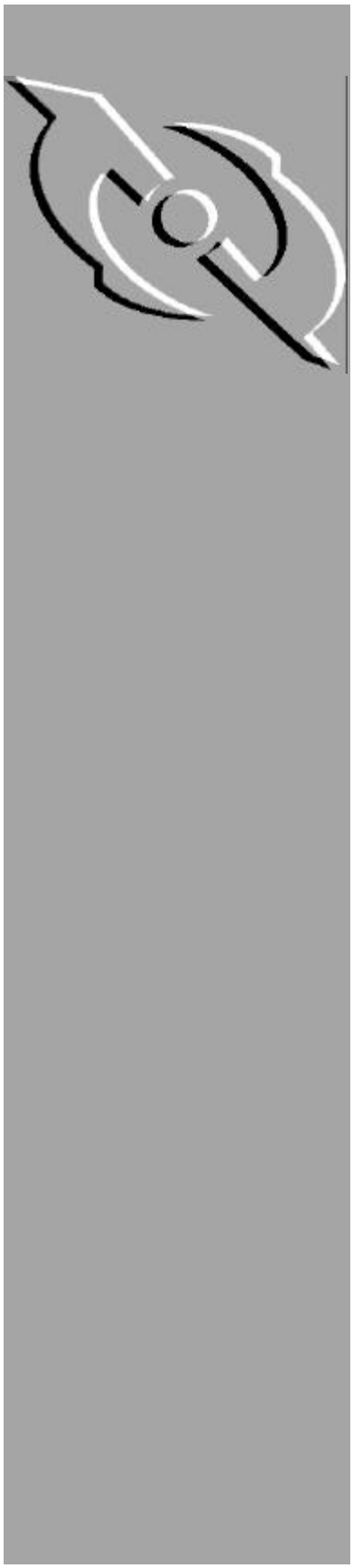

McAfee VirusScan for Windows 95 and Windows 98

User's Guide

Version 4.0

COPYRIGHT

Copyright © 1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

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

Preface

What happened?

If you've ever lost important files stored on your hard disk, watched in dismay as your computer ground to a halt only to display a prankster's juvenile greeting on your monitor, or found yourself having to apologize for abusive e-mail messages you never sent, you know first-hand how computer viruses and other harmful programs can disrupt your productivity. If you haven't yet suffered from a virus "infection," count yourself lucky. But with more than 16,000 known viruses in circulation capable of attacking Windows- and DOS-based computer systems, it really is only a matter of time before you do.

The good news is that of those thousands of circulating viruses, only a comparatively few have the means to do real damage to your data. In fact, the term "computer virus" identifies a broad array of programs that have only one feature in common: they "reproduce" themselves automatically by attaching themselves to host software or disk sectors on your computer, usually without your knowledge. Most viruses cause relatively trivial problems, ranging from the merely annoying to the downright insignificant. Often, the primary consequence of a virus infection is the costs you incur in time and effort to track down the source of the infection and eradicate all of its traces.

Why worry?

So why worry about virus infections, if most attacks do little harm? The problem is twofold: First, although relatively few viruses have destructive effects, that fact says nothing about how widespread the malicious viruses are. In many cases, viruses with the most debilitating effects are the hardest to detect—the virus programmer bent on causing harm will take extra steps to avoid discovery. Second, even relatively "benign" viruses can interfere with the normal operation of your computer and can cause unpredictable behavior in other software. Some viruses contain bugs, poorly written code, or other problems severe enough to cause crashes when they run. Other times, legitimate software has problems running when a virus has, intentionally or otherwise, altered system parameters or other aspects of the computing environment. Tracking down the source of resulting system freezes or crashes drains time and money from more productive activities.

Beyond these problems lies a problem of perception: once infected, your computer can serve as a source of infection for other computers. If you regularly exchange data with colleagues or customers, you could unwittingly pass on a virus that could do more damage to your reputation or your dealings with others than it does to your computer.

The threat from viruses and other malicious software is real, and it is growing worse. The International Computer Security Association has estimated the total worldwide cost in time and lost productivity simply of detecting and cleaning virus infections at $1 billion per year, a figure that doesn't include the costs of data loss and recovery in the wake of attacks that destroyed data.

Where do viruses come from?

As you or one of your colleagues recovers from a virus attack or hears about new forms of malicious software appearing in commonly used programs, you've probably asked yourself a number of questions about how we as computer users got to this point. Where do viruses and other malicious programs come from? Who writes them? Why do those who write them seek to interrupt workflows, destroy data, or cost people the time and money necessary to eradicate them? What can stop them?

Why did this happen to me?

It probably doesn't console you much to hear that the programmer who wrote the virus that erased your hard disk's file allocation table didn't target you or your computer specifically. Nor will it cheer you up to learn that the virus problem will probably always be with us. But knowing a bit about the history of computer viruses and how they work can help you better protect yourself against them.

Virus prehistory

Historians have identified a number of programs that served as virus precursors, or that incorporated features now associated with virus software. Canadian researcher and educator Robert M. Slade traces virus lineage back to special-purpose utilities used to reclaim unused file space and perform other useful tasks in the earliest networked computers. Slade reports that computer scientists at a Xerox Corporation research facility called programs like these "worms," a term coined after the scientists noticed "holes" in printouts from computer memory maps that looked as though worms had eaten them. The term survives to this day to describe programs that make copies of themselves, but without altering host software.

A strong academic tradition of computer prank playing most likely contributed to the shift away from utility programs and toward more malicious uses of the programming techniques found in worm software. Computer science students, often to test their programming abilities, would construct rogue worm programs and unleash them to "fight" against each other, competing to see whose program could "survive" while shutting down rivals. Those same students also found uses for worm programs in practical jokes they played on unsuspecting colleagues.

Some of these students soon discovered that they could use certain features of the host computer's operating system to give them unauthorized access to computer resources. Others took advantage of users who had relatively little computer knowledge to substitute their own programs—written for their own purposes—in place of common or innocuous utilities. These unsophisticated users would run what they thought was their usual software only to find their files erased, to have their account passwords stolen, or to suffer other unpleasant consequences. Such "trojan horse" programs or "trojans," so dubbed for their metaphorical resemblance to the ancient Greek gift to the city of Troy, remain a significant threat to computer users today.

Viruses and the PC revolution

What we now think of as true computer viruses first appeared, according to Robert Slade, soon after the first personal computers reached the mass market in the early 1980s. Other researchers date the advent of virus programs to 1986, with the appearance of the "Brain" virus. Whichever date has the better claim, the link between the virus threat and the personal computer is not coincidental.

The new mass distribution of computers meant that viruses could spread to many more hosts than before, when a comparatively few, closely guarded mainframe systems dominated the computing world from their bastions in large corporations and universities. Nor did the individual users who bought PCs have much use for the sophisticated security measures needed to protect sensitive data in those environments. Most particularly, virus writers found it relatively easy to exploit some PC technologies to serve their own ends.

Boot-sector viruses

Early PCs, for example, "booted" or loaded their operating systems from floppy disks. The authors of the Brain virus discovered that they could substitute their own program for the executable code present on the boot sector of every floppy disk formatted with Microsoft's MS-DOS, whether or not it included system files. Users thereby loaded the virus into memory every time they started their computers with any formatted disk in their floppy drives. Once in memory, a virus can copy itself to boot sectors on other floppy or hard disks. Those who unintentionally loaded Brain from an infected floppy found themselves reading an ersatz "advertisement" for a computer consulting company in Pakistan.

With that advertisement, Brain pioneered another characteristic feature of modern viruses: the payload. The payload is the prank or malicious behavior that, if triggered, causes effects that range from annoying messages to data destruction. It's the virus characteristic that draws the most attention—many virus authors now write their viruses specifically to deliver their payloads to as many computers as possible.

For a time, sophisticated descendants of this first boot-sector virus represented the most serious virus threat to computer users. Variants of boot sector viruses also infect the Master Boot Record (MBR), which stores the partition information your computer needs to figure out where to find each of your hard disk partitions and the boot sector itself.

Realistically, nearly every step in the boot process, from reading the MBR to loading the operating system, is vulnerable to viral sabotage. Some of the most tenacious and destructive viruses still include the ability to infect your computer's boot sector or MBR among their repertoire of tricks. Among other advantages, loading at boot time can give a virus a chance to do its work before your anti-virus software has a chance to run. VirusScan anticipates this possibility by allowing you to create an emergency disk you can use to boot your computer and remove infections.

But boot sector and MBR viruses have a particular weakness: they must spread by means of floppy disks or other removable media, riding concealed in that first track of disk space. As fewer users exchange floppy disks and as software distribution has come to rely on other media, such as CD-ROMs, other virus types have recently eclipsed the boot sector threat. The popularity of large-capacity floppy disks like the Iomega Zip disk and similar disks from Syquest and others, however, could cause a resurgence.

