# User’s Guide

## VirusScan for Windows 95

**McAfee, Inc.**
2805 Bowers Avenue
Santa Clara, CA 95051-0963

| | |
|---|---|
| Phone: | (408) 988-3832 |
| | Monday - Friday |
| | 6:00 A.M. - 6:00 P.M. |
| Fax: | (408) 970-9727 |
| BBS: | (408) 988-4004 |

## COPYRIGHT

## TRADEMARK NOTICES

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

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

## FEEDBACK

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your comments to: McAfee, Inc., Documentation, 2710 Walsh Avenue, Santa Clara, CA 95051-0963, or send a fax to McAfee Documentation at (408) 970-9727, or send e-mail to documentation@cc.mcafee.com.

*Issued May 1997/VirusScan v3.1.0*

# Table of Contents

# Preface

## The Bits and the Bytes

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

### In the beginning

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

The idea was that if one could create a computer program that could make copies of itself, or self-replicate, it might also be possible for that program to evolve. If an error were to occur in the replication process, the resulting code (the bits of information that make up the program) would be mutant. Just as mutant genetic code is what disposes a biological virus to either be more or less able to survive and propagate, mutant digital code might dispose a computer virus to be more or less able to survive in the computer environment. Given enough time, the logical extension of the theory goes, a computer virus could evolve into something approaching artificial intelligence. Science fiction suddenly starts to look more like science and less like fiction.

## What viruses really are

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

## Computers with the sniffles?

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

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

## Who writes viruses?

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

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

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

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

## Only getting worse

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

## New developments

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

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

All that just in the last few years. And viruses as a serious threat have only been around for about ten years. To imagine what is in store as the computer becomes more complicated and more a part of everyday life is frightening. Luckily, you have purchased the best protection against infection available today. And with McAfee's outstanding support and worldwide anti-virus research teams, you can make sure your protection keeps up with the ever-changing computer world.

# 1 Introducing VirusScan

## What is VirusScan?

VirusScan is McAfee's powerful desktop anti-virus solution for Windows 95. Once installed, VirusScan continuously monitors your system for virus activity. When a virus is detected, VirusScan can to attempt to remove the virus, move the infected files to another location, or delete the infected files. VirusScan can also be user-initiated to scan a file, folder, disk, or volume.

VirusScan is an important element of a comprehensive security program that includes a variety of safety measures, such as regular backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program as a preventive measure to protect against future infection. For tips on creating a secure environment, see Appendix A, "Preventing Virus Infection."

### Main features

- NCSA-certified scanner assures detection of 100% of the viruses found "in the wild." Visit the NCSA website (www.NCSA.com) for certification status.

- VirusScan is a native Windows 95 application that provides true 32-bit implementation, long filename support, Windows 95 context-sensitive help, and unobtrusive memory scanning.

- VShield, VirusScan's on-access scanner, provides real-time identification of both known and unknown viruses upon file access, create, copy, rename, and run; disk access; system startup; and system shut down.

- On-demand scanning provides for user-initiated detection of known boot, file, macro, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.
- VirusScan employs the Hunter scan engine for pinpoint virus identification accuracy.
- VirusScan can be configured for an automated response on virus detection including notification, logging, deletion, isolation, or cleaning.
- The VirusScan Scan Window, Activity Log, and Virus Info provide details of scan results, as well as information about detected viruses.
- Free monthly updates of virus signatures are available to assure the best detection and removal rates. See Appendix C, “McAfee Support Services,” for details.
- McAfee’s SecureCast feature allows users to license products and obtain product upgrades with the push of a button.
- McAfee’s ScreenScan utility automatically scans your system for infected files whenever your screen saver is active.

## How virus detection works

VirusScan monitors your computer and searches for characteristics (sequences of code) unique to each known virus. When a virus is detected, VirusScan alerts you or takes an action you have pre-configured. For viruses that are encrypted or mutated, VirusScan uses algorithms that rely on statistical analysis, heuristics, and code disassembly.

## When should I scan for viruses?

VirusScan’s on-access scanner performs scans of your system every time you access, create, copy, rename, or run a file; access a diskette; start up your system; or shut down. It also protects your system against viruses when you upload and download from networks or receive files electronically.

For maximum protection, use VirusScan’s on-demand scanning feature to scan for viruses whenever you add files to your system, such as files copied from a diskette or files downloaded from an online service.

### Scan unknown diskettes

Before executing, installing, or copying files from an unknown diskette, run VirusScan to check the files on the diskette.

### Scan when you install or download new files

When installing new software or downloading executable files from an online service, run VirusScan to check the files before using them.

### Scan on a regular basis

Perform on-demand scans of your system regularly, from as frequently as once a day to once a month, depending on how susceptible your system is to virus infection. See Chapter 5, “Scheduled Scanning,” for information on automatic scheduled scanning.

# How To Contact Us

## Customer service

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

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

## Technical support

McAfee is famous for its dedication to customer satisfaction. McAfee has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating McAfee software and obtaining the latest news and information. For technical support information and issues, we encourage you to visit our website first.

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

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

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

| | |
|---|---|
| CompuServe | GO MCAFEE |
| America Online | keyword MCAFEE |
| Microsoft Network (MSN) | MCAFEE |

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

For corporate-licensed users:

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

For retail-licensed users:

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

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

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

## McAfee training

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

## International contact information

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

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

**McAfee Europe B.V.**
Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: (0) 31 20 586 6100
Fax: (0) 31 20 586 6101

**McAfee France S.A.**
50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908 737
Fax: 33 1 45 227 554

**McAfee Deutschland GmbH**
Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 8989 43 5600
Fax: 49 8989 43 5699

**McAfee (UK) Ltd.**
Hayley House, London Road
Bracknell, Berkshire
RG12 2TH
United Kingdom
Phone: 44 1344 304 730
Fax: 44 1344 306 902

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

# 2 Installing VirusScan

## Before You Start

To prepare for installation of VirusScan, complete the steps below. If you suspect your system is infected with a virus, see “If You Suspect You Have a Virus” on page 77.

| Step | Action |
|---|---|
| 1. | Review the system requirements for VirusScan. |
| 2. | Confirm your system’s Date/Time settings are accurate. |

✍ *Windows 95 does not require DOS memory managers. If you choose to use them, VirusScan95 may falsely detect viruses in memory. To eliminate this possibility, remove the memory manager command lines from your CONFIG.SYS file.*

### System requirements

- IBM-compatible personal computer running Windows 95

  ✍ *Windows 95 must be functioning properly in order to install and use this software. You cannot install VirusScan for Windows 95 onto a Windows 3.1x system.*

- 486 with at least 8MB of memory (16MB recommended), 5 MB of free hard drive space

# Installation Procedure

To install VirusScan on your Windows 95 system, complete the following procedure:

✍ *If you suspect your system is infected by a virus before beginning this procedure, see “If You Suspect You Have a Virus” on page 77.*

**Step** **Action**

**1.** Start your computer.

**2.** Do one of the following:

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

**3.** Select Run from the Start menu.

- If installing from diskette, type:

  ```
  x:\setup.exe
  ```

  where *x* is the drive in which you placed the diskette. Click OK.

- If installing from compact disc, type:

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

  where *x* is the drive in which you placed the CD-ROM. Click OK.

- If installing from downloaded files, type:

  ```
  x:\path\setup.exe
  ```

  where *x:\path* is the location of the files (for example, C:\DOWNLOAD\SETUP.EXE). Click OK.

**Response**: The Welcome screen is displayed.

**Action**: Click Next to continue.

4. When the Welcome screen is displayed, read the information in it then click Next to continue.

5. Complete one of the following steps:

   - To perform a complete installation of VirusScan with the most common options, select Typical.

   - To install VirusScan with the minimum required options, select Compact.

   - To install VirusScan with user-definable options, select Custom. You will be prompted to select which components you want to install.

   ✍ *The Typical installation meets most users' needs.*

6. Select a destination directory for your VirusScan files. Click Browse and enter the directory in the text box provided or navigate to a specific directory. Click Next to continue.

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

   **Response**: VirusScan checks your system for viruses.

8. When the scan is complete, do one of the following:

   - If no infected files are found, click OK. Installation will continue.

   - If a virus is found, VirusScan will prompt you for action. Click Info.

     ❑ If the Memory-resident checkbox is selected, cancel installation and follow the steps in "If You Suspect You Have a Virus" on page 77.

     ❑ If the Memory-resident checkbox is not selected, McAfee recommends that you delete the infected file and recover a clean copy from backups. Click Close, then click Delete. Close the VirusScan window, cancel the installation, and start over.

9. The McAfee Emergency Disks will now be created.

   ✍ *McAfee strongly recommends making the Emergency Disks. If you do not want to make the McAfee Emergency Disks at this time, click Cancel. You can create Emergency Disks at any time after installing VirusScan. See "Creating an Emergency Disk" on page 88.*

   Insert the first blank diskette into your 3.5-inch diskette drive and click Continue. When the first diskette is complete, insert the second blank diskette and click OK.

10. Click Yes to review the What's New text file.

11. Review the modifications made to files on your system and click Next.

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

    **Response**: The system restarts. VirusScan is now running.

## Testing your installation

For information on how to use the Eicar Standard AntiVirus Test File to test your installation of VirusScan, see Appendix B, "Testing Your Installation."

# 3

# On-access Scanning

## What is On-access Scanning?

The VirusScan protection strategy has three parts: on-access scanning, on-demand scanning, and scheduled scanning. This chapter covers on-access scanning.

On-access scanning works through a memory-resident program, VShield, which uses a series of VxD (dynamically loaded virtual device driver) modules to provide real-time protection for your system. On-access scanning helps to prevent virus infection by automatically checking items—such as files, directories, drives, and any media—as they are accessed.

In this chapter, you will find procedures for starting and configuring VShield, VirusScan's on-access scanning component.

# Starting VShield

VShield, VirusScan's on-access scanner, is memory resident and, if configured to load at startup, is active in the background when you start up your system. To ensure VShield is active:

- Look at the McAfee VShield icon in the taskbar or in the VirusScan Console. If the icon is crossed-out, VShield is disabled. To enable VShield, right-click the icon and select Enable.

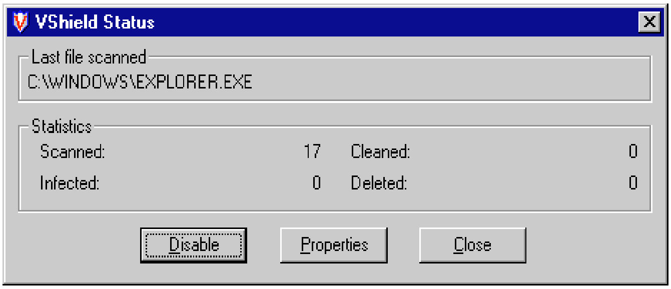
- Run VSHWIN32.EXE, which can be found in the VirusScan installation directory (default: c:\Program Files\McAfee\VirusScan).

By default, VShield is configured to be automatically enabled each time you start Windows. If this configuration has been changed for some reason, you will need to configure VShield to load at startup. For information on how to do this, see below.

## Configuring On-access Scanning

When VShield is enabled, you can configure your scanning options or view the status of files scanned from the VShield Status window (Figure 3-1). To display this window, double-click the VShield icon on the taskbar.

✍ *If VShield is not visible on the taskbar, click Start, point to Programs, point to McAfee VirusScan, and click VirusScan Console. Double-click McAfee VShield in the Description window. Click the Configure button and select the Show Icon on the Taskbar checkbox. VShield options can also be configured directly from this Configuration Manager.*



VShield Status

Last file scanned
C:\WINDOWS\EXPLORER.EXE

Statistics

| | | | |
|---|---|---|---|
| Scanned: | 17 | Cleaned: | 0 |
| Infected: | 0 | Deleted: | 0 |

**Figure 3-1. VShield Status Window**

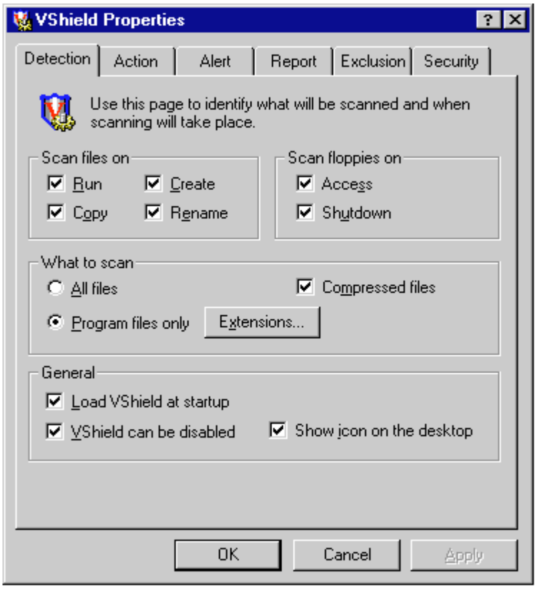
Follow the procedure below to configure on-access scanning.

**Step** **Action**

**1.** Open the VShield Properties window by completing one of the following steps:

- Double-click the Vshield icon and select Properties from the VShield Status window.
- Double-click McAfee VShield in the VirusScan Console. See "Using the VirusScan Console" on page 42 for additional information.
- Run VSHCFG32.EXE, which can be found in the installation directory (default: C:\Program Files\McAfee\VirusScan).

**Response:** The VShield Properties window is displayed, with the Detection property page on top (Figure 3-2).



Use this page to identify what will be scanned and when scanning will take place.

Scan files on
☑ Run ☑ Create
☑ Copy ☑ Rename

Scan floppies on
☑ Access
☑ Shutdown

What to scan
○ All files ☑ Compressed files
● Program files only Extensions...

General
☑ Load VShield at startup
☑ VShield can be disabled ☑ Show icon on the desktop

**Figure 3-2. VShield Properties Window (Detection Property Page)**

## Configuring VShield detection

Use the Detection property page (Figure 3-2) to configure which items should be scanned and when scanning should take place. Take the following steps to configure your detection options:

**Step** **Action**

1. Use the Scan Files On section to select when VShield should scan files. Checked boxes indicate that a scan will be launched when a user attempts to Run, Create, Copy, and/or Rename files.

2. Use the Scan Floppies On section to select when VShield should scan floppy diskettes. A checked box indicates that VShield will scan disks on Access and/or on Shutdown.

   ✍ *McAfee recommends selecting all items in these two sections for maximum protection.*

3. Select what types of files you want VShield to check for viruses.

   - Select All Files if you want VShield to scan all files, no matter what the type.

   - Select Program Files Only to scan only files with certain extensions. To edit which extensions are included in this list, click the Extensions button.

     ✍ *Default extensions are .EXE, .COM, .DO?, and .XL?. The question mark character is a wildcard, so this list will result in a scan that checks Word and Excel document and template (.DOC, .DOT, .XLS, and .XLT) files as well as program files.*

   - Select Compressed Files to scan inside files compressed with PKLITE, LZEXE.

4. Configure your general preferences.

    - Select Load VShield at Startup to activate on-access scanning when you start up your system.

    - Select VShield Can Be Disabled if you want to allow on-access scanning to be disabled.

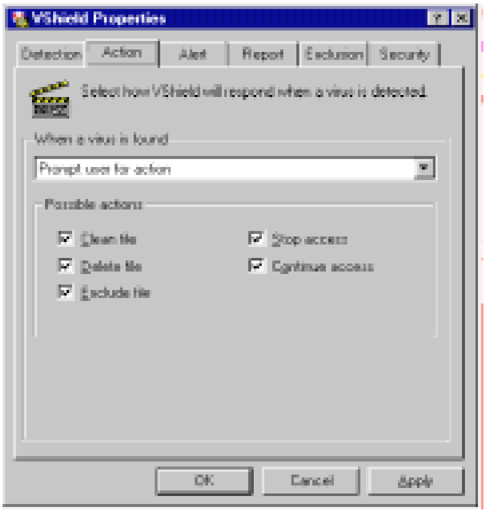
    - Select Show Icon on the Desktop if you want to be able to view the VShield Status window and select VShield properties from a taskbar icon.

    ✍ *McAfee recommends choosing all items. However, if you are a system administrator and want to ensure that VShield remains enabled on your users' systems, do not check the VShield Can Be Disabled and Show Icon on the Desktop boxes when configuring their software. You can also use the Security property page to password protect the VShield settings. See "Configuring VShield security" on page 32, for more information about password protection.*

5. Click Apply to save your changes. To save your changes and exit the VShield Properties window, click OK. To exit the VShield Properties window without saving your changes, click Cancel. To password-protect VShield configuration, see "Configuring VShield security" on page 32.

## Configuring VShield actions

Use the Action property page (Figure 3-3) to select what action VShield should take if a virus is detected.



Select how VShield will respond when a virus is detected.

When a virus is found: Prompt user for action

Possible actions:

☑ Clean file
☑ Delete file
☑ Exclude file
☑ Stop access
☑ Continue access

**Figure 3-3. VShield Properties Window (Action Property Page)**

Take the steps outlined below to configure these settings:

**Step** **Action**

**1.** In When a Virus is Found, select one of the following actions:

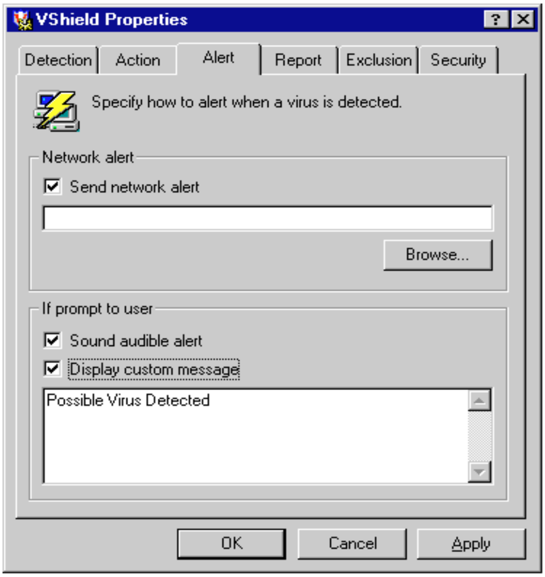
- Prompt User for Action (recommended for attended systems)—if using this option, you must select what options should be given to the user when a virus is found. The possible options are: Clean File, Delete File, Exclude File, Stop Access, and Continue Access.
- Move Infected Files Automatically
  - Specify a path in the Folder To Move To box or choose Browse to locate a folder. This path can be relative. For example, if you type `\Infected` in the text box, an Infected folder will be created on the drive where the infected file was found, and the infected file will be moved there.
  - If an infected file cannot be cleaned or if VShield does not have the proper file access, file access will be denied.

