 Type the subnet mask for the site you want to add to WebScanX's "banned" list here.

A subnet mask is a value used to "remap" a range of addresses within a network on the Internet. If you know the subnet mask value for the machine you want to avoid, enter it here. Otherwise, leave the default value shown.

Because the IP address for a particular site can change frequently, McAfee recommends that you enter most addresses using their domain names instead.

 Click this button to stop WebScanX from trying to connect to the server.


 Click any tab to choose a WebScanX property page.



 Click this button to save your settings in this or any other property page, and close the WebScanX Properties dialog box.


 Click this button to close the WebScanX Properties dialog box without saving your settings.


Note: Clicking **Cancel** does not undo any settings you saved by clicking **Apply**.


 Click this button to save your settings in this or any other property page without closing the WebScanX Properties dialog box.


 Click this button to tell WebScanX whether to start as soon as Windows finishes loading.

Turn the switch off  to keep WebScanX from loading at startup. Turn the switch on  to have WebScanX start whenever you start your computer.


 Click this button to choose recipients for this message from your Lotus cc:Mail directory or one of your MAPI address books.

 Enter the e-mail address for each person who should receive a standard alert message from WebScanX every time it detects a virus.


 Click this button to use your Lotus cc:Mail directory or one of your MAPI address books to designate recipients for copies of WebScanX's standard alert message.

 Enter the e-mail address for each person who should receive a copy of WebScanX's standard alert message each time it detects a virus.


 Enter a title for the standard alert message that WebScanX sends.


 Enter a message of up to 1024 characters that you want to send along with WebScanX's alert message.

This custom text appears in each message sent to the recipients you entered above.


 Click this button to tell WebScanX to use this message, as you've edited it, as its standard alert message.


WebScanX sends this message to the recipients you entered above each time it finds a virus in e-mail you receive.


 Click this button to close this dialog box without saving any changes to WebScanX's standard alert message.

 WebScanX fills this area with a description of the infection. The description includes the filename and the name of the infecting virus.


You may not edit this part of the message.

 Type the path and filename for your log file here.

Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear here.

 Click this button to create or locate the log file you want to use.

Once you choose a log file, the path and filename appear in the text box to the left.

 Select this checkbox to limit the size of your log file so that it doesn't take up excessive hard disk space.

Clearing this checkbox sets no size limits on your log file, but the largest log file WebScanX can record is 999KB in size. When WebScanX reaches this limit, it clears the log file and begins recording over again.

Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.

You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.

Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.

You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.

Select this checkbox to record the names of any virus strains WebScanX finds during a scanning session, and the number of times it finds them.


Select this checkbox to record the settings you chose in the WebScanX Properties dialog box for this scanning session.


Select this checkbox to record the number of infected files WebScanX deletes during a scanning session.


Select this checkbox to summarize the number of files WebScanX examined during this scanning session, the number of infected files it found, and the number it moved or deleted.


The session summary also records other information about the options you chose for this session.


Select this checkbox to record the number of infected files WebScanX moved to a quarantine directory during a scanning session.


 Click this button to tell WebScanX to save a log file with the options you chose.

 Click this button to close this dialog box without saving any changes.

 Type the path and filename for your log file in the text box below.

Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear in the text box below.


 Select any of these checkboxes to record the corresponding information in your log file.

 Select this checkbox to give yourself the option to delete infected files from your system as WebScanX detects them.


When selected, this option appears as a button in the WebScanX Alert dialog box.

 Select this checkbox to give yourself the option to ignore infected files and continue scanning.

When selected, this option appears as a button in the WebScanX Alert dialog box.

 Select this checkbox to give yourself the option to move infected files to a quarantine directory.


When selected, this option appears as a button in the WebScanX Alert dialog box.

 Select this checkbox to give yourself the option to stop scanning immediately.
When selected, this option appears as a button in the WebScanX Alert dialog box.


Select this checkbox to tell WebScanX to beep when it finds an infected file.

Select this checkbox to display a custom message when WebScanX finds an infected file.

Next, enter the message you want to see in the text box below. When selected, this option displays your message as alert text in the WebScanX Alert dialog box.

 Select the Display Custom Message checkbox, then enter the message you want to see in this text box.

When selected, this option displays your message as alert text in the WebScanX Alert dialog box.

 Click this button to save the options you selected and close this dialog box.

 Click this button to close this dialog box without changing any options.

 Select the responses you want WebScanX to offer you when it detects a virus.


Possible actions include: Delete the infected file, move the infected file to a quarantine directory, ignore the infected file and continue scanning, or stop the scan altogether. The options you choose here appear as buttons in the WebScanX Alert dialog box.

 Select any of the checkboxes below to specify which responses you want WebScanX to offer you when it detects a virus.


Possible actions include: Delete the infected file, move the infected file to a quarantine directory, ignore the infected file and continue scanning, or stop the scan altogether. The options you choose here appear as buttons in the WebScanX Alert dialog box.


- Select the checkboxes to
 - Tell WebScanX to beep when it finds an infected file
 - Display a custom message in the WebScanX Alert dialog box


Enter your custom message in the text box.


 Select this checkbox to give yourself the option to deny harmful object access to your system as WebScanX detects them.


When selected, this option appears as a button in the WebScanX Alert dialog box.

 In this text box, enter the password you set to protect your property page settings from unauthorized changes, then click **OK**.


 Click this button to enter your password and close this dialog box.

 Click this button to close this dialog box without entering a password.

 In the text box below, enter the password you set to protect your property page settings from unauthorized changes, then click **OK**.


 Enter the password you use to log on to your cc:Mail system here.

WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Enter the password you use to log on to your cc:Mail system here.



WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Click this button to have WebScanX log on to your cc:Mail system with this password.

 Click this button to close this dialog box without entering a password.


Select this checkbox to scan for viruses in files you download or receive from the Internet via one of the browsers WebScanX supports.

Clear this checkbox to disable this program component.


 Select this checkbox to display the icon
 for this program component.


The icon appears in the toolbar's system tray, to the left of the clock, in systems running Windows 95 and Windows NT 4.0. Right-click it to display a shortcut menu.


The icon appears on the desktop at the bottom left corner of the screen on systems running Windows NT 3.51. Click it to display a shortcut menu.


