McAfee VirusScan for Windows 95 and Windows 98

Getting Started Guide

Version 4.0.1

Network Associates
UK
Minton Place, Victoria St.
Windsor, Berkshire
SL4 1 EG
UK

Network Associates
Canada
139 Main Street, Suite 201
Unionville, Ontario
L3R 2G9
Canada

Network Associates
Australia
Level 1, 500 Pacific Highway
St. Leonards
NSW 2065
Australia

COPYRIGHT

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), WHICH SETS FORTH GENERAL LICENSE TERMS FOR NETWORK ASSOCIATES SOFTWARE. FOR THE SPECIFIC TERMS OF YOUR LICENSE, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees and subject to the terms and conditions of this Agreement, Network Associates hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or is bundled with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified individually for any of such Software products on the applicable product invoicing or packaging.

   a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all proprietary notices.

   b. **Server Use.** To the extent that the applicable product invoicing or packaging sets forth, you may install and use the Software on a Client Device or as a server ("Server") within a multi-user or networked environment ("Server Use") for either (i) connecting, directly or indirectly, to not more than the maximum number of specified Client Devices or "seats"; or (ii) deploying not more than the maximum number of agents (pollers) specified for deployment. If the applicable product invoicing or packaging does not specify a maximum number of Client Devices or pollers, this license gives you a single product use license subject to the provisions of subsection (a) above. A separate license is required for each Client Device or seat that can connect to the Software at any time, regardless of whether such licensed Client Devices or seats are connected to the Software concurrently, or are actually using the Software at any particular time.

Your use of software or hardware that reduces the number of Client Devices or seats that connect to and use the Software simultaneously (e.g., using “multiplexing” or “pooling” hardware or software) does not reduce the number of licenses you must have in total. Specifically, you must have that number of licenses that would equal the number of distinct inputs to the multiplexing or pooling software or hardware “front end.” If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses that you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits set forth in the product invoicing or packaging. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the proprietary notices for the Documentation.

c. **Volume Use.** If the Software is licensed with volume use terms specified in the applicable product invoicing or packaging, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume use terms specify. This license authorizes you to make or download one copy of the Documentation for each such copy of the Software you may make according to the volume use terms, provided that each such copy contains all of the proprietary notices for the Documentation. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software is installed does not exceed the number of licenses you have obtained.

2. **Term.** This license is effective for the period of time specified in the product invoicing or packaging, or in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of the Agreement set forth here conflict with the provisions of the product invoicing or packaging, the README.1ST document, the LICENSE.TXT document, the product invoice, package, or the other text document will constitute the terms of your license grant to use the Software. Either you or Network Associates may terminate your license earlier than the period specified in the appropriate document in accordance with the terms set forth therein. This Agreement and your license will terminate automatically if you fail to comply with any of the limitations or other requirements described. When this agreement terminates, you must destroy all copies of the Software and Documentation. You may terminate this Agreement at any point by destroying the Software and Documentation together with all copies of the Software and Documentation.

3. **Updates.** During the term of your license, you may download revisions, upgrades, or updates to the Software when Network Associates publishes them via its electronic bulletin board system, website or through other online services.

4. **Ownership Rights.** The Software and the Documentation are protected by United States copyright laws and international treaty provisions. Network Associates owns and retains all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. You acknowledge that your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and that you will not acquire any rights to the Software except as expressly set forth in this Agreement. You agree that any copies of the Software and Documentation will contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software, or permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement. You may not transfer any of the rights granted to you under this Agreement. You may not copy the Documentation accompanying the Software. You may not reverse engineer, decompile, or disassemble the Software, except to the extent that the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon the Software in whole or in part. You may not copy the Software except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by Network Associates. Network Associates reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

6. **Warranty and Disclaimer**

   a. **Limited Warranty.** Network Associates warrants that for thirty (30) days from the date of original purchase or distribution the media (for example, the diskettes) on which the Software is contained will be free from defects in materials and workmanship.

   b. **Customer Remedies.** Network Associates' and its suppliers' entire liability, and your exclusive remedy, shall be, at Network Associates' option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media on which the Software is contained with a copy on non-defective media. You must return the defective media to Network Associates at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent that Network Associates is subject to restrictions under United States export control laws and regulations.

   Warranty Disclaimer. To the maximum extent permitted by applicable law, and except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, NETWORK ASSOCIATES MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES, OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATIONS MIGHT NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

Your purchase of or payment for the Software may entitle you to additional warranty rights, which Network Associates will specify in the product invoicing or packaging you received with your purchase, or in the README.1ST , LICENSE.TXT or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the product invoice or packaging, the README.1ST, the LICENSE.TXT, or similar documents, the invoice, packaging, or text file will set forth the terms of your warranty rights for the Software.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL NETWORK ASSOCIATES OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL NETWORK ASSOCIATES BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE NETWORK ASSOCIATES CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF NETWORK ASSOCIATES SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

8. **United States Government.** The Software and accompanying Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department’s list of Specially Designated Nations or the United States Commerce Department’s Table of Denial Orders. By downloading or using the Software, you are agreeing to the foregoing provisions and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

   IN ADDITION, YOU SHOULD BE AWARE THAT EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH

RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE. SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR ON THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY BUSINESS OR PERSONAL USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST, THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION OF ENCRYPTION TECHNOLOGY TO, OR IMPORTATION FROM: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE THAT IT IS YOUR RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS, AND THAT NETWORK ASSOCIATES HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

11. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, “High Risk Activities”). Network Associates expressly disclaims any express or implied warranty of fitness for High Risk Activities.

12. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. The Agreement set forth here is advisory in nature and does not supersede the provisions of any Agreement set forth in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the README.1ST or the LICENSE.TXT document, the text document will constitute the terms of your license grant to use the Software. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Network Associates. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Network Associates or a duly authorized representative of Network Associates. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

13. **Network Associates Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact Network Associates for any other reason, please call (408) 988-3832, fax (408) 970-9727, write Network Associates, Inc. at 3965 Freedom Circle, Santa Clara, California 95054, or visit the Network Associates website at http://www.nai.com.

Table of Contents

Chapter 1. About McAfee VirusScan 9

What is VirusScan? 9

What comes with VirusScan? 10

Deciding when to scan for viruses 13

Recognizing when you don’t have a virus 13

How to contact Network Associates 14

Customer service 14

Technical support 15

Network Associates training 16

Comments and feedback 16

Reporting new items for anti-virus data file updates 16

International contact information 17

Chapter 2. Installing McAfee VirusScan 21

Before You Begin 21

System requirements 21

Installation Steps 22

Validating Your Files 32

Testing Your Installation 34

Chapter 3. Removing Infections From Your System 35

If you suspect you have a virus... 35

Creating an Emergency Disk without the utility 37

Responding to viruses or malicious software 39

Chapter 4. Using VShield 51

What does VShield do? 51

Why use VShield? 51

Which browsers and e-mail clients does VShield support? 52

Using the VShield configuration wizard 53

Using VShield’s shortcut menu 59

Disabling or stopping VShield 60

Chapter 5. Using McAfee VirusScan 63

What is VirusScan? 63

Starting VirusScan 63

Using VirusScan menus 64

Configuring VirusScan Classic 66

Index 73

About McAfee VirusScan 1

What is VirusScan?

VirusScan is the key desktop element in the Network Associates Total Virus Defense suite of security tools. It acts as a tireless online sentry, guarding your system against attacks from viruses and preventing harm from other malicious software. Its powerful set of scanning tools and other enhancements have kept it at the front rank of anti-virus software, but with this latest release, VirusScan adds McAfee WebScanX technology to its protective arsenal—an improvement that helps to keep you safe from threats to your system that have begun to emerge from the Internet.

Advanced web page designs, for example, can incorporate interactive elements composed of Java classes and ActiveX controls. At the same time, millions of users now exchange messages, files and other data via e-mail, often using “attachments” that consist of executable files, document templates and other data. But these convenient new technologies can also hide new dangers. Executable files infected with viruses can lurk on websites, often without the site owner’s knowledge, or can spread via e-mail, whether solicited or not. Sophisticated programmers can design Java applets or ActiveX controls that circumvent the security features built into your browser software to read data stored on your computer’s hard disk, forge e-mail messages to others in your name, or cause other types of harm.

In this environment, taking precautions to protect yourself from malicious software is no longer a luxury, but a necessity. Consider the extent to which you rely on the data on your computer and the time, trouble and money it would take to replace that data if it became corrupted or unusable because of a virus infection. Balance that possibility against the time and effort it takes to put a few common sense security measures in place, and you can quickly see the utility in protecting yourself against infection.

Even if your own data is relatively unimportant to you, neglecting to guard against viruses might mean that your computer could play unwitting host to a virus that could spread to computers that your co-workers and colleagues use. Checking your hard disk periodically with VirusScan significantly reduces your vulnerability to infection and keeps you from losing time, money and data unnecessarily.

VirusScan gives you the tools you need to keep your system intact and secure. Used properly as one part of a comprehensive security program that includes backups, meaningful password protection, training, and awareness, VirusScan can keep your computer safe from debilitating attacks and prevent the spread of malicious software throughout your network.

What comes with VirusScan?

VirusScan consists of several component sets that combine one or more related programs, each of which play a part in defending your computer against viruses and other malicious software. The component sets are:

- **Common Components.** This set consists of data files and other support files that many of the VirusScan component programs share. These files include VirusScan virus definition (.DAT) files, default configuration files, validation files, and other files.

- **Command-Line Scanner.** This set consists of a SCANPM.EXE, a powerful scanning agent for 32-bit environments, and BOOTSCAN.EXE, a smaller, specialized scanner. Both programs allow you to initiate targeted scan operations from the MS-DOS Prompt window or from protected MS-DOS mode. Ordinarily, you'll use VirusScan's graphical user interface (GUI) to perform most scanning operations, but if you have trouble starting Windows or if the VirusScan GUI components will not run in your environment, you can use the command-line scanners as a backup.

  SCANPM.EXE provides you with a full-featured scanner for 16- and 32-bit protected-mode DOS environments and includes support for extended memory and flexible memory allocations. To use the scanner, open an MS-DOS Prompt window or restart your computer in MS-DOS mode, then run SCANPM.EXE from the command line, together with the scan options you want. See Appendix E in the VirusScan User's Guide for a list and description of available options.

  VirusScan uses BOOTSCAN.EXE on its Emergency Disk in order to provide you with a virus-free boot environment. When you run the Emergency Disk creation wizard, VirusScan copies BOOTSCAN.EXE, a specialized set of .DAT files, and boot files to a single floppy disk. With this disk, you can start your computer, then scan its memory and the Master Boot Record, the boot sector, and the system files on your hard disk.

  BOOTSCAN.EXE will not detect or clean macro viruses, but it will detect or clean other viruses that can jeopardize your VirusScan installation or infect files at system startup. Once you identify and respond to those viruses, you can safely run VirusScan to clean the rest of your system, provided you don't run any other programs in the meantime.

- **VirusScan.** This component gives you unmatched control over your scanning operations. You can initiate a scan operation at any time—a feature known as "on-demand" scanning—specify local and network disks as scan targets, choose how VirusScan will respond to any infections it finds, and see reports on its actions. You can start with VirusScan's basic configuration mode, then move to its advanced mode for maximum flexibility. See "Using McAfee VirusScan" on page 63 for an overview.

- **VShield.** This component gives you continuous anti-virus protection from viruses borne on floppy disks, brought in from your network, or loaded into memory. VShield starts when you start your computer, and stays in memory until you shut down. A flexible set of property pages allows you to tell VShield which parts of your system to scan, when to scan them, which parts to leave alone, and how to respond to any infected files it finds. In addition, VShield can alert you when it finds a virus, and can generate reports that summarize each of its actions.

  This latest VShield version includes technology that guards against hostile Java applets and ActiveX controls. With this new capability, VShield can automatically scan e-mail messages and attachments that you receive from the Internet via Lotus cc:Mail, Microsoft Mail or other mail clients that comply with Microsoft's Messaging Application Programming Interface (MAPI). It can also filter out hostile Java classes and ActiveX controls by comparing those that it encounters with a database of classes and controls known to cause harm. When it detects a match, VShield can alert you, or it can automatically deny harmful objects access to your system. VShield can also keep your computer from connecting to dangerous Internet sites. Simply designate the sites your browser software should not visit, and VShield automatically prevents access. Secure password protection for your configuration options prevents others from making unauthorized changes. The same convenient dialog box controls configuration options for all VShield modules. See "Using VShield" on page 51 for an overview.

- **cc:Mail Scan.** This component includes technology optimized for scanning Lotus cc:Mail mailboxes that do not use the MAPI standard. Install and use this component if your workgroup or network uses cc:Mail v7.x or earlier. See "Choosing Detection options" on page 87 of the User's Guide for details.

- **MAPI Scanner**. This component allows you to scan, at your initiative, the Inbox or other mailboxes for MAPI-compliant e-mail client applications. Use it to supplement the continuous background scanning VShield provides for MAPI clients such as Microsoft Exchange and Microsoft Outlook. See "Scanning Microsoft Exchange and Outlook mail" on page 191 of the *VirusScan User's Guide* for details.

- **VirusScan Scheduler.** This component allows you to create tasks for VirusScan to perform. A "task" can include anything from running a scan operation on a set of disks at a specific time or interval, to setting up VShield to run with particular options. The Scheduler comes with a preset list of tasks that ensures a minimal level of protection for your system—you can, for example, immediately scan and clean your C: drive or all disks on your computer, and enable or disable VShield. See "Scheduling Scan Tasks" on page 147 of the *VirusScan User's Guide* for details.

- **McAfee ScreenScan**. This optional component scans your computer as your screen saver runs during idle periods. See "Using ScreenScan" on page 194 of the *VirusScan User's Guide* for details.

- **Documentation.** VirusScan documentation includes:
  - This printed *Getting Started Guide*, which introduces the product, provides installation instructions, outlines how to respond if you suspect your computer has a virus, and provides a brief product overview. The *Getting Started Guide* comes only with the VirusScan copies distributed on CD-ROM discs—you cannot download it from Network Associates website or from other electronic services.
  - A *User's Guide* saved on the VirusScan CD-ROM or installed on your hard disk in Adobe Acrobat .PDF format. The *VirusScan User's Guide* describes in detail how to use VirusScan and includes other information useful as background or as advanced configuration options. Acrobat .PDF files are flexible online documents that contain hyperlinks, outlines and other aids for easy navigation and information retrieval.

    For best results when opening and printing the *User's Guide*, Network Associates recommends using Acrobat Reader 3.0—Reader version 3.0.1 has difficulty correctly printing graphics included in the .PDF file.
  - An online help file. This file gives you quick access to hints and tips about how to use VirusScan. To open the help file from within VirusScan or from within VirusScan Scheduler, choose **Help Topics** from the **Help** menu.

    VirusScan also includes context-sensitive online help. Right-click buttons, lists or other elements within dialog boxes to see brief, descriptive help topics. Click **Help** buttons where you see them to open the main help file to a relevant topic.
  - A README.1ST or LICENSE.TXT file. This file outlines the terms of your license to use VirusScan. Read it carefully—by installing VirusScan you agree to its terms.
  - A WHATSNEW.TXT file. This file contains last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and often describes new product features incorporated into incremental product updates. You'll find the WHATSNEW.TXT file at the root level of your VirusScan CD-ROM disc or in the VirusScan program folder—you can open and print it from Windows Notepad, or from nearly any word-processing software.

Deciding when to scan for viruses

Maintaining a secure computing environment means scanning for viruses regularly. Depending on the degree to which you swap floppy disks with other users, share files over your local area network, or interact with other computers via the Internet, scanning "regularly" could mean scanning as little as once a month, or as often as several times a day. Other good habits to cultivate include scanning right before you back up your data, scanning before you install new or upgraded software, particularly software you download from other computers, and scanning when you start or shut down your computer each day. Use VShield to scan your computer's memory and maintain a constant level of vigilance between scanning operations. Under most circumstances this should protect your system's integrity.

If you connect to the Internet frequently or download files often, you might want to supplement regular scans with scans based on certain events. VirusScan includes a default set of scanning tasks to help you monitor your system at likely points of virus entry, such as

- whenever you insert a floppy disk into your computer's floppy drive
- whenever you start an application or open a file
- whenever you connect to or map a network drive to your system

Even the most diligent scanning can miss new viruses, however, if your scanning software is not up to date. Your VirusScan purchase entitles you to free virus updates for the life of your product, so you can update frequently to keep current. If you install the Network Associates SecureCast client software, VirusScan will even tell you when you should update your data files and offer to download them for you. To learn how to update your software, see Appendix A, "Using SecureCast to Update Your Software" and "Configuring AutoUpdate options" on page 173 of the VirusScan User's Guide.

Recognizing when you don't have a virus

Personal computers have evolved, in their short lifespan, into highly complex machines that run ever more complicated software. Even the most farsighted of the early PC advocates could never have imagined the tasks for which workers, scientists and others have harnessed the modern PC's speed, flexibility and power. But that power comes with a price: hardware and software conflicts abound, applications and operating systems crash, and hundreds of other problems can crop up in unlikely places. In some cases, these failures can resemble the sorts of effects that you see when you have a virus infection with a destructive payload. Other computer failures seem to defy explanation or diagnosis, so frustrated users blame virus infections, perhaps as a last resort.