- Clean Infected Files Automatically
- Delete Infected Files Automatically
  - If you select this option, you must restore a clean copy of the deleted file from backups.
- Deny Access to Infected Files and Continue (recommended for systems left unattended)

2. Click Apply to save your changes. To save your changes and exit the VShield Properties window, click OK. To exit the VShield Properties window without saving your changes, click Cancel. To password-protect VShield configuration, see “Configuring VShield security” on page 32.

## Configuring VShield alerts

Use the Alert property page to select how VShield should warn you when a virus is detected.



Specify how to alert when a virus is detected.

Network alert

☑ Send network alert

If prompt to user

☑ Sound audible alert

☑ Display custom message

Possible Virus Detected

**Figure 3-4. VShield Properties Window (Alert Property Page)**

Take the following steps to configure VShield alerting:

**Step** **Action**

**1.** Check Send Network Alert if you want VShield to send an alert to a network path monitored by NetShield, McAfee’s server anti-virus solution. Use the Browse button to navigate to the directory.

✍ *This directory should be one that contains the Centralized Alerting file, CENTALRT.TXT. For more information on Centralized Alerting, see the NetShield documentation.*

**2.** To alert the user, select Sound Audible Alert and/or Display Custom Message.

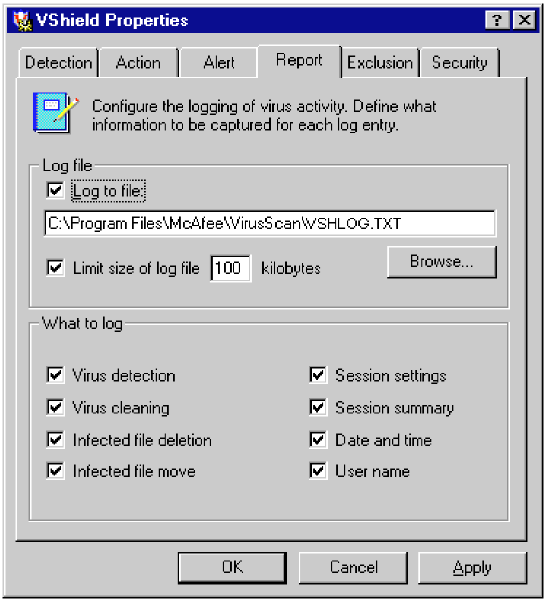
✍ *You can customize the message by simply clicking in the text box and editing the message text.*

**3.** Click Apply to save your changes. To save your changes and exit the VShield Properties window, click OK. To exit the VShield Properties windowVShield Properties window without saving your changes, click Cancel. To password-protect VShield configuration, see “Configuring VShield security” on page 32.

## Configuring VShield reports

Use the Report property page (Figure 3-5) to configure the logging of virus activity and to determine what information will be included in the log entry.

✍ *This log file is a plain text file and can be viewed using any text editor, such as Notepad.*



VShield Properties

Configure the logging of virus activity. Define what information to be captured for each log entry.

Log file

☑ Log to file

C:\Program Files\McAfee\VirusScan\VSHLOG.TXT

☑ Limit size of log file 100 kilobytes

What to log

☑ Virus detection
☑ Virus cleaning
☑ Infected file deletion
☑ Infected file move
☑ Session settings
☑ Session summary
☑ Date and time
☑ User name

**Figure 3-5. VShield Properties Window (Report Property Page)**

Take the steps outlined below to configure report settings.

**Step** **Action**

**1.** Click the Log to File checkbox and enter a path and file in the text box (or choose a path by clicking the Browse button) to enable logging. Limit the size of the log file by selecting the Limit Size checkbox and specifying a size between 10KB and 999KB.

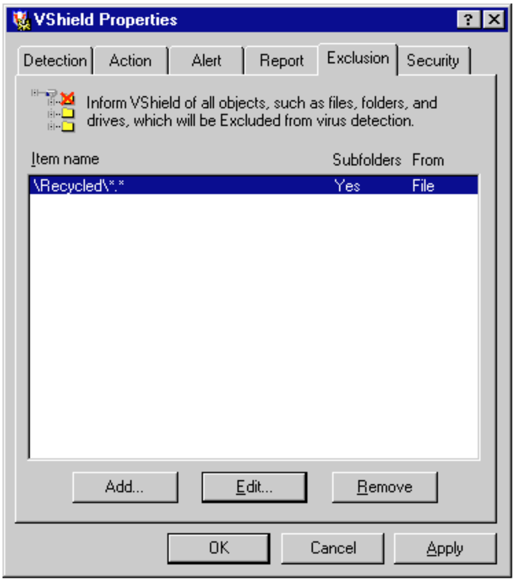
✍ *The default path for the log file is C:\Program Files\McAfee\VirusScan\VSHLOG.TXT. The default maximum log file size is 100KB.*

2. Select from the checkboxes provided to specify what information should be included in the log file. Options include: Virus Detection, Virus Cleaning, Infected File Deletion, Infected File Move, Session Settings, Session Summary, Date and Time, and User Name.

3. Click Apply to save your changes. To save your changes and exit the VShield Properties window, click OK. To exit the VShield Properties window without saving your changes, click Cancel. To password-protect VShield configuration, see "Configuring VShield security" on page 32.

## Configuring VShield exclusions

Use the Exclusion property page (Figure 3-6) to define which items should be excluded from scans.

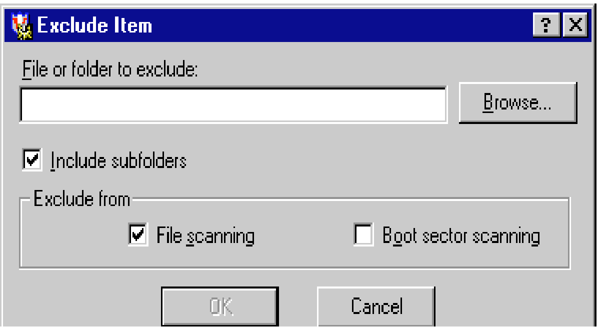


Inform VShield of all objects, such as files, folders, and drives, which will be Excluded from virus detection.

| Item name | Subfolders | From |
|---|---|---|
| \Recycled*.* | Yes | File |

**Figure 3-6. VShield Properties Window (Exclusion Property Page)**

To add an object to the exclusion list, click Add. The Exclude Item dialog box will be displayed (Figure 3-7).



File or folder to exclude:

☑ Include subfolders

Exclude from

☑ File scanning

□ Boot sector scanning

**Figure 3-7. Exclude Item Dialog Box**

Take the following steps to add an item to the Exclusion list:

**Step** **Action**

1. Type the path to the file or folder you wish to exclude from scanning, or click Browse to locate the folder.

   ✍ *The Browse feature only navigates to folders. To exclude files, manually type the filename of the file you want to exclude in the Exclude Item dialog box.*

2. Click Include Subfolders if you want to exclude all subfolders within the selected folder.

3. Indicate whether you want the folder excluded from file scanning or boot sector scanning by placing checkmarks in the boxes provided.

4. Click OK.

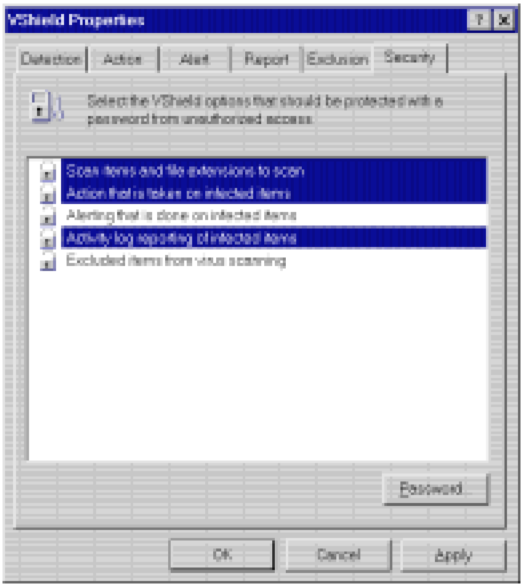
To remove an object from the list, select it and click Remove.

To edit an object on the list, select it and click Edit.

Click Apply to save your changes. To save your changes and exit the VShield Properties window, click OK. To exit the VShield Properties window without saving your changes, click Cancel. To password-protect VShield configuration, see “Configuring VShield security” on page 32.

## Configuring VShield security

Use the Security property page (Figure 3-8) to lock and password-protect settings. This feature is useful if you are a system administrator and you want to keep users from undermining your security program by changing VShield settings.



Select the VShield options that should be protected with a password from unauthorized access.

- Scan items and file extensions to scan
- Action that is taken on infected items
- Alerting that is done on infected items
- Activity log reporting of infected items
- Excluded items from virus scanning

**Figure 3-8. VShield Properties Window (Security Properties Page)**

1. Select items from the list that you want password-protected. Each item corresponds to a property page.

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

3. Click Apply to save your changes. To save your changes and exit the VShield Properties window, click OK. To exit the VShield Properties window without saving your changes, click Cancel.

# 4 On-demand Scanning

## What is On-demand Scanning?

The VirusScan protection strategy has three parts: on-access scanning, on-demand scanning, and scheduled scanning.

Using the on-demand component of VirusScan, you can perform immediate scans of specific items while you're working. VirusScan's on-demand scanner allows you to scan new media or specific files to determine whether a computer virus is present. VirusScan immediately detects known boot, file, macro, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.

On-demand scanning can be configured from either VirusScan's main window or from VirusScan's Advanced configuration window. In this chapter, you'll find procedures for using VirusScan's on-demand component from VirusScan's main window.

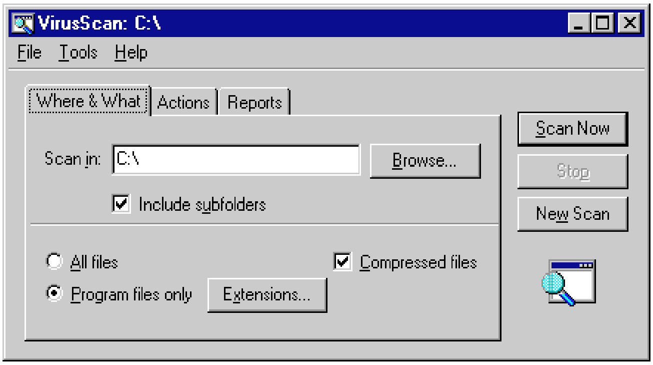
✍ *To configure on-demand scans using the Advanced configuration window, see Chapter 6, "Advanced Settings," for additional instructions.*

# Starting VirusScan

There are two easy methods for starting on-demand scanning in VirusScan:

- Click Start, point to Programs, point to McAfee VirusScan, and click VirusScan.
- Right-click on any drive, folder, or executable or compressed file and select Scan for Viruses.

The VirusScan main window (Figure 4-1) is displayed whenever you start on-demand scanning.



Scan in: C:\

☑ Include subfolders

○ All files

● Program files only

☑ Compressed files

**Figure 4-1. VirusScan Main Window (Where & What Property Page)**

# Configuring On-demand Scanning

To configure an on-demand scan of your system from VirusScan's main window, use the tabbed property pages to specify the desired scan settings.

## Configuring the Where & What property page

Use the Where & What property page to define the scope of a scan.

✍ *The scan settings configured from the Where & What properties page can also be configured from the Detection properties page in the Advanced configuration menu. See "Configuring VirusScan detection" on page 60 for details.*

| Step | Action |
|---|---|
| **1.** | Start VirusScan.<br>**Response**: The main VirusScan window is displayed with the Where & What property page on top. (Figure 4-1 on page 34). |
| **2.** | In the Scan In text box, enter the path of the drive, folder, or individual file you want VirusScan to scan, or choose Browse to navigate to the location. |
| **3.** | To indicate that all subfolders within the selected folder should be scanned, select Include Subfolders. Otherwise, only files located in the selected folder will be scanned. |

4. Do one of the following:

- To scan all file types, click the All Files button.
- To scan only executable and Microsoft Word files, select Program Files Only.

  ✍ *If you select Program Files Only, you can click the Extensions button to edit the types of files VirusScan will examine. The default settings are .COM, .DO?, XL?, and .EXE. When the DO? and XL? extensions are selected, VirusScan scans Microsoft Word and Microsoft Excel documents and templates for macro viruses.*

- To scan files compressed with PKZIP, PKLITE, LHA, WinZip, and LZEXE, select Compressed Files.

5. If you want to save these selections in a settings file, see "Saving scan settings" on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan Now.

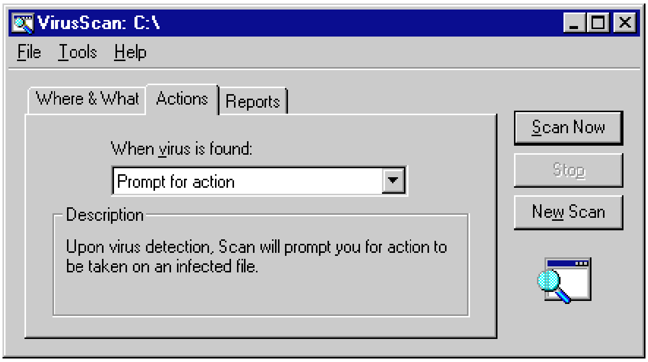
## Configuring VirusScan actions from the main window

The Actions property page is used to define VirusScan's response when a virus is detected.

✍ *VirusScan's Actions settings and additional Action settings can be configured from the Action properties page in the Advanced configuration menu. See "Configuring Advanced Action settings" on page 63 for details.*

| Step | Action |
|---|---|
| 1. | Start VirusScan and select the Actions property page. |

**Response**: The main VirusScan window is displayed with the Actions property page showing (Figure 4-2 on page 37).



When virus is found: Prompt for action

Description

Upon virus detection, Scan will prompt you for action to be taken on an infected file.

**Figure 4-2. VirusScan Main Window (Actions Property Page)**

2. Select an action for VirusScan to take if a virus is found. Options are:

   - Continue Scanning
   - Prompt for Action
   - Move Infected Files to a Folder
   - Clean Infected File
   - Delete Infected File

   A description for each action is displayed when the action is selected. For additional information on these options and virus removal, see Chapter 8, “Removing a Virus.”

3. If you want to save these selections in a settings file, see “Saving scan settings” on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan Now.

## Configuring report settings from the main window

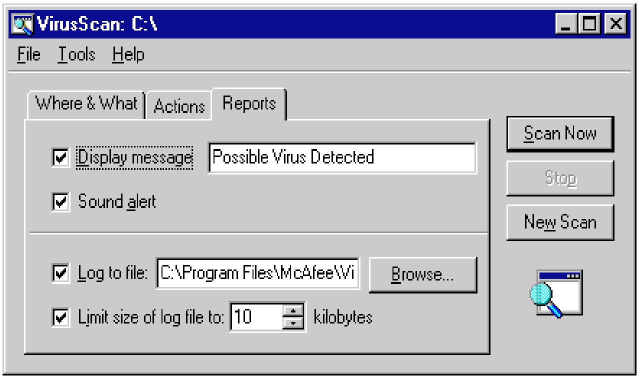
The Reports property page is used to determine VirusScan’s notification, reporting, and logging options. To configure VirusScan’s Reports page, follow the steps below:

✍ *VirusScan’s Reports settings and additional Reports settings can be configured from the Report properties page in the Advanced configuration menu. See “Configuring advanced report settings” on page 66 for details.*

**Step** **Action**

**1.** Start VirusScan and select the Reports property page.

**Response**: The main VirusScan window is displayed with the Reports property page showing (Figure 4-3).



☑ Display message: Possible Virus Detected
☑ Sound alert
☑ Log to file: C:\Program Files\McAfee\Vi
☑ Limit size of log file to: 10 kilobytes

**Figure 4-3. VirusScan Main Window (Reports Property Page)**

**2.** To enter a custom message, click Display Message. If you selected Prompt for Action from the Actions property page, VirusScan can display a custom message to alert users or administrators that a virus was detected.

✍ *You can use this function to add a customized message that will help users better respond to a virus. For example, you can direct users to a virus response center, technical support, or a specific person. To add a longer message, use the Alert property page in the Advanced configuration window. See “Using the Advanced configuration window” on page 59 for more information.*

3. To sound an alert when a virus is detected, click the Sound Alert checkbox.

4. To create a record of your scanning activity, select Log to File. VirusScan will automatically record its activity in the default location, C:\Program Files\McAfee\VirusScan\VSCLOG.TXT. To select another location, enter the path of the drive or folder or click Browse to navigate to the location. Your selection will appear in the Log to File text box.

5. To limit the size of the log file, select Limit Size of Log File and enter the maximum log file size (10KB to 999KB).

   ✍ *The default activity log size is 100KB.*

6. If you want to save these selections in a settings file, see "Saving scan settings" on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan Now.

# Saving scan settings

Save your VirusScan settings by selecting the Save Settings option in the File menu. Your VirusScan settings will be saved in .VSC file format.

If you have made changes to the VirusScan configuration that you want to make the default settings, choose Save as Default. Your changes will be saved to the DEFAULT.VSC file. When Save Settings is selected, the settings are saved in Scan for Viruses.VSC.

The .VSC file is a configuration text file, formatted similarly to the WIN.INI file, which outlines VirusScan's settings. Each variable in the file has a name followed by the equal (=) sign and a value. The values define which settings have been selected for VirusScan configuration.

If you have circumstances that require more than one configuration of VirusScan, save the current VirusScan settings to a separate .VSC file. You will be asked to provide a name for the new file. Once the new settings have been saved, you can run them by double-clicking the .VSC file.

