McAfee VirusScan for
Windows 95 and Windows 98

Getting Started Guide

Version 5.0

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES, INC. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND 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, McAfee 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 bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

(i.e., the required number of licenses 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 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 specified for the licenses you have obtained. 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 Documentation's proprietary notices.

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

2. **Term.** This Agreement is effective for an unlimited duration unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. **Updates.** For the time period specified in the applicable price list or product packaging for the Software you are entitled to download revisions or updates to the Software when and as McAfee publishes them via its electronic bulletin board system, website or through other online services. For a period of ninety (90) days from the date of the original purchase of the Software, you are entitled to download one (1) revision or upgrade to the Software when and as McAfee publishes it via its electronic bulletin board system, website or through other online services. After the specified time period, you have no further rights to receive any revisions or upgrades without purchase of a new license or annual upgrade plan to the Software.

4. **Ownership Rights.** The Software is protected by United States copyright laws and international treaty provisions. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must 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. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the applicable list price or product packaging for the Software. You may not transfer any of the rights granted to you under this Agreement. You may not reverse engineer, decompile, or disassemble the Software, except to the extent 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 or Documentation 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 McAfee. McAfee 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.** McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be free from defects in materials and workmanship.

   b. **Customer Remedies.** McAfee's and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee's option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to McAfee 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 McAfee is subject to restrictions under United States export control laws and regulations.

   c. **Warranty Disclaimer.** Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MCAFEE 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. 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, MCAFEE 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. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL MCAFEE 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 MCAFEE BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE MCAFEE CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF MCAFEE 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 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 OF THE FOLLOWING: 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 THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY PERSONAL OR BUSINESS 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 TO, OR IMPORTATION OF, ENCRYPTION BY: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE IT IS YOUR ULTIMATE RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS AND THAT MCAFEE HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. **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"). McAfee expressly disclaims any express or implied warranty of fitness for High Risk Activities.

11. **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. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. This Agreement supersedes any other communications with respect to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee or a duly authorized representative of McAfee. 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.

12. **McAfee Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call (408) 988-3832, fax (408) 970-9727, or write: McAfee Software, 3965 Freedom Circle, Santa Clara, California 95054. http://www.mcafee.com.

    Statements made to you in the course of this sale are subject to the Year 2000 Information and Readiness Disclosure Act (Public Law 105-271). In the case of a dispute, this Act may reduce your legal rights regarding the use of any statements regarding Year 2000 readiness, unless otherwise specified in your contract or tariff.

Table of Contents

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 now emerging 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 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 consist of one or more related programs that each 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 programs share. These files include VirusScan .DAT files, default configuration files, validation files, the Virus List and similar common files.

- **Command Line Scanners.** This set consists of two powerful scanning agents—SCAN.EXE and BOOTSCAN.EXE, both of which allow you to initiate targeted scan operations from the MS-DOS Prompt window. 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 programs as backups.

  Normally, BOOTSCAN.EXE runs as soon as you start your system. It checks for viruses that hide within the boot sectors on your hard disk, or that load themselves into memory during the boot process. Although you can use SCAN.EXE as an independent program to scan your system from the DOS prompt, VirusScan uses it as the scan program you run from the included Emergency Disk. Its low resource requirements allow you to fit both SCAN.EXE and boot files onto a single floppy disk. With the Emergency Disk, you can boot into a virus-free environment to scan your computer's hard disk and memory. lists the command-line switches you can use when you run SCAN.EXE.

- **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 complete reports on its actions. You can get started quickly with VirusScan's basic configuration mode, or move to its advanced mode for maximum flexibility. See the "McAfee VirusScan Advanced Options User Guide" for details.

- **VirusScan Central**. This component features a simple but dynamic interface that serves as the heart of the VirusScan program suite. Use it to start each of the other components, to see statistics, reports and other information, and to update your VirusScan data files. See "Using VirusScan Central" on page 37 for details.

- **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 what parts of your system to scan, when to scan them, which 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 MAPI-compliant mail clients, and it can filter away 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.

- **cc:Mail Scan.** This component includes technology optimized for scanning Lotus cc:Mail mailboxes that do not use Microsoft's Messaging Application Programming Interface (MAPI) standard. Install and use this component if your workgroup or network uses cc:Mail v7.x or earlier.

- **MAPI Scanner**. This component allows you to scan, at your initiative, the Inbox or other mailbox for e-mail client applications that adhere to Microsoft's Messaging Applications Programming Interface (MAPI). Use it to supplement the continuous background scanning VShield provides for MAPI clients such as Microsoft Exchange and Microsoft Outlook.