Because viruses do leave traces, however, you can usually eliminate a virus infection as a possible cause for computer failure relatively quickly and easily. Running a full VirusScan system scan will uncover all of the known virus variants that can infect your computer, and quite a few of those that have no known name or defined behavior. Although that doesn't give you much help when your problem really results from an interrupt conflict, it does allow you to eliminate one possible cause. With that knowledge, you can then go on to troubleshoot your system with a full-featured system diagnosis utility such as McAfee Nuts & Bolts.

More serious is the confusion that results from virus-like programs, virus hoaxes, and real security breaches. Anti-virus software simply cannot detect or respond to such destructive agents as Trojan horse programs that have never appeared previously, security breaches that enable hackers to prevent network access and crash systems, or the perception that a virus exists where none in fact does.

The best way to determine whether your computer failure resulted from a virus attack is to run a complete scan operation, then pay attention to the results. If VirusScan does not report a virus infection, the chances that your problem results from one are slight—look to other causes for your difficulties. Furthermore, in the very rare event that VirusScan does miss a macro virus or another virus type that has in fact infected your system, the chances are relatively small that serious failures will follow in its wake. You can, however, rely on Network Associates researchers to identify, isolate, and update VirusScan immediately to detect and, if possible, remove the virus when you next encounter it. To learn how you can help the virus researchers help you, see "Reporting new items for anti-virus data file updates" on page xxi of the VirusScan User's Guide.

How to contact Network Associates

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department at +31 20 586 61 00 or write to the following address:

Network Associates International B.V.
Gatwickstraat 25
1043 GL Amsterdam
The Netherlands

Technical support

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

World Wide Web	http://support.nai.com

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

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@nai.com
CompuServe	GO NAI
America Online	keyword MCAFEE

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

For corporate-licensed customers:

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

For retail-licensed customers:

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

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

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers

- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

Network Associates training

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

Comments and feedback

Network Associates appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please address your comments about Network Associates anti-virus product documentation to: Network Associates, Inc., 15220 NW Greenbrier Parkway, Suite 100, Beaverton, OR 97006-5762, U.S.A. You can also send faxed comments to (503) 531-7655 or e-mail to tvd_documentation@nai.com.

Reporting new items for anti-virus data file updates

Network Associates anti-virus software offers you the best available detection and removal capabilities, including advanced heuristic scanning that can detect new and unnamed viruses as they emerge. Occasionally, however, an entirely new type of virus that is not a variation on an older type can appear on your system and escape detection. Because Network Associates researchers are committed to providing you with effective and up-to-date tools you can use to protect your system, please tell them about any new Java classes, ActiveX controls, dangerous websites, or viruses that your software does not now detect. Note that Network Associates reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

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

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

virus_research_europe@nai.com

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

avert-jp@nai.com
Use this address to report harmful items to our office in Japan.

avert_apac@nai.com
Use this address to report harmful items to our Asia-Pacific office.

International contact information

To contact Network Associates outside the United States, use the addresses, phone numbers and fax numbers below.

Network Associates
Australia

Level 1, 500 Pacific Highway
St. Leonards, NSW
Sydney, Australia 2065
Phone: 61-2-8425-4200
Fax: 61-2-9439-5166

Network Associates
Austria

Pulvermuehlstrasse 17
Linz, Austria
Postal Code A-4040
Phone: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates
Belgium

Bessenveldtstraat 25a
Diegem
Belgium - 1831
Phone: 32-2-716-4070
Fax: 32-2-716-4770

Network Associates
do Brasil

Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasil
Phone: (55 11) 5505 1009
Fax: (55 11) 5505 1006

Network Associates
Canada

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

Network Associates
People’s Republic of China

New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Beijing
People’s Republic of China 100044
Phone: 8610-6849-2650
Fax: 8610-6849-2069

NA Network Associates Oy

Kielotie 14 B
01300 Vantaa
Finland
Phone: 358 9 836 2620
Fax: 358 9 836 26222

Network Associates France S.A.

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

Network Associates Deutschland GmbH

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

Network Associates Hong Kong

19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Phone: 852-2832-9525
Fax: 852-2832-9530

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italy
Phone: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

Network Associates Japan, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001 Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0781

Network Associates Latin America

150 South Pine Island Road, Suite 205
Plantation, Florida 33324
United States
Phone: (954) 452-1731
Fax: (954) 236-8031

Network Associates de Mexico

Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico City, Mexico D.F. 11560
Phone: (525) 282-9180
Fax: (525) 282-9183

Network Associates
International B.V.

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

Net Tools Network Associates
South Africa

Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
South Africa 2021
Phone: 27 11 706-1629
Fax: 27 11 706-1569

Network Associates
Spain

Orense 4, 4th Floor
Edificio Trieste
28020 Madrid
Spain
Phone: 34 91 598 18 00
Fax: 34 91 556 14 01

Network Associates
AG

Baeulerwisenstrasse 3
8152 Glattbrugg
Switzerland
Phone: 0041 1 808 99 66
Fax: 0041 1 808 99 77

Network Associates
Portugal

Av. de Liberdade, 114
1250 Lisboa
Portugal
Phone: 351 1 340 45 43
Fax: 351 1 340 45 75

Network Associates
South East Asia

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

Network Associates
Sweden

Datavägen 3A
Box 596
S-175 26 Järfälla
Sweden
Phone: 46 (0) 8 580 88 400
Fax: 46 (0) 8 580 88 405

Network Associates
International Ltd.

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EF
United Kingdom
Phone: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

Installing McAfee VirusScan 2

Before You Begin

Network Associates distributes McAfee VirusScan in two ways: as an archived file that you can download from the Network Associates website or from other electronic services; and on CD-ROM disc. Once you have downloaded a VirusScan archive or placed your VirusScan installation disc in your CD-ROM drive, the installation steps you follow after that are the same for each type of distribution. Review the system requirements shown below to verify that VirusScan will run on your system, then follow the installation steps on page 22.

☐ **NOTE:** Some VirusScan component sets come only with the CD-ROM version of the product. Consult your sales representative for details.

System requirements

VirusScan will install and run on any IBM PC or PC-compatible computer equipped with:

- A processor equivalent to an Intel 80386, or later. Network Associates recommends at least an Intel Pentium-class or compatible processor.
- A CD-ROM drive. If you downloaded your copy of VirusScan, this is an optional item.
- At least 15MB of free hard disk space for a full installation.
- At least 8MB of free random-access memory (RAM).
- Either Microsoft Windows 95 or Windows 98.

Other recommendations

To take full advantage of VirusScan's automatic update features, you should have an Internet connection, either through your local-area network, or via a high-speed modem and an Internet service provider.

☐ **NOTE:** Network Associates does *not* provide Internet connections. Contact a local service provider to learn about rates and terms of service, or see your system administrator to learn about connecting to the Internet through your office network.

Installation Steps

Note which type of VirusScan distribution you have, then follow the corresponding steps to prepare your files for installation.

- **If you downloaded your copy of VirusScan** from the Network Associates website, from a server on your local network, or from another electronic service, make a new, temporary folder on your hard disk, then use WinZip, PKZIP, or a similar utility to extract the VirusScan installation files to that temporary folder. You can download the necessary utilities from most online services.

> 🔔 **IMPORTANT:** If you suspect that your computer has a virus infection, download the VirusScan installation files onto a computer that is ***not*** infected. Install your copy on this computer, then use the McAfee Emergency Disk utility during setup to make a disk you can use to boot your infected computer and remove the virus. See “If you suspect you have a virus...” on page 35 for more information.

- **If your copy of VirusScan came on a CD-ROM disc**, insert that disc into your computer’s CD-ROM drive.

If you inserted a CD-ROM disc, you should see a VirusScan welcome image similar to that shown in Figure 2-1 appear automatically.

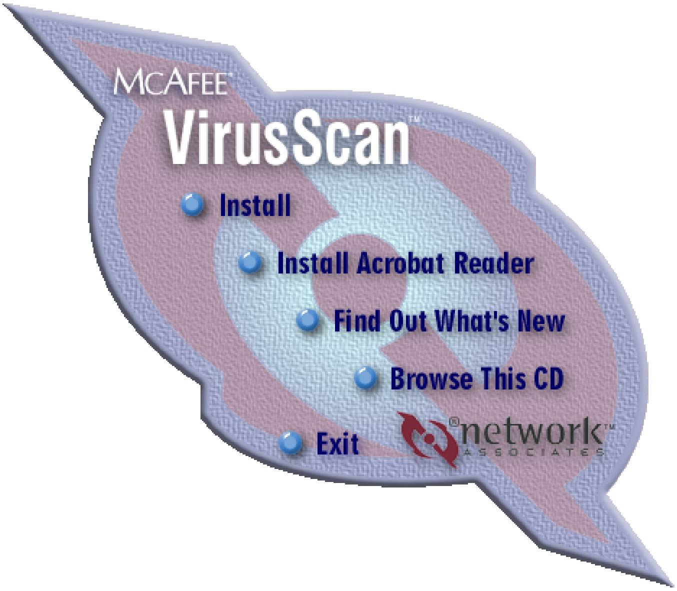


Figure 2-1. McAfee VirusScan welcome image

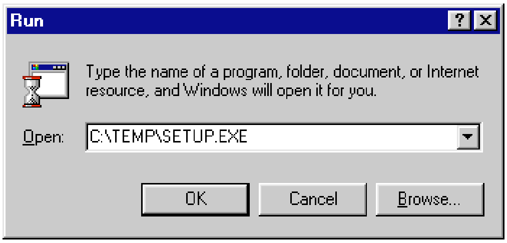
To install VirusScan immediately, click **Install**, then skip to Step 3 on page 24 to continue with Setup.

If the welcome image does not appear, or if you are installing VirusScan from files you downloaded, start with Step 1.

Follow these steps:

1. Choose **Run** from the **Start** menu in the Windows taskbar.

   The Run dialog box will appear (Figure 2-2).



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: C:\TEMP\SETUP.EXE

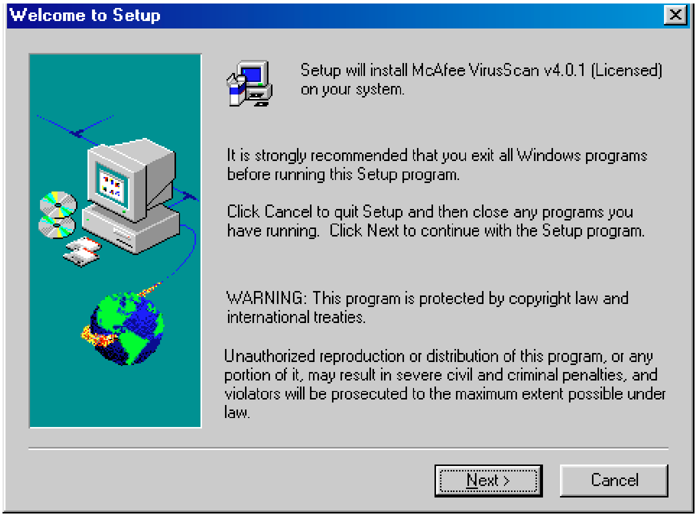
Figure 2-2. Run dialog box

2. Type `<X>:\SETUP.EXE` in the text box provided, then click **OK**.

   Here, <X> represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted VirusScan files. To search for the correct files on your hard disk or CD-ROM disc, click **Browse**.

   NOTE: If your VirusScan copy came on a VirusScan Security Suite or a Total Virus Defense CD-ROM disc, you must also specify which folder contains VirusScan for Windows 95 and Windows 98. See the CONTENTS.TXT file included with either CD-ROM disc for details.

   Setup will start and display its welcome panel (Figure 2-3).



Setup will install McAfee VirusScan v4.0.1 (Licensed) on your system.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and violators will be prosecuted to the maximum extent possible under law.

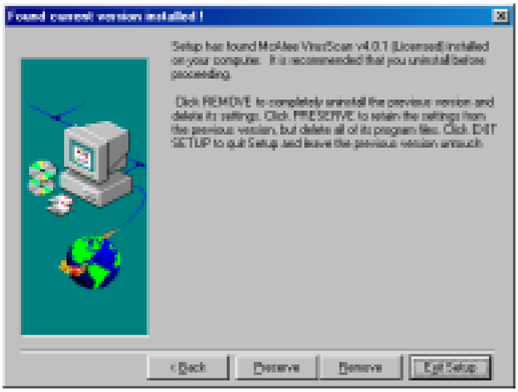
Figure 2-3. Welcome to Setup wizard panel

3. Click **Next>** to continue.

   The next wizard panel displays the VirusScan end-user license agreement. Read this agreement carefully—if you install VirusScan, you agree to abide by the terms of the license.

4. If you do not agree to the license terms, click **No**. Setup will quit immediately. Otherwise, click **Yes** to continue.

   If you install this version of VirusScan over an existing version of VirusScan, Setup will detect the existing version and offer to remove it from your computer (Figure 2-4).



Setup has found McAfee VirusScan v4.0.1 (Licensed) installed on your computer. It is recommended that you uninstall before proceeding.

Click REMOVE to completely uninstall the previous version and delete its settings. Click PRESERVE to retain the settings from the previous version, but delete all of its program files. Click EXIT SETUP to quit Setup and leave the previous version untouch

Figure 2-4. Found Current Version Installed panel

5. To continue, you can

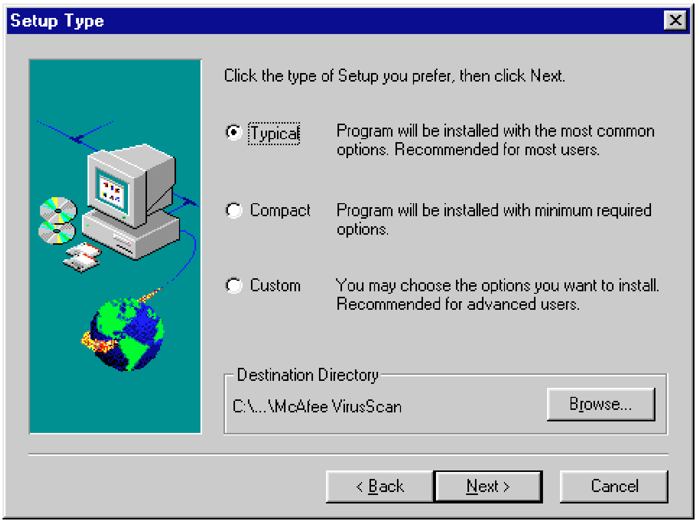
   - Click **Preserve** to retain the settings you chose for the existing VirusScan installation. Setup will retain the settings files, but will remove the rest of the VirusScan program files.

     NOTE: Setup will preserve settings only for VirusScan v4.0.1 and later. If will make every attempt to preserve settings from VirusScan v3.x, but will not attempt to preserve settings from VirusScan v2.x, or WebScanX v3.1.6 or earlier.

   - Click **Remove** to delete the existing VirusScan version and all of its settings from your computer. When it has finished removing the existing VirusScan version, Setup will display the panel shown in Figure 2-5 on page 25. You can then continue with Step 6.

   - Click **Exit Setup** to stop the installation altogether. Setup will prompt you to confirm that you want to quit. Click **Exit Setup** again to quit, or click **Resume** to continue with the installation.

   If you continue, Setup will remove your existing VirusScan version, making sure to preserve your earlier settings if you chose that option. When it finishes removing the earlier VirusScan version, it will display the Setup Type panel (Figure 2-5).



Setup Type

Click the type of Setup you prefer, then click Next.

● Typical — Program will be installed with the most common options. Recommended for most users.

○ Compact — Program will be installed with minimum required options.

○ Custom — You may choose the options you want to install. Recommended for advanced users.

Destination Directory

C:\...\McAfee VirusScan

Figure 2-5. Setup Type panel

6. Select the VirusScan component sets that you want to install. You can choose from these options:

- **Typical.** Select this option to install the VirusScan command-line scanner; the VirusScan on-demand scanner; the VShield on-access scanner; the MAPI client scanner; the VirusScan Scheduler, and common files that all program components use. Network Associates recommends this installation for most users.

- **Compact.** Select this option to install the VirusScan command-line scanners, the VShield on-access scanner, and the VirusScan on-demand scanner. Network Associates recommends this option if you have minimal free disk space or other system constraints.

- **Custom.** Select this option to choose which VirusScan components you want to install. By default, the Custom option installs the same components as the Typical installation, but you can also choose to install cc:Mail Scan, a plug-in option that enables VShield to look for viruses in your Lotus cc:Mail Inbox, and ScreenScan, a scanning utility that examines your system for viruses whenever your screen saver activates.

7. Click **Browse** to locate the folder you want to use for the installation. By default, Setup installs VirusScan in this path:

   C:\Program Files\Network Associates\McAfee VirusScan

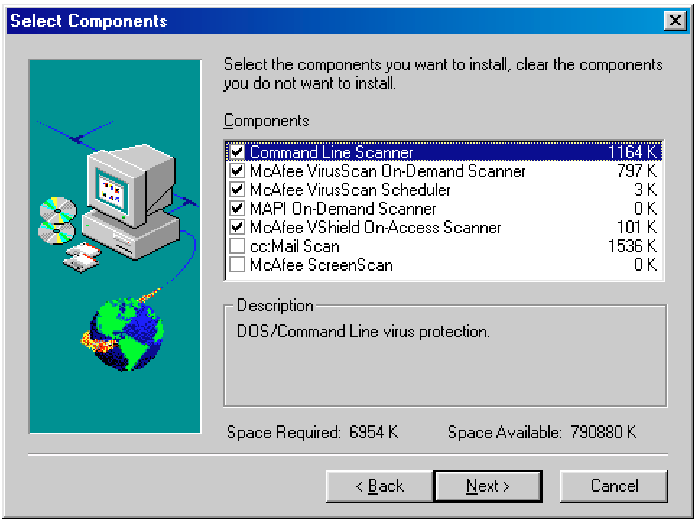
8. When you have chosen the component set that you want to install and have specified a destination, click **Next>** to continue.