# Using the VirusScan Activity Log

The VirusScan Activity Log keeps track of the dates and times you scan your system, as well as associated messages regarding the items scanned and infections found. To view the Activity Log, simply select View Activity Log from the File menu of the VirusScan Main or Advanced configuration window.

✍ *For instructions on using the Advanced configuration window, see Chapter 6, “Advanced Settings.”*

# 5 Scheduled Scanning

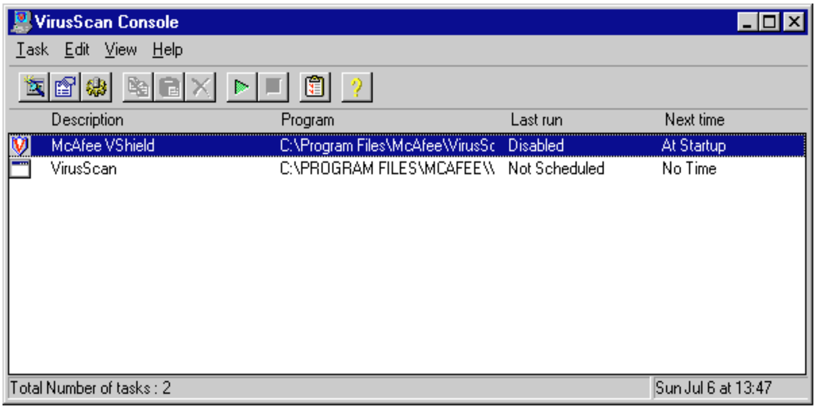
## Using the VirusScan Console

The VirusScan protection strategy has three parts: on-demand scanning, on-access scanning, and scheduled scanning.

Scheduled scanning allows you to configure VirusScan to automatically start a scan at a predetermined time. This can happen once, daily, weekly, monthly, or even hourly.

Use the VirusScan Console to configure scheduled scanning. You can start the VirusScan Console in either of the following ways:

- In the Start menu, point to Programs. Point to McAfee VirusScan and select VirusScan Console.
- From VirusScan's Advanced configuration window, select AV Console from the Tools menu.



| Description | Program | Last run | Next time |
|---|---|---|---|
| McAfee VShield | C:\Program Files\McAfee\VirusSc | Disabled | At Startup |
| VirusScan | C:\PROGRAM FILES\MCAFEE\\ | Not Scheduled | No Time |

Total Number of tasks : 2

Sun Jul 6 at 13:47

**Figure 5-1. VirusScan Console**

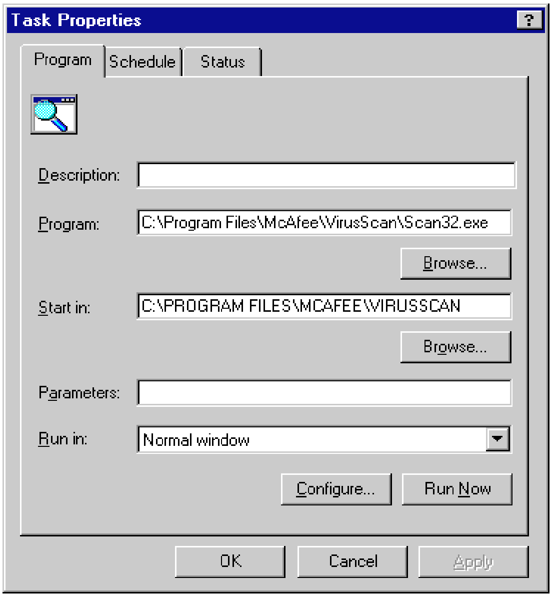
# Scheduling a scan

The VirusScan Console uses scan tasks to track scheduled scanning. Each task can be scheduled and configured separately. Complete the following procedure to create a new scan task.

**Step** **Action**

**1.** Select New Task from the Task menu or right-click on the task list and select New Task.

**Response**: The Task Properties window (Figure 5-2) is displayed with the Program property page on top.



Description:

Program: C:\Program Files\McAfee\VirusScan\Scan32.exe

Start in: C:\PROGRAM FILES\MCAFEE\VIRUSSCAN

Parameters:

Run in: Normal window

**Figure 5-2. Task Properties (Program Property Page)**

**2.** Specify the location of the VirusScan program file.

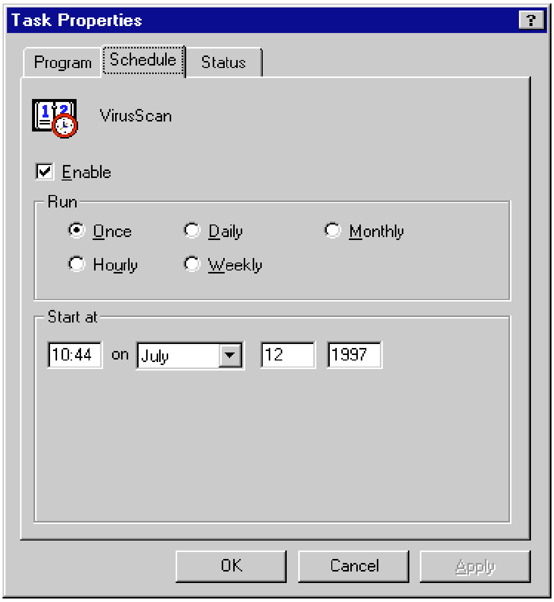
✍ *The default location is C:\Program Files\McAfee\VirusScan\Scan32.exe. It should appear in the Program field automatically. If you want to use the VirusScan Console to schedule another program, enter its path in the Program field instead.*

3. Specify the name of the task in the Description field.

4. Configure the scanning options for the task. To do this, see "Configuring a scan task" on page 47.

5. Move to the next property page by clicking the Schedule tab.

   **Response**: The Task Properties window is displayed with the Schedule property page on top (Figure 5-3).



Task Properties

VirusScan

☑ Enable

Run

● Once ○ Daily ○ Monthly

○ Hourly ○ Weekly

Start at

10:44 on July 12 1997

**Figure 5-3. Task Properties Window (Schedule Property Page)**

6. Use the Schedule page to do the following:

   - Enable or disable the task.

     ✍ *If the task is not enabled, it will not be run on schedule.*

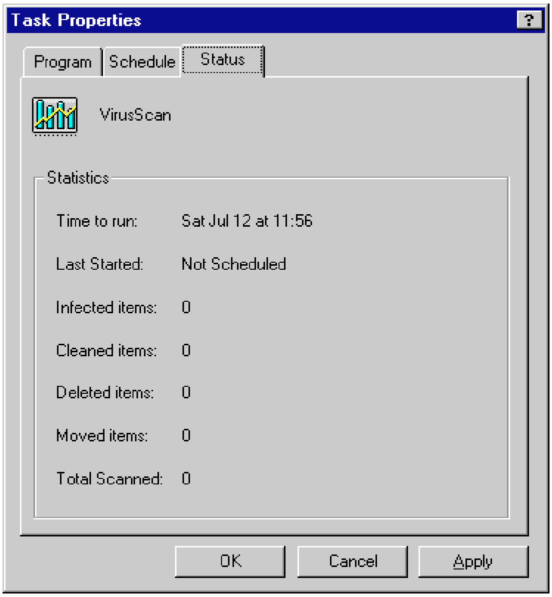
   - Specify the frequency of the scan:

     - ❑ If you select Once, you will need to specify the time and date for the task.
     - ❑ If you select Daily, you will need to select which days of the week the task should run on, as well as the time at which it should run.
     - ❑ If you select Monthly, you will need to select the day of the month on which the task should run and the time at which it should run.
     - ❑ If you select Hourly, you will need to select at how many minutes after the hour the task should run.
     - ❑ If you select weekly, you will need to select on which days the task should run and at what time it should run.

     ✍ *The time must be entered in 24-hour format (i.e. 20:27, not 8:27 p.m.) for all options except Hourly.*

7. Move to the next property page by clicking the Status tab.

**Response**: The Task Properties window is displayed with the Status property page on top (Figure 5-4).



VirusScan

Statistics

Time to run: Sat Jul 12 at 11:56

Last Started: Not Scheduled

Infected items: 0

Cleaned items: 0

Deleted items: 0

Moved items: 0

Total Scanned: 0

**Figure 5-4. Task Properties Window (Status Property Page)**

8. Use the Status property page to view statistics on the task.

9. Click OK to exit the Task Properties window and return to the VirusScan Console.

## Copying, pasting, or deleting a scan task

Tasks can be copied from or pasted to the VirusScan Console task list. This makes creating several tasks with similar configurations quick and easy.

- To copy a task, highlight an existing VirusScan task and select Copy from the Edit menu.
- To paste a task, select Paste from the Edit menu.

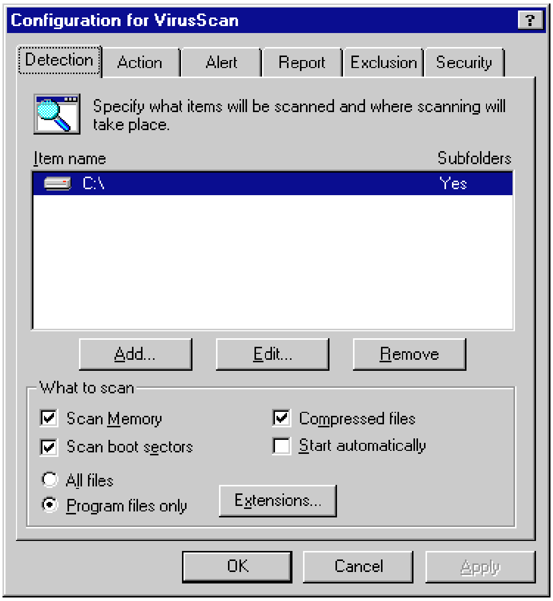
# Configuring a scan task

To configure where and what you want VirusScan to scan for infection, complete the following procedure:

**Step** **Action**

1. From the VirusScan Console, highlight a task and select Properties from the Task menu.

   **Response**: The Scan Configuration window is displayed with the Detection property page on top (Figure 5-5).


Configuration for VirusScan

Specify what items will be scanned and where scanning will take place.

| Item name | Subfolders |
|---|---|
| C:\ | Yes |

What to scan

☑ Scan Memory
☑ Compressed files
☑ Scan boot sectors
□ Start automatically
○ All files
● Program files only

**Figure 5-5. Scan Configuration Window (Detection Property Page)**

2. The Scan Configuration window is organized in six property pages. To move from one to another, click the tabs at the top of the window. The following sections describe each page in detail.

## Using the Detection property page

Complete the following steps to configure the detection options for a scan:

**Step** **Action**

**1.** Select the Detection property page.

**Response**: The Detection property page is displayed (Figure 5-5 on page 47).

**2.** Do one of the following:

- To add an item to the scan list, click Add. Select the item from the Select Item to Scan pull-down list. You can choose from:
  - ❑ My Computer—select this if you want to scan all fixed, removable, and network volumes connected to your computer.
  - ❑ All Removable Media—select this if you want to scan all local removable media such as floppy disks.
  - ❑ All Fixed Disks—select this if you want to scan all local hard drives.
  - ❑ All Network Drives—select this if you want to scan all mapped network volumes.

    ✍ *All directories and subdirectories on the location you select will be scanned.*

- To add a specific drive or folder, click the Select Drive or Folder to Scan option button and specify the path to the item you want to scan.

  ✍ *You may use the Browse button to navigate to the file, drive, or folder.*

**3.** Click OK.

**Response**: The items you selected appear in the Selections list.

**4.** To remove an item from the list to be scanned, select it from the list and click Remove.

5. Select what types of files you want VirusScan to check for viruses.

    - Select All Files if you want VirusScan to scan all files, no matter what the type. This will result in a more thorough, but slower, scan.

    - Select Program Files Only to scan only files with certain extensions. To edit which extensions are included in this list, click the Extensions button.

        ✍ *Default extensions are .EXE, .COM, .DO?, and .XL?. The question mark character is a wildcard, so this list will result in a scan that checks Word and Excel document and template (.DOC, .DOT, .XLS, and .XLT) files as well as program files.*

    - Select Compressed Files to scan inside files compressed with PKLITE, PKZip, LZEXE, WinZip, or LHA.

6. Select Scan Memory if you want to scan your computer's memory for viruses.

7. Select Start Automatically if you want the task to start automatically at a scheduled time. If you do not select Start Automatically, VirusScan will be launched at the scheduled time, but it will not complete the task until you click the Scan Now button.

8. Select Scan Boot Sectors if you want to scan the boot sector(s) of the drive(s) specified in this task.

9. Click Apply to save your changes. To save your changes and exit Scan Configuration, click OK. To exit Scan Configuration without saving your changes, click Cancel. To lock and password-protect these changes, see "Using the Security property page" on page 57.

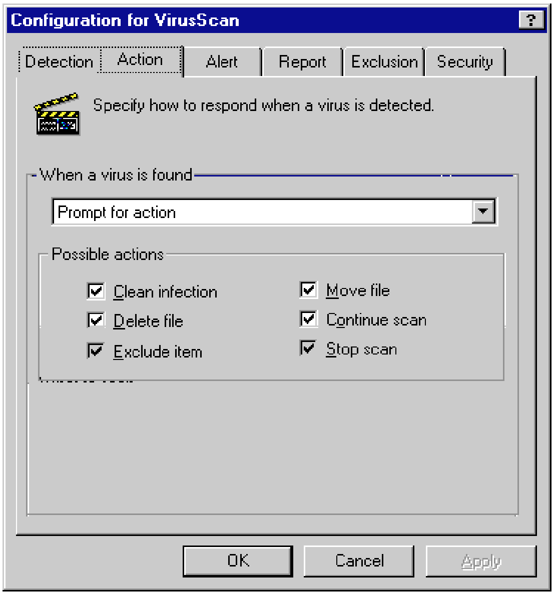
## Using the Action property page

Complete the following steps to configure the action options for a scan:

**Step** **Action**

**1.** Select the Action property page.

**Response**: The Scan Configuration window is displayed with the Action property page on top (Figure 5-6).



Specify how to respond when a virus is detected.

When a virus is found: Prompt for action

Possible actions

- ☑ Clean infection
- ☑ Delete file
- ☑ Exclude item
- ☑ Move file
- ☑ Continue scan
- ☑ Stop scan

**Figure 5-6. Scan Configuration Window (Action Property Page)**

2. Select an action from the pull-down list:

   - Prompt for Action—use this if the computer will be attended when the scan is running. VirusScan will ask the user what to do with each virus as it is found.

     ✍ *Customize which actions you want available to the user by clicking the appropriate checkboxes under Possible Actions.*

   - Move Infected Files to a Directory—select this option if you want VirusScan to automatically move all infected files to a quarantine directory.

     ✍ *You will need to specify a directory to which you want the files moved. The default directory is \Infected. Unless you specify the entire path (i.e. C:\Mystuff\Infected), VirusScan will create the directory at the root of the drive on which the virus was found (i.e. C:\Infected).*

   - Clean Infected File—use this option to have VirusScan automatically clean viruses from infected files.

   - Delete Infected File—select this option if you want VirusScan to automatically delete infected files it finds.

     ✍ *This will permanently remove the infected files from your system. You will have to restore deleted files from backups.*

   - Continue Scanning—use this option only if you want to ignore infected files and continue scanning. VirusScan will not take any action when it detects a virus.

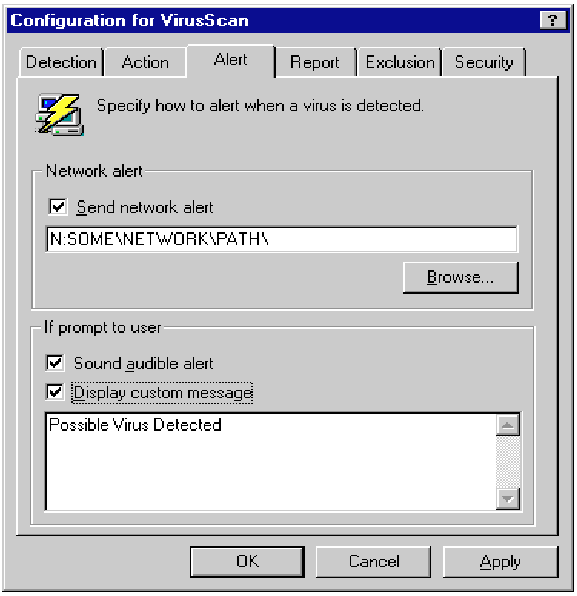
3. Click Apply to save your changes. To save your changes and exit Scan Configuration, click OK. To exit Scan Configuration without saving your changes, click Cancel. To lock and password-protect these changes, see “Using the Security property page” on page 57.

## Using the Alert property page

Complete the following steps to configure the alert options for a scan:

| Step | Action |
|---|---|
| 1. | Select the Alert property page. |

**Response**: The Scan Configuration window is displayed with the Alert property page on top (Figure 5-7 on page 52).


Configuration for VirusScan

Specify how to alert when a virus is detected.

Network alert

☑ Send network alert

N:SOME\NETWORK\PATH\

If prompt to user

☑ Sound audible alert

☑ Display custom message

Possible Virus Detected

**Figure 5-7. Scan Configuration Window (Alert Property Page)**

2. If you want VirusScan to send a Network alert to a server running NetShield, McAfee’s server anti-virus solution, check the Send Network Alert box and specify the path to the alert file.

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

3. If you have selected Prompt for Action on the Action property page, use the If Prompt for Action is Selected section of this page to specify how VirusScan should alert the user.

   - Check the appropriate boxes to configure VirusScan to sound an audible alert and/or display a custom message.

     ✍ *You can edit the custom message to be displayed by typing in the text box.*

4. Click Apply to save your changes. To save your changes and exit Scan Configuration, click OK. To exit Scan Configuration without saving your changes, click Cancel. To lock and password-protect these changes, see “Using the Security property page” on page 57.