File infector viruses

At about the same time as the authors of the Brain virus found vulnerabilities in the DOS boot sector, other virus writers found out how to use existing software to help replicate their creations. An early example of this type of virus showed up in computers at Lehigh University in Pennsylvania. The virus infected part of the DOS command interpreter COMMAND.COM, which it used to load itself into memory. Once there, it spread to other uninfected COMMAND.COM files each time a user entered any standard DOS command that involved disk access. This limited its spread to floppy disks that contained, usually, a full operating system.

Later viruses quickly overcame this limitation, sometimes with fairly clever programming. Virus writers might, for instance, have their virus add its code to the beginning of an executable file, so that when users start a program, the virus code executes immediately, then transfers control back to the legitimate software, which runs as though nothing unusual has happened. Once it activates, the virus "hooks" or "traps" requests that legitimate software makes to the operating system and substitutes its own responses. Particularly clever viruses can even subvert attempts to clear them from memory by trapping the **CTRL+ALT+DEL** keyboard sequence for a warm reboot, then faking a restart. Sometimes the only outward indication that anything on your system is amiss—before any payload detonates, that is—might be a small change in the file size of infected legitimate software.

Stealth, mutating, encrypted, and polymorphic viruses

Unobtrusive as they might be, changes in file size and other scant evidence of a virus infection usually gives most anti-virus software enough of a scent to locate and remove the offending code. One of the virus writer's principal challenges, therefore, is to find ways to hide his or her handiwork. The earliest disguises were a mixture of innovative programming and obvious giveaways. The Brain virus, for instance, redirected requests to see a disk's boot sector away from the actual location of the infected sector to the new location of the boot files, which the virus had moved. This "stealth" capability enabled this and other viruses to hide from conventional search techniques.

Because viruses needed to avoid continuously reinfecting host systems—doing so would quickly balloon an infected file's size to easily detectable proportions or would consume enough system resources to point to an obvious culprit—their authors also needed to tell them to leave certain files alone. They addressed this problem by having the virus write a code "signature" that would flag infected files with the software equivalent of a "do not disturb" sign. Although that kept the virus from giving itself away immediately, it opened the way for anti-virus software to use the code signatures themselves to find the virus.

In response, virus writers found ways to conceal the code signatures. Some viruses would "mutate" or write different code signatures with each new infection. Others encrypted most of the code signature or the virus itself, leaving only a couple of bytes to use as a key for decryption. The most sophisticated new viruses employed stealth, mutation and encryption to appear in an almost undetectable variety of new forms. Finding these "polymorphic" viruses required software engineers to develop very elaborate programming techniques for anti-virus software.

Macro viruses

By 1995 or so, the virus war had come to something of a standstill. New viruses appeared continuously, prompted in part by the availability of ready-made virus "kits" that enabled even some non-programmers to whip up a new virus in no time. Most existing anti-virus software, however, could easily be updated to detect and dispose of the new virus variants, which consisted primarily of minor tweaks to well-known templates.

But 1995 marked the emergence of the Concept virus, which added a new and surprising twist to virus history. Before Concept, most virus researchers thought of data files—the text, spreadsheet, or drawing documents created by the software you use—as immune to infection. Viruses, after all, are programs and, as such, needed to be able to run in the same way executable software did in order to do their damage. Data files, on the other hand, simply stored information that you entered when you worked with your software.

That distinction melted away when Microsoft began adding macro capabilities to Word and Excel, its flagship applications in its Office suite. Using the stripped-down version of its Visual BASIC language included with the suite, users could create document templates that would automatically format and add other features to documents created with Word and Excel. Virus writers seized the opportunity that this presented to conceal and spread viruses in documents that you, the user, created yourself.

The exploding popularity of the Internet and of e-mail software that allowed users to attach files to messages ensured that macro viruses would spread very quickly and very widely. Within a year, macro viruses became the most potent virus threat ever.

On the frontier

Even as viruses grow more sophisticated and continue to threaten the integrity of computer systems we all have come to depend upon, still other dangers have begun to emerge from an unexpected source: the World Wide Web. Once a repository of research papers and academic treatises, the web has transformed itself into perhaps the most versatile and adaptable medium ever invented for communication and commerce.

Because its potential seems so vast, the web has attracted the attention and the developmental energies of nearly every computer-related company in the industry. Convergences in the technologies that have resulted from this feverish pace of invention now give web page designers tools they can use to collect and display information in ways never previously available. Websites can now send and receive e-mail, formulate and execute queries to databases using advanced search engines, send and receive live audio and video, and distribute data and multimedia resources to a worldwide audience.

Much of the technology that makes these features possible consists of small, easily downloaded programs that interact with your browser software and, sometimes, with other software on your hard disk. This same avenue can serve as an entry point into your computer system for other—less benign—programs to use for their own purposes.

Java and ActiveX

These programs, whether beneficial or harmful, come in a variety of forms. Some are special-purpose miniature applications, or “applets,” written in Java, a new programming language first developed by Sun Microsystems. Others are developed using ActiveX, a Microsoft technology that programmers can use for similar purposes.

Both Java and ActiveX make extensive use of prewritten software modules, or “objects,” that programmers can write themselves or take from existing sources and fashion into the plug-ins, applets, device drivers and other software needed to power the web. Java objects are called “classes,” while ActiveX objects are called “controls.” The principle difference between them lies in how they run on the host system. Java applets run in a Java “virtual machine” designed especially to interpret Java programming and translate it into action on the host machine, while ActiveX controls run as native Windows programs that link and pass data between existing Windows software.

The overwhelming majority of these objects are useful, even necessary, parts of any interactive website. But despite the best efforts of Sun and Microsoft engineers to design security measures into them, determined programmers can use Java and ActiveX tools to plant harmful objects on websites, where they can lurk until visitors unwittingly allow them access to vulnerable computer systems.

Unlike viruses, harmful Java and ActiveX objects usually don’t seek self-replication as their primary goal. The web provides them with plenty of opportunities to spread to target computer systems, while their small size and innocuous nature makes it easy for them to evade detection. In fact, unless you specifically tell your browser software to block them, Java and ActiveX objects automatically download to your system whenever you visit a website that hosts them.

Instead, harmful objects exist to deliver their equivalent of a virus payload. Programmers have written objects, for example, that can read data from your hard disk and send it back to the website you visited, that can “hijack” your e-mail account and send out offensive messages in your name, or that can watch data that passes between your computer and other computers.

Where next?

Malicious software has even begun intruding into areas once thought completely out of bounds. Users of the mIRC Internet Relay Chat client, for example, have reported encountering viruses constructed from the mIRC scripting language. Script viruses get sent as plain text, which would ordinarily preclude them from getting infected, but older versions of the mIRC client software would interpret the instructions coded into the script and perform unwanted actions on the recipient’s computer. The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it.

Some virus writers do it for the thrill of it, some to gain notoriety in their own peer group. Still others do it to exact revenge against employers or others they believe have treated them badly. Whatever their motives, they continue to develop new ways to cause you trouble.

How to protect yourself

VirusScan's advanced protection already gives you an important bulwark against infection and damage to your data, but anti-virus software is only one part of the security measures you should take to protect yourself and your data. Most measures are common sense—checking disks you receive from unknown or questionable sources, either with anti-virus software or some kind of verification utility, is always a good idea. Malicious programmers have gone so far as to mimic the programs you trust to guard your computer, pasting a familiar face on software with a less-than-friendly purpose. VirusScan includes the VALIDATE.EXE utility with its distributions to prevent this type of manipulation, but neither it nor any anti-virus software can detect when someone substitutes a trojan or other malicious program for one of your favorite shareware or commercial utilities.

Web and Internet access poses its own risks. VirusScan gives you the ability to block dangerous web sites so that users can't inadvertently download malicious software from known hazards; it also catches hostile objects that get downloaded anyway. But having a top-notch firewall in place to protect your network and implementing other network security measures is a necessity when unscrupulous attackers can penetrate your network from nearly any point on the globe, whether to steal sensitive data or implant malicious code. You should also make sure that your network is not accessible to unauthorized users, and that your have an adequate training program in place to teach and enforce security standards.

To learn about the origin, behavior and other characteristics of particular viruses, consult the Virus Information Library maintained on the Network Associates website. The Virus List that comes with VirusScan also catalogs all of the viruses that the program can detect and summarizes information about their sizes, the types of infections they attempt, and whether VirusScan can remove them from your files.

Network Associates can provide you with other software in the Total Virus Defense (TVD) suite, the most comprehensive anti-virus solution available, and Total Network Security (TNS), the industry's most advanced network security suite. Network Associates backs them both with outstanding support, training and a worldwide network of research and development teams. Contact your Network Associates representative, or visit the Network Associates website, to find out how to enlist the power of Total Virus Defense on your side.

How to contact Network Associates

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department at (408) 988-3832 or write to the following address:

Network Associates, Inc.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203
U.S.A.