   - **If you chose a Typical or a Compact component set**, Setup will show you a wizard panel that confirms your choice of components and the destination directory you specified. By default, Setup will look for existing viruses in your hard disk’s partition and boot sectors, and in your computer’s memory, before it installs VirusScan. Setup also adds a **Scan** command to the shortcut menus that appear when you right-click objects on your desktop or in Windows Explorer.

     If the options shown reflect your choices, click **Next>**. Otherwise, click **<Back** to change them. **Skip to** Step 9 on page 27.

   - **If you chose a Custom component set**, Setup shows you a wizard panel that lists the components available for installation (Figure 2-6). Select the components you want installed and clear the checkboxes next to those you don’t want.

     As you select each component, a description appears near the bottom of the panel. When you have finished your selections, click **Next>**.



Select Components

Select the components you want to install, clear the components you do not want to install.

Components

☑ Command Line Scanner	1164 K
☑ McAfee VirusScan On-Demand Scanner	797 K
☑ McAfee VirusScan Scheduler	3 K
☑ MAPI On-Demand Scanner	0 K
☑ McAfee VShield On-Access Scanner	101 K
□ cc:Mail Scan	1536 K
□ McAfee ScreenScan	0 K

Description

DOS/Command Line virus protection.

Space Required: 6954 K Space Available: 790880 K

Figure 2-6. Select Components panel

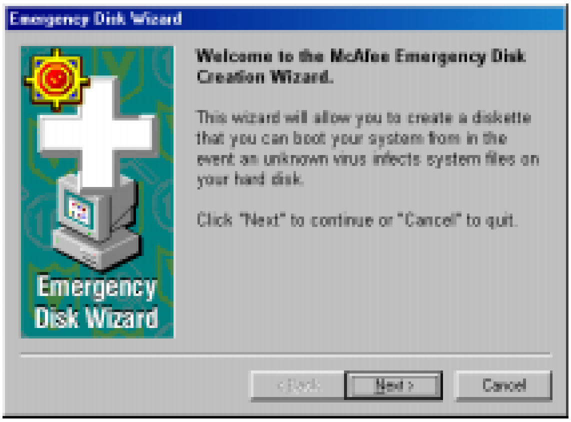
By default, Setup will have VirusScan look for existing viruses in your hard disk’s partition and boot sectors, and in your computer’s memory, before it completes installation. Setup will also add a Scan command to the shortcut menus that appear when you right-click an object on your desktop or in Windows Explorer. Click **Next>** at the bottom of each of the next two panels to continue.

If you do not want Setup to take these actions, clear each checkbox as it appears in each panel, then click **Next>** to continue.

Setup will next start VirusScan briefly to examine your hard disk and memory for viruses before it continues.

9. If VirusScan reports a clean system, click **OK** to continue. If VirusScan detects a virus infection, quit Setup immediately. See “If you suspect you have a virus...” on page 35 to learn what to do next.

10. Setup will begin copying VirusScan files to your computer. As it nears the end of the copy process, Setup will ask you whether you want to create an Emergency Disk (Figure 2-7).



Welcome to the McAfee Emergency Disk Creation Wizard.

This wizard will allow you to create a diskette that you can boot your system from in the event an unknown virus infects system files on your hard disk.

Click "Next" to continue or "Cancel" to quit.

Figure 2-7. Emergency Disk Wizard panel

11. To skip this step, click **Cancel**, then move to Step 16—you can create an Emergency Disk after installation. To create an Emergency Disk now, click **Next>**.

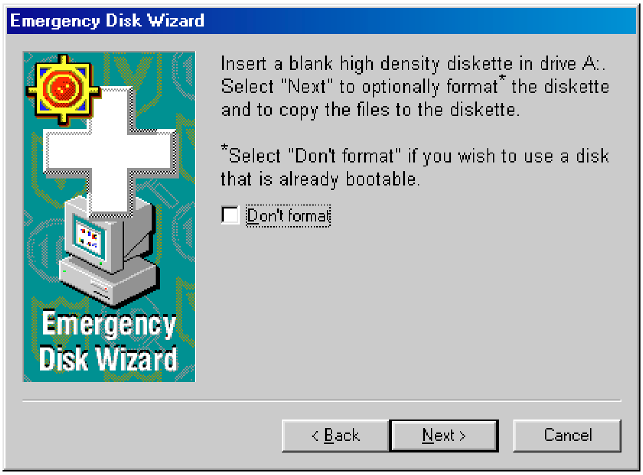
NOTE: Network Associates strongly recommends that you create an Emergency Disk during installation, but after VirusScan has scanned your system for viruses. If VirusScan detects a virus on your system, do *not* create an Emergency Disk on the infected computer.

---

12. The next wizard panel appears (see Figure 2-8 on page 29). Here, you have two choices:

    - If you have a *virus-free, formatted* floppy disk that contains only DOS or Windows system files, insert it into your floppy drive. Next, select the **Don’t format** checkbox, then click **Next>** to continue.

      This tells the Emergency Disk wizard to copy only the VirusScan Command Line component and its support files to the floppy disk. Skip to Step 13 on page 30 to continue.



Emergency Disk Wizard

Insert a blank high density diskette in drive A:. Select "Next" to optionally format* the diskette and to copy the files to the diskette.

*Select "Don't format" if you wish to use a disk that is already bootable.

□ Don't format

Figure 2-8. Second Emergency Disk Wizard panel

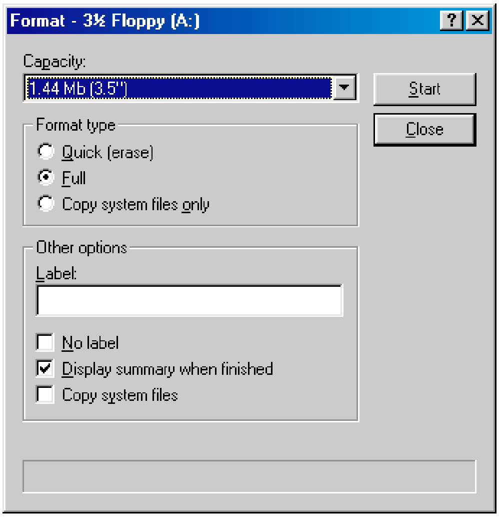
- If you do *not* have a virus-free floppy disk formatted with DOS or Windows system files, you must create one in order to use the Emergency Disk to start your computer. Follow these substeps:

  a. Insert an *unformatted* floppy disk into your floppy drive.

  b. Verify that the **Don’t format** checkbox is clear.

  c. Click **Next>**.

  The Windows disk format dialog box appears (Figure 2-9).



Format - 3½ Floppy (A:)

Capacity: 1.44 Mb (3.5")

Format type
○ Quick (erase)
● Full
○ Copy system files only

Other options
Label:
□ No label
☑ Display summary when finished
□ Copy system files

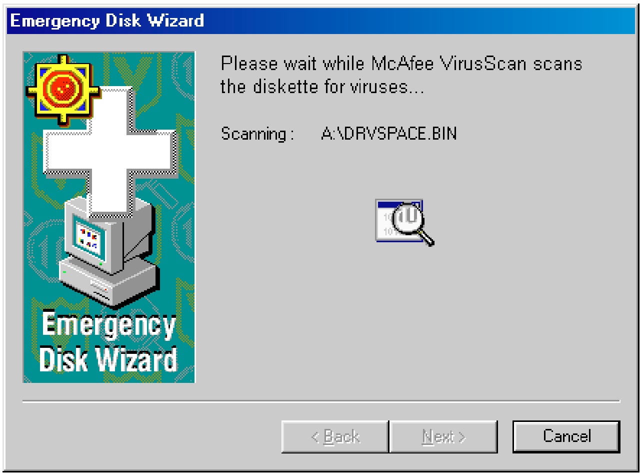
Figure 2-9. Windows format dialog box

d. Verify that the **Full** checkbox in the **Format type** area and the **Copy system files** checkbox in the **Other Options** area are both selected. Next, click **Start**.

   Windows will format your floppy disk and copy the system files necessary to start your computer.

e. Click **Close** when Windows has finished formatting your disk, then click **Close** again to return to the Emergency Disk panel.

13. Click **Next>** to continue. Setup will scan your newly formatted disk for viruses (Figure 2-10).



Emergency Disk Wizard

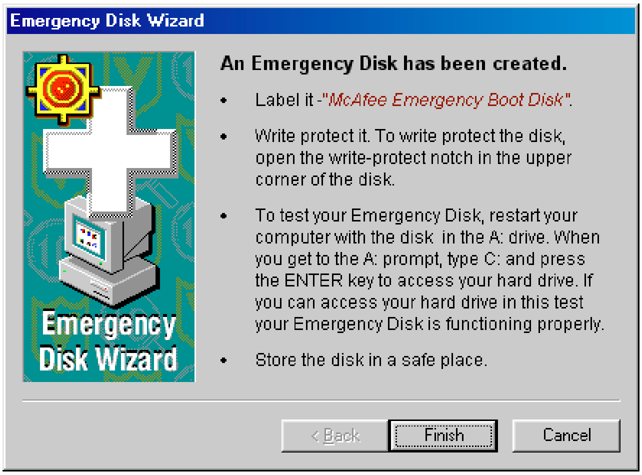
Please wait while McAfee VirusScan scans the diskette for viruses...

Scanning : A:\DRVSPACE.BIN

Figure 2-10. Scanning Emergency Disk for viruses

If VirusScan does not detect any viruses during its scan operation, Setup will immediately copy BOOTSCAN.EXE and its support files to the floppy disk you created. If VirusScan *does* detect a virus, quit Setup immediately. See “If you suspect you have a virus...” on page 35 to learn what to do next.

14. When the wizard finishes copying the Emergency Disk files, it displays the final wizard panel (Figure 2-11).



An Emergency Disk has been created.

- Label it -"*McAfee Emergency Boot Disk*".
- Write protect it. To write protect the disk, open the write-protect notch in the upper corner of the disk.
- To test your Emergency Disk, restart your computer with the disk in the A: drive. When you get to the A: prompt, type C: and press the ENTER key to access your hard drive. If you can access your hard drive in this test your Emergency Disk is functioning properly.
- Store the disk in a safe place.

Figure 2-11. Final Emergency Disk wizard panel

15. Click **Finish** to return to Setup. Next, remove the new Emergency Disk from your floppy drive, label it, lock it, and store it in a safe place.

NOTE: A locked floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position.

Setup will finish copying the VirusScan installation files to your hard disk, then it will list the names of the system files it changed. Setup lists AUTOEXEC.BAT because it adds a line to that file that tells VirusScan to run scan operation each time you start your computer. Setup also backs up your original AUTOEXEC.BAT file and renames it with a different extension in case you need to restore it.

16. Note the file name Setup uses to rename AUTOEXEC.BAT for future reference, then click **Next>** to continue.

17. Setup requires you to restart your computer in order to complete your VirusScan installation. This also ensures that the VShield component begins scanning for viruses immediately. If you have other work you must do, select **No, I will restart my computer later**, then click **Finish**. Otherwise, select **Yes, I want to restart my computer now**, then click **Finish** to reboot your system.

IMPORTANT: Network Associates strongly suggests that you reboot immediately in order to activate VShield's anti-virus protection. If you downloaded your VirusScan copy and want to validate it, do so *before* you reboot. See “Validating Your Files” to learn how to perform this check.

If you administer a network and want to learn how to install VirusScan across that network with minimal user interaction, see “Performing a silent installation” on page 40 of the *VirusScan User’s Guide*. There you will find complete instructions for “recording” your installation options, editing some configuration information in VirusScan’s setup file, and running Setup in its “silent” mode.

Validating Your Files

Downloading or copying files from any outside source places your computer at risk of virus infection—even if the risk is small. Downloading anti-virus software is no exception. Network Associates uses strict and extensive security measures to ensure that the products you purchase and download from its website and its other electronic services are safe, reliable, and free from virus infections. But anti-virus software tends to attract the attention of virus- and Trojan-horse writers, some of whom find it amusing to post infected copies of commercial software, or use the same file names to camouflage their own work.

You can protect yourself from this possibility, or from the possibility that the files you downloaded have become corrupted, by ensuring that you

- Download your files only from the Network Associates website; and
- Validate the files you download.

Network Associates includes a copy of VALIDATE.EXE, its validation software, with each VirusScan package.

To validate your files, follow these steps:

1. Install VirusScan as described in “Installation Steps” on pages 22 to 31.
2. Click **Start** in the Windows taskbar, point to **Programs**, then choose **MS-DOS Prompt**.
3. In the window that appears, change your command-line prompt to point to the directory that contains the VirusScan files you installed. If you chose the default installation options, you’ll find the files in this path:

   C:\Program Files\Network Associates\McAfee VirusScan

To get to this directory, type `cd progra~1\networ~1\mcafee~1` at the command-line prompt, then press ENTER. If you installed VirusScan in a different directory, type the correct path to that directory.

4. Run VALIDATE.EXE. To do so, type `validate *.*` at the command-line prompt.

   VALIDATE.EXE scans all of the files stored in your VirusScan program directory, then generates a file list that includes the file name, its size in bytes, its creation date and time, and two validation codes in separate columns.

   To use VALIDATE.EXE to examine individual files, simply follow `validate` with the name of the file you want to verify at the prompt, or use the DOS wildcards `?` and `*` to specify a range of files.

   NOTE: Network Associates recommends that you redirect the output from VALIDATE.EXE to your printer so that you can review it easily. If you have set your printer to capture output from MS-DOS programs, simply type `validate *.* >prn` at the command-line prompt. To learn how to set your printer to print from MS-DOS programs, consult your Windows documentation.

   To ensure that you have exactly the same files as did the engineers who packaged your copy of VirusScan, you need to compare the validation codes against the packing list supplied with the program. The packing list is a text file that contains the validation codes that Network Associates engineers generated from independent cyclical redundancy check (CRC) processes when they packaged VirusScan for delivery. This method provides a high degree of security and prevents tampering.

5. To display the packing list, type `type packing.lst` at the command-line prompt, then press ENTER.

   NOTE: Network Associates again recommends that you redirect the output from PACKING.LST to your printer. To do so, type `type packing.lst >prn` at the command-line prompt.

6. Compare the output from VALIDATE.EXE to that from PACKING.LST. The sizes, creation dates and times, and validation codes for each executable file name—that is, those with .EXE and .DLL extensions —should match exactly. If they do not, delete the file immediately— do *not* open the file or examine it with any other utility; doing so can risk virus infection.

IMPORTANT: Checking your VirusScan installation with VALIDATE.EXE does not *guarantee* that your copy is free from defects, copying errors, virus infections or tampering, but the program’s security features make it extremely unlikely that anyone has tampered with files that have correct validation codes. See the files LICENSE.TXT or README.1ST included with your copy of VirusScan to learn the license terms that cover your use of the program.

Validation codes for some files, including those with .INI, .VSC, and .VSH extensions, *might not match* those shown in PACKING.LST, as Setup can make changes to these files during installation.

Testing Your Installation

Once you install it, VirusScan is ready to scan your system for infected files. You can test whether it has installed correctly and verify that it can properly scan for viruses by implementing a test developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

To test your installation, follow these steps:

1. Open a standard Windows text editor, such as Notepad, then type:

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

NOTE: The line shown above should appear as *one line* in your text editor window. If you are reading this manual on your computer, you can copy the line directly from the Acrobat file to Notepad.

2. Save the file with the name EICAR.COM. The file size will be 69 or 70 bytes.

3. Start VirusScan and allow it to scan the directory that contains EICAR.COM. When VirusScan examines this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

IMPORTANT: This file is *not a virus*—it cannot spread or infect other files, or otherwise harm your system. Delete the file when you have finished testing your installation to avoid alarming other users.

Removing Infections From Your System 3

If you suspect you have a virus...

First of all, don’t panic! Although far from harmless, *most* viruses that infect your machine will not destroy data, play pranks, or render your computer unusable. Even the comparatively rare viruses that do carry a destructive payload usually produce their nasty effects in response to a trigger event. In most cases, unless you actually see evidence of a payload that has activated, you will have time to deal with the infection properly. The very presence of these small snippets of unwanted computer code can, however, interfere with your computer’s normal operation, consume system resources and have other undesirable effects, so you should take them seriously and be sure to remove them when you encounter them.

A second idea to keep in mind is that odd computer behavior, unexplained system crashes, or other unpredictable events might have causes other than virus infections. If you believe you have a virus on your computer because of occurrences such as these, scanning for viruses might not produce the results you expect, but it will help eliminate one potential cause of your computer problems.

The safest course of action you can take is to install VirusScan and perform an immediate and thorough system scan.

As it installs itself, VirusScan will examine your computer’s memory and your hard disk’s boot sectors to verify that it can safely copy its files to your hard disk without risking their infection. If VirusScan reports during setup that your system appears virus-free, continue with the installation, then perform a full system scan as soon as you restart your computer—file-infector viruses that don’t load into your computer’s memory or hide in your hard disk’s boot blocks might still be lurking somewhere on your system. See Chapter 2, “Installing McAfee VirusScan,” to learn about virus scanning during setup. See Chapter 5, “Using McAfee VirusScan,” to learn how to perform a full system scan.

If VirusScan detects a virus during Setup, you’ll need to remove it from your system before you install the program. To learn how to do so, follow the steps that begin on page 36.