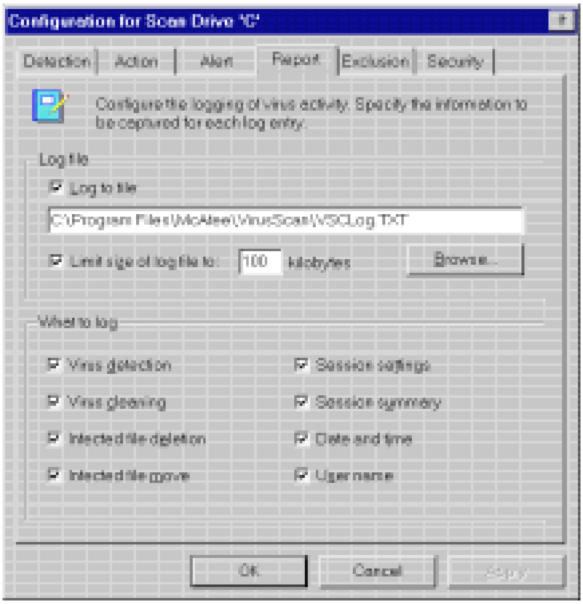
## Using the Report property page

Complete the following steps to configure the reporting options for a scan:

**Step** **Action**

1. Select the Report property page.

   **Response**: The Scan Configuration window is displayed with the Report property page on top (Figure 5-8).



Configure the logging of virus activity. Specify the information to be captured for each log entry.

Log file

☑ Log to file

C:\Program Files\McAfee\VirusScan\VSCLog.TXT

☑ Limit size of log file to: 100 kilobytes

What to log

☑ Virus detection
☑ Virus cleaning
☑ Infected file deletion
☑ Infected file move
☑ Session settings
☑ Session summary
☑ Date and time
☑ User name

**Figure 5-8. Scan Configuration Window (Report Property Page)**

2. To enable logging of scan activity, click the Log to File checkbox and enter the path to a text file.

   ✍ *The default path is C:\Program Files\McAfee\VirusScan\VSClog.TXT. This is a plain text file and can be viewed with any text editor, such as Notepad, as well as by selecting View Activity Log from the File menu.*

3. If you want to limit the size of the log file, click the Limit Size of Log File checkbox and enter a maximum size.

4. Select from the checkboxes provided to specify what information should be included in the log file. The options available are Virus Detection, Virus Cleaning, Infected File Deletion, Infected File Move, Session Settings, Session Summary, Date and Time, and User Name.

5. Click Apply to save your changes. To save your changes and exit Scan Configuration, click OK. To exit Scan Configuration without saving your changes, click Cancel. To lock and password-protect these changes, see “Using the Security property page” on page 57.

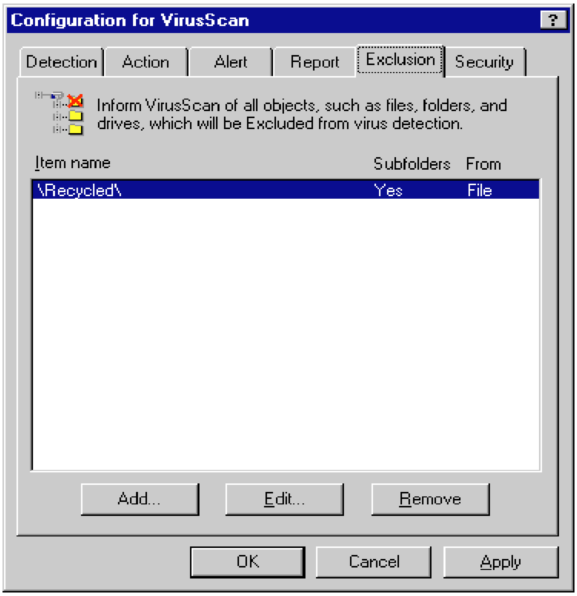
## Using the Exclusion property page

Complete the following steps to configure the exclusion options for a scan:

**Step** **Action**

1. Select the Exclusion property page.

   **Response**: The Scan Configuration window is displayed with the Exclusion property page on top (Figure 5-9 on page 55).



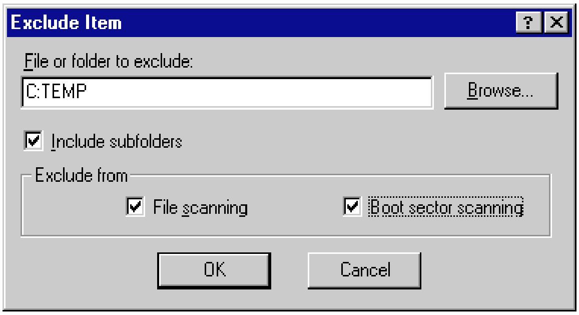
Inform VirusScan of all objects, such as files, folders, and drives, which will be Excluded from virus detection.

| Item name | Subfolders | From |
|---|---|---|
| \Recycled\ | Yes | File |

**Figure 5-9. Scan Configuration Window (Exclusion Property Page)**

2. To add an item to the exclusion list, click Add.

**Response**: The Exclude Item dialog box is displayed (Figure 5-10 on page 56).



Exclude Item

File or folder to exclude: C:TEMP

☑ Include subfolders

Exclude from

☑ File scanning ☑ Boot sector scanning

**Figure 5-10. Exclude Item Dialog Box**

3. Enter the path to the item you want to exclude or click Browse to navigate to the item. You may exclude a file, a folder, or an entire disk.

   ✍ *The Browse feature only navigates to folders. To exclude files, manually type the filename of the file you want to exclude in the Exclude Item dialog box.*

4. If you do not want VirusScan to scan inside subfolders of the folder you have excluded, select Include Subfolders.

5. Select what type(s) of scanning you want to exclude this item from:

   - To exclude the item from file scanning, click File Scanning

   - To exclude the item from boot sector scanning, select Boot Sector Scanning.

6. To add this item to the exclusion list with these settings, click OK. To go back to the VirusScan main window without adding this item, click Cancel.

7. To edit an existing exclusion list item, select the item and click Edit. The Exclude Item dialog box (Figure 5-10) will be displayed. When you have made your changes, click OK.

8. To remove an existing exclusion list item, select the item and click Remove. The item will be removed from the list.

9. Click Apply to save your changes. To save your changes and exit Scan Configuration, click OK. To exit Scan Configuration without saving your changes, click Cancel. To lock and password-protect these changes, see "Using the Security property page" on page 57.

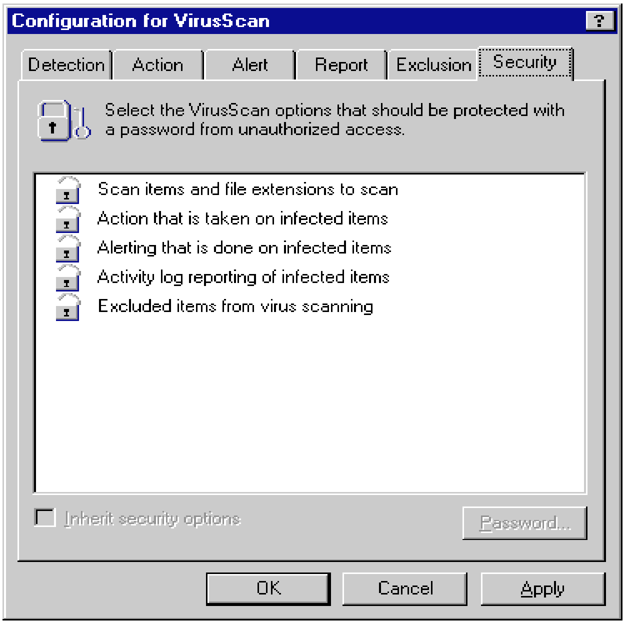
## Using the Security property page

Complete the following steps to configure the security options for a scan:

**Step** **Action**

1. Select the Security property page.

   **Response**: The Scan Configuration window is displayed with the Security property page on top (Figure 5-11).



Select the VirusScan options that should be protected with a password from unauthorized access.

- Scan items and file extensions to scan
- Action that is taken on infected items
- Alerting that is done on infected items
- Activity log reporting of infected items
- Excluded items from virus scanning

□ Inherit security options

**Figure 5-11. Scan Configuration Window (Security Property Page)**

2. Select which of VirusScan’s settings you want password protected:

   - Scan Items and File Extensions to Scan
   - Action That is Taken on Infected Items
   - Alerting That is Done on Infected Items
   - Activity Log Reporting of Infected Items
   - Excluded Items from Virus Scanning

   ✍ *Settings that are password protected will be highlighted in the list, and the lock to their left will appear closed.*

3. Select the Inherit Security Options checkbox if you want the options you have selected to be in place by default on copies of this task.

   ✍ *If you select the Inherit Security Options checkbox on the main VirusScan task, the security options for that task will be inherited for all new tasks as well as for copies of that task.*

4. If you have not already set a password, set one by clicking the Password button. You will be prompted to enter and confirm your password.

   If you have set a password already, you may change it at any time by clicking the Password button. You will be prompted to enter and confirm your new password.

5. Click Apply to save your changes. To save your changes and exit Scan Configuration, click OK. To exit Scan Configuration without saving your changes, click Cancel.

# 6 Advanced Settings

## Using the Advanced configuration window

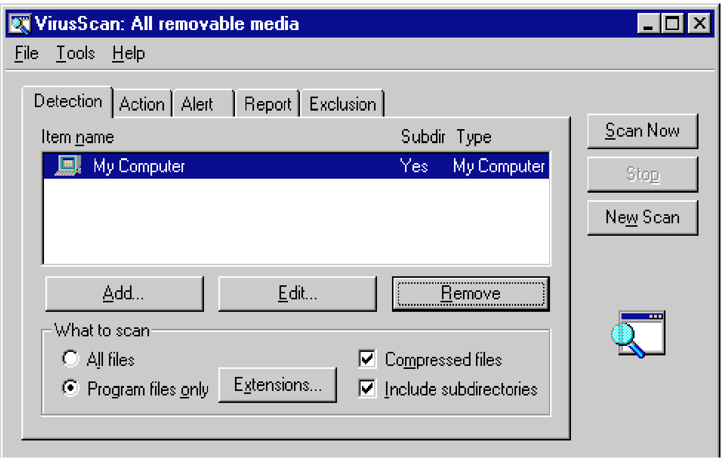
The Advanced configuration window provides additional scan, report, and alert settings. From this configuration window, you can create or modify VirusScan’s detection, action, and report settings, as well as configure network alerting and create a scan exclusions list.

The configurable features of VirusScan are accessible through five property pages. The following sections explain how to use these property pages to configure VirusScan to suit your needs.

### Accessing the Advanced configuration window

To acces the Advanced configuration window, take the following steps:

| **Step** | **Action** |
|---|---|
| **1.** | Start VirusScan.<br>**Response**: The McAfee VirusScan main window is displayed. |
| **2.** | Select Advanced from the Tools menu.<br>**Response**: The Advanced configuration window is displayed with the Detection property page on top (Figure 6-1). |



| Item name | Subdir | Type |
|---|---|---|
| My Computer | Yes | My Computer |

What to scan

○ All files

● Program files only

☑ Compressed files

☑ Include subdirectories

**Figure 6-1. Advanced Configuration Window (Detection Property Page)**

## Configuring VirusScan detection

Use the Detection property page (Figure 6-1) to configure which items should be scanned. Take the following steps to configure your detection options:

*You can also use the Where & What properties page in the main window to specify what items should be included in the scan. See "Configuring the Where & What property page" on page 35 for instructions.*

1. Select where to scan for viruses. The C: drive is selected by default.

2. To add an item to the list, click Add.

   **Response**: The Add Scan Item dialog box (Figure 6-2) is displayed.

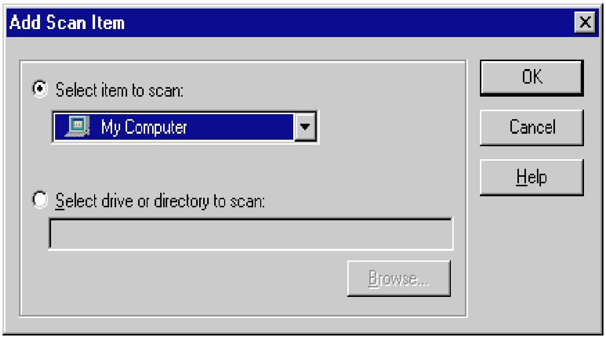


**Figure 6-2. Add Scan Item Dialog Box**

3. Do one of the following:

   - To add an item to the scan list, select it from the Select Item to Scan pull-down list. You can choose from:

     - My Computer—select this if you want to scan all fixed, removable, and network volumes connected to your computer.
     - All Removable Media—select this if you want to scan all local removable media, such as floppy disks.
     - All Fixed Disks—select this if you want to scan all local hard drives.
     - All Network Drives—select this if you want to scan all mapped network volumes.

       ✍ *All directories and subdirectories on the location you select will be scanned.*

   - To add a specific drive, file, or folder, click the Select Drive or Directory to Scan option button and specify the path to the item you want to scan.

     ✍ *You may use the Browse button to navigate to the file, drive, or folder.*

4. Click OK.

   **Response**: The items you selected appear in the Selections list.

5. To remove an item from the list to be scanned, select it from the list and click Remove.

6. Select what types of files you want VirusScan to check for viruses.

   - Select All Files if you want VirusScan to scan all files, no matter what the type. This will result in a more thorough, but slower, scan.

   - Select Program Files Only to scan only files with certain extensions. To edit which extensions are included in this list, click the Extensions button.

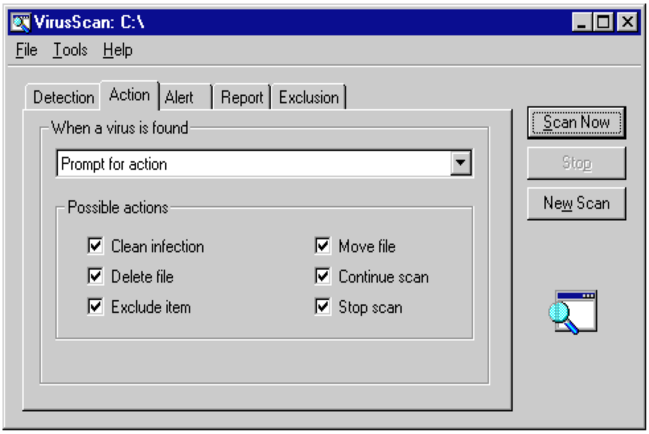
     ✍ *Default extensions are .EXE, .COM, .DO?, and .XL?. The question mark character is a wildcard, so this list will result in a scan that checks Word and Excel document and template (.DOC, .DOT, .XLS, and .XLT) files as well as program files.*

   - Select Compressed Files to scan inside files compressed with PKLITE, PKZip, LZEXE, LHA, and WinZip.

7. If you want to save these selections in a settings file, see "Saving scan settings" on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan Now.

## Configuring Advanced Action settings

Use the Action property page (Figure 6-3) to select what actions VirusScan should take if a virus is detected.



When a virus is found

Prompt for action

Possible actions

☑ Clean infection ☑ Move file

☑ Delete file ☑ Continue scan

☑ Exclude item ☑ Stop scan

**Figure 6-3. Advanced Configuration Window (Action Property Page)**

Complete the following steps to configure these settings:

**Step** **Action**

**1.** Select an action from the pull-down list:

- Prompt for Action—use this if the computer will be attended when the scan is running. VirusScan will ask the user what to do with each virus as it is found.

  ✍ *Customize which actions you want to make available to the user by clicking the appropriate checkboxes under Possible Actions.*

- Move Infected Files to a Directory—choose this option if you want VirusScan to automatically move all infected files to a quarantine directory.

  ✍ *You will need to specify a directory to which you want the files moved. The default directory is \Infected. Unless you specify the entire path (i.e. C:\Mystuff\Infected), VirusScan will create the directory at the root of the drive on which the virus was found (i.e. C:\Infected).*

- Clean Infected File—use this option to have VirusScan automatically clean viruses from infected files.

- Delete Infected File—choose this option if you want VirusScan to automatically delete infected files it finds.

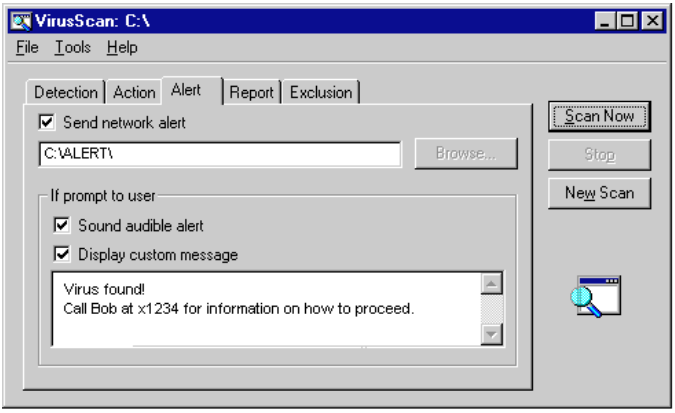
  ✍ *This will permanently remove the infected files from your system. You will have to restore deleted files from backups.*

- Continue Scanning—use this option only if you want to ignore infected files and continue scanning. VirusScan will not take any action when it detects a virus.

2. If you want to save these selections in a settings file, see “Saving scan settings” on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan.

# Configuring alert settings

VirusScan can be configured to send an alert when it detects a virus infection. Use the Alert property page (Figure 6-4) to configure VirusScan's alerting features.



☑ Send network alert

C:\ALERT\

If prompt to user

☑ Sound audible alert

☑ Display custom message

Virus found!
Call Bob at x1234 for information on how to proceed.

**Figure 6-4. Advanced Configuration Window (Alert Property Page)**

**Step** **Action**

**1.** If you want VirusScan to send a Network alert to a computer running NetShield, check the Send Network Alert box and specify the path to the alert file.

✍ *This directory should be one that contains the Centralized Alerting file, CENTALRT.TXT. For more information on Centralized Alerting, see the NetShield documentation.*

**2.** If you have selected Prompt for Action on the Action property page, use the If Prompt for Action is Selected section of this page to specify how VirusScan should get the user's attention.