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. 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 and numbers below.

Network Associates Australia
Level 1, 500 Pacific Highway
St. Leonards, NSW 2065
Australia
Phone: 61-2-9437-5866
Fax: 61-2-9439-5166

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

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

Network Associates International B.V.
Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: 31 20 586 6100
Fax: 31 20 586 6101

NA Network Associates Oy
Kielotie 14B
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 Hong Kong
19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Phone: 852-2832-9525
Fax: 852-2832-9530

Network Associates International Ltd.
Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EG
United Kingdom
Phone: 44 (0)1753 827500
Fax: 44 (0)1753 827520

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 0780

Network Associates Korea
135-090, 18th Floor, Kyoung Am Bldg.
157-27 Samsung-Dong, Kangnam-Ku
Seoul, Korea
Phone: 82-2-555-6818
Fax: 82-2-555-5779

Network Associates Portugal
Rua Gen. Ferreira Marines, 10-6 C
1495 ALGÉS
Portugal
Phone: 351 1 412 1077
Fax: 351 1 412 1488

Network Associates South East Asia
78 Shenton Way
#29-02
Singapore 079120
Phone: 65-222-7555
Fax: 65-220-7255

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

Network Associates South Africa
St. Andrews, Meadowbrook Lane
P.O. Box 7062
Bryanston 2021
South Africa
Phone: 27 11 706-1629
Fax: 27 11 706-1569

Network Associates Spain
Serrano 240, Plta. -1
28016 Madrid
Spain
Phone: 34 91 458 52 21
Fax: 34 91 457 45 17

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. Appendix E, "Using VirusScan Command-Line Options," 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 "Using McAfee VirusScan" on page 125 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 59 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. See “Using VShield” on page 71 for details.

- **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 v6.x or earlier. See “Scanning cc:Mail” on page 181 for details.

- **Exchange Client Scanner**. This component allows you to scan the Inbox or other mailbox for any MAPI-compliant e-mail client software, at any time you wish. Use it to supplement the continuous background scanning VShield provides for MAPI clients such as Exchange and Outlook. See “Scanning Microsoft Exchange and Outlook mail” on page 181 for details.

- **McAfee ScreenScan**. This optional component scans your computer as your screen saver runs during idle periods. See “Using ScreenScan” on page 181 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 153 for details.

- **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.
  - This *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, click  in the upper right-hand corner of the window. 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. To see help topics, right-click buttons, lists or other elements within dialog boxes, or click **Help** buttons where you see them.
  - 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—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. See Appendix A, "Using SecureCast to Update Your Software" for details.

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 for your problem.

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. To learn how you can help the virus researchers help you, see "Reporting new items for anti-virus data file updates" on page xxi.

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. 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 distribution type. Review the system requirements shown below to verify that VirusScan will run on your system, then follow the installation steps on page 32.

> **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 8 MB of free hard disk space.
- At least 8 MB of random-access memory (RAM).
- Either 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. Contact a local service provider to learn about rates and terms of service.

Installation Steps

Choose the 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 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. 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 Rescue 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 43 for more information.

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

If you inserted a CD-ROM disc, you should see the McAfee VirusScan welcome screen appear automatically (Figure 2-1).

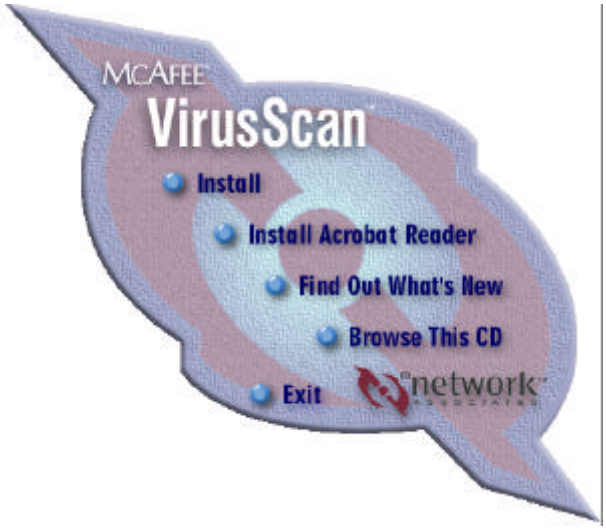

Figure 2-1. McAfee VirusScan welcome screen

To install VirusScan immediately, click **Install**, then skip to Step 5 on page 34 to continue with Setup.

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. Choose **Run** from the **Start** menu.

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

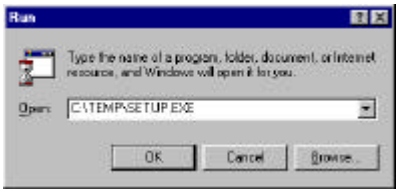

Figure 2-2. The Run dialog box

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, 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. See the CONTENTS.TXT file included on that CD-ROM for details.

   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 2-3).

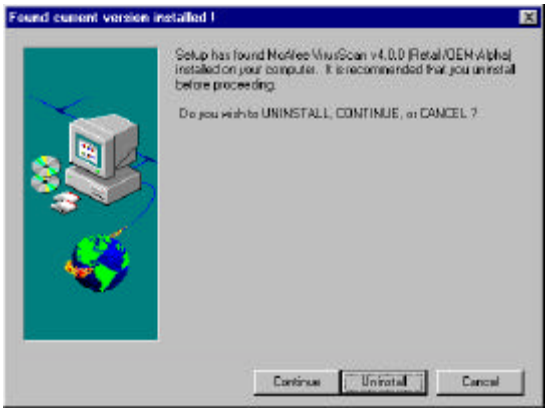

Figure 2-3. Found Current Version Installed panel

3. To continue, you can

   - Click **Uninstall** to remove the existing VirusScan version from your computer. Setup will start the uninstall wizard, then prompt you to remove some files shared by other programs on your system. Click **Yes** to remove these files—Setup will replace them with new versions when you continue with the installation. When it has finished removing the VirusScan copy already on your computer, Setup will continue with Step 4.
   - Click **Continue** to
   - Click **Cancel** to stop the installation altogether. Setup will prompt you to confirm that you want to quit. Click **Exit Setup** to quit, click **Resume** to continue with the installation.

4. Choose which option you want to use. When Setup has finished removing your existing VirusScan copy, it will display the first installation wizard panel (Figure 2-4).

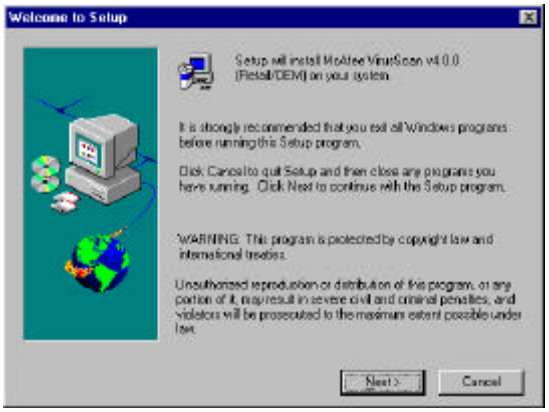

Figure 2-4. The Welcome to Setup wizard panel

5. 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.

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

   The Setup Type panel will appear (see Figure 2-5 on page 35).

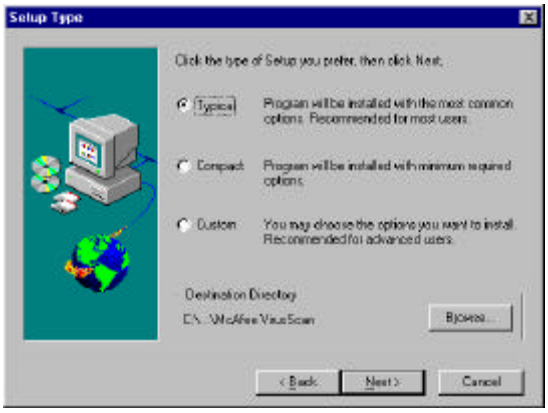

Figure 2-5. The Setup Type panel

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

   - **Typical.** Select this option to install the VirusScan command-line scanners; the VirusScan on-demand scanner; the VShield on-access scanner; VirusScan Central, a utility to launch VirusScan component programs; the Lotus cc:Mail scanner; the Microsoft Exchange client scanner; 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 ScreenScan, a scanning utility that examines your system for viruses whenever your screen saver activates.

8. 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

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

a. **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 10 on page 37.

b. **If you chose a Custom component set**, Setup shows you a wizard panel that lists the components available for installation (Figure 2-6 on page 36). 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>**.