IMPORTANT: To ensure maximum security, you should follow these same steps if VirusScan detects a virus in your computer’s memory later, after you have it installed.

If VirusScan found an infection during installation, follow these steps carefully:

1. Quit Setup immediately, then shut down your computer.

   Be sure to turn the power to your system off completely. Do *not* press CTRL+ALT+DEL or your computer's reset button to restart your system—some viruses can remain intact during this type of "warm" reboot.

2. If your copy of VirusScan came with an Emergency Disk, insert it into your floppy drive.

   NOTE: If your VirusScan copy did not come with a McAfee Emergency Disk, or if you have misplaced your Emergency Disk, you must create a new disk on an *uninfected* computer. Locate a computer that you know is virus-free, then follow the steps outlined in "Creating an Emergency Disk without the utility" on page 37.

3. Start your computer again.

   The Emergency Disk will boot your computer and immediately start BOOTSCAN.EXE, a special-purpose command-line scanner. The program will ask you whether you turned the power to your computer off before you started it with the Emergency Disk. If you did, press Y on your keyboard, then continue with Step 4. If you did not, press N, then turn your computer completely off and begin again.

   Once you start it, BootScan will report its progress as it scans your system, and will try to remove virus code from any infected files it finds. After it completes its scan operation, it will show you its final results: how many files it scanned; how many infected files it found; whether it found a virus in memory or in the boot blocks on your hard disk; and other information.

4. When BootScan finishes examining your system, you can either:

   - **Return to working with your computer.** If BootScan did not find a virus, or if it cleaned any infected files it did find, remove the Emergency Disk from your floppy drive, then restart your computer normally. If you had planned to install VirusScan on your computer but stopped when Setup found an infection, you can now continue with your installation.

   - **Try to clean or delete infected files yourself.** If BootScan found a virus that it could not remove, it will identify the infected files and tell you that it could not clean them, or that it does not have a current remover for the infecting virus.

As your next step, you can:

- **Locate and delete the infected file or files.** You will need to restore any files that you delete from backup files. Be sure to check your backup files for infections also.
- **Try to remove the infection yourself.** Network Associates supplies information and suggestions in its Virus Information Library that can help you remove a virus from an infected file. To see this information, start your preferred web browser application, then enter the following web address:

  http://www.nai.com/vinfo/<document number>.asp

  In the address listed, <document number> represents a technical document in the Virus Information Library. Replace <document number> with one of these numbers:

  0013 0319 0322 0323 0327 1145

  ❐ **NOTE:** Document numbers might change. See the online Virus Information Library table of contents for current information.

Creating an Emergency Disk without the utility

If you misplaced the Emergency Disk that came with your copy of VirusScan, or if you downloaded your VirusScan copy from one of the Network Associates electronic services, you will need to create an Emergency Disk. VirusScan prompts you to create an emergency disk during installation.

If you cannot use VirusScan's Emergency Disk creation utility because you have not yet installed VirusScan, or because VirusScan detected a virus during installation, you can create a clean Emergency Disk without the utility. Follow these steps:

WARNING: If VirusScan detected a virus as it tried to install itself on your computer, create your Emergency Disk on an *uninfected* computer.

1. Open an MS-DOS Prompt window or reboot your computer into DOS mode. To learn how to do so, consult your Windows documentation.
2. Insert a blank, *unformatted* 1.44MB disk into your floppy drive.
3. Type this command at the MS-DOS prompt:

   ```
   format <drive>: /s/u/v
   ```

Substitute the drive letter for your floppy drive in place of `<drive>` in the command shown. Next, press **ENTER.** This tells your system to format the floppy disk you inserted, to overwrite any existing information on it, to copy DOS system files to it, and to have DOS prompt you to enter a volume label for it.

4. When DOS prompts you for a volume label, enter a name up to 11 characters long that distinguishes this disk from others.

5. If you have VirusScan installed on your computer and in its default program directory, change to the correct directory by typing this command at the MS-DOS prompt:

   ```
   cd\progra~1\networ~1\mcafee~1
   ```

   If you do not have VirusScan installed, change to the directory that contains the VirusScan files you extracted, or to the VirusScan directory on your CD-ROM drive.

6. Type the commands listed below at the MS-DOS prompt to copy the correct files to the Emergency Disk. Substitute the drive letter for your floppy drive in place of `<drive>` in the commands shown:

   ```
   copy bootscan.exe <drive>:

   copy scan.dat <drive>:

   copy names.dat <drive>:

   copy clean.dat <drive>:

   copy license.dat <drive>:

   copy messages.dat <drive>:

   copy edwiz16.exe <drive>:
   ```

7. Copy to the Emergency Disk any other DOS utilities you need to start your computer, debug your system software, manage any extended or expanded memory you have, or perform other tasks at startup. If you use a disk compression utility, be sure to copy the drivers you need to uncompress your files.

8. When you have finished copying files to the Emergency Disk, label it, lock it, and store it in a safe place.

NOTE: A locked floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don’t see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position. Because no software can save to a locked disk, viruses cannot infect files stored on one.

Responding to viruses or malicious software

Because VirusScan consists of several component programs, any one of which could be active at one time, your possible responses to a virus infection or to other malicious software will depend upon which program detected the harmful object, how you have that program configured to respond, and other circumstances. The following sections give an overview of the default responses available with each program component. To learn about other possible responses, see the chapter that discusses each component in detail.

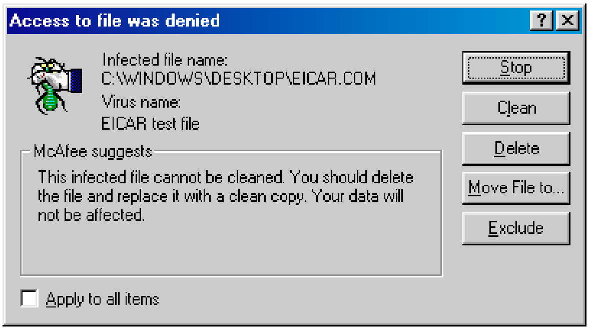
Responding when VShield detects malicious software

VShield consists of four related modules that provide you with continuous background scanning protection against viruses, harmful Java and ActiveX objects, and dangerous websites. A fifth module controls security settings for the other four. You can configure and activate each module separately, or use them together to provide maximum protection. See Chapter 4, “Using VShield,” to learn about each module’s configuration options. Because each module detects different objects or scans different virus entry points, each has a different set of default responses.

System Scan module

By default, this module looks for viruses each time you run, copy, create, or rename any file on your system, or whenever you read from a floppy disk. Because it does so, System Scan can serve as a backup in case any of the other VShield modules does not detect a virus that you download with, for example, an FTP client application. In its initial configuration, when the module finds a virus during any of these operations, it will prevent you from opening, saving or copying the infected file and will ask you what you want to do about the virus (Figure 3-12).

The response options you see in this dialog box come from default choices or choices you make in the System Scan module’s Action page. See “Choosing Action options” on page 79 of the *VirusScan User’s Guide* to learn how to choose which options appear here.



Access to file was denied

Infected file name:
C:\WINDOWS\DESKTOP\EICAR.COM
Virus name:
EICAR test file

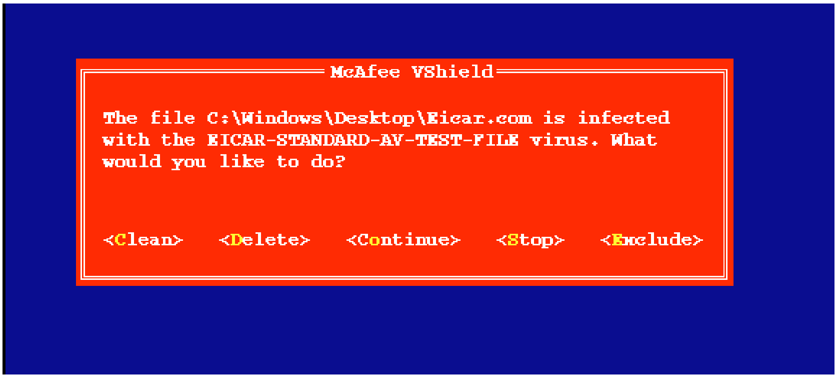
McAfee suggests

This infected file cannot be cleaned. You should delete the file and replace it with a clean copy. Your data will not be affected.

□ Apply to all items

Figure 3-12. Initial System Scan response options

If you've selected the **Continue access** checkbox in the module's Action page, you'll see instead a full-screen warning that offers you response options (Figure 3-13).



McAfee VShield

The file C:\Windows\Desktop\Eicar.com is infected with the EICAR-STANDARD-AV-TEST-FILE virus. What would you like to do?

Figure 3-13. System Scan response options

To take one of the listed actions, click a button in the dialog box, or type the letter highlighted in yellow when you see the full-screen warning. If you want the same response to apply to all infected files that VShield finds during this scan operation, select the **Apply to all items** checkbox in the dialog box. Your choices are:

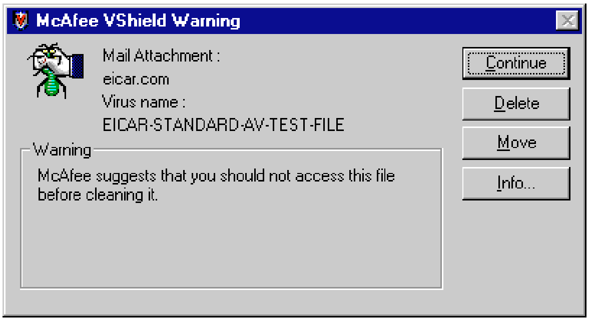
- **Clean the file.** Click **Clean** in the dialog box, or type `C` when you see the full-screen warning, to tell VShield to try to remove the virus code from the infected file. If VShield succeeds, it will restore the file to its original state.

  If VShield cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will note this result in its log file, but will take no other action. In most cases, you should delete such files and restore them from backups.

- **Delete the file.** Click **Delete** in the dialog box, or type D when you see the full-screen warning, to tell VShield to delete the infected file immediately. By default, VShield notes the name of the infected file in its log file so that you have a record of which files it flagged as infected. You can then restore deleted files from backup copies.
- **Move the file to a different location.** Click **Move File to** in the dialog box. This opens a browse window you can use to locate your quarantine folder or another folder you want to use to isolate infected files. Once you select a folder, VShield moves the infected file to it immediately.
- **Continue working.** Type O when you see the full-screen warning to tell VShield to let you continue working with the file and not take any other action. Normally, you would use this option to bypass files that you know do not have viruses. If you have its reporting option enabled, VShield will note each incident in its log file.
- **Stop the scan operation.** Click **Stop** in the dialog box, or type S when you see the full-screen warning, to tell VShield to deny you any access to the file but not to take any other action. Denying access to the file prevents you from opening, saving, copying or renaming it. To continue, you must click **OK**. If you have its reporting option enabled, VShield will note each incident in its log file.
- **Exclude the file from scan operations.** Click **Exclude** in the dialog box, or type E when you see the full-screen warning, to tell VShield to exclude this file from future scan operations. Normally, you would use this option to bypass files that you know do not have viruses.

E-mail Scan module

This module looks for viruses in e-mail messages you receive via corporate e-mail systems such as cc:Mail and Microsoft Exchange. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-14). A fourth option provides you with additional information.



Mail Attachment :
eicar.com
Virus name :
EICAR-STANDARD-AV-TEST-FILE

Warning

McAfee suggests that you should not access this file before cleaning it.

Figure 3-14. E-mail Scan module response options

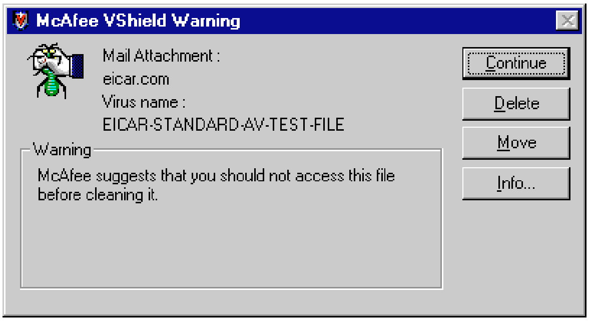
Click the button that corresponds to the response you want. Your choices are:

- **Continue.** Click this to tell VShield to take no action and to resume scanning. VShield will continue until it finds another virus on your system or until it finishes the scan operation. Normally, you would use this option to bypass files that you know do not have viruses, or if you plan to leave your computer unattended as you download e-mail. VShield will note each incident in its log file.
- **Delete.** Click this to tell VShield to delete the infected file attachment from the e-mail message you received. By default, VShield notes the name of the attachment in its log file.
- **Move.** Click this to tell VShield to create a quarantine directory where it found the virus, then move the infected file to it. If you use Microsoft Exchange, Microsoft Outlook or other MAPI mail clients, for example, the quarantine directory will appear as a folder called INFECTED in your mailbox on the mail server. If you use a POP-3 or similar mail client, the quarantine folder will appear at the root level of your hard disk as soon as you download an infected file.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not take any action against the virus VShield detected. See “Viewing File and Virus Information” on page 48 for details.

When you choose your action, VShield will implement it and add a notice to the top of the e-mail message that contained the infected attachment. The notice gives the file name of the infected attachment, identifies the name of the infecting virus, and describes the action VShield took in response.

Download Scan module

This module looks for viruses in e-mail messages and other files you receive over the Internet via a web browser or such e-mail client programs as Eudora Light, Netscape Mail, Outlook Express, and others. It will *not* detect files you download with FTP client applications, terminal applications, or through similar channels. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-15). A fourth option provides you with additional information.



Mail Attachment :
eicar.com
Virus name :
EICAR-STANDARD-AV-TEST-FILE

Warning
McAfee suggests that you should not access this file before cleaning it.

Figure 3-15. Download Scan response options

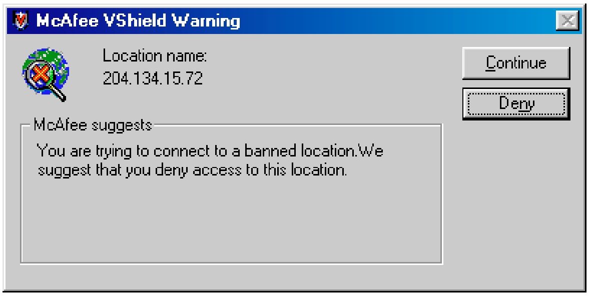
Click the button that corresponds to the response you want. Your choices are:

- **Continue.** Click this to tell VShield to take no action and to resume scanning. VShield will continue until it finds another virus on your system or until it finishes the scan operation. Normally, you would use this option to bypass files that you know do not have viruses, or if you plan to leave your computer unattended as you download e-mail or other files. VShield will note each incident in its log file.
- **Delete.** Click this to tell VShield to delete the infected file or e-mail attachment you received. By default, VShield notes the name of the infected file in its log file.
- **Move.** Click this to tell VShield to create a quarantine directory where it found the virus, then move the infected file to it. If you use a POP-3 or SMTP mail client, the quarantine folder will appear as a folder called INFECTED at the root level of your hard disk as soon as you download an infected file.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not take any action against the virus. See “Viewing File and Virus Information” on page 48 for more details.

When you choose your action, VShield will implement it and add a notice to the top of the e-mail message that contained the infected attachment. The notice gives the file name of the infected attachment, identifies the name of the infecting virus, and describes the action VShield took in response.

Internet Filter module

This module looks for hostile Java classes or ActiveX controls whenever you visit a website or download files from the Internet. You can also use the module to block your browser from connecting to dangerous Internet sites. In its initial configuration, the module will ask you whenever it encounters a potentially harmful object whether you want to **Deny** the object access to your system or you want to **Continue** and allow the object access. It will offer you the same choice when you try to connect to a potentially dangerous website (Figure 3-16).



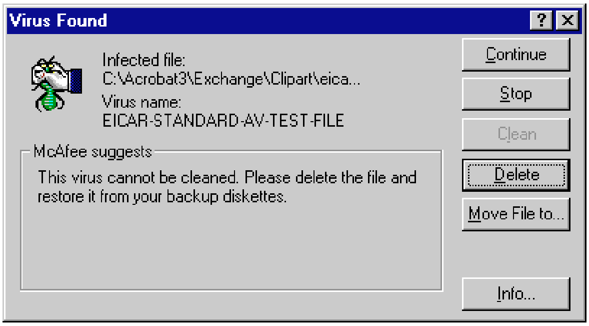
Location name:
204.134.15.72

McAfee suggests
You are trying to connect to a banned location.We suggest that you deny access to this location.

Figure 3-16. Internet Filter response options

Responding when VirusScan detects a virus

When you first install VirusScan and start a scan operation, the program will look at all files on your C: drive that are susceptible to virus infection. This provides you with a basic level of protection that you can extend by configuring VirusScan to suit your own needs. In its initial configuration, the program will prompt you for a response when it finds a virus (Figure 3-17).