- **McAfee ScreenScan**. This optional component scans your computer as your screen saver runs during idle periods.

- **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.

- **Safe & Sound**. This component lets you create automatic or interactive backups of selected drives, directories, files or file types. You can back up to a protected volume file (a separate area on the drive). A protected volume file contains information about each file in every sector to ensure that files can be recovered even if the hard drive's directories and data are severely damaged or lost. You can also create mirror backups that instantly back up data as you save it, make backups after a time delay when the PC is idle, or create manual backups.
- **Documentation.** VirusScan documentation includes:
  - A printed *Getting Started Guide*, which introduces the product, provides installation instructions, outlines how to respond if you suspect your computer has a virus, and gives an overview of VirusScan Central and its basic scan operations.
  - A *User's Guide* saved on the VirusScan CD-ROM or installed on your hard disk in Adobe Acrobat .PDF format. The *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 from within the product itself. To open the help file from VirusScan Central, select Help in the upper right-hand corner of the window.

    VirusScan also includes context-sensitive online help. To see help topics, right-click buttons, lists or other elements within dialog boxes, or click **Help** buttons where you see them.
  - A README.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 README.TXT file at the root level of your VirusScan CD-ROM—you can open and print it from Windows Notepad, or from nearly any word-processing software.
  - A README.1ST file. This file outlines the terms of your license to use VirusScan. Read it carefully—by installing VirusScan you agree to its terms.

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 in between scanning operations. Under most circumstances this should protect your system 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 the likely points of virus entry, such as

- Whenever you insert a floppy disk into your floppy drive
- Whenever you start an application or open a file
- Whenever a file’s size or other identifying characteristics change

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. VirusScan will even tell you when you should update your data files and offer to download them for you.

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 speed, flexibility and power of the modern PC. 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.

More serious, however, 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.

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 other electronic services; and on CD-ROM. Once you have downloaded a VirusScan archive or placed your VirusScan installation disc in your CD-ROM drive, the installation steps are the same. Review the system requirements shown below to verify that VirusScan will run on your system, then follow the installation steps on page 16.

- **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 80486 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 20 MB of free hard disk space.
- At least 16MB of random-access memory (RAM).
- Microsoft Windows 95 or Microsoft 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. To obtain an Internet connection, contact a local Internet service provider.

Installation Steps

Select from the following:

- **If you downloaded your copy of VirusScan** from the Network Associates website or 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. These utilities are available from most online services.

  E **IMPORTANT:** If you suspect that your computer has a virus infection, download and install the VirusScan installation files onto a computer that is ***not*** infected. Then use the McAfee Rescue Disk utility during setup to make a disk that you can use to boot your infected computer and remove the virus. For more information, see "If you suspect you have a virus..." on page 21.

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

After inserting the CD-ROM, the McAfee VirusScan welcome screen should automatically appear (Figure 2-1).

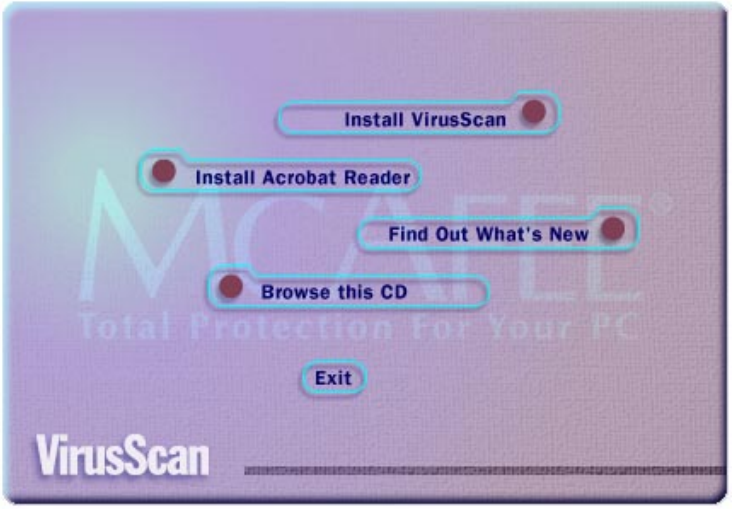

Figure 2-1. McAfee VirusScan welcome screen

To install VirusScan immediately, click **Install VirusScan** and follow the on-screen instructions.

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

Follow these steps:

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

   The Run dialog box appears (Figure 2-2).

Figure 2-2. The Run dialog box

2. Type <X>:\SETUP.EXE and 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 files on your hard disk or CD-ROM, click **Browse**.