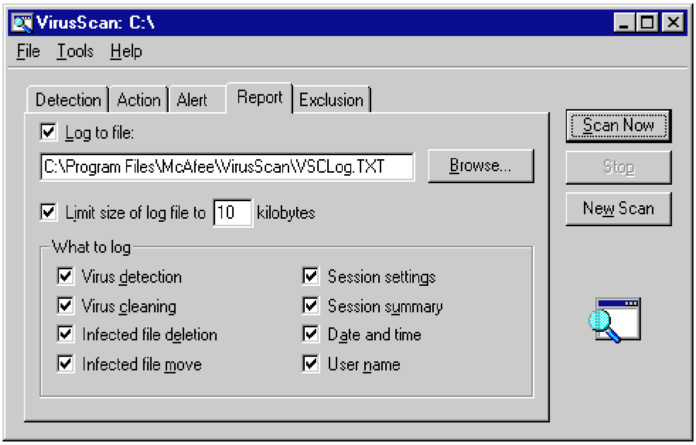
- Check the appropriate boxes to configure VirusScan to sound an audible alert and/or display a custom message.

  ✍ *You can edit the custom message to be displayed by typing in the text box.*

**3.** If you want to save these selections in a settings file, see "Saving scan settings" on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan.

# Configuring advanced report settings

Use the Report property page (Figure 6-5) to configure the logging of virus activity and to determine what information will be included in the log entry.



☑ Log to file:

C:\Program Files\McAfee\VirusScan\VSCLog.TXT

☑ Limit size of log file to 10 kilobytes

What to log

| | |
|---|---|
| ☑ Virus detection | ☑ Session settings |
| ☑ Virus cleaning | ☑ Session summary |
| ☑ Infected file deletion | ☑ Date and time |
| ☑ Infected file move | ☑ User name |

**Figure 6-5. Advanced Configuration Window (Report Property Page)**

1. To enable logging of scan activity, click the Log to File checkbox and enter the path to a text file.

   ✍ *The default path is C:\Program Files\McAfee\VirusScan\VSClog.TXT. This is a plain text file and can be viewed with any text editor, such as Notepad, as well as by selecting View Activity Log from the File menu.*

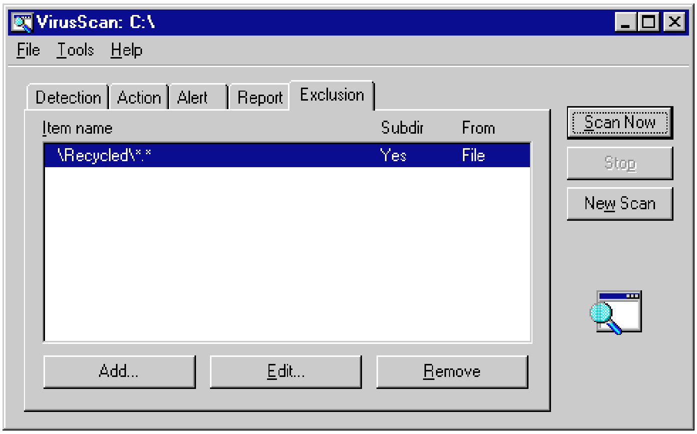
2. If you want to limit the size of the log file, click the Limit Size of Log File checkbox and enter a maximum size.

3. Select from the checkboxes provided to specify what information should be included in the log file. The options available are Virus Detection, Virus Cleaning, Infected File Deletion, Infected File Move, Session Settings, Session Summary, Date and Time, and User Name.

4. If you want to save these selections in a settings file, see "Saving scan settings" on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan.

## Configuring exclusion settings

Use the Exclusion property page (Figure 6-6) to define which items should be excluded from scans.

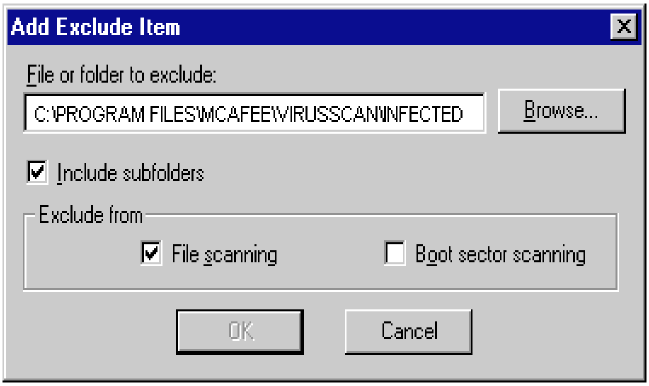


| Item name | Subdir | From |
|---|---|---|
| \Recycled*.* | Yes | File |

**Figure 6-6. Advanced Configuration Window (Exclusion Property Page)**

1. To add an item to the exclusion list, click Add.

   **Response**: The Exclude Item dialog box is displayed (Figure 6-7).



File or folder to exclude: C:\PROGRAM FILES\MCAFEE\VIRUSSCAN\INFECTED

☑ Include subfolders

Exclude from

☑ File scanning
□ Boot sector scanning

**Figure 6-7. Exclude Item Dialog Box**

2. Enter the path to the item you want to exclude or click Browse to navigate to the item. You may exclude a file, a folder, or an entire disk.

   ✍ *The Browse feature only navigates to folders. To exclude files, manually type the filename of the file you want to exclude in the Exclude Item dialog box.*

3. If you do not want VirusScan to scan inside subfolders of the folder you have excluded, select Include Subfolders.

4. Select what type(s) of scanning you want to exclude this item from:

   - To exclude the item from file scanning, click File Scanning

   - To exclude the item from boot sector scanning, select Boot Sector Scanning.

5. To add this item to the exclusion list with these settings, click OK. To go back to the VirusScan main window without adding this item, click Cancel.

To edit an existing exclusion list item, select the item and click Edit. The Exclude Item dialog box (Figure 6-7) will be displayed. When you have made your changes, click OK.

To remove an existing exclusion list item, select the item and click Remove. The item will be removed from the list.

If you want to save these selections in a settings file, see “Saving scan settings” on page 40. To further configure VirusScan, select another property page. To scan now with the current settings, click Scan Now.

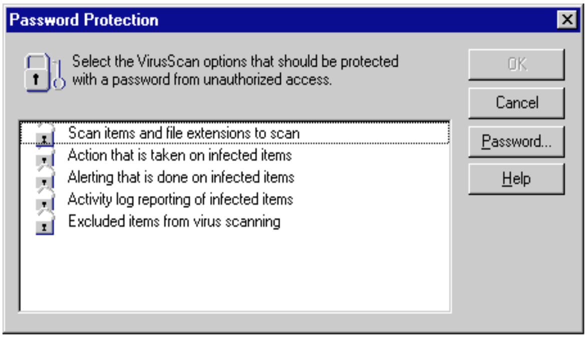
# Using the Advanced Tools menu

From the Advanced Tools menu, you can password-protect scan configurations, access the Virus List, and start the VirusScan Console. The following sections provide instructions on using and configuring these features to suit your needs.

## Password Protecting scan settings

VirusScan settings can be password-protected to prevent unintentional changes from being made. To use password protection, complete the following procedure:

| Step | Action |
|---|---|
| 1. | Start VirusScan.<br>**Response**: The McAfee VirusScan main window is displayed. |
| 2. | Select Advanced from the Tools menu.<br>**Response**: The Advanced configuration window is displayed. |
| 3. | From the Tools menu, select Password Protect.<br>**Response**: The Password Protection dialog box is displayed (Figure 6-8). |



Password Protection

Select the VirusScan options that should be protected with a password from unauthorized access.

- Scan items and file extensions to scan
- Action that is taken on infected items
- Alerting that is done on infected items
- Activity log reporting of infected items
- Excluded items from virus scanning

**Figure 6-8. Password Protection Dialog Box**

4. Select items from the list that you want to be password-protected.

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

6. To return to VirusScan with these settings, click OK. To Cancel your changes and return to VirusScan, click Cancel.

## Returning to VirusScan's main window

To return to the VirusScan Classic or Main window, select Classic from the Advanced Tools menu. See Chapter 4, "On-demand Scanning," for detailed instructions on using VirusScan's Main window.

## Displaying the Virus List

The Virus List is a comprehensive list of viruses detected by VirusScan. The list provides a description of the viruses, including the infector type, virus characteristics, virus size, and cleaning status. To display and use the Virus List, follow the instructions outlined below.

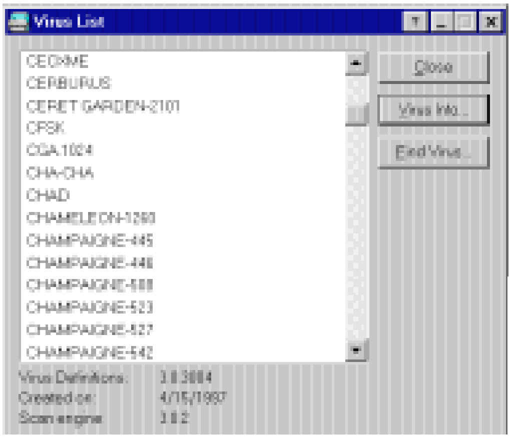
**Step** **Action**

1. Start VirusScan.

   **Response**: The McAfee VirusScan main window is displayed (See Figure 6-1 on page 60).

2. Select Virus List from the Tools menu.

**Response**: The Virus List dialog box is displayed (Figure 6-9).



CEOXME
CERBURUS
CERET GARDEN-2101
CFSK
CGA 1024
CHA-CHA
CHAD
CHAMELEON-1260
CHAMPAIGNE-445
CHAMPAIGNE-448
CHAMPAIGNE-508
CHAMPAIGNE-523
CHAMPAIGNE-527
CHAMPAIGNE-542

Virus Definitions: 3.0.3004
Created on: 4/15/1997
Scan engine: 3.0.2

Figure 6-9. Virus List Dialog Box

3. To display information on a virus, select it from the list and click Virus Info. To find a specific virus, click Find Virus and type the name of the virus in the text box provided. When the name of the virus you are looking for appears in the virus list, close the text box and click Virus Info.

- The Virus Information section describes what the selected virus infects:
  - ❑ Files, if listed, indicates that the virus infects files. If the virus targets files with specific extensions or files of a specific type, the extensions appear to the right of Infects.
  - ❑ Boot Sectors, if listed, indicates that the virus infects the boot sector.
  - ❑ MBRs, if listed, indicates that the virus infects the Master Boot Record.
- Virus Size describes the amount, in bytes, that the virus increases the size of a file it infects.

  ✍ *The default size for an MBR or boot sector virus is 512 bytes.*

- The Characteristics section describes the behavior of the selected virus:
  - ❑ Memory Resident, if selected, indicates that the virus is a memory resident program that acts similar to a TSR or a device driver and remains active in memory while the computer is running.
  - ❑ Encrypted, if selected, indicates that the virus attempts to evade detection by self-encrypting.
  - ❑ Polymorphic, if selected, indicates that the virus attempts to evade detection by changing its internal structure or its encryption techniques.
  - ❑ Repairable, if selected, indicates that a remover for the virus is available.
  - ❑ Macro, if selected, indicates that the virus infects macros, such as those used by applications like Microsoft Word and Excel.

## Accessing the VirusScan Console

The VirusScan Console is used for scheduling and creating customized scan tasks. You can access the Console from the Advanced configuration window by selecting Console from the Tools menu.

✍ *For additional instructions on accessing and using the VirusScan Console, see “Using the VirusScan Console” on page 42.*

# 7 Using ScreenScan

## What is ScreenScan?

The ScreenScan component of VirusScan offers maximum protection against infection by scanning your system for viruses every time your screen saver is active. Once installed, ScreenScan minimizes the risk of viral damage by automatically checking your system's drives, files, and folders for infection—alerting you if viruses are discovered.

Through a simple configuration process, you can specify which items should be scanned and where scanning should take place. This chapter describes how to set up and configure ScreenScan to meet your needs.

✍ *Many of the task-related procedures described in this chapter are further explained in context-sensitive help files, which are accessed by right-clicking on the tasks themselves.*

# Configuring ScreenScan

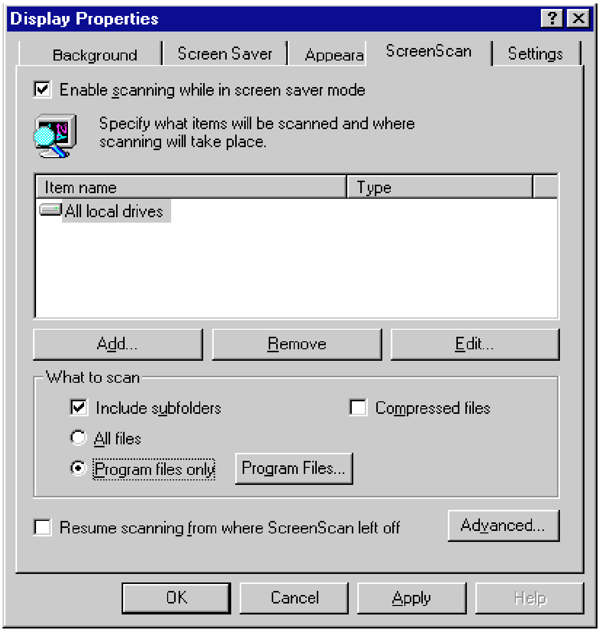
Upon installation, this configuration process should be followed to set up ScreenScan to meet your specific needs. McAfee also recommends reconfiguring ScreenScan after changing screen savers.

**Step** **Action**

**1.** Complete one of the following steps:

- Click Start, point to Settings, and click Control Panel. Double-click the Display icon. Select the ScreenScan tab.
- Position the mouse pointer in a space on your desktop not occupied by an element. Click the right mouse button. Click Properties and select the ScreenScan tab.

**Response**: The ScreenScan property page is displayed (Figure 7-1).



☑ Enable scanning while in screen saver mode

Specify what items will be scanned and where scanning will take place.

| Item name | Type |
|---|---|
| All local drives | |

What to scan

☑ Include subfolders □ Compressed files

○ All files

● Program files only

□ Resume scanning from where ScreenScan left off

**Figure 7-1. ScreenScan Property Page**

2. Select the Enable Scanning While in Screen Saver Mode checkbox.

3. Specify which items (drives and folders) should be scanned:

    - To add an item to the list, click the Add button. Select the item from the Item To Scan box. For the most comprehensive scan, select All Local Drives. If specifying a Drive or Folder, enter the path of the item in the Description box or click Browse to choose an item. Click OK.

    - To remove an item from the list, select the item and click Remove.

    - To edit items on the list, click Edit and make the desired changes.

    ✍ *Repeat this step until all scan items are selected.*

4. Define additional parameters of your scan:

    - To scan inside compressed files, select the Compressed Files checkbox.

    - To scan the subfolders of all items on your list, select the Include Subfolders checkbox.

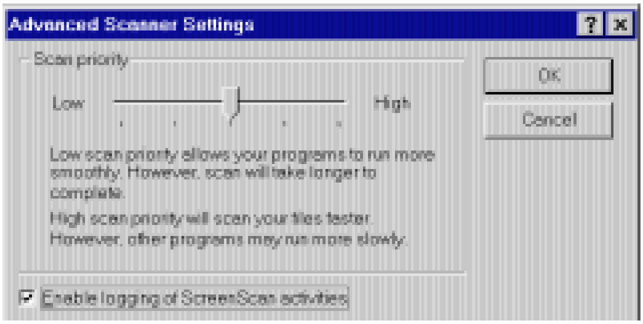
5. Select Program Files Only to scan only files with certain extensions. To edit which extensions are included in this list, click the Extensions button.

    ✍ *Default extensions are .EXE, .COM, .DO?, and .XL?. The question mark character is a wildcard, so this list will result in a scan that checks Word and Excel document and template (.DOC, .DOT, .XLS, and .XLT) files as well as program files.*

6. If you do not want ScreenScan to restart its scan with each launch of the screen saver, select the Resume Scanning Where Scan Left Off checkbox. If this box is not selected, ScreenScan will start each scan with the first item listed, regardless of whether the previous scan was completed.

7. Click the Advanced button.

   **Response**: The Advanced Scanner Settings dialog box is displayed (Figure 7-2).



Low scan priority allows your programs to run more smoothly. However, scan will take longer to complete.

High scan priority will scan your files faster. However, other programs may run more slowly.

☑ Enable logging of ScreenScan activities

**Figure 7-2. Advanced Scanner Settings Dialog Box**

- Set the Scan Priority slider to determine how much of your system's resources you want the task to take. A lower setting reserves more resources for other applications, but results in a slower scan.

- If you want ScreenScan to log its activity to a file in the installation directory, select the Enable Logging of ScreenScan Activity checkbox.

8. Click OK to exit Advanced Scanner Settings.

9. To save your settings, click Apply. To ignore changes and retain previously defined settings, click Cancel. Click OK to save your settings and exit Display Properties.

   **Response**: Configuration is complete. ScreenScan will scan for viruses when the screen saver is active.

# 8

# Removing a Virus

## If You Suspect You Have a Virus

If you have or suspect you have a virus before installing VirusScan, you should follow this procedure to create a virus-free environment.

**Step** **Action**

**1.** Turn off your computer.

✍ *Do not reboot using the reset button or* CTRL+ALT+DELETE*; if you do, some viruses might remain intact.*

**2.** Make an Emergency Disk. See "Making a clean start-up diskette" on page 89 for details.

**3.** Insert the Emergency Disk in your computer's A: drive.

**4.** Turn on your computer.

**5.** If you were able to create the Emergency Disk with the automatic creation utility, simply follow the on-screen instructions. If you are using a manually-created clean boot diskette, do the following:

- At the command prompt, type `scan /ADL /ALL /CLEAN`. This will start the command-line version of VirusScan. It will display its progress on-screen.

✍ *For detailed information on the VirusScan command-line options, see Appendix D, "Reference."*

## If viruses were removed

If VirusScan successfully removes all the viruses, shut down your computer and remove the diskette. You may now restart your computer and resume work. If you were installing VirusScan, begin the installation procedure described in Chapter 2, “Installing VirusScan.”

To find and eliminate the source of infection, scan all your diskettes immediately after installation.