 Select this button to scan for viruses in all files that you download or receive from the Internet.

Select this checkbox to scan for viruses in files compressed with LHA, LZEXE, PkLite, PkZip, or WinZip.

 Select this button to scan for viruses only in those files most susceptible to infection.

WebScanX identifies susceptible files by looking at their filename extensions. To see the extensions list WebScanX uses, click .


 Click this button to see the list WebScanX uses to identify those files most susceptible to virus infection.


 Choose from this list how you want WebScanX to respond when it finds an infected file.

You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.

 Choose from this list how you want WebScanX to respond when it finds an infected file.



You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.

 If you choose **Prompt for user action** from the list to the left, click this button to tell WebScanX which response options you want to see when it finds a virus.


 If you have chosen **Move infected files to a folder** from the list to the left, click this button to choose a quarantine folder into which WebScanX can move infected files.

Select this checkbox to alert your network administrator via NetShield when WebScanX finds an infected file.

NetShield is McAfee's server anti-virus solution.



 Enter the path to the NetShield directory that contains the file CENTALRT.TXT here, or click
 to browse for the correct directory.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


 Click this button to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box to the left.

WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


- Select this checkbox to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings


 Enter the path to your log file here or click
 to create or locate a log file.

 Click this button to create or locate a WebScanX log file, or enter the name and path of an existing log file in the text box to the left.

 Choose which files you want WebScanX to examine for viruses by clicking these buttons.

You may choose to scan all files you download or receive from the Internet, or only those files most susceptible to infection. You may also choose to scan compressed files.


 Click the checkbox to send an alert message to your network administrator whenever WebScanX detects a virus in an e-mail message you receive.

Next, click  to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box.

WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


- Select the checkbox below to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings

Next, enter the path to your log file in the text box below, or click to create a new file or locate an existing file.


 Use this property page to tell WebScanX how to scan for viruses in files you download or receive from the Internet via one of the browsers it supports.

 Type your cc:Mail user name here.


WebScanX logs on to your cc:Mail account with your user name in order to scan incoming mail for viruses.

 Type your cc:Mail user name here.

WebScanX logs on to your cc:Mail account with your user name in order to scan incoming mail for viruses.

 Type your cc:Mail account password here.

WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Type your cc:Mail account password here.


WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.


 Type the path to your cc:Mail post office or server in the text box.


WebScanX uses this path to locate your cc:Mail Inbox and check it periodically for new e-mail.

 Type the path to your cc:Mail post office or server in the text box.


WebScanX uses this path to locate your cc:Mail Inbox and check it periodically for new e-mail.

 Click this button to have WebScanX log on to your cc:Mail account and scan your e-mail for viruses.

 Click this button to close this dialog box without logging on to your cc:Mail account.


 Click this button to save this list of IP addresses and close this dialog box.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to close this dialog box without changing the list of IP addresses.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to add an IP address to the list WebScanX uses to identify harmful Internet sites.

 Select an IP address from the list to the left, then click this button to delete it.


 WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.

 Enter all or part of the name of the person you want to add to your receipt list in the text box.


 Enter all or part of the name of the person you want to add to your receipt list here.

 This list shows the names of each person you have chosen to receive your message.


To add recipients, enter a name in the text box above, then click **Add**.


 Choose the cc:Mail directory you want to search from this list.


Your cc:Mail server lists those directories available to you here.


 Choose the cc:Mail directory you want to search from this list.

Your cc:Mail server lists those directories available to you here.

 Click this button to add a name to your recipient list.

 Select a name in the recipient list, then click this button to delete it.

 Click this button to send your message to the names shown in the recipient list.

 Enter all or part of the name of the person you want to add to your recipient list in the text box below.


Your cc:Mail server searches for the name you want in one of the directories available to you. Choose the directory you want to search from the list at the bottom of this dialog box. When you find the correct name, click **Add** to add it to your recipient list. Each name you select appears in the list below the text box. Repeat these steps to continue adding names to the recipient list.




Click this button to use the quarantine directory you specified and close this dialog box.




Click this button to close this dialog box without specifying a quarantine directory.


 In the text box, type the path and folder name you want to use for your cc:Mail quarantine directory.


WebScanX moves infected cc:Mail files it finds to this folder if you choose **Move infected files to a folder** in the Action list.


 In the text box, type the path and folder name you want to use for your cc:Mail quarantine directory.


WebScanX moves infected cc:Mail files it finds to this folder if you choose **Move infected files to a folder** in the Action list.


 Enter the path and name of the directory you want to use to store infected files.


By default, WebScanX creates a directory called Infected in its program directory. You can also click  to browse for an existing directory.


 Enter the path and name of the directory you want to use to store infected files.


By default, WebScanX creates a directory called Infected in its program directory. You can also click  to browse for an existing directory.

 Click this button to browse for the folder you want to use as your quarantine directory.

 Click this button to use the directory you have specified to store infected files.



 Click this button to close this dialog box without specifying a quarantine directory or changing the name of an existing directory.

 Enter the path and name of the directory you want to use to store infected files in the text box below.

By default, WebScanX creates a directory called Infected in its program directory. You can also click  to browse for an existing directory.

Select this checkbox to scan for harmful Java classes, ActiveX controls or Internet sites.

Clear this checkbox to disable this program component.

 Select this checkbox to display the icon
 for this program component.

The icon appears in the toolbar's system tray, to the left of the clock, in systems running Windows 95 and Windows NT 4.0. Right-click it to display a shortcut menu.


The icon appears on the desktop at the bottom left corner of the screen on systems running Windows NT 3.51. Click it to display a shortcut menu.


 Select this checkbox to scan for harmful ActiveX controls as you visit Internet sites.


WebScanX compares the ActiveX controls you encounter with a database of controls known to cause harm. It alerts you when it finds a potentially harmful control, then responds according to how you tell it to in the Action area below.


Select this checkbox to scan for harmful Java classes as you visit Internet sites.


WebScanX compares the Java classes you encounter with a database of classes known to cause harm. It alerts you when it finds a potentially harmful class, then responds according to how you tell it to in the Action area below.


 Select this checkbox to block your browser software from visiting Internet sites you designate with a numeric IP address.