   - **NOTE:** If your VirusScan copy came on a VirusScan Security Suite or a Total Virus Defense CD-ROM, you must also specify which folder contains VirusScan for Windows 98. For more information, see the CONTENTS.TXT file included on that CD-ROM.

   The first installation wizard panel appears (Figure 2-3).

Figure 2-3. The Welcome to Setup wizard panel

3. Click **Next>** and follow the on-screen instructions.

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 by ensuring that you

- Download your files only from the Network Associates website or bulletin-board system; 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.
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\McAfee\McAfee VirusScan

   To get to this directory, type `cd progra~1\mcafee\mcafee~1` at the command 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 *.* >lpt1` 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 from 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 >lpt1` 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 file name 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.

E **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.

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 EICAR, a coalition of anti-virus vendors headquartered in Europe, 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 the following line:

```
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.

   E **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 for 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.

If VirusScan detects a virus in 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 22.

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. Insert the McAfee Emergency Disk that came with your copy of VirusScan 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" on page 23.

3. Start your computer again.

   The Emergency Disk will boot your computer and immediately start SCAN.EXE, a command-line version of VirusScan. 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.

   - **NOTE:** If you do not see SCAN.EXE start, type this command at the A> prompt:

     ```
     SCAN /ADL /ALL /CLEAN
     ```

     This tells Scan to look for viruses in all of your files on all of your local drives.

   Once you start it, Scan 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 Scan finishes examining your system, you can either:

   - **Return to working with your computer.** If Scan 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 Scan found a virus, but could not remove the virus code from the file, it will identify the infected file and tell you that it could not clean the file, 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 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 that can help you remove a virus from an infected file. To learn how, visit the Network Associates website at http://www.nai.com/vinfo. Look for one of these documents in the online Virus Information Library:

     #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

If you misplace your copy of the Emergency Disk that comes with VirusScan, or if you downloaded your VirusScan copy from one of the Network Associates electronic services, you will need to create an Emergency Disk for your use.

\+ **WARNING:** If VirusScan detected a virus as it tried to install itself on your computer, you must install VirusScan on an *uninfected* computer, then create your Emergency Disk on that system. You can then start the infected system with the Emergency Disk, remove the infecting virus, then install VirusScan on that system. Be sure to remove the VirusScan copy from the first system unless you have a license that allows you to install multiple VirusScan copies.

To create an Emergency Disk with the VirusScan Emergency Disk utility, follow these steps:

1. Insert a blank 1.44MB disk into your floppy drive.
2. Start VirusScan Central.
3. Click **Options**, point to **Tools**, and Select **Emergency Disk**. The Emergency Disk Wizard opens. (Figure 3-4). Click **Next>**.
4. If you did select the Create a Rescue Disk Set option, the first Emergency Disk Wizard panel appears.

Figure 3-4. First Emergency Disk Wizard panel

5. Click **Next>**.
6. The second Emergency Disk Wizard panel appears.

Figure 3-5. Second Emergency Disk Wizard panel

7. Select from the following:

- If the disk is formatted, select the Don't Format option and click **Next>**.

  You are prompted to insert a disk.

  Insert the floppy disk into your floppy drive and click **Next>**.

  The wizard begins creating the Emergency Disk. When it is finished, click **Finish**, write protect the disk, and label it "McAfee Emergency Boot Disk."

- If the disk is not formatted, select Format using the installed operating system option, click **Next>**, and follow these substeps:

  a. Insert an unformatted floppy disk into your floppy drive and click **Next>**.

     The Format dialog box appears.

  b. Select **Full** in the **Format type** area, select the **Copy system files** checkbox in the **Other Options** area, and click **Start**.

  c. Windows will format your floppy disk and copy the necessary system files. Click **Close** when it has finished.

     You are returned to the Emergency Disk Wizard.

  d. Click **Next>**.

     The wizard begins creating the Emergency Disk. When it is finished, click **Finish**, write protect the disk, and label it "McAfee Emergency Boot Disk."

- If the disk is formatted with system files, select the Create an NAI-OS emergency disk option and click **Next>**.

  You are prompted to insert a disk.

  Insert the floppy disk into your floppy drive and click **Next>**.

  The wizard begins creating the Emergency Disk. When it is finished, click **Finish**, write protect the disk, and label it "McAfee Emergency Boot Disk."

- **NOTE:** A write-protected 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 software cannot write to a write-protected disk, viruses cannot infect it.

Creating an Emergency Disk without the utility

If you cannot use the 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 by following these steps:

+ **WARNING:** If VirusScan detected a virus as it tried to install itself on your computer, you must 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 a: /s/u/v
   ```

   Next, press **ENTER** 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 “E-disk” or another 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\mcafee\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 these commands at the MS-DOS prompt to copy the correct files to the Emergency Disk:

   ```
   copy bootscan.exe a:

   copy emscan.dat a:

   copy emnames.dat a:

   copy emclean.dat a:
   ```

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. 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. In its initial configuration, the module will prompt you for a response when it detects a virus during any of these operations (Figure 3-6).