## If viruses were not removed

If VirusScan cannot remove a virus, you will receive one of the following messages:

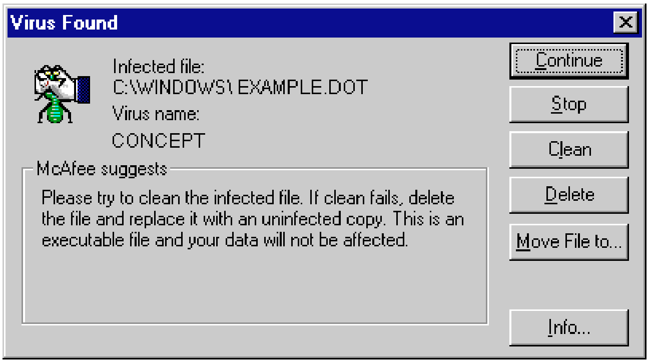
- Virus could not be removed.
- There is no remover currently available for the virus.

If you receive either of these messages, refer to documents related to manually removing viruses on the McAfee Web Site. For contact information, see “How To Contact Us” on page 14.

## Removing a virus found in a file

When VirusScan detects a virus in a file, it will display the infected files and take the action you specified during configuration. See “Configuring On-demand Scanning” on page 35.

- If you selected Prompt for Action from the When Virus Is Found drop-down menu, VirusScan will display the Virus Found dialog box upon virus detection (Figure 8-1).



Infected file:
C:\WINDOWS\ EXAMPLE.DOT
Virus name:
CONCEPT

McAfee suggests

Please try to clean the infected file. If clean fails, delete the file and replace it with an uninfected copy. This is an executable file and your data will not be affected.

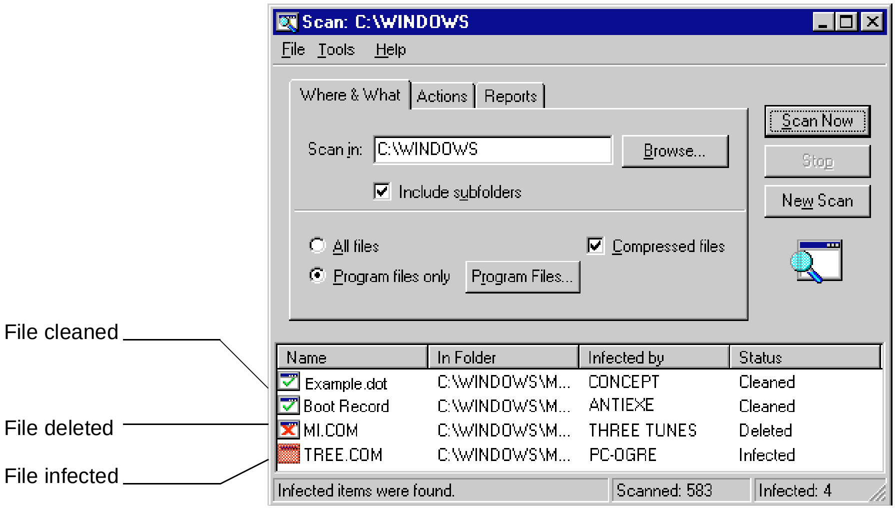
**Figure 8-1. Virus Found Dialog Box**

From this prompt, you have the following choices:

- Continue. Continues scanning until all files have been scanned. You can then respond to the infection or infections by following the steps described in "Responding to a virus infection" on page 81.
- Stop. Ends the scan session.
- Clean. Attempts to remove the virus from the file.
- Delete. Deletes and permanently removes the infected file.
- Move File To. Allows you to move infected files to a quarantine folder.

✍ *Click Info for more information about the virus discovered.*

As you respond to these infected files, icons are displayed in the VirusScan main window which correspond to the action you have taken (Figure 8-2).



Scan in: C:\WINDOWS

☑ Include subfolders

○ All files

● Program files only

☑ Compressed files

| Name | In Folder | Infected by | Status |
|---|---|---|---|
| ✓ Example.dot | C:\WINDOWS\M... | CONCEPT | Cleaned |
| ✓ Boot Record | C:\WINDOWS\M... | ANTIEXE | Cleaned |
| ☒ MI.COM | C:\WINDOWS\M... | THREE TUNES | Deleted |
| ▨ TREE.COM | C:\WINDOWS\M... | PC-OGRE | Infected |

Infected items were found. Scanned: 583 Infected: 4

**Figure 8-2. VirusScan Main Window (With infected files displayed)**

- If you selected Move Infected Files to a Folder, Clean Infected File, or Delete Infected File during configuration, VirusScan will automatically perform the action when it finds a virus. Files acted upon will be displayed in the VirusScan main window (see Figure 8-2).

- If you selected Continue Scanning during configuration, VirusScan will continue until all the files are scanned. When the scan is finished, any infected files found will be listed in the VirusScan main window (see Figure 8-2 on page 80). You can then respond to infections individually by following the steps below.

## Responding to a virus infection

To respond to a virus infection, select the infected file. Then go to the File menu or right-click on the infected file and take the following steps:

**Step** **Action**

**1.** To view basic information about the virus infecting your file, select Virus Info. To view detailed information, refer to the McAfee Virus Information Library, which is described in "McAfee Virus Information Library" on page 100.

**2.** To view basic information on the infected file, select File Info.

**3.** Select how VirusScan will respond to the infected file. Options include: Clean File, Delete File, or Move To.

> ✍ *If you select Move To, specify a path or choose Browse to navigate to the desired destination.When this option is selected, VirusScan automatically generates a text file called INFECTED.LOG in the specified folder, which logs the name of the file and where it was found.*

**4.** Repeat this process for all infected files.

VirusScan can remove many virus infections, but some viruses damage infected files beyond repair. If VirusScan cannot safely remove the virus, a message is displayed indicating the name of the unrecoverable file.

✍ *If VirusScan reports that it could not remove the virus from the infected file (the infected file is corrupted beyond repair), note the name and location of the file so you can restore it from backups. Scan your system again with the Delete Infected File checkbox selected.*

## Removing a virus found in memory

If VirusScan detects a virus on your system, immediately clean your system to prevent the virus from spreading throughout your system or network.You can remove viruses from files if you know or suspect an infection has occurred.

However, if a virus is resident in memory, or if the virus has infected the Master Boot Record (MBR) or boot sector, the most secure way to clean your system is to shut down your computer. Then, reboot from the Emergency Disk (see "Creating an Emergency Disk" on page 88) and remove the virus using VirusScan DOS commands (see "VirusScan Command-line Options" on page 102).

✍ *If a virus was detected in memory, use only the VirusScan DOS commands to clean your system. VirusScan for DOS is provided as the command-line component of VirusScan for Windows 95.*

If VirusScan for DOS is unable to remove a virus from the Master Boot Record, refer to documents on the McAfee Web Site or Automated Fax Response System related to manually removing viruses. For contact information, see "How To Contact Us" on page 14.

## Understanding false alarms

A false alarm is a report of a virus in a file or in memory when a virus does not actually exist. False alarms are more likely if you are using more than one brand of virus protection software, because some anti-virus programs store their virus signature strings unprotected in memory.

Always assume that any virus found by VirusScan is real and dangerous, and take necessary steps to remove it from your system. If, however, you have reason to believe that VirusScan is generating false alarms (for example, it has detected a virus in only one file that you have been using safely for years), refer to the list of potential sources below:

- If more than one anti-virus program is running, VirusScan may report a false alarm. Set up your computer so that only one anti-virus program is running at a time. Then turn off your computer, wait a few seconds, and turn it on again to make sure that all code from other anti-virus programs is cleared from memory.

- Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer’s reference manual for details.

- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. VirusScan may detect these modifications as a possible infection, even though no virus may be present. Check your computer’s reference manual to determine if your PC has self-modifying boot code. To solve this problem, save validation/recovery information to the executable files themselves; this method does not save information about the boot sector or Master Boot Record.

- VirusScan may report viruses in the boot sector or Master Boot Record of certain copy-protected diskettes.

# A

# Preventing Virus Infection

## Keys to a Secure System Environment

VirusScan is an effective tool for preventing, detecting, and recovering from virus infection. It is most effective, however, when used in conjunction with a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

To create a secure system environment and minimize your chance of infection, McAfee recommends that you take the following steps:

**Step** **Action**

**1.** Follow the installation procedures as outlined in Chapter 2, “Installing VirusScan.” If you suspect you have a virus, take steps to clean your system before installing VirusScan. For this procedure, see “If You Suspect You Have a Virus” on page 77.

**2.** Configure your AUTOEXEC.BAT file to load VShield automatically at start-up.

✍ *Your AUTOEXEC.BAT is automatically modified if you followed the recommended installation procedures.*

**3.** Create an Emergency Disk, which contains the command-line version of VirusScan, by following the procedure outlined in “Creating an Emergency Disk” on page 88. Make sure the diskette is write-protected so that it cannot become infected.

**4.** Make frequent backups of important files. Even with VirusScan, some viruses (as well as fire, theft, or vandalism) can render a disk unrecoverable without a recent backup.

# Detecting New and Unknown Viruses

There are two ways for you to deal with new and unknown viruses that may infect your system:

- Update your VirusScan data files
- Validate the VirusScan program files

## Updating your VirusScan data files

To offer the best virus protection possible, McAfee continually updates the files VirusScan uses to detect viruses. After a certain time period, VirusScan will notify you to update the virus definition database. For maximum protection, it is important to update these files on a regular basis.

### What is a data file?

The files CLEAN.DAT, NAMES.DAT, SCAN.DAT, and MCALYZE.DAT all provide virus information to the VirusScan software and make up the data files referred to in this section.

### Why would I need a new data file?

New viruses are discovered at a rate of more than 200 a month. Often, these viruses are not detected using older data files. The data files that came with your copy of VirusScan may not detect a virus that was discovered after you bought the product.

McAfee's virus researchers are working constantly to update the data files with more and newer virus definitions. The new data files are released approximately every four to six weeks.

✍ *McAfee cannot guarantee backward compatibility of the virus signature files with a previous version's software.*

## Using SecureCast electronic updating

VirusScan’s new SecureCast component gives you several options for keeping your installation up-to-date, with varying levels of user interaction. One option, which uses BackWeb’s Internet “push” technology, automatically updates your installation on a regular basis. If you choose this option, you will install BackWeb’s client software, which will perform invisible downloads of updates whenever you are connected to the internet. If you are not connected long enough for a full download at one time, the software will automatically piece out the work and notify you when a complete update package has arrived.

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

## Updating your data files manually

To update your McAfee data files manually, without using SecureCast, take the following steps.

**Step** **Action**

**1.** Download the data file (for example, DAT-3006.ZIP) from one of McAfee’s electronic services. On most services, it is located in the anti-virus area.

✍ *Please note that your ability to access 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.*

**2.** Copy the file to a new directory.

**3.** The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don’t have the decompression software, you can download PKUNZIP (shareware) from McAfee electronic sites.

**4.** Locate the directories on the hard drive where VirusScan is currently installed. Typically, the files are stored in C:\Program Files\McAfee\VirusScan.

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

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

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

## Validating the VirusScan program files

When you download a file from any source other than the McAfee bulletin board or other McAfee service, it is important to verify that it is authentic, unaltered, and uninfected. To ensure that your version of VirusScan is authentic, McAfee anti-virus software includes a utility program called Validate. When you receive a new version of VirusScan, run Validate on all of its program files. For details on the Validate program, see the README.1ST text file which accompanied your software.

# Creating an Emergency Disk

In case your system becomes infected, you should have Emergency Disks. This section describes how to create them.

Your system must be virus-free to make the Emergency Disks. Any virus residing on your system could be transferred to your Emergency Disks and reinfect your system.

If you suspect your computer is infected, go to another computer and scan it. If it is virus-free, follow the steps below, which detail how to use the Emergency Disk creation utility included with VirusScan.

✍ *If the computer does not have VirusScan installed on it, skip ahead to "Making a clean start-up diskette" on page 89, which details how to manually create a clean boot diskette. This can serve as a substitute for the Emergency Disks until you have installed VirusScan and can create the Emergency Disks.*

## The McAfee Emergency Disk

If you do not have the McAfee Emergency Disks, and have installed VirusScan, complete the following procedure to make the Emergency Disks:

| Step | Action |
|---|---|
| **1.** | Click Start, then point to programs, McAfee VirusScan. |
| **2.** | Click Create Emergency Disk. |
| **3.** | Insert the first 3.5-inch diskette and click Continue. When the first diskette is complete, insert the second diskette and click OK. |

## Making a clean start-up diskette

If you can not use the McAfee Emergency Disk creation utility because you have not installed VirusScan or have discovered an infection during installation, follow the steps below.

✍ *Your system must be virus-free to make a boot diskette. Any virus residing in your system could be transferred to your boot diskette and reinfect your system. If your computer is infected, go to another computer, scan it, and if it is virus-free, follow the steps below.*

Start this procedure from a command prompt (`C:\>`). If you are in Windows, you will need to exit Windows or open a DOS window to get the prompt. Then complete the following procedure:

**Step** **Action**

**1.** Insert a blank diskette in drive A:.

**2.** Format the diskette by typing the following command:

```
format a: /s/u/v
```

This overwrites any information already on the diskette and copies the necessary system files for booting your system.

✍ *If you are using DOS 5.0 or earlier, do not type the* `/u`*. If you are unsure of which version you are using, type* `ver` *at the* `C:\>` *prompt.*

**3.** When the system prompts you for a volume label, enter an appropriate name using no more than eleven characters.

**4.** Change to the VirusScan (default: `C:\Program Files\McAfee\VirusScan`) directory.

**5.** Copy the command-line version of VirusScan to the diskette by typing the following commands at the prompt:

```
copy scanpm.exe a:

copy scan.dat a:

copy clean.dat a:

copy names.dat a:
```

6. Change back to the root directory by typing `cd\`.

7. Copy the fdisk program by typing one of the following commands at the `C:\>` prompt:

   `copy c:\dos\fdisk.* a:` (for systems that have been upgraded from Windows 3.1x to Windows 95)

   `copy c:\windows\command\fdisk.* a:` (for Windows 95 systems that have not been upgraded from Windows 3.1x)

✍ *If you use a disk compression utility, be sure to copy the drivers required to access the compressed drives onto the clean boot diskette. See the documentation for that utility for more information about those drivers.*

8. Label and write protect this diskette, then store it in a secure place. See "Write-Protecting a Diskette" on page 91 for more information.

9. Repeat the last step for any other useful programs you want to add to the diskette. Here are some programs you might want:

   - debug.*
   - diskcopy.*
   - fdisk.*
   - format.*
   - label.*
   - mem.*
   - sys.*
   - unerase.*
   - xcopy.*

   ✍ *If you use a disk compression utility, be sure to copy the drivers required to access the compressed diskettes onto the Emergency Disk. See the documentation for your compression utility for more information about those drivers.*

# Write-Protecting a Diskette

Floppy diskettes are convenient, portable devices for storage and retrieval of computer data. Diskettes are used to save files (write) and recover files (read). They are also the most common vehicle viruses use to invade your computer's system.

One way to help avoid infection via floppy diskette is to *write-protect* diskettes for read only data. If your system does become infected with a virus, the write-protection feature keeps your clean diskettes from also becoming infected, preventing reinfection after your system is cleaned.

✍ *Any diskettes that are not write-protected should be scanned and cleaned before you write-protect them.*

## Write-protecting 3.5” floppy diskettes

| **Step** | **Action** |
|---|---|
| **1.** | Position the diskette face down with the metal slide facing you.<br>Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide up and down across the hole. |
| **2.** | To write-protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the hole is open. |

# B

# Testing Your Installation

The Eicar Standard AntiVirus Test File is a world-wide combined effort by anti-virus vendors to set one standard for customers to verify their anti-virus installations. To test your installation, copy the following line into its own file and name it EICAR.COM.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

✍ *The characters in this file must all appear on one line.*

Upon completion, you will have a 69- or 70-byte file.

When this file is scanned, VirusScan will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

THIS FILE IS NOT A VIRUS! Delete the file when installation testing is completed so unsuspecting users are not unnecessarily alarmed.

✍ *Because the Eicar Standard AntiVirus Test File is not a true virus infection, you will not be able to clean or repair the infected file.*

C

# McAfee Support Services

McAfee is pleased to offer many different types of technical assistance to customers. These flexible support programs are designed to meet the needs of individuals and businesses at any level. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal support plan, McAfee helps to ensure that you receive the level of technical assistance you require.

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

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

# One-Button Web Support

McAfee is pleased to offer its customers the convenience of easy electronic access to product information and upgrades through One-Button Web Support.

✍ *This feature is only available in the retail and evaluation versions of VirusScan. It is not available in the corporate version.*

✍ *To use this feature, you will need an internet connection and a web browser installed.*

To use One-Button Web Support, complete the following steps:

| Step | Action |
|---|---|
| **1.** | Start VirusScan. |
| **2.** | From the Help menu, choose Go to Web Support. |
|  | **Response**: Your web browser will open to the McAfee Web Support page. |

# Customer Service Programs

## Free VirusScan support program

All registered owners of single-node (one computer) VirusScan products purchased at local retail stores or downloaded from the McAfee Store on our website, are entitled to:

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

### Support services

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

# Free VirusScan Deluxe support program

All registered owners of single-node (one computer) VirusScan Deluxe products purchased at local retail stores or downloaded from McAfee Store on our website, are entitled to:

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

## Support services

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

# Free subscription maintenance and support program

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

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

## Support services

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

# Optional support plans

✍ *Contact McAfee for current pricing structures.*

## Option 1: One-year personal support plan

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

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

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

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

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

# Professional Services Programs

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

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

## Training

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

## Consulting

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

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

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

## Jump Start program

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

## Enterprise support

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

The Enterprise Support Program offers the following features:

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

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

## Optional 7 x 24 enterprise support

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

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

# D

# Reference

## VirusScan Command-line Options

The following table lists all of the VirusScan options you can use when you're running the DOS command-line scanner, SCAN.EXE. To run VirusScan from the command line, first use the `cd` command to change directories to the directory in which VirusScan was installed. Then, type `scan /?` to display a list of options and descriptions of how they can be used.