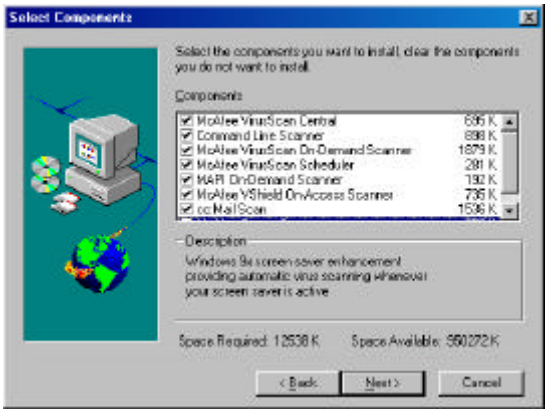

Figure 2-6. The Select Components dialog box

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>** to continue.

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

10. If you asked Setup to scan your system area before installation, it will start VirusScan briefly to examine your hard disk and memory for viruses before it continues. 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 43 to learn what to do next.

11. 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. To skip this step, click **Cancel**, then move to Step 13—you can create an Emergency Disk after installation. To create an Emergency Disk now, click **OK**.

    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. If you do not have a *virus-free* floppy disk formatted with DOS or Windows system files, you must create one in order to continue. Follow these substeps:

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

    b. Click **Start** in the Windows taskbar, point to **Programs**, then choose **Windows Explorer**.

    c. Locate your floppy disk in the list shown in the left pane of the Explorer window, then click it with your right mouse button. Next, choose **Format** from the shortcut menu that appears.

    d. Select **Full** in the **Format type** area in the dialog box that appears, then select the **Copy system files** checkbox in the **Other Options** area. Next, click **Start**.

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

    f. Press **ALT+TAB** or click the VirusScan Setup button in the Windows taskbar to return to Setup.

13. Setup will finish copying files to your hard disk, then it will summarize the changes it made to your system files. Ordinarily, you should see only your AUTOEXEC.BAT file listed. Setup backs up your original AUTOEXEC.BAT file and renames it with a different extension in case you need to restore it. Note the name it uses for future reference, then click **Next>** to continue.

14. Setup requires you to restart your computer in order to complete your VirusScan installation and to ensure 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" on page 38 to learn how to perform this check.

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 as described in "Installation Steps" on pages 32 to 38.
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 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.

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.

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. See Chapter 6, "Using McAfee VirusScan," to learn how to perform a full system scan.

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 44.

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.

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 45.

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, *unformatted* 1.44MB disk into your floppy drive.
2. Double-click My Computer to open the window that displays the disks on your system.
3. Right-click the 3½ Floppy (A:) icon, then choose **Format** from the shortcut menu that appears.
4. Select the **Full** button in the **Format type** area, then select the **Copy system files** checkbox in the **Other options** area. To distinguish this disk from others, enter "E-disk" or another name up to 11 characters long in the **Label** text box.
5. Click **Start** to begin formatting the disk.
6. When Windows has finished formatting, click **Close** twice to quit the formatting utility.
7. Click **Start**, point to **Programs**, then to **McAfee VirusScan**. Next, choose **Create Emergency Disk** to start the VirusScan Emergency Disk utility.
8. Click **Continue** in the dialog box that appears (Figure 3-1).

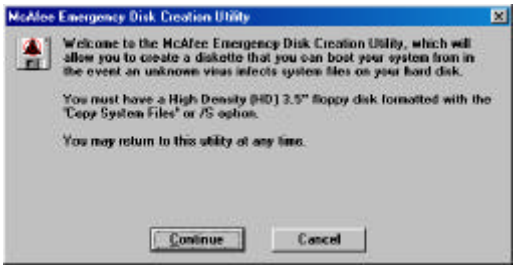

Figure 3-1. Emergency Disk Creation Utility

9. If you left the disk you formatted in Step 5 in your floppy drive, click **OK** in the dialog box that appears. If you ejected the formatted disk, re-insert it into your floppy drive, then click **OK**.

   The Emergency Disk utility will copy the files you need to start your computer and scan your system to the floppy disk.

10. When the utility has finished, click **OK** to close the dialog box. Label your new Emergency Disk, 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.

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, overwrite any existing information on it, 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\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 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. See "Using VShield" on page 71 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. In its initial configuration, the module will prompt you for a response when it detects a virus during any of these operations. You'll see a full-screen warning that offers you several response options (see Figure 3-2 on page 49).

Figure 3-2. System Scan response options

To take one of the listed actions, type the letter highlighted in yellow. Your choices are:

- **Clean.** Type C 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.** Type D 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.
- **Continue.** Type O 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.** Type S 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.** Type E 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 3-3). A fourth option provides you with additional information.

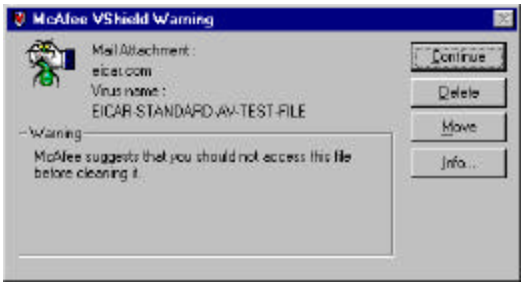

Figure 3-3. E-mail Scan module response options

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.** Click this to see information about the infecting virus or the infected file. This choice does not take any action against the virus VShield detected. See “Viewing File and Virus Information” on page 56 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 you receive over the Internet via 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 3-4). A fourth option provides you with additional information.

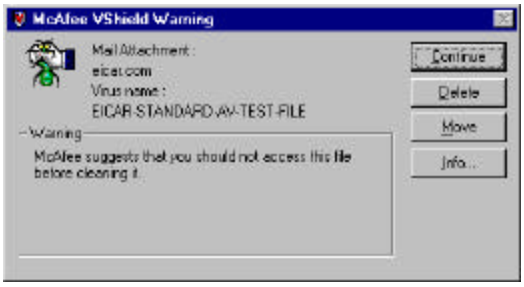

Figure 3-4. Download Scan response options

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

- **Delete.** Click this to tell VShield to delete the infected file 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.
- **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.
- **Info.** Click this to see information about the infecting virus or the infected file. This choice does not take any action against the virus VShield detected. See “Viewing File and Virus Information” on page 56 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 3-5).

Figure 3-5. 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 3-6).

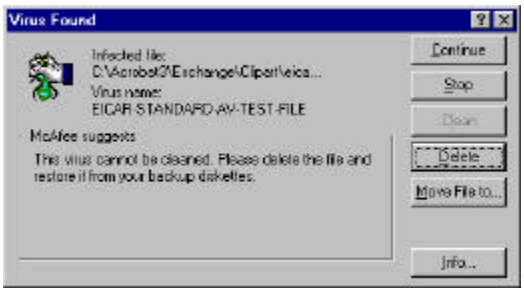

Figure 3-6. VirusScan response options

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 it finds in the lower portion of its main window (Figure 3-7), 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.

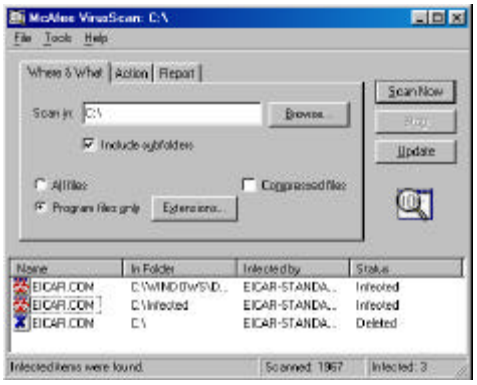

Figure 3-7. VirusScan main window

- **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 3-7) 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 3-6, 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.** VirusScan will open a dialog box that displays information about the infecting virus or the infected file. This choice does not take any action against the virus that VirusScan detected. See "Viewing File and Virus Information" on page 56 for more details.

Responding when E-mail Scan detects a virus

VirusScan's E-mail Scan 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 3-8).

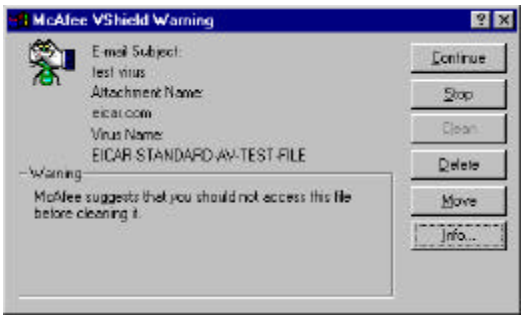

Figure 3-8. E-mail Scan response options

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 3-9 on page 55), 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 3-9 on page 55) 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.