Figure 3-6. System Scan response options

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

- **Stop.** Click this to tell VShield to take no action. Normally, you would use this option to bypass files that you know do not have viruses. VShield will note each incident in its log file.
- **Clean.** Click this 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.** 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 infected attachment in its log file so that you can restore it from a backup copy.
- **Move File to.** Click this to tell VShield to move infected files to a quarantine directory as it finds them. By default, VShield 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 VShield found an infected file in T:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VShield would copy the file to T:\INFECTED.
- **Exclude file.** Click this to tell VShield not to scan the file from now on. Unless you know the file is not infected, this option is not recommended.

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 3-7). A fourth option provides you with additional information.

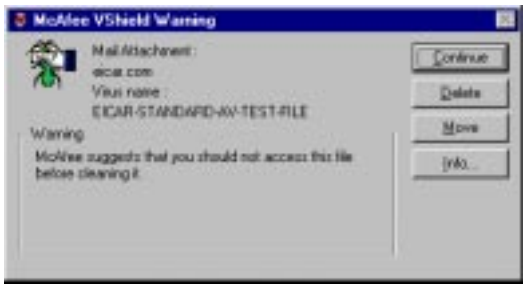

Figure 3-7. E-mail Scan module response options

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. 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 infected attachment in its log file so that you can restore it from a backup copy.
- **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.** Opens the Virus Information Center where you can view information about the virus (requires Internet connection). This choice does not cause the program to take any action against the virus it detected. See "Opening the Virus Information Center" on page 44 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.

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. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-8). A fourth option provides you with additional information.

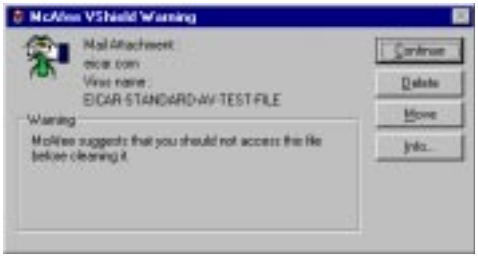

Figure 3-8. Download Scan response options

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

- **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 so that you can restore the file from a backup copy.
- **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.
- **Continue.** Click this to tell VShield to take no action and to resume scanning. 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.
- **Info.** Opens the Virus Information Center where you can view information about the virus (requires Internet connection). This choice does not cause the program to take any action against the virus it detected. See "Opening the Virus Information Center" on page 44 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 whether 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 3-9).

Figure 3-9. 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 3-10).

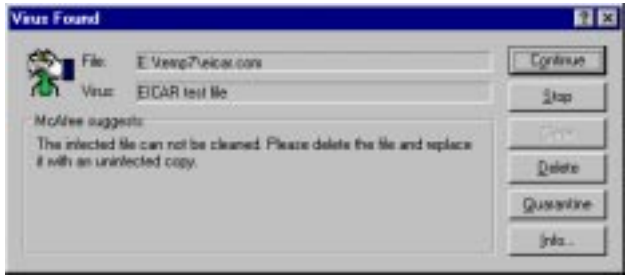

Figure 3-10. VirusScan response options

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

- **Continue.** VirusScan will proceed with its scan operation, list each infected file in the lower portion of its main window (Figure 3-11), and record each detection in its log file, but it will 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.