Next, click  to see or add to the list WebScanX uses to identify dangerous Internet sites.

 Click this button to see or add to the list of IP addresses that WebScanX uses to identify dangerous Internet sites.


 Select this checkbox to tell WebScanX to block your browser software from visiting Internet sites you designate with a Uniform Resource Locator (URL) or domain name.

Next, click  to see or add to the list WebScanX uses to identify dangerous Internet sites.


 Click this button to see or add to the list of URLs or domain names that WebScanX uses to identify dangerous Internet sites.

 Choose here how you want WebScanX to respond when it finds a harmful Java class or ActiveX control.



You can tell WebScanX to ask you what you want to do when it detects a virus, or to block the harmful object from your system automatically.

 Choose from this list how you want WebScanX to respond when it finds a harmful Java class or ActiveX control.


You can tell WebScanX to ask you what you want to do when it detects a virus, or to block the harmful object from your system automatically.

 Select this checkbox to alert your network administrator via NetShield when WebScanX finds a harmful Java class or ActiveX control.

NetShield is McAfee's server anti-virus solution.



 Enter the path to the NetShield directory that contains the file CENTALRT.TXT here, or click
 to browse for the correct directory.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


 Click this button to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box to the left.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.

- Select this checkbox to save a log file that records
 - How many Internet sites WebScanX examined for danger
 - How many Java classes and ActiveX controls it examined
 - How many harmful objects or dangerous sites it blocked
 - Other information about your WebScanX settings

 Enter the path to your log file here or click
 to create or locate a log file.


 Click this button to create or locate a WebScanX log file, or enter the path to an existing log file in the text box to the left.


 Use this property page to tell WebScanX to scan for harmful Java classes and ActiveX controls, or dangerous Internet sites.


 Select the checkboxes below to tell WebScanX which objects or sites to examine for potential harm.

- Select the checkbox to save a log file that records
 - How many Internet sites WebScanX examined for danger
 - How many Java classes and ActiveX controls it examined
 - How many harmful objects or dangerous sites it blocked
 - Other information about your WebScanX settings


Next, enter the path to your log file in the text box below, or click to create a new file or locate an existing file.


 Click the checkbox below to send an alert to your network administrator via NetShield, McAfee's server anti-virus solution.


Next, enter the path to the NetShield directory that contains the file CENTALRT.TXT in the text box or click  to browse for it.


 Select the checkboxes to tell WebScanX which harmful objects to look for as you visit Internet sites.


You may choose to look for both ActiveX controls and Java classes, or either object separately.


 Select the checkboxes below to tell WebScanX to block your browser software from visiting dangerous Internet sites.


You may choose to identify dangerous sites either with numeric IP addresses, with URLs or domain names, or with both methods. Click the  buttons to the right of each checkbox to see or add to the list that WebScanX uses to identify dangerous Internet sites.


 Select the property page settings you want to protect from unauthorized changes in this list.

You may select all property pages or any individual page. A  appears to the left of protected pages.


 Click this button to designate a password to protect your property page settings from unauthorized changes.


 Select the property page settings you want to protect from unauthorized changes in the list below.


You may select all property pages or any individual page. A  appears to the left of protected pages.


 Click this button to add the filename extension to the list WebScanX uses to identify files susceptible to infection.

To add another extension, click **Add** in the Program File Extensions dialog box.


 Click this button to close this dialog box without adding a new filename extension.

 In the text box below, type the filename extension you want to add to the list WebScanX uses to identify files susceptible to infection.


 In this text box, type the filename extension you want to add to the list WebScanX uses to identify files susceptible to infection.


 WebScanX uses the list of filename extensions below to identify those files most susceptible to virus infection.

Click **Add** to add another extension to the list. Select an extension from the list, then click **Delete** to remove it. Click **Default** to return the list to its original configuration.


 WebScanX uses this list of filename extensions to identify those files most susceptible to virus infection.


Click **Add** to add another extension to the list. Select an extension from the list, then click **Delete** to remove it. Click **Default** to return the list to its original configuration.


 Click this button to tell WebScanX to identify files with the extensions listed as those most susceptible to virus infection.


 Click this button to close this dialog box without changing the list of filename extensions WebScanX uses to identify files susceptible to virus infection.


 Click this button to add a filename extension to the list WebScanX uses to identify files susceptible to virus infection.

 Select one of the filename extensions in the list to the left, then click this button to delete it.

 Click this button to return the list of filename extensions to its original configuration.

 Type the path and filename for your log file here.

Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear here.

 Click this button to create or locate the log file you want to use.

Once you choose a log file, the path and filename appear in the text box to the left.

Select this checkbox to limit the size of your log file so that it doesn't take up excessive hard disk space.


Clearing this checkbox sets no size limits on your log file, but the largest log file WebScanX can record is 999KB in size. When WebScanX reaches this limit, it clears the log file and begins recording over again.

Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.


You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.


Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.


You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.

 Click this button to tell WebScanX to save a log file with the options you chose.


 Click this button to close this dialog box without saving any changes.


 Type the path and filename for your log file in the text box below.


Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear in the text box below.

 Type the domain name you want to add to WebScanX's "banned" list here.


Do **not** include a transport protocol--"http://," for example--in the address you enter.

 Click this button to add the domain name you entered to WebScanX's "banned" list and close this dialog box.


 Click this button to close this dialog box without adding an address to WebScanX's "banned" list.


 Click this button to save this list of domain names and close this dialog box.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to close this dialog box without changing the list of domain names.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to add a domain name to the list WebScanX uses to identify harmful Internet sites.

 Select a domain name from the list to the left, then click this button to delete it.


 WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 To download new definition files, choose a site near your location from the list, then click **OK**. Choosing a nearby site speeds your file transfer time.


 Click this button to download your new definition files from the location you specified.


 Click this button to cancel your update request.

This is a context-sensitive Help file that is called from an application.


 Click this button to close this dialog box.


 Click this button to ignore infected files and continue scanning.


 Click this button to delete the infected file from your system.


 Click this button to move the infected file to a quarantine directory.


To create or designate a quarantine directory, open the WebScanX Properties dialog box.


 This shows the name of the file or object WebScanX scanned.


 This shows the name of the virus carried in the infected file.

 Click this button to stop scanning immediately.