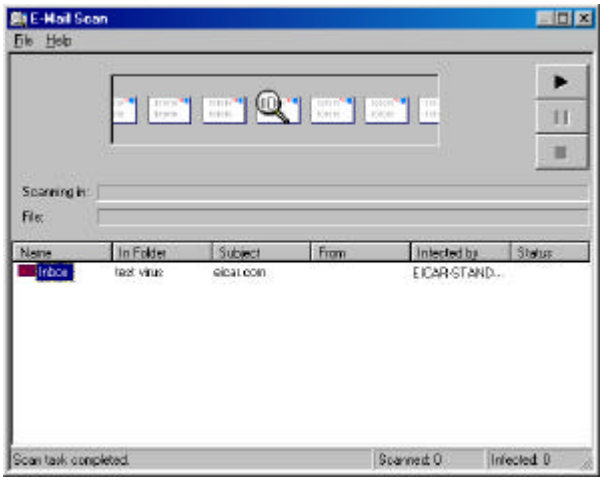

Figure 3-9. E-mail Scan window

- **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 3-8, **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, E-mail Scan 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.** E-mail Scan will open a dialog box that displays information about the infecting virus or the infected file. This choice does not take any action against the virus that E-mail Scan 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 open a property page that shows you detailed information about the infected file and the infecting virus (Figure 3-10).

Figure 3-10. Infected File Information property page

The Item Information page names the file, lists its type and size in bytes, gives its creation and modification dates and describes its attributes. The Virus Information page names the infecting virus and gives other information about its characteristics, including:

- **Which data structures it infects.** Most viruses infect either executable files or the master boot record and boot blocks of your hard disk.
- **How large the virus is, in bytes.**
- **Other characteristics.** Examples include:
  - **Memory Resident.** This means that the virus copies itself from its location on your hard disk into your computer's memory, where it can then infect any file that you run or save to disk.
  - **Encrypted.** This means that the virus encrypts its identifying "code signature"—the byte pattern it uses to tell itself which files it has already infected—so that it will not re-infect the same file. This can make identifying the virus much more difficult.
  - **Polymorphic.** This means that the virus uses a variety of techniques to conceal its code signature. These techniques include: encryption; "mutation," in which the virus alters or scrambles its code signature each time it infects another file; and "stealth," in which the virus redirects system queries that attempt to read its location on disk.
  - **Repairable.** This means that VirusScan or VShield has a "remover" specifically designed to delete the virus code from the infected file and restore it to its original state.

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 they use 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 the unprotected code signature that another program uses and report it as a virus. 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).

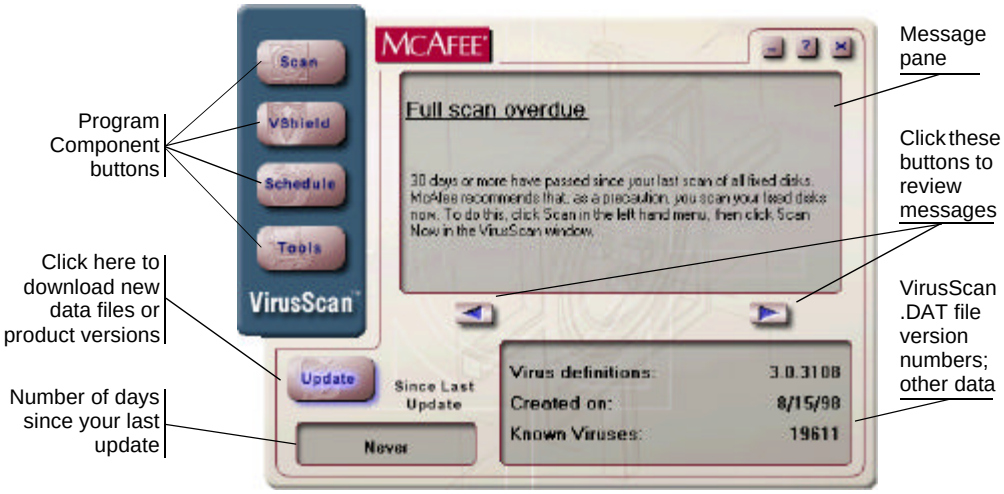

Figure 4-1. VirusScan Central window

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

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

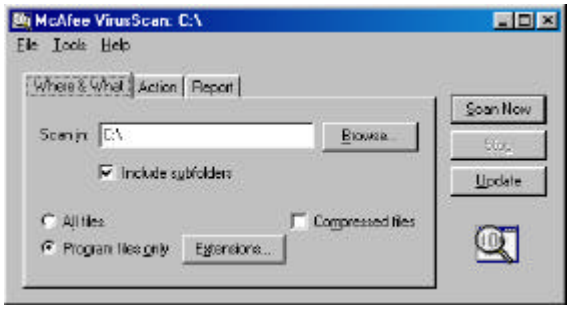

Figure 4-2. VirusScan Classic window

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

Click **Scan Now** to start scanning your system with these default options.

VirusScan Classic will start to look for viruses immediately. A reporting area that appears 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 52 to learn what to do when you have a virus on your system.

If VirusScan Classic finds no viruses on your system, choose **Close** from the **Scan** menu after the program finishes scanning to return to VirusScan Central.

To choose different scanning options, or to configure VirusScan Classic or VirusScan Advanced suit your particular needs, see Chapter 6, "Using McAfee VirusScan."

Configuring VShield

Click **VShield** in the VirusScan Central window to open the VShield configuration dialog box (Figure 4-3).

Figure 4-3. VShield Configuration dialog box

VShield runs continously 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. See "Using VShield" on page 71 to learn how to set up this module for use with your e-mail system.

- **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 Lite, 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. See "Using VShield" on page 71 to learn how to set up security for your VShield settings.

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

To learn more about the configuration options available with VShield, see Chapter 5, "Using VShield."

Starting the Scheduler

Click **Scheduler** in the VirusScan Central window to open the Scheduler window (Figure 4-4).

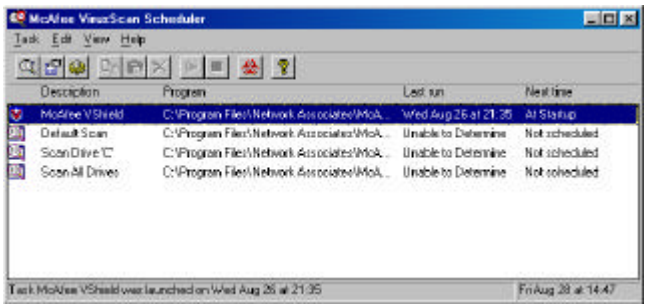

Figure 4-4. VirusScan Scheduler window

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 give you basic protection for your system. To learn how to enable and schedule any or all of these tasks, or how to create other tasks that suit your needs, see Chapter 7, "Scheduling Scan Tasks."

Using VirusScan Tools

Click **Tools** in the VirusScan Central window to slide another button palette into place on top of the original button palette (Figure 4-5).

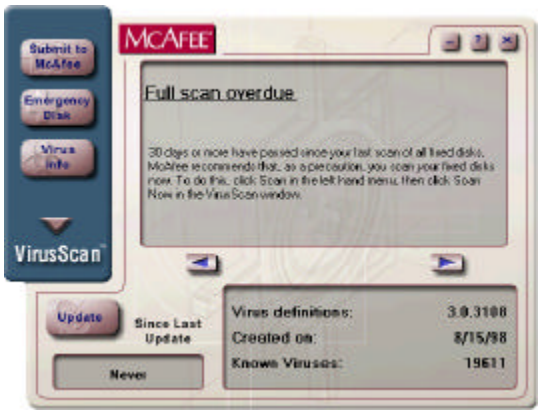

Figure 4-5. VirusScan Central window with VirusScan Tools palette

To return to the original button palette, click below the **Virus Info** button.

The VirusScan Tools set includes a utility that enables you to submit files to McAfee Labs that you believe are infected with new virus types, a utility to create an Emergency Disk similar to the one that came with your copy of VirusScan, and a link to the Network Associates online Virus Information Library. The following sections describe each tool.

Submitting possible viruses to McAfee Labs

Click **Submit to McAfee** to start the McAfee Labs A.V.E.R.T Response Center wizard (Figure 4-6).

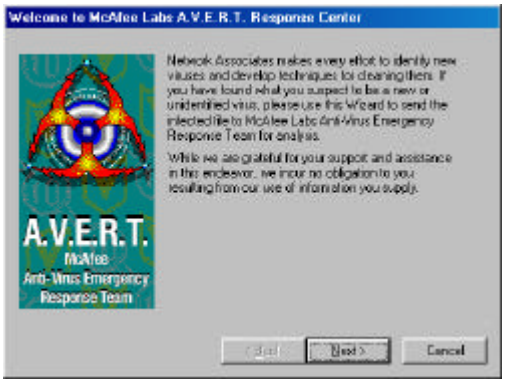

Figure 4-6. A.V.E.R.T. Response Center welcome panel

This wizard helps you to gather and send any files you believe have new or previously unreported viruses to McAfee Labs anti-virus researchers. To use it, you must have an existing e-mail account with an Internet service provider or through your company network. Click **Next>** to continue.

The Your Contact Information panel appears (Figure 4-7).