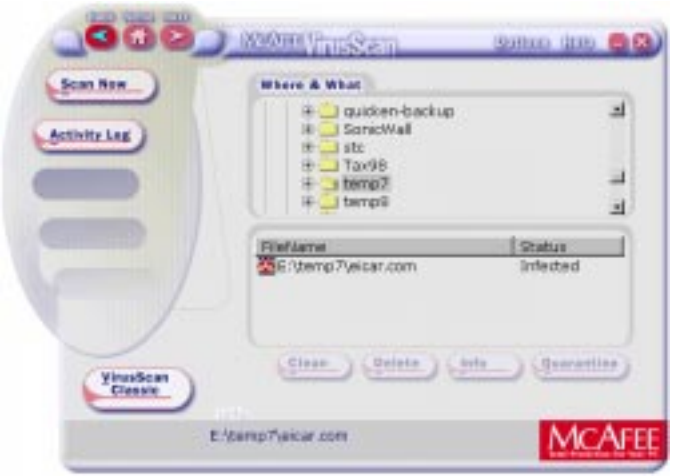

Figure 3-11. VirusScan main window

- **Stop.** VirusScan 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 3-11) 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.** VirusScan 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 3-10, 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.** VirusScan will immediately delete the file from your system. 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.** VirusScan 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.** Opens the Virus Information Center where you can view information about the virus (requires Internet connection). This choice does not cause the program to take any action against the virus it detected. See "Opening the Virus Information Center" on page 44 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, capabilities that VShield lacks. In its initial configuration, E-Mail Scan will prompt you for a response when it finds a virus (Figure 3-12).

Figure 3-12. 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 (see Figure 3-13 on page 34), and record each detection in its log file, but it will take no other action to respond to the virus. Once E-Mail Scan 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 (see Figure 3-13 on page 34) 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.

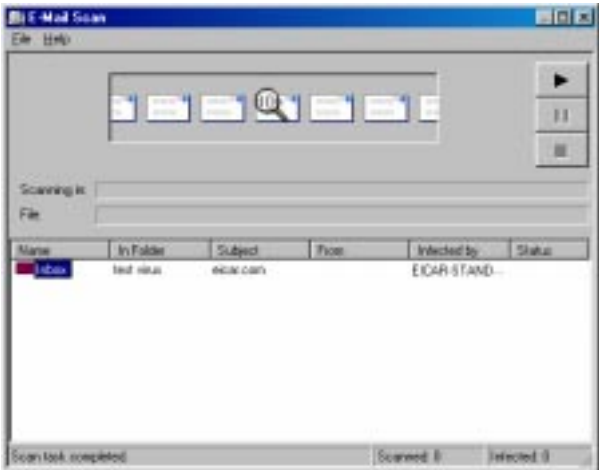

Figure 3-13. E-Mail Scan window

- **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 3-12, **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 file to.** 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.** Opens the Virus Information Center where you can view information about the virus. This choice does not cause the program to take any action against the virus it detected. See "Opening the Virus Information Center" on page 44 for more details.

Understanding false detections

A false detection occurs when VirusScan sends a virus alert message or makes a log file entry that identifies a virus where none actually exists. You are more likely to see false detections if you have anti-virus software from more than one vendor installed on your computer, because some anti-virus software stores the code signatures it uses for detection unprotected in memory.

The safest course to take when you see an alert message or log entry is to treat it as a genuine virus threat, and to take the appropriate steps to remove the virus from your system. If, however, you believe that VirusScan has generated a false detection—it has, for example, flagged a file as infected when you have used it safely for years—verify that you are not seeing one of these situations before you call Network Associates:

- **You have more than one anti-virus program running.** If so, VirusScan might detect unprotected code signatures that another program uses and report them as viruses. To avoid this problem, configure your computer to run only one anti-virus program, then shut the computer down and turn off the power. Wait a few seconds before you start the computer again so that the system can clear the other program's code signature strings from memory.
- **You have a BIOS chip with anti-virus features.** Some BIOS chips provide anti-virus features that can trigger false detections when VirusScan runs. Consult the user's guide for your computer to learn about how its anti-virus features work and how to disable them if necessary.
- **You have an older Hewlett-Packard or Zenith PC.** Some older models from these manufacturers modify the boot sectors on their hard disks each time they start up. VirusScan might detect these modifications as viruses, when they are not. Consult the user's guide for your computer to learn whether it uses self-modifying boot code. To solve the problem, use the command-line version of VirusScan to add validation information to the startup files themselves. This method does not save information about the boot sector or the master boot record.
- **You have copy-protected software.** Depending on the type of copy protection used, VirusScan might detect a virus in the boot sector or the master boot record on some floppy disks or other media.

If none of these situations apply, contact Network Associates technical support or send e-mail to AVresearch@nai.com with a detailed explanation of the problem you encounter.

Using VirusScan Central 4

What is VirusScan Central?

VirusScan Central integrates the VirusScan suite of program components into a single, comprehensive interface that puts virus scanning, task scheduling, data file updating, and other tasks within easy reach. With its simple, one-click access to key scanning tools, VirusScan Central lets you get started with basic anti-virus security measures immediately. Once you have assessed your security requirements and become more familiar with VirusScan's configuration options, VirusScan Central opens the way to more advanced options available in each program component. A built-in message pane, meanwhile, keeps you in touch with program operations and suggests ways to improve your anti-virus security measures.