 Click this button to deny the Java class or ActiveX control access to your system.

 This shows the name of the file or object WebScanX scanned.


 Click any of the buttons shown in this dialog box to respond when WebScanX detects a virus or encounters a harmful Java or ActiveX object.

To determine which options appear here, open the WebScanX Properties dialog box, click one of the tabs to display the property page for the scan type whose options you want to change, then choose **Prompt for user action** from the Action list. Next, click  to open the Action dialog box.

 This shows the last action you asked WebScanX to take to respond to an infected file.

 Type your cc:Mail user name here.


WebScanX logs on to your cc:Mail account with your user name in order to scan incoming mail for viruses.


 Type your cc:Mail account password here.


WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Type the path to your cc:Mail post office or server in the text box.

WebScanX uses this path to locate your cc:Mail Inbox and check it periodically for new e-mail.


 Click this button to have WebScanX log on to your cc:Mail account and scan your e-mail for viruses.


 Click this button to close this dialog box without logging on to your cc:Mail account.

 Enter the password you use to log on to your cc:Mail system here.


WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Click this button to have WebScanX log on to your cc:Mail system with this password.


 Click this button to close this dialog box without entering a password.

 Click this button to enable or disable this program component.


If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.


 This shows the name of the last Java class or ActiveX control that WebScanX examined.


 This shows the IP address for the last web or Internet site that WebScanX examined.


 This number shows how many Java classes or applets WebScanX examined.

 This number shows how many ActiveX controls WebScanX examined.


 This number shows how many Internet sites WebScanX examined.

 This number shows how many harmful Java applets or classes WebScanX found.

 This number shows how many harmful ActiveX controls WebScanX found.

 This number shows how many harmful Internet sites WebScanX blocked your browser software from visiting.


 Click this button to open the WebScanX Properties dialog box.


 Click this button to close the WebScanX Status dialog box.

» This area summarizes


» The number of Java classes or applets, ActiveX controls and Internet sites WebScanX examined


» The number of harmful sites or objects it blocked from your system


 This shows the name of the last Java class or ActiveX control that WebScanX examined.

 The numbers in this row show how many Java applets or classes WebScanX examined and how many it blocked from your system.


 The numbers in this row show how many ActiveX controls WebScanX examined and how many it blocked from your system.

 The numbers in this row show how many Internet sites WebScanX examined and how many it blocked your browser software from visiting.


 The numbers in this column show how many objects and Internet sites WebScanX blocked.


 The numbers in this column show how many objects and Internet sites WebScanX examined.


 This shows the IP address for the last web or Internet site that WebScanX examined.

 Click this button to enable or disable this program component.


If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.

 This shows the path and filename for the most recent item that WebScanX examined.


 This number shows how many files WebScanX examined.


 This number shows how many infected files WebScanX found.

 This number shows how many infected files WebScanX moved to a quarantine directory.

 This number shows how many infected files WebScanX deleted from your system.

 Click this button to open the WebScanX Properties dialog box.

 Click this button to close this dialog box.

 This shows the path and filename for the most recent item that WebScanX examined.


>> This area summarizes


>> The number of files that WebScanX examined for viruses

>> The number of infected files it found


>> The number of infected files it moved to a quarantine directory

>> The number of infected files it deleted from your system


 This number shows how many files WebScanX examined.


 This number shows how many infected files WebScanX found.

 This number shows how many infected files WebScanX moved to a quarantine directory.


 This number shows how many infected files WebScanX deleted from your system.


 Click this button to open the WebScanX Properties dialog box.


 Click this button to close the WebScanX Status dialog box.

 Click this button to enable or disable this program component.

If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.


 This shows the path and filename for the most recent item WebScanX examined.

 This shows how many files WebScanX examined.

 This shows how many infected files WebScanX found.

 This shows how many infected files WebScanX moved to a quarantine directory.

 This shows how many infected files WebScanX deleted from your system.

 This shows the path and filename for the most recent item that WebScanX examined for viruses.


>> This area summarizes


>> The number of files that WebScanX examined for viruses

>> The number of infected files it found

>> The number of infected files it moved to a quarantine directory


>> The number of infected files it deleted from your system


 This shows how many files WebScanX examined.


 This shows how many infected files WebScanX found.

 This shows how many infected files WebScanX moved to a quarantine directory.


 This shows how many infected files WebScanX deleted from your system.


 Click this button to ignore infected files and continue scanning.


 Click this button to delete the infected file from your system.


 Click this button to move the infected file to a quarantine directory.


To create or designate a quarantine directory, open the WebScanX Properties dialog box.


 This shows the name of the file or object WebScanX scanned.


 This shows the name of the virus carried in the infected file.


 Click this button to stop scanning immediately.

 Click this button to deny the Java class or ActiveX control access to your system.

 This shows the name of the file or object WebScanX scanned.

 Click any of the buttons shown in this dialog box to respond when WebScanX detects a virus or encounters a harmful Java or ActiveX object.

To determine which options appear here, open the WebScanX Properties dialog box, click one of the tabs to display the property page for the scan type whose options you want to change, then choose **Prompt for user action** from the Action list. Next, click  to open the Action dialog box.

 This message tells you that you might need to update your WebScanX virus definition (.DAT) files or upgrade your WebScanX software.


Because as many as 200 new viruses and harmful Java and ActiveX objects emerge each month, the definition files included with your copy of WebScanX can become out of date within a couple of months. Updates to your .DAT files are free from the McAfee Web Site for the life of your product. Please note that McAfee cannot guarantee that updated .DAT files will continue to work with older versions of the scanning software.

 Click this button to connect directly with the McAfee Web Site to **upgrade** your copy of WebScanX.


Upgrade means a new version of the entire product, or its executable files and definition files. *Update* means revisions only to the virus definition files.

 Click this button to connect directly with the McAfee Web Site to **update** your copy of WebScanX.

Upgrade means a new version of the entire product, or its executable files and definition files. *Update* means revisions only to the virus definition files.

 Click this button to close this dialog box without connecting to the McAfee Web Site.



Select this checkbox to tell WebScanX to show this same message in 30 days.

 This message tells you that you might need to update your WebScanX virus definition (.DAT) files or upgrade your WebScanX software.