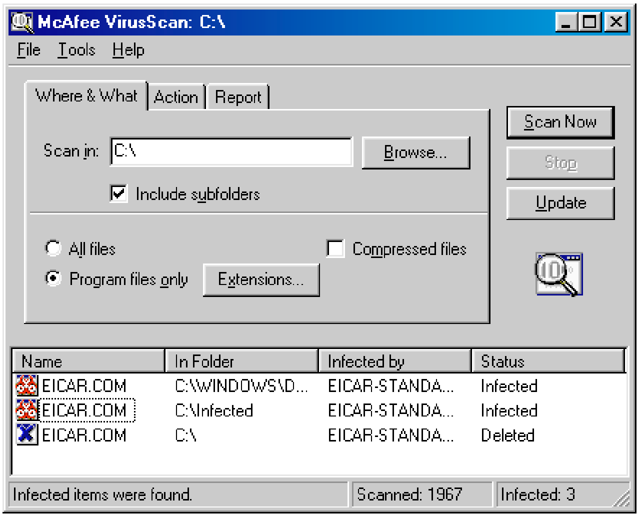
Infected file:
C:\Acrobat3\Exchange\Clipart\eica...
Virus name:
EICAR-STANDARD-AV-TEST-FILE

McAfee suggests
This virus cannot be cleaned. Please delete the file and restore it from your backup diskettes.

Figure 3-17. VirusScan response options

To respond to the infection, click one of the buttons shown. You can tell VirusScan to:

- **Continue.** Click this to proceed with the scan operation and have VirusScan list each infected file in the lower portion of its main window (Figure 3-18), record each detection in its log file, but take no other action to respond to the virus. Once VirusScan has finished examining your system, you can right-click each file listed in the main window, then choose an individual response from the shortcut menu that appears.



McAfee VirusScan: C:\

Scan in: C:\

☑ Include subfolders

○ All files

● Program files only

□ Compressed files

Name	In Folder	Infected by	Status
EICAR.COM	C:\WINDOWS\D...	EICAR-STANDA...	Infected
EICAR.COM	C:\Infected	EICAR-STANDA...	Infected
EICAR.COM	C:\	EICAR-STANDA...	Deleted

Infected items were found. Scanned: 1967 Infected: 3

Figure 3-18. VirusScan main window

- **Stop.** Click this to stop the scan operation immediately. VirusScan will list the infected files it has already found in the lower portion of its main window (Figure 3-18) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.

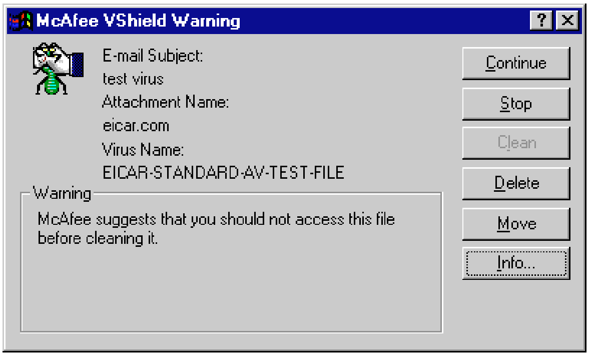
- **Clean.** Click this to have VirusScan try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses. In the example shown in Figure 3-17, VirusScan failed to clean the EICAR Test Virus—a mock “virus” written specifically to test whether your anti-virus software installed correctly. Here, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.

- **Delete.** Click this to delete the file from your system immediately. By default, VirusScan will record the name of the infected file in its log so that you can restore the file from a backup copy.

- **Move file to.** Click this to open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not take any action against the virus that VirusScan detected. See “Viewing File and Virus Information” on page 48 for more details.

Responding when E-Mail Scan detects a virus

VirusScan’s E-Mail Scan program component lets you scan incoming Microsoft Exchange or Microsoft Outlook e-mail messages for viruses at your initiative. You can start it from within either e-mail client and use it to supplement VShield’s continuous e-mail background scanning. E-Mail Scan also offers the ability to clean infected file attachments or stop the scan operation, a capability that complements VShield’s continuous monitoring. In its initial configuration, E-Mail Scan will prompt you for a response when it finds a virus (Figure 3-19).



E-mail Subject:
test virus
Attachment Name:
eicar.com
Virus Name:
EICAR-STANDARD-AV-TEST-FILE

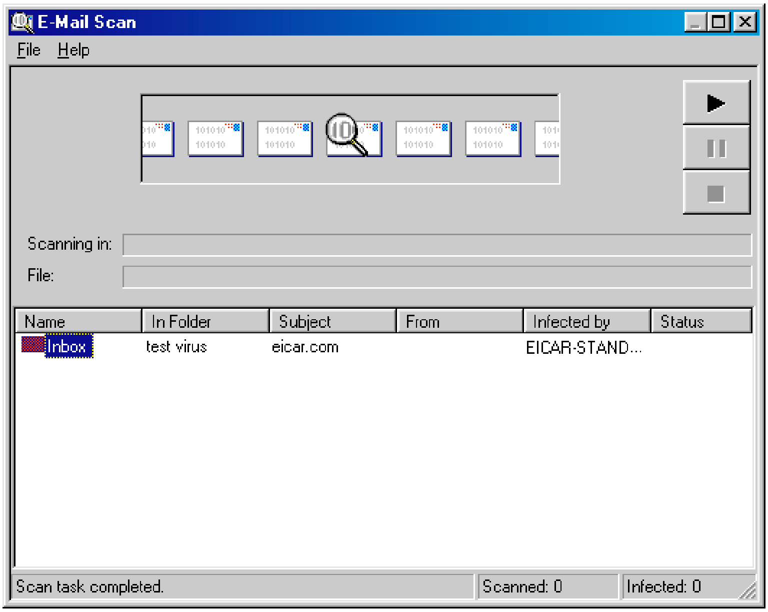
McAfee suggests that you should not access this file before cleaning it.

Figure 3-19. E-Mail Scan response options

To respond to the infection, click one of the buttons shown. You can tell E-Mail Scan to:

- **Continue.** E-Mail Scan will proceed with its scan operation, list each infected file it finds in the lower portion of its main window (Figure 3-20), and record each detection in its log file, but it will take no other action to respond to the virus. E-Mail Scan will continue until it finds another virus on your system or until it finishes the scan operation. Once it has finished examining your system, you can right-click each file listed in the main window, then choose an individual response from the shortcut menu that appears.

- **Stop.** E-Mail Scan will stop its scan operation immediately. It will list the infected files it has already found in the lower portion of its main window (Figure 3-20) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.



Name	In Folder	Subject	From	Infected by	Status
Inbox	test virus	eicar.com		EICAR-STAND...	

Scan task completed. | Scanned: 0 | Infected: 0

Figure 3-20. E-Mail Scan window

- **Clean.** E-Mail Scan will try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses. In the example shown in Figure 3-19, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.

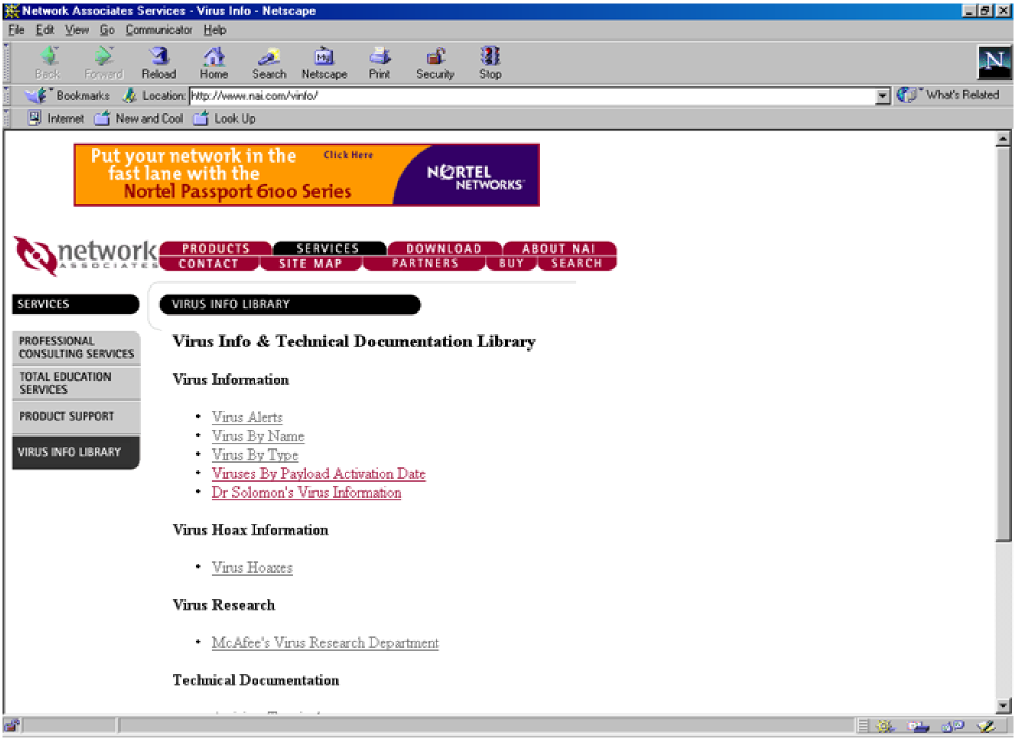
- **Delete.** E-Mail Scan will immediately delete the file from your system. By default, the program will record the name of the infected file in its log so that you can restore the file from a backup copy.

- **Move.** E-Mail Scan will open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.

- **Info.** E-Mail Scan will open a dialog box that displays information about the infecting virus or the infected file. This choice does not cause the program to take any action against the virus it detected. See “Viewing File and Virus Information” for more details.

Viewing File and Virus Information

Clicking **Info** in any of the virus response dialog boxes will connect you to the Network Associates online Virus Information Library, provided you have an Internet connection and web browsing software available on your computer (Figure 3-21).


Network Associates Services - Virus Info - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://www.nai.com/vinfo/
What's Related
Internet New and Cool Look Up
Put your network in the fast lane with the Nortel Passport 6100 Series
Click Here
NORTEL NETWORKS
network ASSOCIATES
PRODUCTS SERVICES DOWNLOAD ABOUT NAI
CONTACT SITE MAP PARTNERS BUY SEARCH
SERVICES
PROFESSIONAL CONSULTING SERVICES
TOTAL EDUCATION SERVICES
PRODUCT SUPPORT
VIRUS INFO LIBRARY
VIRUS INFO LIBRARY

Virus Info & Technical Documentation Library

Virus Information

- Virus Alerts
- Virus By Name
- Virus By Type
- Viruses By Payload Activation Date
- Dr Solomon's Virus Information

Virus Hoax Information

- Virus Hoaxes

Virus Research

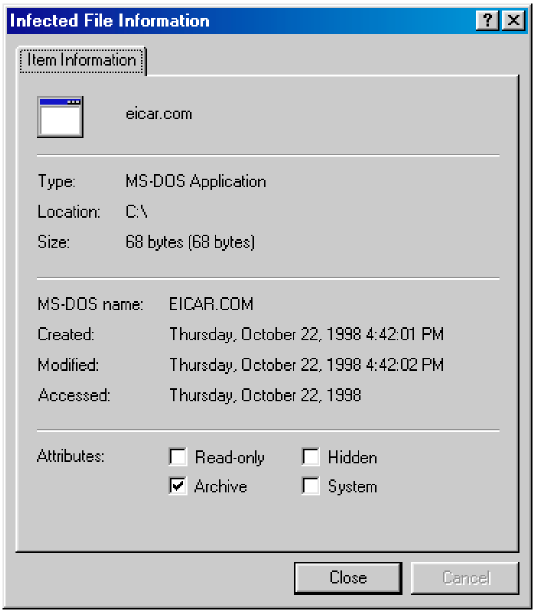
- McAfee's Virus Research Department

Technical Documentation

Figure 3-21. Online Virus Information Library

The Virus Information Library contains documents that give a detailed overview of each virus that VirusScan can detect or clean. That information includes how the virus infects and alters files, the sorts of payloads it deploys, how to recognize an infection, and other data. The Library also gives tips on preventing virus infection and removing viruses that VirusScan cannot remove from infected files.

If you choose **File Info** from the **File** menu in the VirusScan main window (see Figure 3-18 on page 45), or right-click a file listed either in the VirusScan main window or the E-Mail Scan window (see Figure 3-20 on page 47), then choose **File Info** from the shortcut menu that appears, VirusScan will open an Infected Item Information dialog box that names the file, lists its type and size in bytes, gives its creation and modification dates, and describes its attributes (see Figure 3-22 on page 49).



eicar.com

Type: MS-DOS Application
Location: C:\
Size: 68 bytes (68 bytes)

MS-DOS name: EICAR.COM
Created: Thursday, October 22, 1998 4:42:01 PM
Modified: Thursday, October 22, 1998 4:42:02 PM
Accessed: Thursday, October 22, 1998

Attributes: ☐ Read-only ☐ Hidden
☑ Archive ☐ System

Figure 3-22. Infected File Information property page

Using VShield 4

What does VShield do?

VShield scans your system in the background, as you work with your files, in order to protect you from viruses borne on floppy disks, brought in from your network, embedded in file attachments that come with e-mail messages, or loaded into memory. It starts when you start your computer, and stays in memory until you shut down. VShield also includes technology that guards against hostile Java applets and ActiveX controls, and that keeps your computer from connecting to dangerous Internet sites.

This chapter discusses basic VShield configuration options. To learn about the full range of available options, see Chapter 4 in the *VirusScan User's Guide*.

Why use VShield?

VShield has unique capabilities that make it an integral part of VirusScan's comprehensive anti-virus security package. These include:

- **"On-access" scanning.** This means that VShield scans for viruses in files that you open, copy, save, or otherwise modify, and files that you read from or write to floppy disks. It therefore can detect and stop viruses as soon as they appear on your system. This gives you an extra measure of anti-virus protection between each scan operation that you perform.

- **Malicious object detection and blocking.** VShield can block harmful ActiveX and Java objects from gaining access to your system, before they pose a threat. VShield does this by scanning the hundreds of objects you download as you connect to the web or to other Internet sites, and the file attachments you receive with your e-mail. It compares these items against a current list of harmful objects that it maintains, and blocks those that could cause problems.

- **Internet site filtering.** VShield comes with a list of dangerous web- or Internet sites that pose a hazard to your system, usually in the form of downloadable malicious software. You can add any other site that you want to keep your browser software from connecting to, either by listing its Internet Protocol (IP) address or its domain name.

- **Automatic operation.** VShield integrates with a wide range of browser software and e-mail client applications based on Microsoft's Messaging Application Programming Interface (MAPI) standard. This allows VShield to log on to and scan your e-mail attachments for viruses before they ever reach your computer.

Which browsers and e-mail clients does VShield support?

VShield works seamlessly with many of the most popular web browsers and e-mail client software available for the Windows platform. To work with your browser, VShield requires no setup beyond what you have already done to connect your computer to the Internet. You must configure VShield, however, to work correctly with your e-mail client software. See See “Using the VShield configuration wizard” on page 53 or “Using VShield’s shortcut menu” on page 59 to learn how to do the required setup.

Web browsers tested and known to work correctly with VShield are:

- Netscape Navigator v3.x
- Netscape Navigator v4.0.x (not including v4.0.6)
- Microsoft Internet Explorer v3.x
- Microsoft Internet Explorer v4.x

E-mail clients tested and known to work with VShield’s Download Scan module are:

- Microsoft Outlook Express
- Qualcomm Eudora v3.x and v4.x
- Netscape Mail (included with most versions of Netscape Navigator and Netscape Communicator)
- America Online mail v3.0 and v4.0

In order to work with VShield’s E-mail Scan module, you must use particular versions of Lotus cc:Mail, or your e-mail client software must support Microsoft’s MAPI standard. Those clients tested and known to work correctly with the E-mail Scan module are:

- Microsoft Exchange v4.0, v5.0 and v5.5
- Microsoft Outlook 97 and Outlook 98
- Lotus cc:Mail v6.x and v7.x (not MAPI-compliant)
- cc:Mail v8.0 and v8.01 (MAPI-compliant version only)

Other MAPI-compliant client software will most likely work correctly with VShield, but Network Associates does not certify VShield compatibility with client software not listed above.

Using the VShield configuration wizard

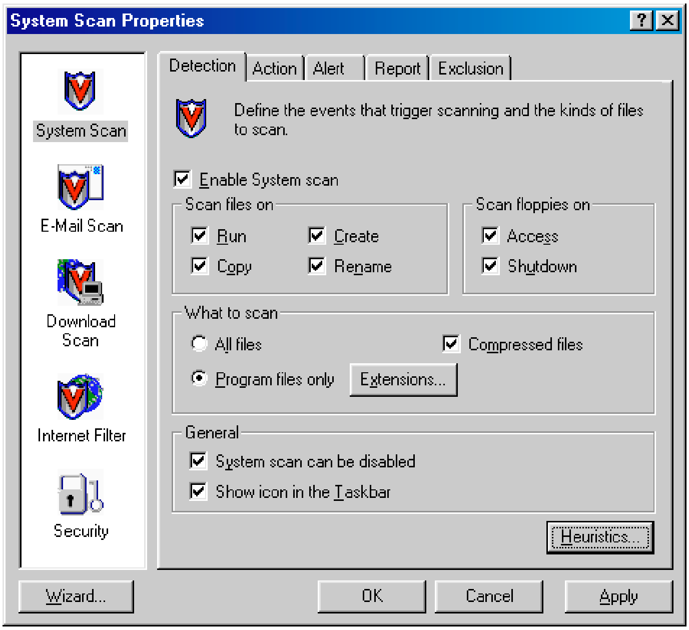
After you install VirusScan and restart your computer, VShield loads into memory immediately and begins working with a default set of options that give you basic anti-virus protection. Unless you disable it or one of its modules—or stop it entirely—you never have to worry about starting VShield or scheduling scan tasks for it.

To ensure more than a minimal level of security, however, you should configure VShield to work with your e-mail client software and have it examine your Internet traffic closely for viruses and malicious software. VShield's configuration wizard can help you set up many of these options right away. You can use the VShield Properties dialog box itself to tailor the program to work better in your environment as you become more familiar with VShield and your system's susceptibility to harmful software.