Starting VirusScan Central

To start VirusScan Central, click **Start**, point to **Programs**, then to **McAfee VirusScan**. Next, choose **McAfee VirusScan Central**.

The VirusScan Central window will appear (Figure 4-1).

Figure 4-1. VirusScan Central window

The buttons along the left side of the window take you to different VirusScan component programs. The next section describes how to start and run default operations with each program.

Starting VirusScan program components

Each VirusScan program component specializes in scanning different parts of your system, detecting certain kinds of malicious software, or updating program files. You can start and run each component separately, or you can use them together to provide your system with comprehensive and up-to-date protection.

Starting VirusScan

To begin scanning your system immediately, click **Scan** in the VirusScan Central window. VirusScan Central will start VirusScan, a component that lets you initiate scan operations immediately, or "on demand" (Figure 4-2).

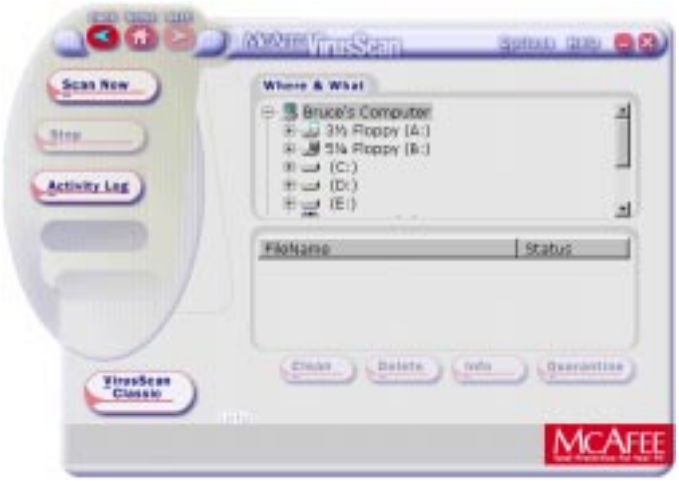

Figure 4-2. VirusScan window

By default, VirusScan 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. VirusScan will also record its actions and summarize its current settings in a log file that you can review later.

To start scanning your system now, click **Scan Now**.

VirusScan will start to look for viruses immediately. A reporting area at the bottom of the window allows you to track its progress and respond to any infected files it finds. See "Responding when VirusScan detects a virus" on page 31 to learn what to do when you have a virus on your system.

If VirusScan finds no viruses on your system, click **Home** after the program finishes scanning to return to VirusScan Central.

Configuring VShield

To open the VShield configuration dialog box, click **VShield** in the VirusScan Central window (Figure 4-3).

Figure 4-3. VShield Configuration dialog box

VShield runs continuously in the background to scan for viruses and other malicious software in your system, in your e-mail, and in files you download from the Internet. When you first install VirusScan and restart your computer, VShield goes to work immediately, using a default set of options designed to give you a basic level of protection.

By default, VShield starts with three of its five modules enabled. You can enable other modules, or you can change the configuration options for any module from within the VShield configuration dialog box.

To enable each module with its default options, click its icon in the list at the left of the dialog box. As you do so, the dialog box will display a set of property pages for that module. The modules include:

- **System Scan.** Select the **Enable System Scan** checkbox to start this module with its default options. This tells VShield to look for viruses in those files most susceptible to virus infection; to scan those files whenever you open, save, rename, or copy them; to scan floppy disks whenever your system reads from them or writes to them, or when your system shuts down; to sound an alert and prompt you for a response if it detects a virus; and to record its actions and summarize its current settings in a log file that you can review later. By default, VShield excludes the Recycle Bin from its scan operations.

- **E-mail Scan.** Select the **Enable Scanning of E-mail attachments** checkbox to start this module. E-mail Scan does not have default settings, so you will need to configure it to work in your environment.

- **Download Scan.** Select the **Enable Internet download scanning** checkbox to scan all files you download from the Internet. This tells VShield to look for viruses in those files most susceptible to virus infection; to scan those files whenever you download them from the Internet; to sound an alert and prompt you for a response if it detects a virus; and to record its actions and summarize its current settings in a log file that you can review later.

  To have VShield use these same settings to scan files attached to e-mail messages you receive from the Internet, select the **Internet Mail (Requires Download Scan)** checkbox in the E-mail Scan module's Detection page. VShield then routinely scans mail you receive via Eudora Pro, Netscape Navigator, and other POP-3 e-mail clients.