Because as many as 200 new viruses and harmful Java and ActiveX objects emerge each month, the definition files included with your copy of WebScanX can become out of date within a couple of months. Updates to your .DAT files are free from the McAfee Web Site for the life of your product. Please note that McAfee cannot guarantee that updated .DAT files will continue to work with older versions of the scanning software.


Select this checkbox to scan for viruses in e-mail files you receive from the Internet via Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant e-mail client.

Clear this checkbox to disable this program component.


 Select this checkbox to display the icon
 for this program component.

The icon appears in the toolbar's system tray, to the left of the clock, in systems running Windows 95 and Windows NT 4.0. Right-click it to display a shortcut menu.


The icon appears on the desktop at the bottom left corner of the screen on systems running Windows NT 3.51. Click it to display a shortcut menu.


 Select this button to scan for viruses in e-mail you receive from the Internet via Microsoft Mail or any MAPI-compliant e-mail client.


Next, in the Detection area, choose whether you want WebScanX to examine all e-mail you receive for viruses, or only those attachments most susceptible to virus infection.


 Select this button to scan for viruses in e-mail you receive from the Internet via Lotus cc:Mail.

Next, in the Detection area, specify how frequently WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.


 Select this button to tell WebScanX to look for viruses in all new e-mail you receive from the Internet via Microsoft Mail or any MAPI-compliant e-mail client.


 Select this button to tell WebScanX to look for new e-mail in a particular folder.


Next, click  to designate the folder WebScanX should watch.


 Click this button to designate the folder WebScanX should check for new e-mail.


If you have not yet logged on to your e-mail system, WebScanX asks you to choose or create a user profile for use with Microsoft Mail or a MAPI-compliant mail system. See the documentation for Microsoft Messaging for more details.


 In the text box, enter how often, in seconds, WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.


 In the text box, enter how often, in seconds, WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.

 Choose which files you want to examine from among those you receive from the Internet via your e-mail client software.


Choose **All attachments** to examine every message you receive. Choose **Program files only** to examine only those files most susceptible to infection. To see the list WebScanX uses to identify susceptible files, click . You can also tell WebScanX to examine compressed files.

 Choose which files you want to examine from among those you receive from the Internet via your e-mail client software.


Choose **All attachments** to examine every message you receive. Choose **Program files only** to examine only those files most susceptible to infection. To see the list WebScanX uses to identify susceptible files, click .

 Click this button to see the list WebScanX uses to identify those files most susceptible to virus infection.


Select this checkbox to scan for viruses in files compressed with LHA, LZEXE, PkLite, PkZip, or WinZip.


 Choose from this list how you want WebScanX to respond when it finds an infected file.


You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.


 Choose here how you want WebScanX to respond when it finds an infected file.


You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.


 If you choose **Prompt for user action** from the list to the left, click this button to tell WebScanX which response options you want to see when it finds a virus.


 If you have chosen **Move infected files to a folder** from the list to the left, click this button to choose a quarantine folder into which WebScanX can move infected files.


 Select this checkbox to send an alert message to the person who sent you e-mail that carried a virus.

WebScanX sends a standard alert message each time it detects a virus. To see or compose the message WebScanX sends, click .

 Click this button to see or compose the alert message that WebScanX sends to the person who sent you an infected e-mail message.



 Select this checkbox to send a message to other people to alert them about infected e-mail.

WebScanX sends a standard alert message each time it detects a virus. To see or compose the message WebScanX sends, click .


 Click this button to see or compose the message that WebScanX sends to alert others about infected e-mail.

Select this checkbox to alert your network administrator via NetShield when WebScanX finds an infected file.

NetShield is McAfee's server anti-virus solution.



 Enter the path to the NetShield directory that contains the file CENTALRT.TXT here, or click
 to browse for the correct directory.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


 Click this button to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box to the left.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


- Select this checkbox to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings

 Enter the path to your log file here or click
 to create or locate a log file.


 Click this button to create or locate a WebScanX log file, or enter the name and path of an existing log file in the text box to the left.

 In the text box, enter how often, in seconds, WebScanX should check your cc:Mail server to see if new e-mail has arrived. You should tell WebScanX to check the server about twice as frequently as your cc:Mail client software does.

 Use this property page to tell WebScanX how to scan for viruses in files you download or receive from the Internet via Lotus cc:Mail, Microsoft Mail, or any MAPI-compliant e-mail client software.


 Choose which files you want WebScanX to examine for viruses by clicking these buttons.


You may choose to scan all files you download or receive from the Internet via your client software, or only those files most susceptible to infection. You may also choose to scan compressed files.


 Select the checkboxes below to specify who WebScanX should alert when it detects a virus.


- Select the checkbox below to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings


Next, enter the path to your log file in the text box below, or click to create a new file or locate an existing file.

 In the text box below, enter the password you want to use to protect your property page settings from unauthorized changes.


 In this text box, enter the password you want to use to protect your property page settings from unauthorized changes.

 In the text box below, reenter the password you want to use in order to confirm your choice.

 In this text box, reenter the password you want to use in order to confirm your choice.


 Click this button to use the password you entered and close this dialog box.


 Click this button to close this dialog box without designating a password or changing an existing password.


 Type the numeric IP address you want to add to WebScanX's "banned" list here.

IP addresses consist of up to 12 numbers in groups of three separated by periods: 123.456.789.101, for example. To determine the IP address for a particular site, see the status bar in your browser software as you connect.

Because the IP address for a particular site can change without notice, McAfee recommends that you enter most addresses using their domain names instead.


 Click this button to add the IP address you entered to WebScanX's "banned" list and close this dialog box.


 Click this button to close this dialog box without adding an IP address to WebScanX's "banned" list.


 Type the subnet mask for the site you want to add to WebScanX's "banned" list here.

A subnet mask is a value used to "remap" a range of addresses within a network on the Internet. If you know the subnet mask value for the machine you want to avoid, enter it here. Otherwise, leave the default value shown.

Because the IP address for a particular site can change frequently, McAfee recommends that you enter most addresses using their domain names instead.

 Click this button to stop WebScanX from trying to connect to the server.


 Click any tab to choose a WebScanX property page.



 Click this button to save your settings in this or any other property page, and close the WebScanX Properties dialog box.