To start the VShield configuration wizard, either:

- Start the VirusScan Scheduler, then select the VShield icon in the task list. Next, click in the Scheduler toolbar. To learn how to start and use the VirusScan Scheduler, see "Starting the VirusScan Scheduler" on page 148 of the *VirusScan User's Guide*; or
- Locate the VShield icon in the Windows system tray, then click it with your right mouse button. Point to **Properties** in the shortcut menu that appears, then choose **System Scan**.

Either method opens the VShield Properties dialog box (Figure 4-1).



System Scan Properties

Detection | Action | Alert | Report | Exclusion

Define the events that trigger scanning and the kinds of files to scan.

☑ Enable System scan

Scan files on
☑ Run ☑ Create
☑ Copy ☑ Rename

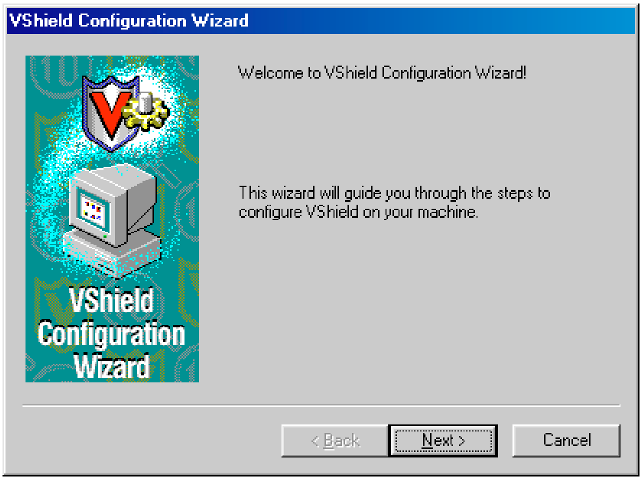
Scan floppies on
☑ Access
☑ Shutdown

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

General
☑ System scan can be disabled
☑ Show icon in the Taskbar

Figure 4-1. VShield Properties dialog box

Click **Wizard** in the lower-left corner of the dialog box to display the first configuration wizard panel (Figure 4-2).



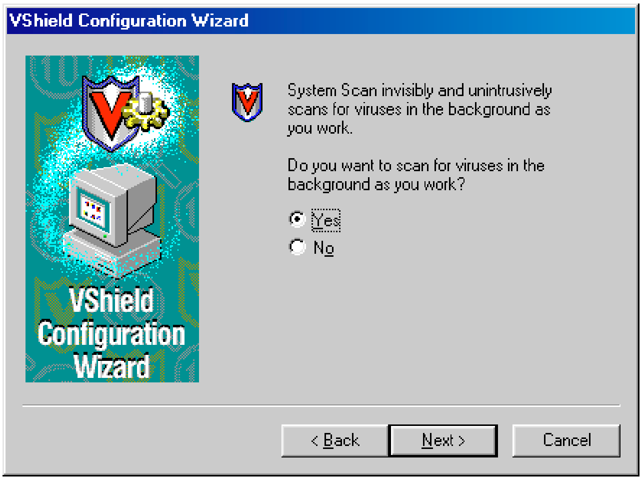
VShield Configuration Wizard

Welcome to VShield Configuration Wizard!

This wizard will guide you through the steps to configure VShield on your machine.

Figure 4-2. VShield Configuration Wizard - Welcome panel

Click **Next>** to display the System Scan configuration panel (Figure 4-3).



VShield Configuration Wizard

System Scan invisibly and unintrusively scans for viruses in the background as you work.

Do you want to scan for viruses in the background as you work?

● Yes
○ No

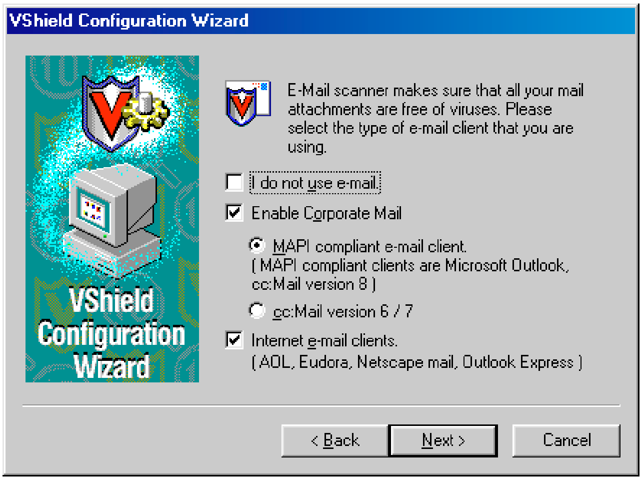
Figure 4-3. VShield Configuration Wizard - System Scan panel

Here you can tell VShield to look for viruses in files susceptible to infection whenever you open, run, copy, save or otherwise modify them. Susceptible files include various types of executable files and document files with embedded macros, such as Microsoft Office files. VShield will also scan files stored on floppy disks whenever you read from or write to them, or when you shut down your computer.

If it finds a virus, VShield will sound an alert and prompt you for a response. The program will also record its actions and summarize its current settings in a log file that you can review later.

To enable these functions, select **Yes**, then click **Next>**. Otherwise, select **No**, then click **Next>** to continue.

The E-mail Scan wizard panel will appear (Figure 4-4).



VShield Configuration Wizard

E-Mail scanner makes sure that all your mail attachments are free of viruses. Please select the type of e-mail client that you are using.

□ I do not use e-mail.

☑ Enable Corporate Mail

● MAPI compliant e-mail client. (MAPI compliant clients are Microsoft Outlook, cc:Mail version 8)

○ cc:Mail version 6 / 7

☑ Internet e-mail clients. (AOL, Eudora, Netscape mail, Outlook Express)

Figure 4-4. VShield Configuration Wizard - E-mail Scan panel

If you do not use e-mail or do not have an Internet connection, select the **I do not use e-mail** checkbox, then click **Next>** to continue. Otherwise, select the checkbox that corresponds to the type of e-mail client you use. Your choices are:

- **Enable Corporate Mail.** Select this checkbox if you use a proprietary e-mail system at work or in a networked environment. Most such systems use a central network server to receive and distribute mail that individual users send to each other from client applications. Such systems might send and receive mail from outside the network or from the Internet, but they usually do so through a "gateway" application run from the server.

  VShield supports corporate e-mail systems that fall into two general categories:

  - **MAPI-compliant e-mail client**. Select this button if you use an e-mail client that adheres to the MAPI standard. Examples of such clients include Microsoft Exchange, Microsoft Outlook, and version 8.0 or later of Lotus cc:Mail.

  - **Lotus cc:Mail.** Select this button if you use cc:Mail versions 6.x or 7.x, which use a proprietary Lotus protocol for sending and receiving mail.

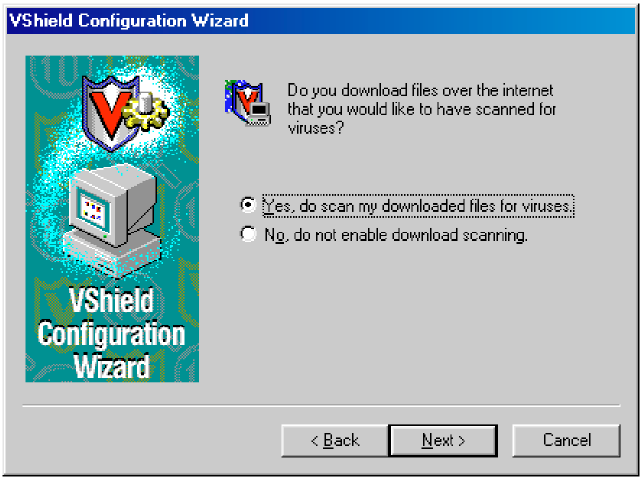
- **Internet e-mail clients.** Select this checkbox if you use a Post Office Protocol (POP-3) or Simple Mail Transfer Protocol (SMTP) e-mail client that sends and receives standard Internet mail directly or through a dial-up connection. If you send and receive e-mail from home and use Netscape Mail, America Online, or such popular clients as Qualcomm's Eudora or Microsoft's Outlook, be sure to select this option.

When you have specified which e-mail system you use, click **Next>** to continue.

NOTE: If you use both types of mail systems, select both checkboxes. Note that VShield supports only one type of *corporate* e-mail system at a time, however. If you need to verify which e-mail system your office uses, check with your network administrator.

Be sure also to distinguish between Microsoft Outlook and Microsoft Outlook Express. Although the two programs share similar names, Outlook 97 and Outlook 98 are MAPI-compliant corporate e-mail systems, while Outlook Express sends and receives e-mail through the POP-3 and SMTP protocols. To learn more about these programs, consult your Microsoft documentation.

The next wizard panel sets options for VShield's Download Scan module (Figure 4-5).



VShield Configuration Wizard

Do you download files over the internet that you would like to have scanned for viruses?

● Yes, do scan my downloaded files for viruses.

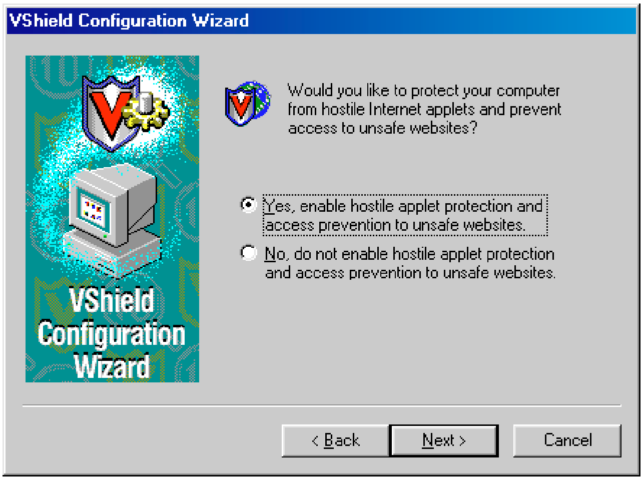
○ No, do not enable download scanning.

Figure 4-5. VShield Configuration Wizard - Download Scan panel

To have VShield look for viruses in each file that you download from the Internet, select the **Yes, do scan my downloaded files for viruses** checkbox, then click **Next>** to continue. VShield will look for viruses in those files most susceptible to infection and will scan compressed files as you receive them.

Otherwise, select the **No, do not enable download scanning** checkbox, then click **Next>** to continue.

The next wizard panel sets options for VShield's Internet Filter module (see Figure 4-6 on page 58).



VShield Configuration Wizard

Would you like to protect your computer from hostile Internet applets and prevent access to unsafe websites?

● Yes, enable hostile applet protection and access prevention to unsafe websites.

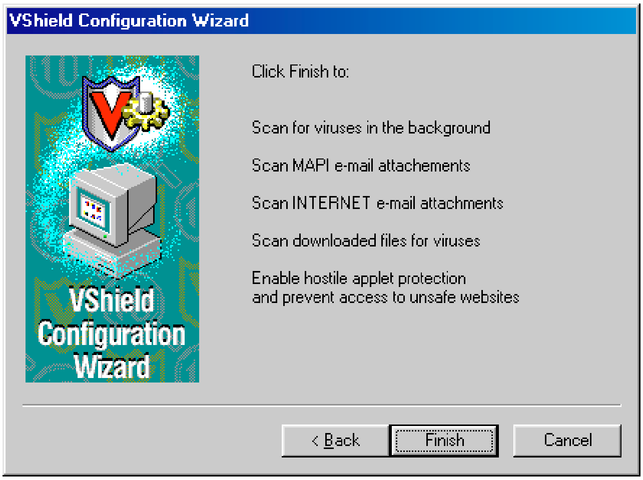
○ No, do not enable hostile applet protection and access prevention to unsafe websites.

Figure 4-6. VShield Configuration Wizard - Internet Filter panel

Select **Yes, enable hostile applet protection and access prevention to unsafe websites**, then click **Next>** to have VShield block Java applets and ActiveX controls that can cause your system harm. This option will also keep your web browser from connecting to potentially dangerous web- or other Internet sites. VShield maintains a list of harmful objects and sites that it uses to check the sites you visit and the objects you encounter. If it finds a match, it can either block it automatically, or offer you the chance to allow or deny access.

To disable this function, select **No, do not enable hostile applet protection and access prevention to unsafe websites**, then click **Next>** to continue.

The final wizard panel summarizes the options you chose (Figure 4-7).



Click Finish to:

Scan for viruses in the background

Scan MAPI e-mail attachements

Scan INTERNET e-mail attachments

Scan downloaded files for viruses

Enable hostile applet protection
and prevent access to unsafe websites

Figure 4-7. VShield Configuration Wizard - summary panel

If the summary list accurately reflects your choices, click **Finish** to save your changes and return to the VShield Properties dialog box. Otherwise, click **<Back** to change any options you chose, or **Cancel** to return to the VShield Properties dialog box without saving any of your changes.

Using VShield's shortcut menu

VShield groups several of its common commands in a shortcut menu associated with its system tray icon 🛡. Double-click this icon to display the VShield Status dialog box. Click the icon with your right mouse button to display these commands:

- **Status.** Choose this to open the VShield Status dialog box.
- **Properties.** Point to this, then choose one of the VShield modules listed to open the VShield Properties dialog box to the property page for that module.
- **Enable.** Point to this, then choose one of the VShield modules listed to activate or deactivate it. Those modules displayed in the menu with checkmarks are active; those without are inactive.
- **About.** Choose this to display VShield's version number and serial number, the version number and creation date for the current .DAT files in use, and a Network Associates copyright notice.
- **Exit.** Choose this to stop all VShield modules from scanning and to unload VShield from memory.

Disabling or stopping VShield

Once it starts, VShield displays a small icon in the Windows system tray. *Disabling* VShield leaves it running in memory, but keeps it from performing scan functions. When you disable all of its modules, VShield leaves a “cancelled” icon in the Windows system tray that you can use to enable it again.

Stopping VShield removes it from memory entirely—its Windows system tray icon will also disappear. To enable it again at that point, you must open the VShield Properties dialog box and enable each module individually again (see “Using VShield’s shortcut menu” for details) or start it again from VirusScan Scheduler.

You can disable or stop VShield in any of four ways:

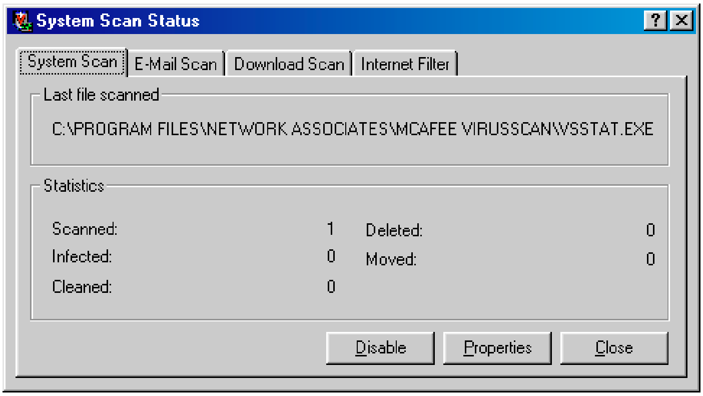
- **From the VShield shortcut menu.** Click the VShield icon in the Windows system tray with your right mouse button to display its shortcut menu, then choose **Exit**.

  VShield will stop immediately, unload itself from memory and remove its icon from the Windows system tray.

  To disable individual VShield modules, right-click the VShield icon, point to **Enable**, then choose each module individually. Those with checkmarks beside them are active; those without checkmarks are disabled.

  > **NOTE:** See “Using VShield’s shortcut menu” on page 59 to learn more about other menu choices.

- **From the VShield Status dialog box.** Double-click the VShield icon in the Windows system tray to display the VShield Status dialog box (Figure 4-8).



Last file scanned

C:\PROGRAM FILES\NETWORK ASSOCIATES\MCAFEE VIRUSSCAN\VSSTAT.EXE

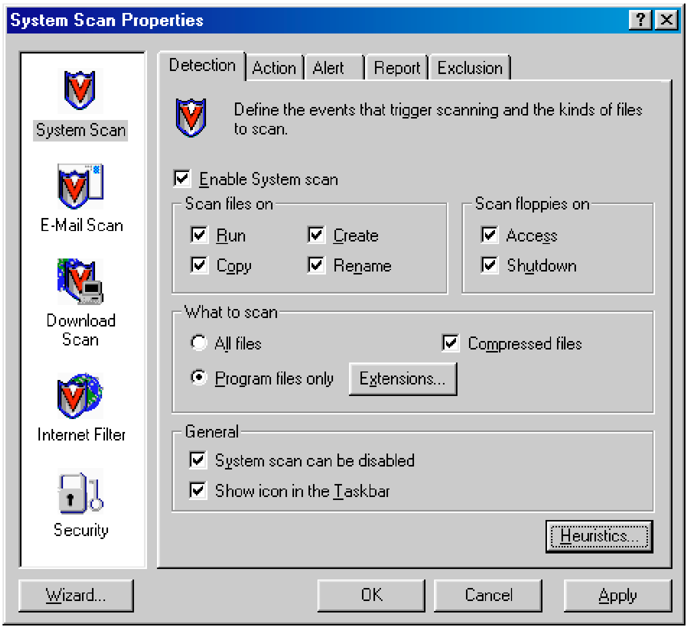
Statistics

Scanned: 1 Deleted: 0
Infected: 0 Moved: 0
Cleaned: 0

Figure 4-8. VShield Status dialog box

For each module that you want to disable, click the corresponding tab, then click **Disable**. VShield will disable that module immediately. When you have disabled all of its modules, VShield will display 🚫 in the Windows system tray. To activate each module again, open the Status dialog box, then click **Enable** in each property page.