- **Internet Filter.** Select the **Enable Java & ActiveX filter** checkbox to start this module. This tells VShield to block any hostile Java classes and ActiveX controls you encounter when you visit websites or connect to other Internet resources; to block certain Internet sites completely; to sound an alert and prompt you for a response if it detects a potentially harmful object; and to record its actions and summarize its current settings in a log file that you can review later.

- **Security.** Select the **Enable password protection** checkbox to activate this module. The Security module does not have any default settings, so you will need to choose a password and decide which of the VShield property pages you want to protect from unauthorized changes.

When you have enabled the modules you want to run and chosen configuration options, click **OK** to return to VirusScan Central.

Starting the Scheduler

To open the Scheduler window, click **Scheduler** in the VirusScan Central window (Figure 4-4).

Figure 4-4. VirusScan Scheduler window

The Scheduler runs scan operations and other tasks at dates and times you choose. The Scheduler is not a scanning program; rather, it relies on such programs as VirusScan or VShield to perform scan operations. Use the Scheduler to run unattended scan operations when they will not interfere with your work, or at regular intervals to maintain your system's security. The Scheduler comes with four pre-configured scan tasks, which provide basic protection for your system.

Using Quarantine Explorer

Many VirusScan components allow you to move infected files to a quarantine folder. This moves infected files from areas where they can be accessed and enables you to clean or delete them at your convenience.

To open the Quarantine Explorer window, click **Quarantine** in the VirusScan Central window (Figure 4-5).

Figure 4-5. Quarantine Explorer window

Quarantine Explorer lists all currently quarantined files. From this page you, can clean an infected file, delete an infected file, restore a file, add a file to the quarantine list, or submit a file that you suspect of being infected to McAfee.

Using VirusScan Tools

To run Safe & Sound, create an emergency diskette, or view virus information, click **Options**, point to Tools, and select a Tool (Figure 4-6).

Figure 4-6. VirusScan Central window with VirusScan Tools palette

The VirusScan Tools set includes a utility that enables backs up your files, a utility to create an Emergency Disk similar to the one that came with your copy of VirusScan, and a link to the Virus Information Center. The following sections describe each tool.

Using Safe & Sound

To start the Safe & Sound Backup Utility(Figure 4-7), click **Options**, point to Tools, and click **Safe & Sound**.

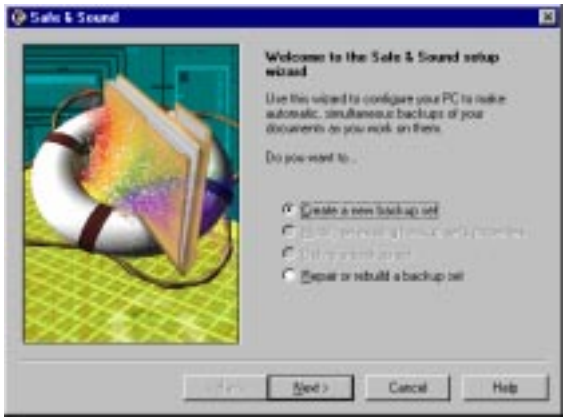

Figure 4-7. Safe & Sound: First Wizard Panel

This utility lets you create automatic or interactive backups of selected drives, directories, files or file types. You can back up to a protected volume file (a separate area on the drive) or a folder. A protected volume file contains information about each file in every sector to ensure that files can be recovered even if the hard drive's directories and data are severely damaged or lost. You can also create mirror backups that instantly back up data as you save it or when the PC is idle.

Creating an Emergency Disk

To start the McAfee Emergency Disk creation utility (Figure 4-8), click **Options**, point to Tools, and click **Emergency Disk**.

Figure 4-8. Emergency Disk Creation Utility dialog box

This utility copies portions of the VirusScan command-line component onto a floppy disk that you can use to boot your computer and scan your system for viruses.

This disk is similar to the Emergency Disk that comes with your copy of VirusScan. However, to create an emergency disk with the utility, you will need a floppy disk formatted with bootable DOS system files. See "Creating an emergency disk" on page 23 to learn how to use the utility.

Opening the Virus Information Center

To open the Virus Information Center, click **Options**, point to Tools, and click **Virus Info**.

NOTE: Access to the Virus Information Center requires an Internet connection. For more information, contact an Internet Service Provider (ISP).

The Virus List is a complete catalog of the more than 16,000 distinct virus strains that VirusScan can detect, remove, or both. The list names the virus and lists its characteristics for quick reference.

To learn about a particular virus, click the first letter of the virus name in the Find Viruses Alphabetically area. Then, scroll through the list until you find the virus that you want to know about and click the virus name.