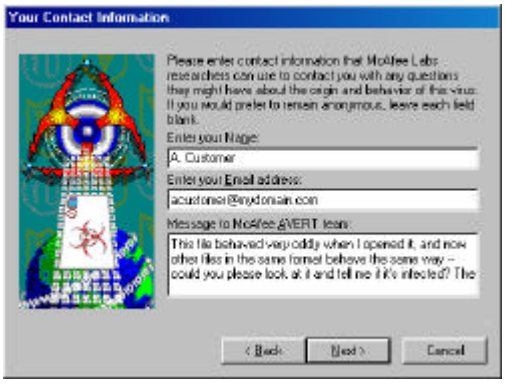

Figure 4-7. A.V.E.R.T Response Center Your Contact Information panel

Enter your name and your e-mail address in the text boxes provided. McAfee Labs researchers need this information to contact you in case they have questions about the behavior of the virus, about where you found it, or about other circumstances related to your submission. *If you prefer to remain anonymous, you can simply leave these text boxes blank.*

Next, in the text box at the bottom of the wizard panel, enter a message that describes the virus behavior you noticed, the circumstances in which you discovered the virus or that led you to suspect an infection, information about your computer environment, and any other information you believe might help the research team to identify an infection. The more detail you add to your message, the faster McAfee Labs can identify and isolate any infecting viruses present in the files you send. You can enter as long a message as you want to in the text box provided.

When you have finished entering information, click **Next>** to continue.

The Choose Files to Submit panel appears (Figure 4-8).

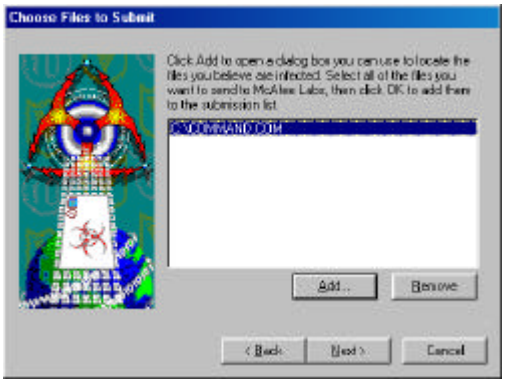

Figure 4-8. A.V.E.R.T Response Center Choose Files to Submit panel

Click **Add** to open a dialog box you can use to locate the files that you suspect are infected. When you have located a file, click **OK** to return to this wizard panel. Repeat this step until you have added all the files you want to send to McAfee Labs. To remove a file shown in the wizard panel, select it, then click **Remove**.

When you have added all of the files you want to send, click **Next>** to continue.

The Choose Upload Options panel appears (see Figure 4-9 on page 66).

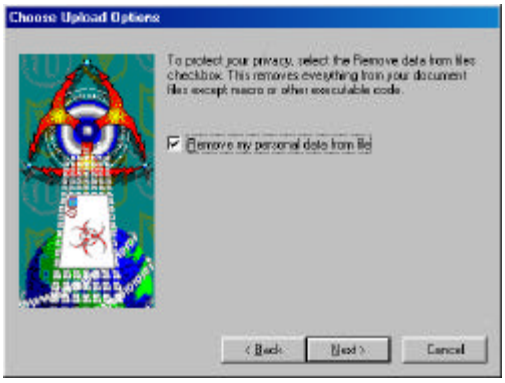

Figure 4-9. A.V.E.R.T. Response Center Choose Upload Options panel

To remove any confidential, personal, or sensitive information from Microsoft Office files or from other infectable data files you want to send, select the **Remove my personal data from file** checkbox. The wizard will strip out the data from the file and leave only the infectable macro code for McAfee Labs researchers to examine. If you plan to send executable files only, clear the checkbox. Click **Next>** to continue.

The Choose E-mail Service panel appears (Figure 4-10).

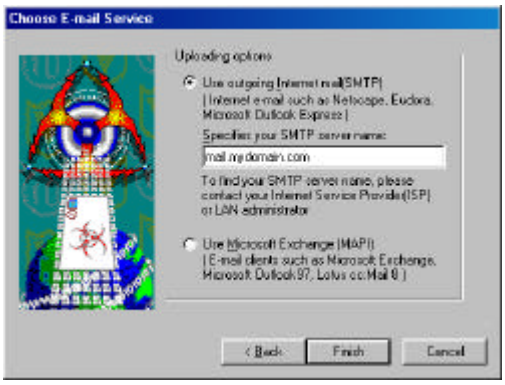

Figure 4-10. A.V.E.R.T. Response Center Choose E-mail Service panel

Here you can select the type of e-mail service you want to use to send your files and message. You have two options:

- If you have a dial-up connection to an Internet service provider or use a POP-3 e-mail client application such as Eudora Light, Netscape Mail, or Microsoft Outlook Express—either via a modem or through a network connection—select the **Outgoing Internet Mail (SMTP)** checkbox.

Next, enter the name of the server that sends your mail out to the Internet. Usually, this will be a Simple Mail Transfer Protocol (SMTP) server that you connect to when you dial your internet service provider or when you send mail through a network server. If you don't know the name of the server you use, check with your network administrator or contact your Internet service provider.

- If you use an e-mail client application that complies with the MAPI (Messaging Application Programming Interface) standard—such as Microsoft Exchange or Outlook, Lotus cc:Mail 8.0 or later, or others—select the **Use Microsoft Exchange (MAPI)** checkbox.

When you have selected an e-mail service, click **Finish** to send your files and message to McAfee Labs.

> **NOTE:** If you are not logged into your mail service, your e-mail client will prompt you to log in so that it can send this message.

Creating an Emergency Disk

Click **Emergency Disk** to start the McAfee Emergency Disk creation utility (Figure 4-11).

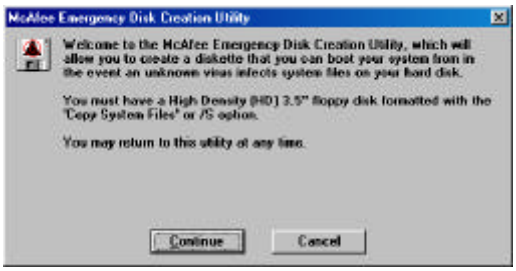

Figure 4-11. Emergency Disk Creation Utility dialog box

This utility copies portions of the VirusScan command-line component to create a disk you can use to boot your computer and scan your system for viruses. In most respects, the disk you create with the utility is similar to the Emergency Disk that comes with your copy of VirusScan. To create an emergency disk with the utility, however, you need a floppy disk formatted with bootable DOS system files. See "Creating an emergency disk" on page 45 to learn how to use the utility.

Opening the Virus List

Click **Virus Info** to open the Virus List window (Figure 4-12).

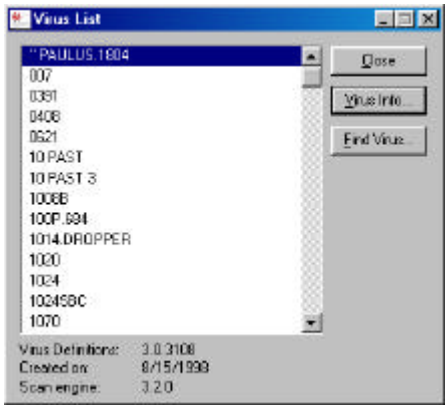

Figure 4-12. Virus List window

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, scroll through the list to locate the one you want to know about, select it, then click **Virus Info** at the right edge of the window. If you know the name of a particular virus you want to locate, click **Find Virus**, then enter the virus name in the text box provided. The Virus List will scroll immediately to the name you entered. Click **Close** in the Find What Virus box, select the virus name in the list, then click **Virus Info**.

A Virus Information window for the virus you selected will appear (Figure 4-13). Click >> or << to move backward or forward in the Virus List.

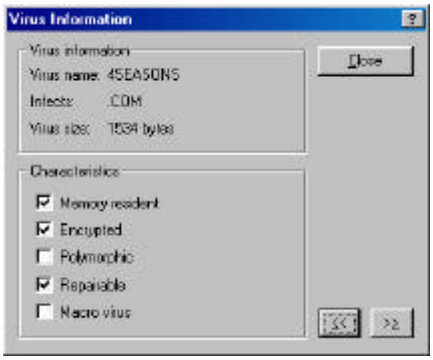

Figure 4-13. Virus Information window

The Virus Information page tells you this about each virus:

- **Virus Name.** The name given to the virus usually results from agreement among anti-virus vendors who follow certain naming conventions, but occasionally different vendors will call the same virus by different names.
- **Infects.** Most viruses infect either executable files or the master boot record and boot blocks of your hard disk. Some rare virus strains infect other file types, such as mIRC script files or Java language files.
- **Virus Size.** This is the size of the virus code itself, in bytes. In some cases, a change in a file's size by the number of bytes listed here can alert you to an infection.
- **Characteristics.** Virus characteristics can include the types of strategies a virus will use to conceal itself and whether its code can be safely removed from an infected file. The Information page provides these specifics:
  - **Memory Resident.** A checkmark in this box means that the virus copies itself from its location on your hard disk into your computer's memory, where it can then infect any file that you run or save to disk.
  - **Encrypted.** A checkmark in this box means that the virus encrypts its identifying "code signature"—the byte pattern it uses to tell itself which files it has already infected—so that it will not re-infect the same file. This can make identifying the virus much more difficult.
  - **Polymorphic.** A checkmark in this box means that the virus uses a variety of techniques to conceal its code signature. These techniques include: encryption; "mutation," in which the virus alters or scrambles its code signature each time it infects another file; and "stealth," in which the virus redirects system queries that attempt to read its location on disk.
  - **Repairable.** A checkmark in this box means that VirusScan or VShield has a "remover" specifically designed to delete the virus code from the infected file and restore it to its original state.
  - **Macro Virus.** A checkmark in this box means that the virus infects Microsoft Office data files that include code written in Microsoft's Visual Basic for Applications, or other macro languages.