- **From the VShield Properties dialog box.** Right-click the VShield icon in the Windows system tray, point to **Properties**, then choose **System Scan** from the shortcut menu that appears to display the VShield Properties dialog box (Figure 4-9).



System Scan Properties

Define the events that trigger scanning and the kinds of files to scan.

☑ Enable System scan

Scan files on
☑ Run ☑ Create
☑ Copy ☑ Rename

Scan floppies on
☑ Access
☑ Shutdown

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

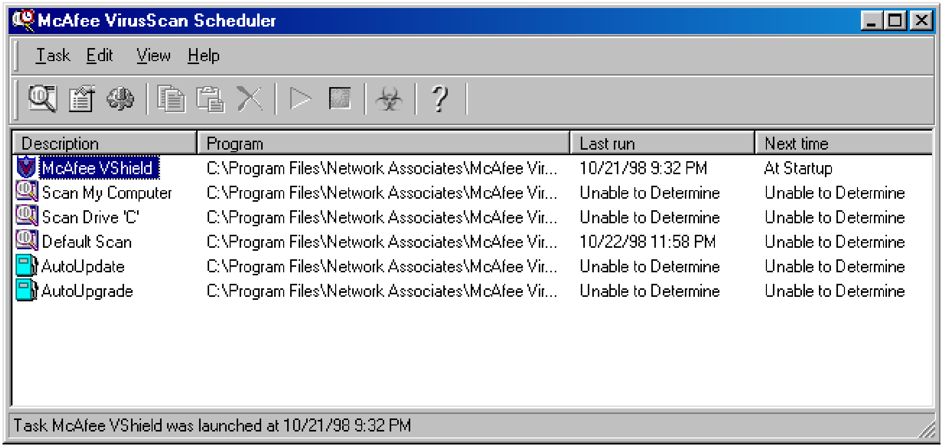
General
☑ System scan can be disabled
☑ Show icon in the Taskbar

Figure 4-9. VShield Properties dialog box

For each module that you want to disable, click the corresponding icon along the left side of the dialog box, then click the Detection tab. Next, clear the **Enable** checkbox at the top of each page. As you do so, VShield will disable that module. When you have disabled all of its modules, VShield will display 🚫 in the Windows system tray, unless you have cleared the **Show icon in the taskbar** checkbox.

To activate each module again, open the VShield Properties dialog box, then select the **Enable** checkbox in each module’s Detection page.

- **From VirusScan Scheduler.** Click **Start** in the Windows taskbar, point to **Programs**, then to **McAfee VirusScan**. Next, choose **McAfee VirusScan Scheduler** to open the Scheduler window (Figure 4-10).



Description	Program	Last run	Next time
McAfee VShield	C:\Program Files\Network Associates\McAfee Vir...	10/21/98 9:32 PM	At Startup
Scan My Computer	C:\Program Files\Network Associates\McAfee Vir...	Unable to Determine	Unable to Determine
Scan Drive 'C'	C:\Program Files\Network Associates\McAfee Vir...	Unable to Determine	Unable to Determine
Default Scan	C:\Program Files\Network Associates\McAfee Vir...	10/22/98 11:58 PM	Unable to Determine
AutoUpdate	C:\Program Files\Network Associates\McAfee Vir...	Unable to Determine	Unable to Determine
AutoUpgrade	C:\Program Files\Network Associates\McAfee Vir...	Unable to Determine	Unable to Determine

Task McAfee VShield was launched at 10/21/98 9:32 PM

Figure 4-10. VirusScan Scheduler window

Select **McAfee VShield** in the task list, then choose **Disable** from the **Task** menu. VShield will disable all VShield modules and display 🚫 in the Windows system tray. To start VShield again, select the VShield task, then choose **Enable** from the **Task** menu.

To stop VShield entirely, select **McAfee VShield** in the task list, then click ■ in the Scheduler toolbar. VShield will stop immediately, unload itself from memory and remove its icon from the Windows system tray. To activate it again, select the VShield task, then click ▶.

Using McAfee VirusScan 5

What is VirusScan?

The VirusScan name applies both to the entire set of desktop anti-virus program components described in this *Getting Started Guide*, and to a particular component of that set: SCAN32.EXE, or the VirusScan “on-demand” scanner. “On demand” means that you as a user control when VirusScan starts and ends a scan operation, which targets it examines, what it does when it finds a virus, or any other aspect of the program’s operation. Other VirusScan components, by contrast, operate automatically or according to a schedule you set. VirusScan originally consisted solely of an on-demand scanner—features since integrated into the program now provide a cluster of anti-virus functions that give you maximum protection against virus infections and attacks from malicious software.

The VirusScan on-demand component operates in two modes: the VirusScan “Classic” interface gets you up and running quickly, with a minimum of configuration options, but with the full power of the VirusScan anti-virus scanning engine; the VirusScan Advanced mode adds flexibility to the program’s configuration options, including the ability to run more than one scan operation concurrently.

This chapter describes how to use VirusScan in its Classic mode. To learn how to use VirusScan Advanced, and configure other VirusScan options, see Chapter 5 in the *VirusScan User’s Guide*.

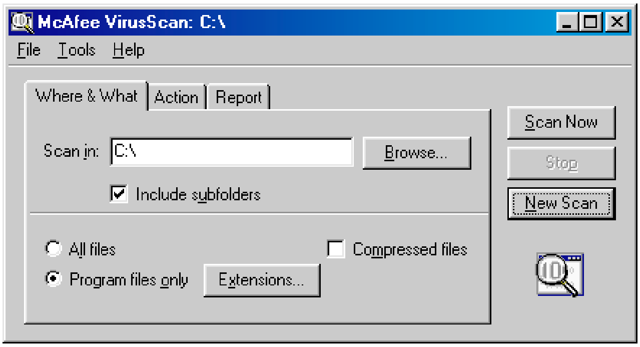
Starting VirusScan

VirusScan Classic comes with a single, default scan operation pre-configured and ready to run. You can start this scan operation to look for viruses on your C: drive immediately, or you can configure and run your own scan operations to suit your needs. VirusScan Advanced also comes with a single pre-configured scan operation, which scans all of your local hard disks.

To start VirusScan, either

- Click **Start** in the Windows taskbar, point to **Programs**, then to **McAfee VirusScan**. Next, choose **McAfee VirusScan** from the list that appears; or
- Click **Start**, then choose **Run** from the menu that appears. Type SCAN32.EXE in the Run dialog box, then click **OK**.

Both methods open the VirusScan Classic window (see Figure 5-1 on page 64).



Scan in: C:\

☑ Include subfolders

○ All files

● Program files only

☐ Compressed files

Figure 5-1. VirusScan Classic window

Click **Scan Now** at the right of the window to start the default scan task immediately, or configure a scan task that suits your needs by clicking the tabs at the top of the window and choosing options in each property page.

Using VirusScan menus

The menus along the top of the VirusScan window allow you to change some aspects of the program’s operation. You can:

- **Save or restore default settings.** By default, VirusScan Classic will look for viruses in those files most susceptible to virus infection. It will scan your computer’s memory and system areas, examine your C: drive and all of its subfolders, then sound an alert and prompt you for a response if it detects a virus. The program will also record its actions and summarize its current settings in a log file that you can review later.

  If you make changes to these settings and want to save your changes so that they become the new default settings, choose **Save As Default** from the **File** menu, or click the **New Scan** button to the right of the VirusScan Classic window. VirusScan will ask you to confirm that you want to replace the file that records the default settings. Click **Overwrite** or **OK** to continue. VirusScan will record your options and use them for every scan operation you run after that.

  NOTE: If you make changes to the default settings but decide that you want to return to the settings VirusScan came with originally, use Windows Explorer to locate and delete the file DEFAULT.VSC in the VirusScan program directory. When you next start VirusScan, it will restore its default settings and save them into a new DEFAULT.VSC file. To learn about the .VSC file format, see Appendix C, “Understanding the .VSC File Format,” in the *VirusScan User’s Guide*.

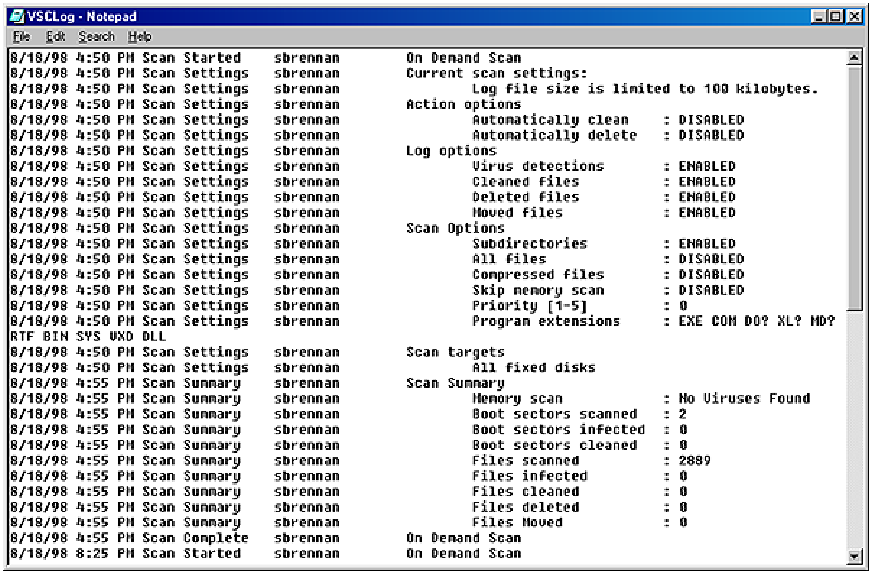
- **Save new settings.** If you need different VirusScan configurations in order to run various scan operations, or if you want to run a scan operation with the same configuration on more than one computer, you can save your configuration options into a .VSC file with its own name. A .VSC file is a text file that records VirusScan configuration options, much like Windows .INI files record program startup options.

  To save your settings, first configure VirusScan with the options you want, then choose **Save Settings** from the **File** menu. Type a descriptive name in the Save As dialog box, choose a location for the file on your hard disk, then click **Save**. You can then copy this file to any other computer that should also use those settings. See “Configuring VirusScan Classic” on page 66 or “Configuring VirusScan Advanced” on page 60 of the *VirusScan User’s Guide* for more details.

  To run VirusScan with these settings, simply locate and double-click the .VSC file you saved. This will start VirusScan with the settings loaded.

- **Open the VirusScan activity log.** Choose **View Activity Log** from the **File** menu to open the log file VirusScan uses to record its actions and settings.

  The log file will open in a Notepad window (Figure 5-2). You can print, edit, copy or otherwise treat this file as you would any ordinary text file. To learn more about what information the log file records, see “Choosing Report options” on page 69 of the *VirusScan User’s Guide*.



```
8/18/98 4:50 PM Scan Started    sbrennan        On Demand Scan
8/18/98 4:50 PM Scan Settings   sbrennan        Current scan settings:
8/18/98 4:50 PM Scan Settings   sbrennan                Log file size is limited to 100 kilobytes.
8/18/98 4:50 PM Scan Settings   sbrennan        Action options
8/18/98 4:50 PM Scan Settings   sbrennan                Automatically clean    : DISABLED
8/18/98 4:50 PM Scan Settings   sbrennan                Automatically delete   : DISABLED
8/18/98 4:50 PM Scan Settings   sbrennan        Log options
8/18/98 4:50 PM Scan Settings   sbrennan                Virus detections       : ENABLED
8/18/98 4:50 PM Scan Settings   sbrennan                Cleaned files          : ENABLED
8/18/98 4:50 PM Scan Settings   sbrennan                Deleted files          : ENABLED
8/18/98 4:50 PM Scan Settings   sbrennan                Moved files            : ENABLED
8/18/98 4:50 PM Scan Settings   sbrennan        Scan Options
8/18/98 4:50 PM Scan Settings   sbrennan                Subdirectories         : ENABLED
8/18/98 4:50 PM Scan Settings   sbrennan                All files              : DISABLED
8/18/98 4:50 PM Scan Settings   sbrennan                Compressed files       : DISABLED
8/18/98 4:50 PM Scan Settings   sbrennan                Skip memory scan       : DISABLED
8/18/98 4:50 PM Scan Settings   sbrennan                Priority [1-5]         : 0
8/18/98 4:50 PM Scan Settings   sbrennan                Program extensions     : EXE COM DO? XL? MD?
RTF BIN SYS VXD DLL
8/18/98 4:50 PM Scan Settings   sbrennan        Scan targets
8/18/98 4:50 PM Scan Settings   sbrennan                All fixed disks
8/18/98 4:55 PM Scan Summary    sbrennan        Scan Summary
8/18/98 4:55 PM Scan Summary    sbrennan                Memory scan            : No Viruses Found
8/18/98 4:55 PM Scan Summary    sbrennan                Boot sectors scanned   : 2
8/18/98 4:55 PM Scan Summary    sbrennan                Boot sectors infected  : 0
8/18/98 4:55 PM Scan Summary    sbrennan                Boot sectors cleaned   : 0
8/18/98 4:55 PM Scan Summary    sbrennan                Files scanned          : 2889
8/18/98 4:55 PM Scan Summary    sbrennan                Files infected         : 0
8/18/98 4:55 PM Scan Summary    sbrennan                Files cleaned          : 0
8/18/98 4:55 PM Scan Summary    sbrennan                Files deleted          : 0
8/18/98 4:55 PM Scan Summary    sbrennan                Files Moved            : 0
8/18/98 4:55 PM Scan Complete   sbrennan        On Demand Scan
8/18/98 8:25 PM Scan Started    sbrennan        On Demand Scan
```

Figure 5-2. VirusScan Activity Log

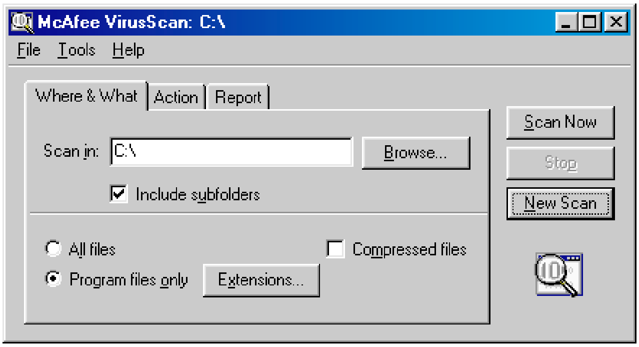
- **Quit VirusScan.** Choose **Close** from the **File** menu to quit VirusScan. Quitting VirusScan stops any active scan operations, but does *not* affect VShield’s continuous background operations. Unless you save them, any configuration options you chose will also disappear when you quit VirusScan.
- **Change VirusScan modes.** Choose **Advanced** from the **Tools** menu to switch from VirusScan Classic to VirusScan Advanced. To switch back to VirusScan Classic, choose **Classic** from the **Tools** menu.
- **Activating password protection.** Choose **Password Protect** from the **Tools** menu to open a dialog box where you can choose which VirusScan configuration options you want to lock in order to prevent unauthorized changes. See “Enabling password protection” on page 73 of the *VirusScan User’s Guide* for details.
- **Start VirusScan Scheduler.** Choose **Scheduler** from the **Tools** menu to open VirusScan Scheduler, a utility that lets you configure and run unattended scan operations. To learn how to use the Scheduler, see “Scheduling Scan Tasks” on page 147 of the *VirusScan User’s Guide*.
- **Open the online help file.** Choose **Help Topics** from the **Help** menu to see a list of VirusScan help topics. To see a context-sensitive description of buttons, lists and other items in the VirusScan window, choose **What’s this?** from the **Help** menu, then click an item with your left mouse button after your mouse cursor changes to ↖?. You can see these same help topics if you right-click an element in the VirusScan window, then choose **What’s This?** from the menu that appears.

Configuring VirusScan Classic

To perform a scan operation, VirusScan needs to know what you want it to scan, what you want it to do if it finds a virus, and how it should let you know when it has. You can also tell VirusScan to keep a record of its actions. A series of property pages controls the options for each task—click each tab in the VirusScan Classic window to set up VirusScan for your task.

Choosing Where & What options

VirusScan initially assumes that you want to scan your C: drive and all of its subfolders, and to restrict the files it scans only to those susceptible to virus infection (Figure 5-3).



Scan in: C:\

☑ Include subfolders

○ All files

● Program files only

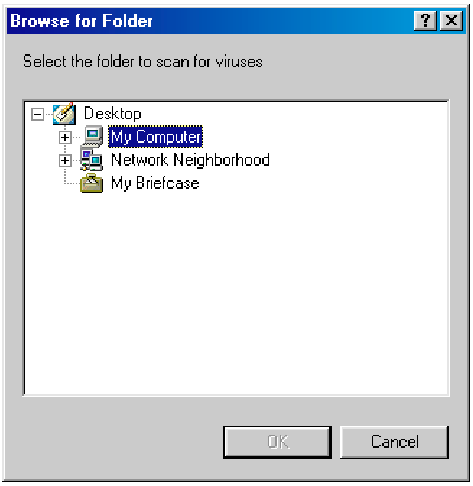
□ Compressed files

Figure 5-3. VirusScan Classic window - Where & What page

To modify these options, follow these steps:

1. Choose a volume or folder on your system or on your network that you want VirusScan to examine for viruses.

   You can type a path to the target volume or folder in the **Scan in** text box, or click **Browse** to open the Browse for Folder dialog box (Figure 5-4).