Updating VirusScan

To start the wizard that will guide you through updating your data (.DAT) files or your product version, click **Update** and follow the on-screen instructions.

Product Support A

BEFORE YOU CONTACT McAfee Software for technical support, locate yourself near the computer with McAfee Guard Dog installed and verify the information listed below:

- Have you sent in your product registration card?
- Version of McAfee VirusScan
- Customer number if registered
- Model name of hard disk (internal or external)
- Version of system software
- Amount of memory (RAM)
- Extra cards, boards or monitors
- Name and version of conflicting software
- EXACT error message as on screen
- What steps were performed prior to receiving error message?
- A complete description of problem

How to Contact McAfee

Customer service

To order products or obtain product information, contact the McAfee Customer Service department at (972) 308-9960 or write to the following address:

McAfee Software
3965 Freedom Circle
Santa Clara, CA 95054
U.S.A.

You can also order products online at http://store.mcafee.com

If you need further assistance or have specific questions about our products, send your questions via email to the appropriate address below:

- For general questions about ordering software: mcafeestore@beyond.com
- For help in downloading software: mcafeedownloadhelp@beyond.com
- For a status on an existing order: mcafeeorderstatus@beyond.com

To inquire about a promotion: mcafeepromotions@beyond.com

Technical support

Support via the web

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web (http://www.mcafee.com) a valuable resource for answers to technical support issues.

We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

Take advantage of the McAfee Product KnowledgeCenter—your free online product support center - 24 hours a day, 7 days a week (http://support.mcafee.com/tech_supp/pkc.asp).

Support forums and telephone contact

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

Table A-1.

World Wide Web	www.mcafee.com
CompuServe	GO MCAFEE
America Online	keyword MCAFEE
Microsoft Network	mcafee

If the automated services do not have the answers you need, please contact McAfee at the following numbers Monday through Friday between 9:00 AM and 6:00 PM Pacific time for 30-day free support, and 24 hours a day - 7 days a week for Per Minute or Per Incident support.

Table A-1.

30-Day Free Telephone Support	972-308-9960
Per Minute Telephone Support	1-900-225-5624
Per Incident Telephone Support ($35)	1-800-950-1165

McAfee training

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

Disclaimer: Time and telephone numbers are subject to change without prior notice.

Download Information (License ID #: VSF500R) B

As a valued McAfee customer, we are committed to keeping your system FREE from virus infection. To protect against the newest virus threats, keep your VirusScan installation up to date!

Per your McAfee Software License Agreement, you are eligible for one (1) FREE Upgrade within ninety (90) days of purchase. This document explains the different ways you can access your FREE VirusScan upgrade.

If you have difficulties downloading or applying the upgrade files through any of the methods listed below, you can call McAfee Technical Support at 972-855-7044.

SecureCast™ (For Windows 95/98 Retail Version):

SecureCast is the easiest way to Update & Upgrade your copy of VirusScan for Windows 95/98. With a click of a button, SecureCast will automatically deliver your software Updates and your FREE product Upgrade to your system. To update your copy of VirusScan, just click the Update button on the VirusScan Central interface.

Internet Access

You will need a World Wide Web (WWW) browser, such as Internet Explorer, Netscape or the AOL web browser to access the McAfee web site.

1. Enter the WWW address for the McAfee Home Page into the appropriate area of your Internet browser. Type: http://www.mcafee.com
2. When the McAfee Home page is loaded, click the "download" tab
3. When the download centers page is loaded (http://www.mcafee.com/centers/download/), look for the highlighted, underlined "Upgrades" and click on this link.
4. On the Upgrade information page, click on the Upgrade McAfee Antivirus link
5. On the McAfee Antivirus Upgrade page enter the Licensed ID#: identified at the top of this card in the appropriate location. Press submit.
6. On the McAfee Antivirus customer identification page enter your email address in location provided and press submit.

7. If previously registered, the thank you page is displayed. To begin download of product - click on the download button.

8. If not previously registered, the McAfee Product Registration page is displayed. You will be asked to enter your Last Name, First Name, Postal Code, Country, State and a password that you make up. Press submit. Once submitted a thank you page is displayed. An access URL will be emailed automatically to email address that you have entered.

9. When the email is opened you will be instructed to click on the url enclosed. A thank you is displayed with a download button. Click on the download button to begin downloading the upgrade.

10. After the file is downloaded and saved to your hard drive, extract or unzip the file (if necessary), and run the setup program.

The information provided in this article is provided "as is" without warranty of any kind. In no event shall McAfee be liable for any damages incurred by use or misuse of the information contained in this article. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Index

I

J

L

M

O

P

Q

R

W