✍ *When specifying a filename as part of a command-line option, you must include the full path to the file if it is not located in the directory in which VirusScan is installed.*

| Command-line Option | Description |
|---|---|
| `/?` or `/HELP` | Does not scan. Instead, displays a list of VirusScan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options). |
| `/ADL` | Scans all local drives (including compressed and PCMCIA drives, but not diskettes), in addition to those specified on the command line.<br>To scan both local and network drives, use /ADL and /ADN together in the same command line. |
| `/ADN` | Scans all network drives for viruses, in addition to those specified on the command line.<br>To scan both the local drives and network drives, use /ADL and /ADN together in the same command line. |

| Command-line Option | Description |
|---|---|
| `/AF filename` | Stores validation/recovery codes in *filename.*<br>Helps you detect new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector, and Master Boot Record on a hard disk or diskette in a file you specify. The log file is about 89 bytes per file validated.<br>You must specify a *filename*, which can include the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. If *filename* exists, VirusScan updates it. /AF adds about 300% more time to scanning.<br>✍ */AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.*<br>*The /AF option does not store any information about the Master Boot Record or boot sector of the drive being scanned.* |
| `/ALERTPATH <directory>` | Designates `<directory>` as a network path monitored by NetShield for Centralized Alerting. |
| `/ALL` | Overrides the default settings by scanning all files.<br>This option substantially increases the scanning time required. Use it if you have found a virus or suspect one.<br>✍ *The list of extensions for standard executables has changed from previous releases of VirusScan.* |
| `/APPEND` | Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists. |

| Command-line Option | Description |
|---|---|
| `/AV` | To help you detect and recover from new or unknown viruses, /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights.<br>To exclude self-modifying or self-checking files, and damaged files that might cause false alarms, use the /EXCLUDE option. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.<br>✍ *The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned.* |
| `/BOOT` | Scans only the boot sector and Master Boot Record on the specified drive. |
| `/CF filename` | Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in *filename*. If a file or system area has changed, VirusScan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning.<br>Using any of the /AF, /CF, or /RF options together in a command line returns an error.<br>✍ *Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF, VirusScan continuously reports that the boot sector has been modified even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.* |
| `/CLEAN` | Cleans infected files. |
| `/CLEANDOC` | Cleans viruses from infected Word document files. |

| Command-line Option | Description |
|---|---|
| `/CLEANDOCALL` | Cleans all macros from infected Word document files. |
| `/CONTACTFILE filename` | Identifies a file containing a message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation.<br>Any character is valid except a backslash (\). Messages that begin with a slash (/)or a hyphen (-) should be placed in quotation marks. |
| `/CV` | Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, VirusScan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning.<br>Using any of the /AV, /CV, or /RV options together in the same command line returns an error.<br>✍ *The /CV option does not check the boot sector for changes.* |
| `/DEL` | Deletes infected files. |
| `/EXCLUDE filename` | Excludes any files listed in *filename* from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Self-modifying or self-checking files can cause a false alarm during a scan. |
| `/FAST` | Speeds up the scan.<br>Reduces scanning time by about 15%. Using the /FAST option, VirusScan examines a smaller portion of each file for viruses.<br>Using /FAST might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one. |
| `/FORCE` | Cleans partition table viruses by writing a generic Master Boot Record over the disk’s boot record. |

| **Command-line Option** | **Description** |
|---|---|
| `/FREQUENCY hours` | The number of hours that must occur between subsequent successful scans (Example: `/FREQUENCY 1`).<br>In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of *hours* specified, the greater the scan frequency and the greater your protection against infection. |
| `/LOAD filename` | Performs a scan using the information saved in *filename*.<br>You can store all custom settings in a separate configuration file (an ASCII text file), then use /LOAD to load those settings from that file. |
| `/LOCK` | Halts the system to stop further infection if VirusScan finds a virus.<br>/LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use /LOCK, we recommend you use it with /CONTACTFILE to tell users what to do or whom to contact if a virus is found and the system locks up. |
| `/LOG` | Stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the root of the current drive. |

| Command-line Option | Description |
|---|---|
| `/MANY` | Scans multiple diskettes consecutively in a single drive. VirusScan prompts you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly.<br>The VirusScan program should reside on a disk that will not be removed during the scan.<br>For example, if you are scanning disks in the computer's A: drive, and you are running the program from a disk in the A: drive, the program will become unavailable as soon as you remove the diskette to put another in. The following command causes an error during execution:<br>`a:\scan a: /many` |
| `/MAXFILESIZE xxx.x` | Scans only files with size not more than `xxx.x` megabytes. |
| `/MEMEXCL` | Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.)<br>This command-line option has been added to prevent VirusScan from checking areas in upper memory which might contain memory-mapped hardware and might cause false alarms. |
| `/MOVE directory` | Moves all infected files found during a scan to the specified directory. To preserve drive and directory structure, this option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files. |
| `/NOBEEP` | Disables the tone that sounds whenever VirusScan finds a virus. |
| `/NOBREAK` | Disables CTRL-C and CTRL-BREAK during scans.<br>Users will not be able to halt scans in progress using CTRL-C or CTRL-BREAK. Use this option in conjunction with /LOG to create a meaningful audit trail of regularly scheduled scans. |

| Command-line Option | Description |
|---|---|
| /NOCOMP | Skips checking of compressed executables created with the LZEXE or PKLITE file-compression programs.<br>Reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file-compression programs. VirusScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, VirusScan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/ recovery codes. |
| /NODDA | No direct disk access.<br>Prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT.<br>You might need to use this option on some device-driven drives. |
| /NODOC | Does not scan Word document files. |
| /NOEMS | Prevents VirusScan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs. |
| /NOEXPIRE | Disables the “expiration date” message if the VirusScan data files are out of date. |

| Command-line Option | Description |
|---|---|
| `/NOMEM` | Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free.<br>VirusScan can check system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0KB to 640KB, VirusScan checks system memory from 640KB to 1088KB that can be used by computer viruses on 286 and later systems. Memory above 1088KB is not addressed directly by the processor and is not presently susceptible to viruses. |
| `/PAUSE` | Enables screen pause.<br>If you specify /PAUSE, the “Press any key to continue” prompt appears when VirusScan fills up a screen with messages (for example, when you’re using the /SHOWLOG or /VIRLIST options). Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with many drives or that have severe infections without requiring you to attend.<br>We recommend that you omit /PAUSE when keeping a record of VirusScan’s messages using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR). |
| `/PLAD` | Preserve last access dates (on proprietary drives only).<br>Prevents changing the last access date attribute for files stored on a network drive in a proprietary network. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning. |

| **Command-line Option** | **Description** |
|---|---|
| `/REPORT filename` | Creates a report of infected files and system errors.<br>Saves the output of VirusScan to *filename* in ASCII text file format. If *filename* exists, /REPORT erases and replaces it (or, if you use /APPEND, adds the report information to the end of the existing file).<br>You can include the destination drive and directory (such as `D:\VSREPRT\ALL.TXT`), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use /RPTALL, /RPTCOR, /RPTMOD, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report. |
| `/RF filename` | Removes recovery and validation data from *filename* created by the /AF option.<br>If *filename* resides on a shared network drive, you must be able to delete files on that drive. Using any of the /AF, /CF, or /RF options together in the same command line returns an error. |
| `/RPTALL` | Adds list of files scanned to the report file (used with /REPORT). |
| `/RPTCOR` | When used in conjunction with /REPORT, adds the names of corrupted files to the report file.<br>A corrupted file may be a file that has been damaged by a virus. You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.<br>✍ *There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).* |

| Command-line Option | Description |
|---|---|
| /RPTERR | Adds a list of system errors to the report file. This option is used in conjunction with /REPORT.<br>System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line. |
| /RPTMOD | Adds list of modified files to the report file. This option is used in conjunction with /REPORT.<br>VirusScan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line. |
| /RV | Removes validation and recovery data from files validated with the /AV option.<br>To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV, or /RV options together in the same command line returns an error. |
| /SHOWLOG | Displays the contents of SCAN.LOG.<br>SCAN.LOG stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the current directory and the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch.<br>The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option. |

| Command-line Option | Description |
|---|---|
| `/SUB` | Scans subdirectories inside a directory.<br>By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. Do not use /SUB if you are scanning an entire drive. |
| `/VIRLIST` | Displays the name and a brief description of each virus that VirusScan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line.<br>You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS, enter:<br>`scan /virlist > filename.txt`<br>✍ *Because VirusScan can detect many viruses, this file is more than 250 pages long.* |

# Scan32 Command Line Options

The following table lists additional VirusScan command options you can use when you're running Scan32.EXE from the command line.

Example of options:

SCAN32 [<switches>] [<scanitem>]

SCAN32 <config.VSC> [<override_switches>] [<override_scanitem>]

SCAN32 [/SERVER <servername>] /TASK <taskid> [<override_switches>] [<override_scanitem>]

| Command-line Option | Description |
|---|---|
| `/[NO]SPLASH` | Displays initial splash screen.<br>Default: /SPLASH |
| `/[NO]AUTOSCAN` | Scan32 automatically initiates scanning when started.<br>Default: <depends on UI type> |
| `/[NO]AUTOEXIT` | Scan32 automatically exits if no viruses are found. If viruses are found, Scan32 does not exit (see / ALWAYSEXIT).<br>Default: <depends on UI type> |
| `/[NO]ALWAYSEXIT` | Scan32 automatically exits when scan is complete. Scan32 exits even if viruses are detected (see / AUTOEXIT).<br>Default: <depends on UI type> |
| `/[NO]SUB` | Scans all subfolders.<br>Default: /SUB |
| `/[NO]ALL` | Scans all files, regardless of their file extension.<br>Default: /NOALL |

| Command-line Option | Description |
|---|---|
| /[NO]COMP | Scans compressed files and ZIP files.<br>Default: /COMP |
| /UICONFIG \| /UIEXONLY \| /UINONE | Specifies the type of graphical user interface displayed:<br>UICONFIG - A fully-configurable interface that allows the user to specify which items to scan.<br>UIEXONLY - An "execution-only" interface that takes all options from the command line, registry, or VSC file. This value implies /AUTOSCAN and /AUTOEXIT.<br>UINONE - No visible user interface. All options must be taken from the command line, registry or VSC file. Activity logging should be used to obtain the scan results. This value implies /AUTOSCAN and /ALWAYSEXIT.<br>Default: /UICONFIG |
| /CONTINUE \| /PROMPT \| /CLEAN \| /DELETE \| /MOVE <FOLDER> | Specifies what action to take when a virus is detected:<br>CONTINUE - Logs information about the infection and continues scanning.<br>PROMPT - Pauses the scan to ask the user which action to take (see /MSG).<br>CLEAN - Attempts to clean the infected item and continues with the scan.<br>DELETE - Attempts to delete the infected item and continues with the scan.<br>MOVE - Attempts to move the infected files and continues scanning.<br>Default: /CONTINUE |
| /[NO]MSG <message> | Displays a custom message when the /PROMPT option is specified and a virus is detected.<br>Default: /NOMSG |

| Command-line Option | Description |
|---|---|
| `/[NO]BEEP` | Plays an audible tone on completion of a scan if infected items were found.<br>Default: /BEEP |
| `/RPTSIZE <n>` | Specifies the maximum size of the activity log file (in kilobytes). When the file exceeds this size, it is truncated to zero bytes.<br>Default: /RPTSIZE 100 |
| `/[NO]MEM` | Performs a memory scan.<br>Default: /MEM |
| `/[NO]BOOT` | Performs a boot record scan. The Master Boot Record (MBR) is scanned and the boot sector of each drive where a scan item resides is scanned.<br>Default: /BOOT |
| `/EXT extensions` | Lists the file extension types to scan, unless the /ALL option is specified. To modify this list, the entire list must be entered with each entry separated by a space, for example: /EXT "EXE COM SYS ZIP".<br>Default: /EXT "EXE COM BIN SYS DO? OVL DLL APP CMD" |
| `/DEFEXT extensions` | A list of program extensions to default to when user selects “New Scan” from the configurable (see /CONFIG) user interface. The entire list must be quoted and each entry separated by a space, for example: /DEFEXT “EXE COM SYS ZIP”.<br>Default: /DEFEXT “EXE COM BIN SYS DO? OVL DLL APP CMD PRG” |
| `/PRIORITY <n>` | Sets the priority of the scan process using a value between 1 and 5.<br>Default: /PRIORITY 3 |

| Command-line Option | Description |
|---|---|
| `/TASK <taskid>` | Specifies:<br>(a) configuration data should be read from the registry.<br>The taskid is a registry key found under: HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\VirusScan\Tasks.<br>This parameter may be used with or without the /SERVER option. If /SERVER is omitted, the local registry is used.<br>(b) when used with the /CANCEL option, the task is terminated.<br>Default: (none) |
| `/SERVER <servername>` | Specifies that configuration data should be read from the registry on the specified server. The /TASK option must be used with this parameter.<br>Default: (none) |
| `/CANCEL` | Specifies that a running task should be canceled. The /TASK parameter must be used with this option to specify which task is to be canceled.<br>Default: (none) |
| `/[NO]LOG [<logfile>]` | Enables activity logging and optionally, changes the name of the log file.<br>Default: /LOG “VirusScan Activity Log.txt” |
| `/LOGALL` | Specifies that all scan activity is logged. This option is equivalent to specifying /LOGDETECT /LOGCLEAN /LOGDELETE /LOGMOVE /LOGSETTINGS /LOGSUMMARY /LOGDATETIME /LOGUSER<br>Default: /LOGALL |
| `/[NO]LOGDETECT` | Logs the detection of infected items.<br>Default: /LOGDETECT |

| Command-line Option | Description |
|---|---|
| `/[NO]LOGCLEAN` | Logs the results of attempts to clean infected items.<br>Default: /LOGCLEAN |
| `/[NO]LOGDELETE` | Logs the results of attempts to delete infected items.<br>Default: /LOGDELETE |
| `/[NO]LOGMOVE` | Logs the results of attempts to move infected items.<br>Default: /LOGMOVE |
| `/[NO]LOGSETTINGS` | Logs the list of configuration settings used for each scan.<br>Default: /LOGSETTINGS |

# VirusScan DOS Error Levels

When you run VirusScan in the DOS environment, a DOS error level is set. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan.

✍ *See your DOS operating system documentation for more information.*

VirusScan can return the following error levels:

| **ERRORLEVEL** | **Description** |
|---|---|
| 0 | No errors occurred; no viruses were found. |
| 1 | Error occurred while accessing a file (reading or writing). |
| 2 | A VirusScan data file is corrupted. |
| 3 | An error occurred while accessing a disk (reading or writing). |
| 4 | An error occurred while accessing the file created with the /AF option; the file has been damaged. |
| 5 | Insufficient memory to load program or complete operation. |
| 6 | An internal program error has occurred (out of memory error). |
| 7 | An error occurred in accessing an international message file (MCAFEE.MSG). |
| 8 | A file required to run VirusScan, such as SCAN.DAT, is missing. |
| 9 | Incompatible or unrecognized option(s) or option argument(s) specified in the command line. |
| 10 | A virus was found in memory. |
| 11 | An internal program error occurred. |

| ERRORLEVEL | Description |
|---|---|
| 12 | An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or VirusScan was unable to remove the virus. |
| 13 | One or more viruses were found in the Master Boot Record, boot sector, or files. |
| 14 | The SCAN.DAT file is out of date; upgrade VirusScan data files. |
| 15 | VirusScan self-check failed; it may be infected or damaged. |
| 16 | An error occurred while accessing a specified drive or file. |
| 17 | No drive, directory, or file was specified; nothing to scan. |
| 18 | A validated file has been modified (/CF or /CV options). |
| 19-99 | Reserved. |
| 100+ | Operating system error; VirusScan adds 100 to the original number. |
| 102 | CTRL+C or CTRL+BREAK was used to interrupt the Scan. (You can disable CTRL+C or CTRL+BREAK with the /NOBREAK command-line option.) |

# VSH File Format

The VSH file is a configuration text file, formatted similarly to the Windows INI file, which outlines VShield's settings. Each variable in the file has a name followed by the equal (=) sign and a value. The values define which settings have been selected for VShield configuration. The variables are arranged in seven groups: General, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, SecurityOptions, and ExclusionOptions. To edit the VSH file, open it with a text editor, such as Notepad.