Select the folder to scan for viruses

Figure 5-4. Browse for Folder dialog box

   Click ⊞ to expand the listing for an item shown in the dialog box. Click ⊟ to collapse an item. You can select hard disks, folders or files as scan targets, whether they reside on your system or on other computers on your network. You cannot select My Computer, Network Neighborhood, or multiple volumes as scan targets from VirusScan Classic—to choose these items as scan targets, you must switch to VirusScan Advanced.

When you have selected your scan target, click **OK** to return to the VirusScan Classic window.

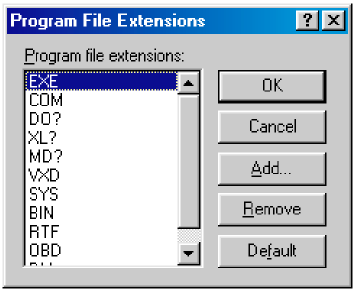
2. Select the **Include subfolders** checkbox to have VirusScan look for viruses in any folders inside your scan target.

3. Specify the types of files you want VirusScan to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have VirusScan look for viruses in files compressed with these formats: .??_, .CAB, LZEXE, LZH, PKLite, .TD0, and .ZIP. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

   - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations.

     To do so, select the **Program files only** button. To see or designate the file name extensions VirusScan will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 5-5).



EXE
COM
DO?
XL?
MD?
VXD
SYS
BIN
RTF
OBD

Figure 5-5. Program File Extensions dialog box

By default, VirusScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .MD?, .VXD, .SYS, .BIN, .RTF, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, .MD?, and .OBD extensions are Microsoft Office files, all of which can harbor macro virus infections. The ? character is a wildcard that enables VirusScan to scan both document and template files.

- To add to the list, click **Add**, then type the extensions you want VirusScan to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Remove**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

To have VirusScan examine all files on your system, whatever their extensions, select the **All files** button. This will slow your scan operations down considerably, but will ensure that your system is virus free.

4. Click the Action tab to choose additional VirusScan options.

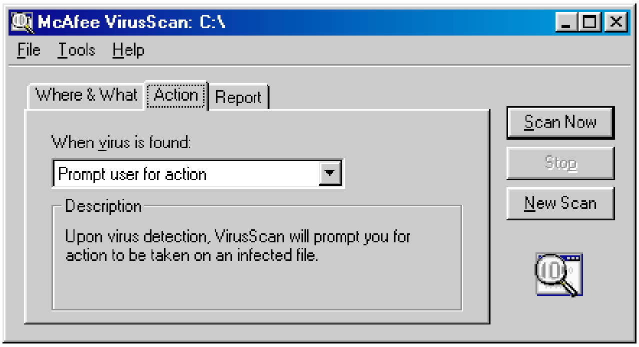
   To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Action options

When VirusScan detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VirusScan to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the VirusScan Classic window to display the correct property page (Figure 5-6).



When virus is found:

Prompt user for action

Description

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

Figure 5-6. VirusScan Classic window - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each response. Your choices are:

- **Prompt User for Action.** Choose this response if you expect to be at your computer when VirusScan scans your disk—VirusScan will display an alert message when it finds a virus and offer you the full range of its available response options.

- **Move infected files automatically**. Choose this response to have VirusScan move infected files to a quarantine directory as soon as it finds them. By default, VirusScan moves these files to a folder named INFECTED that it creates at the root level of the drive on which it found the virus. For example, if VirusScan found an infected file in T:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VirusScan would copy the file to T:\INFECTED.

  You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.

- **Clean infected files automatically.** Choose this response to tell VirusScan to remove the virus code from the infected file as soon as it finds it. If VirusScan cannot remove the virus, it will note the incident in its log file. See “Choosing Report options” on page 69 of the *VirusScan User’s Guide* for details.

- **Delete infected files automatically.** Use this option to have VirusScan delete every infected file it finds immediately. Be sure to enable its reporting feature so that you have a record of which files VirusScan deleted. You will need to restore deleted files from backup copies. If VirusScan cannot delete an infected file, it will note the incident in its log file.

- **Continue scanning.** Use this option only if you plan to leave your computer unattended while VirusScan checks for viruses. If you also activate the VirusScan reporting feature (see “Choosing Report options” on page 69 of the *User’s Guide* for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Report tab to choose additional VirusScan options.

   To start a scan operation immediately with just the options you’ve chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

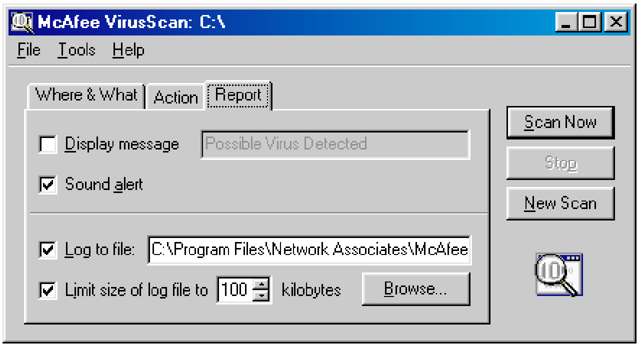
Choosing Report options

By default, VirusScan beeps to alert you when it finds a virus. You can use the Report page to enable or disable this alert, or to add an alert message to the Virus Found dialog box that appears when VirusScan finds an infected file. This alert message can contain any information, from a simple warning to instructions about how to report the incident to a network administrator.

This same page determines the size and location of VirusScan’s log file. By default, the program lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSCLOG.TXT. You can have VirusScan write its log to this file, or you can use any text editor to create a text file for VirusScan to use. You can then open and print the log file for later review from within VirusScan or from your text editor.

To choose VirusScan alert and log options, follow these steps:

1. Click the Report tab in the VirusScan Classic window to display the correct property page (Figure 5-7).



☐ Display message: Possible Virus Detected

☑ Sound alert

☑ Log to file: C:\Program Files\Network Associates\McAfee

☑ Limit size of log file to 100 kilobytes

Figure 5-7. VirusScan Classic window - Report page

2. Choose the types of alert methods you want VirusScan to use when it finds a virus. You can have VirusScan:

    - **Display a custom message.** Select the **Display message** checkbox, then enter the message you want to appear in the text box provided. You can enter a message up to 225 characters in length.

      NOTE: To have VirusScan display your message, you must have selected **Prompt user for action** as your response in the Action page (see “Choosing Action options” on page 69 for details).

    - **Beep.** Select the **Sound alert** checkbox.

3. Select the **Log to file** checkbox.

   By default, VirusScan writes log information to the file VSCLOG.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

4. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

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

5. Click a different tab to change any of your VirusScan settings.

   To start a scan operation immediately with the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Index

A

action options, choosing
- in VirusScan Classic, 69 to 70

ActiveX controls
- as malicious software, 9

alert messages
- audible, sounding, 71

America Online
- mail client, supported in VShield, 52
- technical support via, 15

anti-virus software
- reporting new viruses not detected by to Network Associates, 16

audible alert messages, sounding, 71

authenticating Network Associates files, use of VALIDATE.EXE for, 32 to 34

B

background scan tasks, configuring
- in configuration wizard, 55

BOOTSCAN.EXE
- use of on Emergency Disk, 36

browsers supported in VShield, 52

C

.CAB (Compressed Application Binary) files, scanning, 68

cc:Mail
- as e-mail client supported in VShield, 52
- choosing correct options for
  - in configuration wizard, 56

checking files with VALIDATE.EXE, 32 to 34

components, included with VirusScan, 10 to 12

compressed files
- scanning, 68

CompuServe, technical support via, 15

computer problems, attributing to viruses, 35

configuration
- of VirusScan Classic, 66 to 72
- of VShield
  - using wizard, 53 to 59

configuration wizard
- Download Scan module options, choosing with, 57
- E-mail Scan module options, choosing with, 56
- Internet Filter module options, choosing with, 58
- starting, 53
- System Scan module options, choosing with, 55
- using, 53 to 59

corporate e-mail systems, choosing
- in configuration wizard, 56

crashes, when not attributable to viruses, 13 to 14

Customer Care
- contacting, 14

D

.DAT file updates
- reporting new items for, 16

defaults

scan targets, 68

descriptions, of VirusScan program components, 10 to 12

detection

options

adding scan targets, 67

Disable

in **Task** menu, 62

VShield, 60 to 62

disks

choosing as scan targets, 67

floppy

locking or write-protecting, 38

distribution of VirusScan

electronically and on CD-ROM disc, 21

Download Scan module

default response options for, 42 to 43

set up

using configuration wizard, 57

E

EICAR "virus," use of to test installation, 34

e-mail

addresses for reporting new viruses to Network Associates, 16

client software

choosing in configuration wizard, 57

supported in VShield, 52

E-mail Scan module

set up

using configuration wizard, 56

E-Mail Scan program component, default responses when virus found, 46 to 48

Emergency Disk

creating

on uninfected computer, 36

without the creation wizard, 37 to 38

files to copy for, 38

use of BOOTSCAN.EXE on, 36

use of to reboot system, 36

Enable

in VShield shortcut menu, 60

Eudora and Eudora Pro

as e-mail clients supported in VShield, 52

Exchange

as e-mail client supported in VShield, 52

Exit, in VShield shortcut menu, 60

extensions, use of to identify scan targets, 68

F

File Info

in **File** menu, 49

file information, viewing, 48 to 49

File menu

File Info, 49

file name extensions

use of to identify vulnerable files, 68

file validation using VALIDATE.EXE, 32 to 34

files

choosing as scan targets, 67

infected

cleaning, 69 to 70

cleaning yourself when VirusScan cannot, 36

deleting, 69 to 70

moving, 69 to 70

VSCLOG.TXT, as VirusScan log, 71 to 72

floppy disks

locking or write-protecting, 38

folders

choosing as scan targets, 67

H

Help

opening from VirusScan Classic and VirusScan Advanced, 66

Help Topics

in **Help** menu, 66

hostile objects

Java classes and ActiveX controls as, 9

I

infected files

cleaning yourself when VirusScan cannot, 36

moving, 70

removing viruses from, 35 to 48

use of quarantine folder to isolate, 70

installation

aborting if virus detected during, 35 to 37

testing effectiveness of, 34

Internet

dangers from, 9

e-mail clients, choosing

in configuration wizard, 56

Internet Explorer

as browser supported in VShield, 52

Internet Filter module

default response options for, 44

set up

using configuration wizard, 58

J

Java classes

as malicious software, 9

L

log file

creating with text editor, 71 to 72

limiting size of, 72

VSCLOG.TXT as, 71 to 72

Lotus cc:Mail

as e-mail client supported in VShield, 52

choosing correct options for

in configuration wizard, 56

LZEXE files, scanning, 68

LZH files, scanning, 68

M

malicious software

ActiveX controls as, 9

Java classes as, 9

MAPI (Messaging Application Programming Interface) e-mail clients

choosing in configuration wizard, 56

supported in VShield, 52

McAfee Emergency Disk

creating

on uninfected computer, 36

files to copy for, 38

use of to reboot system, 36

menus, shortcut

use of from system tray

for VShield, 59

Microsoft

Exchange, Outlook and Outlook Express, as e-mail clients supported in VShield, 52

Internet Explorer

as browser supported in VShield, 52

N

Netscape Navigator and Netscape Mail

as browser and e-mail client supported in VShield, 52

Network Associates

contacting

Customer Care, 14

outside the United States, 17

via America Online, 15

via CompuServe, 15

within the United States, 15

training, 16

new viruses, reporting to Network Associates, 16

O

objects, Java and ActiveX

as malicious software, 9

online help

opening from VirusScan Classic and VirusScan Advanced, 66

options

VirusScan Classic

Action, 69 to 70

Report, 71 to 72

Where & What, 66 to 69

Outlook and Outlook Express

as e-mail clients supported in VShield, 52

distinguishing between, 57

P

panic, avoiding when your system is infected, 35

PKLite files, scanning, 68

POP-3 e-mail clients, choosing options for

in configuration wizard, 57

program components, included with VirusScan, 10 to 12

program extensions, designating as scan targets, 68

Properties

in VShield shortcut menu, 53

VShield

setting with configuration wizard, 53 to 59

Q

Qualcomm Eudora and Eudora Pro

as e-mail clients supported in VShield, 52

quarantine folder, use of to isolate infected files, 70

quick start for VShield configuration, 53 to 59

quitting VShield, 60 to 62

R

reasons to run VShield, 51

rebooting, with the McAfee Emergency Disk, 36

remover

actions available when VirusScan has none, 36

report file

limiting size of, 72

VSCLOG.TXT as, 71 to 72

report options, choosing

in VirusScan Classic, 71 to 72

reporting viruses not detected to Network Associates, 16

rescue disk, creating without the creation wizard, 37 to 38

response options

choosing

when Download Scan module finds a virus, 42 to 43

when E-mail Scan module finds a virus, 41 to 42

when Internet Filter module finds harmful objects, 44

when System Scan module finds a virus, 39 to 41

when the E-Mail Scan program component detects a virus, 46 to 48

when VirusScan detects a virus, 44 to 46

setting

for VirusScan Classic, 69 to 70

responses, default, when infected by viruses, 35 to 48

restarting

with the McAfee Emergency Disk, 36

right-clicking

use of to display shortcut menus for VShield, 59

S

scan operations, deciding when to start, 13

scan task

action options, configuring, 69 to 70

logging options, configuring

in VirusScan Classic, 71 to 72

report options, configuring

for VirusScan Classic, 71 to 72

targets for

adding, 67

Where & What options, configuring, 66 to 69

settings

VShield, choosing with configuration wizard, 53 to 59

Setup

aborting if virus detected during, 35 to 37

shortcut menus

use of with VShield, 59

SMTP e-mail clients

choosing options for

in configuration wizard, 57

software conflicts, as potential cause for computer problems, 13 to 14

Start menu

using to start VirusScan Classic, 63

Status dialog box

using to disable and enable VShield modules, 60 to 61

Stop

VShield, 60 to 62

system crashes, attributing to viruses, 35

system requirements

for VirusScan, 21

System Scan

in VShield shortcut menu, 53

System Scan module

default response options for, 39 to 41

set up

using configuration wizard, 55

system tray

location of VShield icon, 53

T

targets for scanning

adding, 67

task

action options, configuring, 69 to 70

adding scan targets to, 67

logging options, configuring

in VirusScan Classic, 71 to 72

report options, configuring

for VirusScan Classic, 71 to 72

Where & What options, configuring, 66 to 69

Task menu

Disable, 62

taskbar

location of VShield icon in, 53

.TD0 files, scanning, 68

technical support

e-mail address for, 15

information needed from user, 15

online, 15

phone numbers for, 15

testing your installation, 34

text

editor, use of to create log file, 71 to 72

Total Virus Defense

VirusScan as component of, 9

training for Network Associates products, 16

scheduling, 16

U

uninfected computer, use of to create Emergency Disk, 36

V

VALIDATE.EXE, use of to verify Network Associates software, 32 to 34

Virus Information Libarary, connecting to from VirusScan, 48 to 49

Virus Information Library

use of to learn how to remove viruses, 37

viruses

deciding when to start scan operations for, 13

default response to

when E-Mail Scan program component detects, 46 to 48

when VirusScan detects, 44 to 46

when VShield detects, 39 to 44

effects of, 35 to 48

recognizing when computer problems do not result from, 13 to 14

removing

before installation, necessity of and steps for, 35 to 37

from infected files, 35 to 48

reporting new strains to Network Associates, 16

viewing information about, 48 to 49

VirusScan

Action options

configuring in VirusScan Classic, 69 to 70

as component of Total Virus Defense suite, 9

components included with, 10 to 12

default responses to virus detection, 44 to 46

description of program components, 10 to 12

distribution methods, 21

files to copy for Emergency Disk, 38
installation
as best protection against infection, 35
what to do when virus found during, 35 to 37
introducing, 9
main window
use of to select responses to infections, 45
overview of features, 9
property pages
Action, 69 to 70
Where & What, 66 to 69
validating with VALIDATE.EXE, 32
what it does, 63
VirusScan Classic
Action options, choosing, 69 to 70
Report options, choosing, 71 to 72
starting, 63
Where & What options, choosing, 66 to 69
VirusScan Command Line
use of when booting with Emergency Disk, 36
VirusScan Scheduler
disabling and enabling VShield from, 61
VSCLOG.TXT, as VirusScan report file, 71 to 72
VShield
browsers and e-mail clients supported in, 52
configuration wizard
starting, 53
using, 53 to 59
default responses to virus detection, 39 to 44
disabling and enabling, 60 to 62
Download Scan module
default response options for, 42 to 43
E-mail Scan module
default response options for, 41 to 42
icon in system tray, 53
using to disable VShield, 60
Internet Filter module
default response options for, 44
Properties dialog box
using to disable and enable VShield modules, 61
Wizard button in, 54
reasons to run, 51
shortcut menu
Enable, 60
Exit, 60
Properties, 53
System Scan, 53
Status dialog box, using to disable and enable VShield modules, 60 to 61
stopping and unloading from memory, 60 to 62
System Scan module
default response options for, 39 to 41
unloading from memory, 60 to 62
what it does, 51
Vshield
components included with VirusScan, 10 to 12

W

Where & What options
choosing in VirusScan Classic, 66 to 69
Windows Compressed files (.??_), scanning, 68

Windows Start menu, using to start VirusScan Classic., 63

Wizard, button in VShield Properties dialog box, 54

write protection, enabling for floppy disks, 38

Z

.ZIP files, scanning, 68