 Click this button to close the WebScanX Properties dialog box without saving your settings.


Note: Clicking **Cancel** does not undo any settings you saved by clicking **Apply**.


 Click this button to save your settings in this or any other property page without closing the WebScanX Properties dialog box.


 Click this button to tell WebScanX whether to start as soon as Windows finishes loading.

Turn the switch off  to keep WebScanX from loading at startup. Turn the switch on  to have WebScanX start whenever you start your computer.


 Click this button to choose recipients for this message from your Lotus cc:Mail directory or one of your MAPI address books.

 Enter the e-mail address for each person who should receive a standard alert message from WebScanX every time it detects a virus.


 Click this button to use your Lotus cc:Mail directory or one of your MAPI address books to designate recipients for copies of WebScanX's standard alert message.

 Enter the e-mail address for each person who should receive a copy of WebScanX's standard alert message each time it detects a virus.


 Enter a title for the standard alert message that WebScanX sends.


 Enter a message of up to 1024 characters that you want to send along with WebScanX's alert message.

This custom text appears in each message sent to the recipients you entered above.

 Click this button to tell WebScanX to use this message, as you've edited it, as its standard alert message.


WebScanX sends this message to the recipients you entered above each time it finds a virus in e-mail you receive.


 Click this button to close this dialog box without saving any changes to WebScanX's standard alert message.

 WebScanX fills this area with a description of the infection. The description includes the filename and the name of the infecting virus.


You may not edit this part of the message.

 Type the path and filename for your log file here.

Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear here.

 Click this button to create or locate the log file you want to use.

Once you choose a log file, the path and filename appear in the text box to the left.

 Select this checkbox to limit the size of your log file so that it doesn't take up excessive hard disk space.

Clearing this checkbox sets no size limits on your log file, but the largest log file WebScanX can record is 999KB in size. When WebScanX reaches this limit, it clears the log file and begins recording over again.

Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.

You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.

Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.

You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.

Select this checkbox to record the names of any virus strains WebScanX finds during a scanning session, and the number of times it finds them.


Select this checkbox to record the settings you chose in the WebScanX Properties dialog box for this scanning session.


Select this checkbox to record the number of infected files WebScanX deletes during a scanning session.


Select this checkbox to summarize the number of files WebScanX examined during this scanning session, the number of infected files it found, and the number it moved or deleted.


The session summary also records other information about the options you chose for this session.


Select this checkbox to record the number of infected files WebScanX moved to a quarantine directory during a scanning session.


 Click this button to tell WebScanX to save a log file with the options you chose.

 Click this button to close this dialog box without saving any changes.

 Type the path and filename for your log file in the text box below.

Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear in the text box below.


 Select any of these checkboxes to record the corresponding information in your log file.

 Select this checkbox to give yourself the option to delete infected files from your system as WebScanX detects them.


When selected, this option appears as a button in the WebScanX Alert dialog box.

 Select this checkbox to give yourself the option to ignore infected files and continue scanning.

When selected, this option appears as a button in the WebScanX Alert dialog box.

 Select this checkbox to give yourself the option to move infected files to a quarantine directory.


When selected, this option appears as a button in the WebScanX Alert dialog box.

 Select this checkbox to give yourself the option to stop scanning immediately.
When selected, this option appears as a button in the WebScanX Alert dialog box.


Select this checkbox to tell WebScanX to beep when it finds an infected file.

Select this checkbox to display a custom message when WebScanX finds an infected file.

Next, enter the message you want to see in the text box below. When selected, this option displays your message as alert text in the WebScanX Alert dialog box.

 Select the Display Custom Message checkbox, then enter the message you want to see in this text box.

When selected, this option displays your message as alert text in the WebScanX Alert dialog box.

 Click this button to save the options you selected and close this dialog box.

 Click this button to close this dialog box without changing any options.

 Select the responses you want WebScanX to offer you when it detects a virus.


Possible actions include: Delete the infected file, move the infected file to a quarantine directory, ignore the infected file and continue scanning, or stop the scan altogether. The options you choose here appear as buttons in the WebScanX Alert dialog box.

 Select any of the checkboxes below to specify which responses you want WebScanX to offer you when it detects a virus.


Possible actions include: Delete the infected file, move the infected file to a quarantine directory, ignore the infected file and continue scanning, or stop the scan altogether. The options you choose here appear as buttons in the WebScanX Alert dialog box.


- Select the checkboxes to
 - Tell WebScanX to beep when it finds an infected file
 - Display a custom message in the WebScanX Alert dialog box


Enter your custom message in the text box.


 Select this checkbox to give yourself the option to deny harmful object access to your system as WebScanX detects them.


When selected, this option appears as a button in the WebScanX Alert dialog box.

 In this text box, enter the password you set to protect your property page settings from unauthorized changes, then click **OK**.


 Click this button to enter your password and close this dialog box.

 Click this button to close this dialog box without entering a password.

 In the text box below, enter the password you set to protect your property page settings from unauthorized changes, then click **OK**.


 Enter the password you use to log on to your cc:Mail system here.

WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Enter the password you use to log on to your cc:Mail system here.



WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Click this button to have WebScanX log on to your cc:Mail system with this password.

 Click this button to close this dialog box without entering a password.


Select this checkbox to scan for viruses in files you download or receive from the Internet via one of the browsers WebScanX supports.

Clear this checkbox to disable this program component.


 Select this checkbox to display the icon
 for this program component.


The icon appears in the toolbar's system tray, to the left of the clock, in systems running Windows 95 and Windows NT 4.0. Right-click it to display a shortcut menu.


The icon appears on the desktop at the bottom left corner of the screen on systems running Windows NT 3.51. Click it to display a shortcut menu.


 Select this button to scan for viruses in all files that you download or receive from the Internet.

Select this checkbox to scan for viruses in files compressed with LHA, LZEXE, PkLite, PkZip, or WinZip.


 Select this button to scan for viruses only in those files most susceptible to infection.

WebScanX identifies susceptible files by looking at their filename extensions. To see the extensions list WebScanX uses, click .


 Click this button to see the list WebScanX uses to identify those files most susceptible to virus infection.


 Choose from this list how you want WebScanX to respond when it finds an infected file.

You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.

 Choose from this list how you want WebScanX to respond when it finds an infected file.