✍ *In Boolean variables, possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.*

## General

| Variable | Description |
|---|---|
| bLoadAtStartup | Type: Boolean (1/0)<br>Defines if VShield should be loaded at system startup<br>Default value: 1 |
| bCanBeDisabled | Type: Boolean (1/0)<br>Defines if VShield can be disabled<br>Default value: 1 |
| bShowTaskbarIcon | Type: Boolean (1/0)<br>Defines whether VShield taskbar icon is displayed<br>Default value: 1 |
| bNoSplash | Type: Boolean (1/0)<br>Instructs VShield to not show splash screen when program is launched<br>Default value: 0 |

## DetectionOptions

| Variable | Description |
|---|---|
| szProgramExtensions | Type: String<br>Defines extensions to be scanned<br>Default value: EXE COM DO? XL? |
| szDefaultProgramExtensions - | Type: String<br>Defines extensions to be used as default program extensions during scan configuration<br>Default value: EXE COM DO? XL? |

| Variable | Description |
|---|---|
| bScanOnExecute | Type: Boolean (1/0)<br>Instructs VShield to scan when files are run<br>Default value: 1 |
| bScanOnOpen | Type: Boolean (1/0)<br>Instructs VShield to scan when files are opened<br>Default value: 1 |
| bScanOnCreate | Type: Boolean (1/0)<br>Instructs VShield to when files are created<br>Default value: 1 |
| bScanOnRename | Type: Boolean (1/0)<br>Instructs VShield to when files are renamed<br>Default value: 1 |
| bScanOnBootAccess | Type: Boolean (1/0)<br>Instructs VShield to scan the boot record of a disk drive the first time it is accessed<br>Default value: 1 |
| bScanAllFiles | Type: Boolean (1/0)<br>Instructs program to scan inside all files<br>Default value: 0 |
| bScanCompressed | Type: Boolean (1/0)<br>Instructs program to scan inside compressed files (PkLite, LZEXE)<br>Default value: 1 |

## AlertOptions

| Variable | Description |
|---|---|
| bNetworkAlert | Type: Boolean (1/0)<br>Instructs VShield to send a network alert to a folder being monitored by NetShield for Centralized Alerting.<br>Default Value: 0 |
| szNetworkAlertPath | Type: String<br>Specifies path being monitored by NetShield for Centralized Alerting.<br>Default Value: None |

## ActionOptions

| Variable | Description |
|---|---|
| szCustomMessage | Type: String<br>Defines custom message to be displayed upon virus detection if action is set to Prompt for Action<br>Default value: `Possible Virus Detected` |
| szMoveToFolder | Type: String<br>Defines folder to which infected files should be moved<br>Default value: `\Infected` |

| | |
|---|---|
| uVshieldAction | Type: Integer (1-5)<br>Instructs VShield to take the action specified when a virus is detected<br>Possible values:<br>1 - Prompt for action<br>2 - Move infected files to a folder<br>3 - Clean infected files automatically (Deny access if files can't be cleaned)<br>4 - Delete infected files automatically<br>5 - Deny access to infected files<br>Default value: 1 |
| bButtonClean | Type: Boolean (1/0)<br>Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected<br>Default value: 1 |

| Variable | Description |
|---|---|
| bButtonDelete | Type: Boolean (1/0)<br>Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected<br>Default value: 1 |
| bButtonExclude | Type: Boolean (1/0)<br>Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected<br>Default value: 1 |
| bButtonStop | Type: Boolean (1/0)<br>Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected<br>Default value: 1 |
| bButtonContinue | Type: Boolean (1/0)<br>Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected<br>Default value: 1 |
| bDisplayMessage | Type: Boolean (1/0)<br>Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection<br>Default value: 0 |

## ReportOptions

| Variable | Description |
|---|---|
| szLogFileName | Type: String<br>Defines log file name<br>Default value: C:\Program Files\McAfee\Viruscan\Vshlog.txt |
| bLogToFile | Type: Boolean (1/0)<br>Defines if scan results should be logged into log file<br>Default value: 1 |
| bLimitSize | Type: Boolean (1/0)<br>Defines if size of the log file should be limited<br>Default value: 1 |
| uMaxKilobytes | Type: Integer (10-999)<br>Defines maximum size of the log file in kilobytes<br>Default value: 100 |
| bLogDetection | Type: Boolean (1/0)<br>Defines if scanning results should be logged<br>Default value: 1 |
| bLogClean | Type: Boolean (1/0)<br>Defines if cleaning results should be logged<br>Default value: 1 |
| bLogDelete | Type: Boolean (1/0)<br>Defines if infected file delete operations should be logged<br>Default value: 1 |

| Variable | Description |
|---|---|
| bLogMove | Type: Boolean (1/0)<br>Defines if infected file move operations should be logged<br>Default value: 1 |
| bLogSettings | Type: Boolean (1/0)<br>Defines if session settings should be logged on shutdown<br>Default value: 1 |
| bLogSummary | Type: Boolean (1/0)<br>Defines if session summary should be logged on shutdown<br>Default value: 1 |
| bLogDateTime | Type: Boolean (1/0)<br>Defines if time and date of an event should be logged<br>Default value: 1 |
| bLogUserName | Type: Boolean (1/0)<br>Defines if user name should be logged<br>Default value: 1 |

## SecurityOptions

| Variable | Description |
|---|---|
| szPasswordProtect | Type: String<br>This option is not user-configurable.<br>Default Value: 0 |
| szPasswordCRC | Type: String<br>This option is not user-configurable.<br>Default Value: 0 |

## ExclusionOptions

| Variable | Description |
|---|---|
| szExclusionsFileName | Type: String<br>This option is not user-configurable. |
| NumExcludedItems | Type: Integer (0-n)<br>Defines the number of items excluded from on-access scanning<br>Default value: 0 |

| | |
|---|---|
| ExcludedItem_x, where x is a zero-based index | Type: String<br>Instructs VShield to exclude the item from on-access scanning<br>Default value: `\Recycled|*.*|1|1 *`<br>* The string is separated into fields using the pipe (\|) character:<br>Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system.<br>Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename.<br>Field 3 - Integer (1-3)<br>Possible values:<br>1 - Exclude from file-access scanning<br>2 - Exclude from boot-record scanning<br>3 - Exclude from both boot-record and file-access scanning<br>Field 4 - Boolean (1/0)<br>Possible values:<br>1 - Instructs VShield to exclude subfolders of the excluded item<br>2 - Instructs VShield to not exclude subfolders |

# VSC File Format

The VSC file is a configuration text file, formatted similarly to the Windows INI file, which outlines VirusScan's settings. Each variable in the file has a name followed by the equal (=) sign and a value. The values define which settings have been selected for VirusScan configuration. The variables are arranged in eight groups: ScanOptions, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, ScanItems, SecurityOptions, and ExcludedItems. To edit the VSC file, open it with a text editor, such as Notepad.

✍ *In Boolean variables, possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.*

## ScanOptions

| Variable | Description |
|---|---|
| bAutoStart | Type: Boolean (0/1)<br>Instructs VirusScan to automatically start scan when launched<br>Default Value: 0 |
| bAutoExit | Type: Boolean (0/1)<br>Instructs VirusScan to exit automatically when finished scanning if no viruses were found<br>Default Value: 0 |
| bAlwaysExit | Type: Boolean (0/1)<br>Instructs VirusScan to exit automatically when finished scanning even if viruses were found<br>Default Value: 0 |
| bSkipMemoryScan | Type: Boolean (0/1)<br>Instructs VirusScan to skip memory scan<br>Default Value: 0 |
| bSkipBootScan | Type: Boolean (0/1)<br>Instructs VirusScan to skip boot sector scanning<br>Default Value: 0 |
| bSkipSplash | Type: Boolean (0/1)<br>Instructs VirusScan to skip display of the VirusScan splash screen on startup<br>Default Value: 0 |

## DetectionOptions

| Variable | Description |
|---|---|
| bScanAllFiles | Type: Boolean (0/1)<br>Instructs VirusScan to scan all file types<br>Default Value: 0 |
| bScanCompressed | Type: Boolean (0/1)<br>Instructs VirusScan to Scan in compressed files<br>Default Value: 1 |
| szProgramExtensions | Type: String<br>Specifies which file extensions VirusScan will scan<br>Default Value: EXE COM DO? XL? |
| szDefaultProgramExtensions | Type: String<br>Specifies default value for szProgramExtensions<br>Default Value: EXE COM DO? XL? |

## AlertOptions

| Variable | Description |
|---|---|
| bNetworkAlert | Type: Boolean (0/1)<br>Instructs VirusScan to send an alert (.ALR) file to a network path being monitored by NetShield for Centralized Alerting when a virus is found<br>Default Value: 0 |
| bSoundAlert | Type: Boolean (0/1)<br>Instructs VirusScan to sound an audible alert when a virus is detected<br>Default Value: 1 |

| Variable | Description |
|---|---|
| szNetworkAlertPath | Type: String<br>Specifies the network alert path being monitored by NetShield for Centralized Alerting. The folder this path points to should contain the Centralized Alerting file, CENTALRT.TXT<br>Default Value: None |

## ActionOptions

| Variable | Description |
|---|---|
| bDisplayMessage | Type: Boolean (0/1)<br>Instructs VirusScan to display a message upon detection of a virus<br>Default Value: 0 |
| ScanAction | Type: Integer (0-5)<br>Instructs ViruScan to take the action specified when a virus is detected<br>Possible values:<br>0 - Prompt for action<br>1 - Move automatically<br>2 - Clean automatically<br>3 - Delete automatically<br>4 - Continue<br>Default Value: 0 |
| bButtonClean | Type: Boolean (0/1)<br>Instructs VirusScan to display the Clean button if ScanAction=0<br>Default Value: 1 |
| bButtonDelete | Type: Boolean (0/1)<br>Instructs VirusScan to display the Delete button if ScanAction=0<br>Default Value: 1 |
| bButtonExclude | Type: Boolean (0/1)<br>Instructs VirusScan to display the Exclude button if ScanAction=0<br>Default Value: 1 |

| Variable | Description |
|---|---|
| bButtonMove | Type: Boolean (0/1)<br>Instructs VirusScan to display the Move button if ScanAction=0<br>Default Value: 1 |
| bButtonContinue | Type: Boolean (0/1)<br>Instructs VirusScan to display the Continue button if ScanAction=0<br>Default Value: 1 |
| bButtonStop | Type: Boolean (0/1)<br>Instructs VirusScan to display the Stop button if ScanAction=0<br>Default Value: 1 |
| szMoveToFolder | Type: String<br>Indicates where infected files should be moved<br>Default Value: \Infected |
| szCustomMessage | Type: String<br>Indicates text of message to be displayed on virus detection<br>Default Value: Possible Virus Detected |

## ReportOptions

| Variable | Description |
|---|---|
| bLogToFile | Type: Boolean (0/1)<br>Instructs VirusScan to log scan activity to a file<br>Default Value: 1 |
| bLimitSize | Type: Boolean (0/1)<br>Instructs VirusScan to limit the size of the log file<br>Default Value: 1 |
| uMaxKilobytes | Type: Integer (10-999)<br>Specifies maximum size of log file in kilobytes<br>Default Value: 10 |
| bLogDetection | Type: Boolean (0/1)<br>Instructs VirusScan to log virus detection<br>Default Value: 1 |
| bLogClean | Type: Boolean (0/1)<br>Instructs VirusScan to log virus cleaning<br>Default Value: 1 |
| bLogDelete | Type: Boolean (0/1)<br>Instructs VirusScan to log file deletions<br>Default Value: 1 |
| bLogMove | Type: Boolean (0/1)<br>Instructs VirusScan to log file moves<br>Default Value: 1 |
| bLogSettings | Type: Boolean (0/1)<br>Instructs VirusScan to log session settings<br>Default Value: 1 |

| Variable | Description |
|---|---|
| bLogSummary | Type: Boolean (0/1)<br>Instructs VirusScan to log session summaries<br>Default Value: 1 |
| bLogDateTime | Type: Boolean (0/1)<br>Instructs VirusScan to log date and time of scan activity<br>Default Value: 1 |
| bLogUserName | Type: Boolean (0/1)<br>Instructs VirusScan to log user name<br>Default Value: 1 |
| szLogFileName | Type: String<br>Specifies path to log file<br>Default Value: C:\Program Files\McAfee\Virus-can\VSCLOG.TXT |

## ScanItems

| Variable | Description |
|---|---|
| ScanItem_x, where x is a zero-based index | Type: String<br>Instructs VirusScan to scan the item<br>Default value: `C:\|1` *<br>* The string is separated into fields using the pipe (\|) character:<br>Field 1 - Path of item to scan.<br>Field 2 - Boolean (1/0)<br>Possible values:<br>1 - Instructs VirusScan to scan subfolders of the item<br>2 - Instructs VirusScan not to scan subfolders of the item |

## SecurityOptions

| Variable | Description |
|---|---|
| szPasswordProtect | Type: String<br>This variable is not user-configurable<br>Default Value: 0 |
| szPasswordCRC | Type: String<br>This variable is not user-configurable<br>Default Value: 0 |
| szSerialNumber | Type: String<br>This variable is not user-configurable<br>Default Value: 0 |

## ExcludedItems

| Variable | Description |
|---|---|
| NumExcludeItems | Type: Integer (0-n)<br>Defines the number of items excluded from scanning<br>Default value: 1 |
| ExcludedItem_x, where x is a zero-based index | Type: String<br>Instructs VirusScan to exclude the item from scanning<br>Default value: `\Recycled\|*.*\|1\|1 *`<br>* The string is separated into fields using the pipe (\|) character:<br>Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system.<br>Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename.<br>Field 3 - Integer (1-3)<br>Possible values:<br>1 - Exclude from file scanning<br>2 - Exclude from boot-record scanning<br>3 - Exclude from both boot-record and file scanning<br>Field 4 - Boolean (1/0)<br>Possible values:<br>1 - Instructs VirusScan to exclude subfolders of the excluded item<br>2 - Instructs VirusScan to not exclude subfolders |

# Glossary

The following list defines some terms you might encounter while using VirusScan to guard your computer against viruses.

## BIOS

A read-only memory chip that contains the coded instructions for using hardware such as a keyboard or monitor. Always present in portable computers, a BIOS (boot ROM) is not susceptible to infection (unlike the boot sector on a disk). Some BIOS chips contain anti-virus features that can generate a false alarm, installation failure, and other problems.

## boot

To start a computer. The computer will load start-up instructions from a disk's boot ROM (BIOS) or boot sector. See also "cold boot" and "warm boot."

## boot sector

A portion of a disk that contains the coded instructions for the operating system to start the computer.

## boot sector infection

Contamination of the boot sector by a virus. A boot sector infection is particularly dangerous because information in the boot sector is loaded into memory first, *before* virus protection code can be executed. The only certain way to eliminate a boot sector infection is to start your computer from a clean start-up diskette, then remove the infection using VirusScan.

## boot disk

A write-protected diskette that contains the computer’s system and start-up files. You can use this diskette to start up your computer. It is important to use a virus-free boot disk to guarantee that a virus is not introduced into the computer.

## cold boot

To turn on a computer, or to restart a computer by turning it off, waiting a few seconds, and turning it on again. Other methods of restarting (such as pressing a reset button or pressing CTRL+ALT+DEL) may not remove all traces of a virus infection from memory. See also “boot” and “warm boot.”

## compressed executable

A file that has been compressed using a file compression utility such as LZEXE or PKLITE. See also “compressed file.”

## compressed file

A file that has been compressed using a file compression utility such as PKZIP. See also “compressed executable.”

## conventional memory

Up to 640KB (1MB) of main memory in which DOS executes programs.

## corrupted file

A file that has been irreparably damaged, by a virus for example.

## detection

Scanning memory and disks for clues that a virus may be present. Some detection methods include searching for common viral patterns or strings, comparing suspicious file activity with known virus activity, and monitoring files for unauthorized changes.

## disinfect

To eradicate a virus so that it can no longer spread or cause damage to a system.

## exception list

List of files to which validation codes should not be added because they have built-in virus detection, contain self-modifying code, or are unlikely to be infected by a virus. Such files are usually skipped in validation checking because they may trigger a false alarm.

## executable (file)

A file containing coded instructions to be executed by the computer. Executable files include programs and overlays (auxiliary program code which cannot be executed directly by the user).

## expanded memory

Computer memory above the DOS 1MB limit of conventional memory that is accessed by memory paging. You need special software, conforming to an expanded memory specification, to take advantage of expanded memory.

## extended memory

Linear memory above the DOS 1MB limit of conventional memory. Often used for RAM disks and print spoolers.

## false alarm

Reporting a viral infection when none is present.

## fast

A scanning option that is faster than normal but less comprehensive (because it checks a smaller portion of each file).

## infected file

A file contaminated by a virus.

## macro virus

A virus that infects macros, such as those used by applications like Microsoft Word and Excel. Though the text of a document created in one of these applications contains no executable code, and therefore is not infectable, a document can carry infectable macros with it. Macro viruses are the fastest-growing segment of the worldwide virus threat—the number of known macro viruses doubles every three months.

## Master Boot Record (MBR)

A portion of a hard disk that contains a partition table that divides the drive into "chunks," some of which may be assigned to operating systems other than DOS. The MBR accesses the boot sector.

## memory

A storage medium where data or program code are kept temporarily while being used by the computer. DOS supports up to 640KB of conventional memory. Beyond that limit may be accessed as expanded memory, extended memory, or an upper memory block (UMB).

## memory infection

Contamination of memory by a virus. The only certain way to eliminate memory infection is to *shut down your computer,* restart from a clean start-up diskette, and clean up the source of the infection using VirusScan.

## modified file

A file that has changed after validation codes have been added, possibly by a virus.

## overlay infection

Virus contamination of a file containing auxiliary program code that is loaded by the main program.

## polymorphic virus

A virus that attempts to evade detection by changing its internal structure or its encryption techniques.

## read operation

Any operation in which information is read from a disk, including a hard drive, floppy diskette, CD-ROM, or network drive. DOS commands that perform read operations include DIR (directory listing), TYPE (display contents of a file), and COPY (copy files). See also “write operation.”

## recovery codes

Information that VirusScan records about an executable file in order to recover (repair) it if it is damaged by a virus. See also “validation codes.”

## self-modifying program

Software that changes its own program files, often to protect against viruses or illegal copying. These programs should be included in an exception list to prevent these modifications from being reported as a false alarm by VirusScan.

## system errors

Errors that can prevent VirusScan from completing its job successfully. System error conditions include disk format errors, media errors, file system errors, network errors, device access errors, and report failures.

## unknown virus

A virus not yet identified and listed in SCAN.DAT. VirusScan can detect unknown viruses by observing changes in files that could result from infection.

## upper memory block (UMB)

Memory in the range 640KB to 1024KB, just above the DOS 640KB limit of conventional memory.

## validate

To check that a file is authentic and has not been altered. Most validation methods rely on computing a statistic based on all the data in the file, which is unlikely to remain constant if the file itself is changed.

## validation codes

Information that VirusScan records about an executable file in order to detect subsequent infection by a virus. See also "recovery codes."

## virus

A software program that attaches itself to another program on a disk or lurks in a computer's memory, and spreads from one program to another. Viruses may damage data, cause computers to crash, display messages, and so on.

## warm boot

To restart (reset) a computer by pressing CTRL+ALT+DEL. See also "boot" and "cold boot."

## write operation

Any operation in which information is recorded to a disk. Commands that perform write operations include those that save, move, or copy files. See also "read operation."

## write protection

A mechanism to protect files or disks from being changed. A file may be write protected by changing its system attributes. A diskette may be write protected by sliding its movable corner tab so that the square hole is open (3.5" diskettes) or by covering its corner notch with a write-protect tab (5.25" diskettes).

# Index