For more comprehensive information about viruses, visit the online Virus Information Library at the Network Associates website. Use your browser to connect to this address:

http://www.nai.com/vinfo/

Updating VirusScan

Click **Update** to start the Network Associates SecureCast wizard that will guide you through updating your data (.DAT) files or your product version. See “Using SecureCast to Update Your Software” on page 179 to learn how to use the wizard.

Using VShield 5

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. Secure password protection for your configuration options prevents others from making unauthorized changes.

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 you perform.
- **Malicious object detection and blocking.** VShield can block harmful ActiveX and Java objects from 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 73 or "Setting VShield properties" on page 78 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 then 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 VirusScan Central, then click **VShield** in the button palette at the left of the window. To learn how to start and use VirusScan Central, see "Starting VirusScan Central" on page 59.
- 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 5-1).

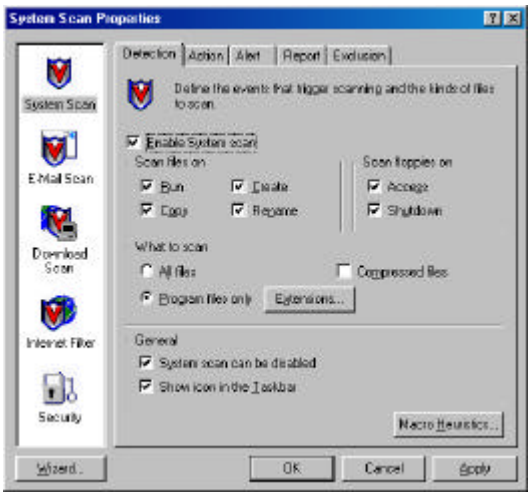

Figure 5-1. VShield Properties dialog box

Click **Wizard** in the lower left corner of the dialog box to display the first configuration wizard panel (Figure 5-2).

Figure 5-2. VShield configuration wizard - welcome panel

Click **Next>** to display the System Scan configuration panel (Figure 5-3).

Figure 5-3. 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 5-4).

Figure 5-4. 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 5-5).

Figure 5-5. 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 5-6 on page 77).

Figure 5-6. VShield configuration wizard - Internet Filter panel

Select **Yes, enable hostile applet protection**, then click **Next>** to have VShield block Java applets and ActiveX controls that it knows 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 those you visit. 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**, then click **Next>** to continue.

The final wizard panel summarizes the options you chose (Figure 5-7).

Figure 5-7. 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.

Setting VShield properties

To ensure its optimal performance on your computer or in your network environment, VShield needs to know what you want it to scan, what you want it to do if it finds a virus or other malicious software, and how it should let you know when it has. You can use the configuration wizard to enable most of VShield's protective options, but if you want complete control over the program's performance and the ability to adapt it to your needs, choose your options in the VShield Properties dialog box.

The VShield Properties dialog box consists of a series of property pages that control the settings for each program module. To choose your options, click the icon for the appropriate program module, then click each tab in the VShield Properties dialog in turn.

To open the VShield Properties dialog box, either:

- Start VirusScan Central, then click **VShield** in the button palette at the left of the window. To learn how to start and use VirusScan Central, see "Starting VirusScan Central" on page 59.
- 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 5-8).

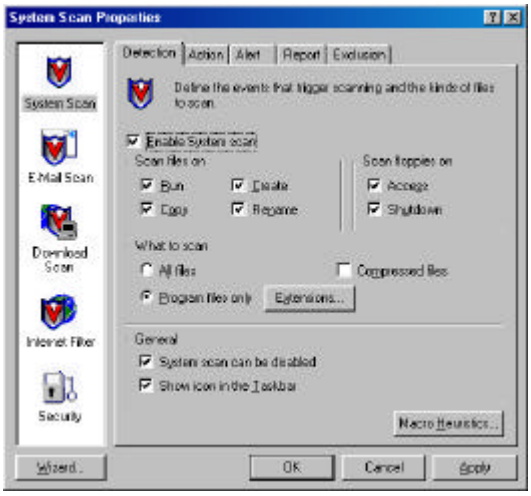

Figure 5-8. System Scan Properties dialog box - Detection page

Configuring the System Scan module

VShield's System Scan module can check your system for viruses each time you open, run, save, or modify files on your hard disk, and each time you read from or write to a floppy disk. To choose your options, click the System Scan icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield initially assumes that you want it to scan for viruses each time you work with any file susceptible to virus infection, whether on your hard disk or on floppy disks (see Figure 5-8 on page 78). Although these default options balance scan performance with security, your environment might require different settings.

To modify these settings, verify that the Enable System Scan checkbox is selected, then follow these steps:

1. Tell VShield when and where you want it to look for viruses. You can have it

   - **Scan files as you work with them.** Each time you open, copy, save, rename, or otherwise use files on your hard disk, virus code can execute and spread infections to other files. To prevent this, select any combination of the **Run**, **Copy**, **Create** and **Rename** checkboxes—selecting all options offers you the best security. VShield will delay each operation very slightly as it scans each file.

   - **Scan files on floppy disks.** Boot-sector viruses can hide in the boot blocks of any formatted floppy disk, then load into memory as soon as your computer reads your floppy drive. Select the **Access** checkbox to have VShield examine floppy disks each time your computer reads them. Select the **Shutdown** checkbox to have VShield scan any floppy disks you leave in your drive as you shut down your computer. This ensures that no viruses can load when your computer reads your floppy drive at startup.

2. Specify the types of files you want VShield to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have VShield look for viruses in files compressed in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats. 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 VShield will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 5-9).

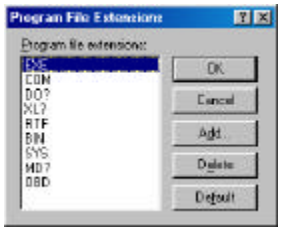

Figure 5-9. Program File Extensions dialog box

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

NOTE: VShield's default program extension list differs from that for VirusScan, because scanning .DLL and .VXD files—common files that Windows uses constantly, would slow down system performance dramatically. To ensure that VShield scans these file types, add their extensions to the dialog box. As an alternative, consider running frequent VirusScan scan operations if you must scan these file types regularly.

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

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

- **Scan all files.** To have VShield examine any file on your system that you use in any way, whatever their extensions, select the **All files** button. This will slow your system down considerably, but will ensure that it is virus free.

3. Set a sensitivity level for heuristic scanning. Click **Macro Heuristics** to open the Macro Heuristics Scan Settings dialog box (Figure 5-10).

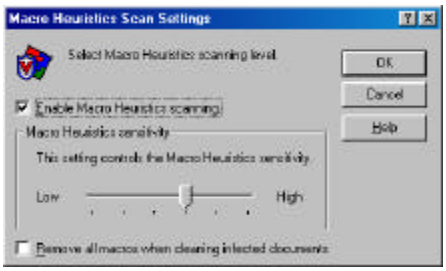

Figure 5-10. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables VShield to recognize new macro viruses based on their resemblance to similar viruses it already knows. To do this, VShield first identifies all Microsoft Word, Microsoft Excel, and other Microsoft Office files that have embedded macros, then it compares the macro code to its virus signature database. Exact matches it identifies with the virus name; code signatures that resemble existing viruses cause VShield to tell you it has found a "probable" macro virus. Unless you know that the file does not contain a virus, you should treat "probable" infections with the same caution you would confirmed infections.

To activate heuristic scanning, follow these steps:

a. Select the **Enable macro heuristics scanning** checkbox.

b. Set the sensitivity level you want VShield to use when it looks for macro viruses. Drag the slider to the left to set a low level of sensitivity—this causes VShield to look for as close a match as possible between the macros it finds in the file and existing virus code signatures before it labels a file as infected.

   Drag the slider to the right to set a high level of sensitivity—this causes VShield to look with suspicion at nearly all macro code and to identify a wider range of files as potentially infected.