You can tell WebScanX to ask you what you want to do when it detects a virus, to move the infected file to a quarantine directory, to delete the infected file from your system immediately, or to ignore the infected file and continue scanning.

 If you choose **Prompt for user action** from the list to the left, click this button to tell WebScanX which response options you want to see when it finds a virus.


 If you have chosen **Move infected files to a folder** from the list to the left, click this button to choose a quarantine folder into which WebScanX can move infected files.

Select this checkbox to alert your network administrator via NetShield when WebScanX finds an infected file.

NetShield is McAfee's server anti-virus solution.



 Enter the path to the NetShield directory that contains the file CENTALRT.TXT here, or click
 to browse for the correct directory.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


 Click this button to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box to the left.

WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


- Select this checkbox to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings


 Enter the path to your log file here or click
 to create or locate a log file.

 Click this button to create or locate a WebScanX log file, or enter the name and path of an existing log file in the text box to the left.

 Choose which files you want WebScanX to examine for viruses by clicking these buttons.

You may choose to scan all files you download or receive from the Internet, or only those files most susceptible to infection. You may also choose to scan compressed files.


 Click the checkbox to send an alert message to your network administrator whenever WebScanX detects a virus in an e-mail message you receive.

Next, click  to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box.

WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.

- Select the checkbox below to save a log file that records
 - How many files WebScanX examined for viruses
 - How many infected files it found, and either moved to a folder or deleted
 - Other information about your WebScanX settings

Next, enter the path to your log file in the text box below, or click to create a new file or locate an existing file.


 Use this property page to tell WebScanX how to scan for viruses in files you download or receive from the Internet via one of the browsers it supports.

 Type your cc:Mail user name here.


WebScanX logs on to your cc:Mail account with your user name in order to scan incoming mail for viruses.

 Type your cc:Mail user name here.

WebScanX logs on to your cc:Mail account with your user name in order to scan incoming mail for viruses.

 Type your cc:Mail account password here.

WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.

 Type your cc:Mail account password here.


WebScanX logs on to your cc:Mail account with your password in order to scan incoming mail for viruses.


 Type the path to your cc:Mail post office or server in the text box.


WebScanX uses this path to locate your cc:Mail Inbox and check it periodically for new e-mail.

 Type the path to your cc:Mail post office or server in the text box.


WebScanX uses this path to locate your cc:Mail Inbox and check it periodically for new e-mail.

 Click this button to have WebScanX log on to your cc:Mail account and scan your e-mail for viruses.

 Click this button to close this dialog box without logging on to your cc:Mail account.


 Click this button to save this list of IP addresses and close this dialog box.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to close this dialog box without changing the list of IP addresses.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to add an IP address to the list WebScanX uses to identify harmful Internet sites.

 Select an IP address from the list to the left, then click this button to delete it.


 WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.

 Enter all or part of the name of the person you want to add to your receipt list in the text box.


 Enter all or part of the name of the person you want to add to your recipient list here.

 This list shows the names of each person you have chosen to receive your message.


To add recipients, enter a name in the text box above, then click **Add**.


 Choose the cc:Mail directory you want to search from this list.


Your cc:Mail server lists those directories available to you here.


 Choose the cc:Mail directory you want to search from this list.

Your cc:Mail server lists those directories available to you here.

 Click this button to add a name to your recipient list.

 Select a name in the recipient list, then click this button to delete it.

 Click this button to send your message to the names shown in the recipient list.

 Enter all or part of the name of the person you want to add to your recipient list in the text box below.


Your cc:Mail server searches for the name you want in one of the directories available to you. Choose the directory you want to search from the list at the bottom of this dialog box. When you find the correct name, click **Add** to add it to your recipient list. Each name you select appears in the list below the text box. Repeat these steps to continue adding names to the recipient list.




Click this button to use the quarantine directory you specified and close this dialog box.




Click this button to close this dialog box without specifying a quarantine directory.


 In the text box, type the path and folder name you want to use for your cc:Mail quarantine directory.


WebScanX moves infected cc:Mail files it finds to this folder if you choose **Move infected files to a folder** in the Action list.


 In the text box, type the path and folder name you want to use for your cc:Mail quarantine directory.


WebScanX moves infected cc:Mail files it finds to this folder if you choose **Move infected files to a folder** in the Action list.


 Enter the path and name of the directory you want to use to store infected files.


By default, WebScanX creates a directory called Infected in its program directory. You can also click  to browse for an existing directory.


 Enter the path and name of the directory you want to use to store infected files.


By default, WebScanX creates a directory called Infected in its program directory. You can also click  to browse for an existing directory.

 Click this button to browse for the folder you want to use as your quarantine directory.

 Click this button to use the directory you have specified to store infected files.



 Click this button to close this dialog box without specifying a quarantine directory or changing the name of an existing directory.

 Enter the path and name of the directory you want to use to store infected files in the text box below.

By default, WebScanX creates a directory called Infected in its program directory. You can also click  to browse for an existing directory.


Select this checkbox to scan for harmful Java classes, ActiveX controls or Internet sites.

Clear this checkbox to disable this program component.

 Select this checkbox to display the icon
 for this program component.

The icon appears in the toolbar's system tray, to the left of the clock, in systems running Windows 95 and Windows NT 4.0. Right-click it to display a shortcut menu.


The icon appears on the desktop at the bottom left corner of the screen on systems running Windows NT 3.51. Click it to display a shortcut menu.


 Select this checkbox to scan for harmful ActiveX controls as you visit Internet sites.


WebScanX compares the ActiveX controls you encounter with a database of controls known to cause harm. It alerts you when it finds a potentially harmful control, then responds according to how you tell it to in the Action area below.


Select this checkbox to scan for harmful Java classes as you visit Internet sites.


WebScanX compares the Java classes you encounter with a database of classes known to cause harm. It alerts you when it finds a potentially harmful class, then responds according to how you tell it to in the Action area below.


 Select this checkbox to block your browser software from visiting Internet sites you designate with a numeric IP address.


Next, click  to see or add to the list WebScanX uses to identify dangerous Internet sites.

 Click this button to see or add to the list of IP addresses that WebScanX uses to identify dangerous Internet sites.


 Select this checkbox to tell WebScanX to block your browser software from visiting Internet sites you designate with a Uniform Resource Locator (URL) or domain name.

Next, click  to see or add to the list WebScanX uses to identify dangerous Internet sites.

 Click this button to see or add to the list of URLs or domain names that WebScanX uses to identify dangerous Internet sites.

 Choose here how you want WebScanX to respond when it finds a harmful Java class or ActiveX control.



You can tell WebScanX to ask you what you want to do when it detects a virus, or to block the harmful object from your system automatically.

 Choose from this list how you want WebScanX to respond when it finds a harmful Java class or ActiveX control.


You can tell WebScanX to ask you what you want to do when it detects a virus, or to block the harmful object from your system automatically.

Select this checkbox to alert your network administrator via NetShield when WebScanX finds a harmful Java class or ActiveX control.

NetShield is McAfee's server anti-virus solution.



 Enter the path to the NetShield directory that contains the file CENTALRT.TXT here, or click
 to browse for the correct directory.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.


 Click this button to browse for the NetShield directory that contains the file CENTALRT.TXT, or enter the path to the correct directory in the text box to the left.


WebScanX requires NetShield, McAfee's server anti-virus solution, to provide centralized virus alerting to your network administrator.

- Select this checkbox to save a log file that records
 - How many Internet sites WebScanX examined for danger
 - How many Java classes and ActiveX controls it examined
 - How many harmful objects or dangerous sites it blocked
 - Other information about your WebScanX settings

 Enter the path to your log file here or click
 to create or locate a log file.


 Click this button to create or locate a WebScanX log file, or enter the path to an existing log file in the text box to the left.


 Use this property page to tell WebScanX to scan for harmful Java classes and ActiveX controls, or dangerous Internet sites.


 Select the checkboxes below to tell WebScanX which objects or sites to examine for potential harm.

- Select the checkbox to save a log file that records
 - How many Internet sites WebScanX examined for danger
 - How many Java classes and ActiveX controls it examined
 - How many harmful objects or dangerous sites it blocked
 - Other information about your WebScanX settings


Next, enter the path to your log file in the text box below, or click to create a new file or locate an existing file.


 Click the checkbox below to send an alert to your network administrator via NetShield, McAfee's server anti-virus solution.


Next, enter the path to the NetShield directory that contains the file CENTALRT.TXT in the text box or click  to browse for it.


 Select the checkboxes to tell WebScanX which harmful objects to look for as you visit Internet sites.


You may choose to look for both ActiveX controls and Java classes, or either object separately.


 Select the checkboxes below to tell WebScanX to block your browser software from visiting dangerous Internet sites.


You may choose to identify dangerous sites either with numeric IP addresses, with URLs or domain names, or with both methods. Click the  buttons to the right of each checkbox to see or add to the list that WebScanX uses to identify dangerous Internet sites.


 Select the property page settings you want to protect from unauthorized changes in this list.

You may select all property pages or any individual page. A  appears to the left of protected pages.


 Click this button to designate a password to protect your property page settings from unauthorized changes.


 Select the property page settings you want to protect from unauthorized changes in the list below.


You may select all property pages or any individual page. A  appears to the left of protected pages.


 Click this button to add the filename extension to the list WebScanX uses to identify files susceptible to infection.

To add another extension, click **Add** in the Program File Extensions dialog box.


 Click this button to close this dialog box without adding a new filename extension.

 In the text box below, type the filename extension you want to add to the list WebScanX uses to identify files susceptible to infection.


 In this text box, type the filename extension you want to add to the list WebScanX uses to identify files susceptible to infection.


 WebScanX uses the list of filename extensions below to identify those files most susceptible to virus infection.

Click **Add** to add another extension to the list. Select an extension from the list, then click **Delete** to remove it. Click **Default** to return the list to its original configuration.


 WebScanX uses this list of filename extensions to identify those files most susceptible to virus infection.


Click **Add** to add another extension to the list. Select an extension from the list, then click **Delete** to remove it. Click **Default** to return the list to its original configuration.


 Click this button to tell WebScanX to identify files with the extensions listed as those most susceptible to virus infection.


 Click this button to close this dialog box without changing the list of filename extensions WebScanX uses to identify files susceptible to virus infection.


 Click this button to add a filename extension to the list WebScanX uses to identify files susceptible to virus infection.

 Select one of the filename extensions in the list to the left, then click this button to delete it.


 Click this button to return the list of filename extensions to its original configuration.

 Type the path and filename for your log file here.

Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear here.

 Click this button to create or locate the log file you want to use.

Once you choose a log file, the path and filename appear in the text box to the left.

 Select this checkbox to limit the size of your log file so that it doesn't take up excessive hard disk space.


Clearing this checkbox sets no size limits on your log file, but the largest log file WebScanX can record is 999KB in size. When WebScanX reaches this limit, it clears the log file and begins recording over again.


Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.


You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.


Select the checkbox to the left to limit the size of your log file. Next, enter in this text box the largest amount of data, in kilobytes, that you want WebScanX to record.


You may enter a value between 10KB and 999KB. By default, WebScanX sets the size limit at 100KB.

 Click this button to tell WebScanX to save a log file with the options you chose.


 Click this button to close this dialog box without saving any changes.


 Type the path and filename for your log file in the text box below.


Otherwise, click  to create or locate the log file you want to use. Once you choose a log file, the path and filename appear in the text box below.

 Type the domain name you want to add to WebScanX's "banned" list here.


Do **not** include a transport protocol--"http://," for example--in the address you enter.

 Click this button to add the domain name you entered to WebScanX's "banned" list and close this dialog box.


 Click this button to close this dialog box without adding an address to WebScanX's "banned" list.


 Click this button to save this list of domain names and close this dialog box.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to close this dialog box without changing the list of domain names.


WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.


 Click this button to add a domain name to the list WebScanX uses to identify harmful Internet sites.

 Select a domain name from the list to the left, then click this button to delete it.

 WebScanX uses this list to identify harmful Internet sites and keep your browser software from connecting to them.

 To download new definition files, choose a site near your location from the list, then click **OK**. Choosing a nearby site speeds your file transfer time.

 Click this button to download your new definition files from the location you specified.

 Click this button to cancel your update request.