> **NOTE:** Higher levels of sensitivity can cause VShield to falsely identify a file as infected, but it does so out of caution. Until virus researchers have examined the suspicious file and positively eliminated any possibility of infection, the potential exists for nearly all macro code to harbor new viruses. The sensitivity setting exists for you to choose the level that works best for your environment.

c. Determine how you want to treat infected macro files. Select **Remove all macros when cleaning infected documents** to eliminate all infectable code from the document and leave only data. To try to remove only the virus code from the document's macros, leave this checkbox clear.

> **NOTE:** Use this feature with caution: removing all macros from a document can cause it to lose data or to become corrupted and unusable.

d. Click **OK** to save your settings and return to the VShield Properties dialog box.

4. Choose VShield management options. These options let you control your interaction with VShield. You can

   - **Display the VShield icon in the Windows system tray.** Select the Show Icon in the Taskbar checkbox to have VShield display this icon in the system tray. Double-clicking the icon opens the VShield Status dialog box. Right-clicking the icon displays a shortcut menu. See "Using VShield's shortcut menu" on page 120 and "Tracking VShield status information" on page 120 for more details.
   - **Disable the System Scan module at will.** Select the System Scan can be disabled checkbox in order to have the option to disable this module. Note that Network Associates recommends that you leave System Scan enabled for maximum protection. Clearing this checkbox removes the disable command from VShield's shortcut menu and the disable button from the VShield Status dialog box.

     > **TIP:** To ensure that nobody else who uses your computer will disable VShield, or to enforce an anti-virus security policy among VirusScan users on your network, clear this checkbox, then protect the settings with a password. This will keep other users from disabling VShield from VirusScan Scheduler, or from the VShield Properties dialog box. See "Configuring the Security module" on page 117 for details.

5. Click the Action tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield 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 VShield 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 System Scan module to display the correct property page (Figure 5-11).

Figure 5-11. System Scan Properties dialog box - 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 choice. Your choices are:

   - **Prompt for user action.** Use this option if you want VShield to ask you what to do when it finds a virus—the program will display an alert message and offer you a range of possible responses. Choose which response options you want to see in the alert message from among these:

     – **Clean file.** This option tells VShield to try to remove the virus code from the infected file.

     – **Delete file.** This option tells VShield to delete the infected file immediately.

     – **Exclude file.** This option tells VShield not to scan the file from now on.

  - **Continue access.** This option tells VShield to allow you to continue working with the file and not take any other action. If you have its reporting options enabled, VShield records the incident in its log file.
  - **Stop access.** This option tells 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 options enabled, VShield records the incident in its log file.

- **Move infected files automatically**. Use this option to have VShield move infected files to a quarantine directory as soon 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.

  You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.
- **Clean infected files automatically.** Use this option to tell VShield to remove the virus code from the infected file as soon as it finds it. If VShield cannot remove the virus, it will notify you in its message area and, if you have its reporting features enabled, will note the incident in its log file. See "Choosing Report options" on page 86 for details.
- **Delete infected files automatically.** Use this option to have VShield delete every infected file it finds immediately. Be sure to enable its reporting feature so that you have a record of which files VShield deleted. You will need to restore deleted files from backup copies.
- **Deny access to infected files and continue.** This tells VShield to mark the file "off limits" and continue with its normal scanning operations. Use this option only if you plan to leave your computer unattended for long periods. If you also activate VShield's reporting feature (see "Choosing Report options" on page 86 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 Alert tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want VShield to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you or others in a variety of ways. Use the Alerts property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the System Scan module to display the correct property page (Figure 5-12).

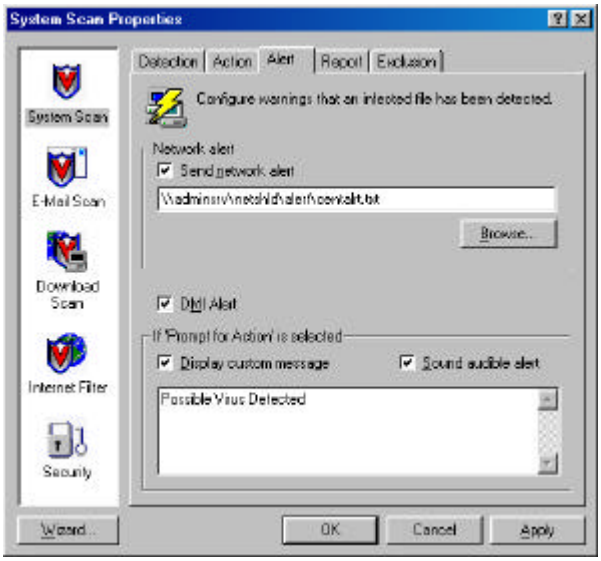

Figure 5-12. System Scan Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

4. If you chose **prompt for user action** as your response in the Action page (see "Choosing Action options" on page 83 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. Click the Report tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's System Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSHLOG.TXT. You can have VShield write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor.

The VSHLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VShield found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Report property page to determine which information VShield will include in its log file.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the System Scan module to display the correct property page (Figure 5-13).

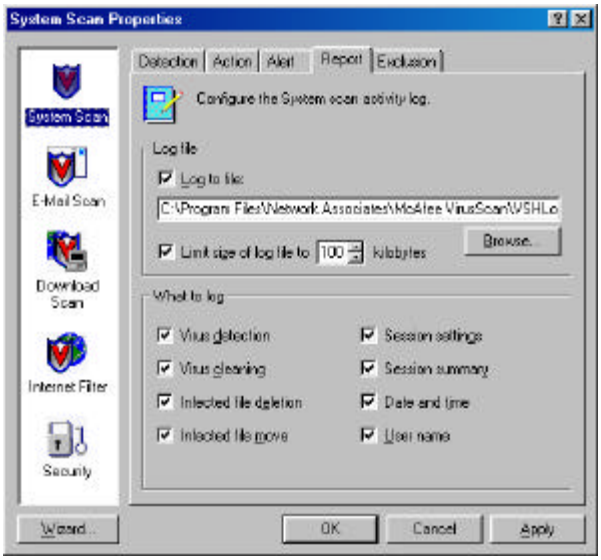

Figure 5-13. System Scan Properties dialog box - Report page

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

   By default, VShield writes log information to the file VSHLOG.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.

3. 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, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VShield to record in its log file. You can choose to record this information:

   - **Virus detection.** Select this checkbox to have VShield note the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VShield note the number of infected files from which it removed the infecting virus.

- **Infected file deletion.** Select this checkbox to have VShield note the number of infected files it deleted from your system.
- **Infected file move.** Select this checkbox to have VShield note the number of infected files it moved to your quarantine directory.
- **Session settings.** Select this checkbox to have VShield list the options you choose in the System Scan Properties dialog box for each scanning session.
- **Session summary.** Select this checkbox to have VShield summarize its actions during each scanning session. Summary information includes the number of files VShield scanned, the number and type of viruses it detected, the number of files it moved or deleted, and other information.
- **Date and time.** Select this checkbox to have VShield append the date and time to each log entry it records.
- **User name.** Select this checkbox to have VShield append the name of the user logged in to your computer at the time it records each log entry.

5. Click the Exclusion tab to choose additional VShield options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Having VShield examine these files can take a long time and produce few results. You can speed up scan operations by telling VShield to look only at susceptible file types (see "Choosing Detection options" on page 79 for details), or you can tell VShield to ignore entire files or folders that you know will not get infected.

Once you use VirusScan to scan your system thoroughly, you can tell VShield to ignore those files and folders that do not change or that are not normally vulnerable to virus infection.

To keep VShield from scanning certain files and folders, follow these steps:

1. Click the Exclusion tab in the System Scan module to display the correct property page (Figure 5-13).

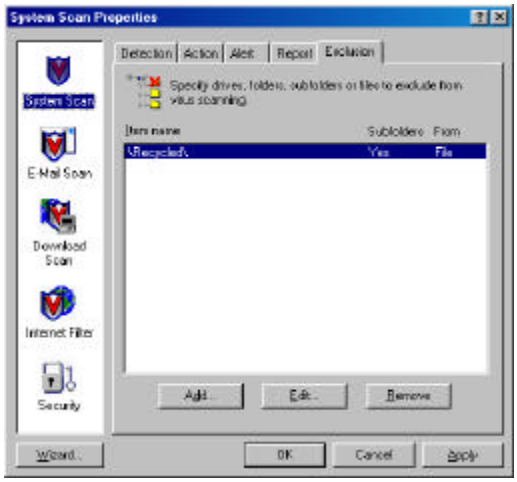

Figure 5-14. System Scan Properties dialog box - Exclusion page

The Exclusion page will initially list only your Recycle Bin. VShield excludes the Recycle Bin from scan operations because Windows will not run files stored there.

2. Specify the items you want to exclude. You can

   - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 5-15).

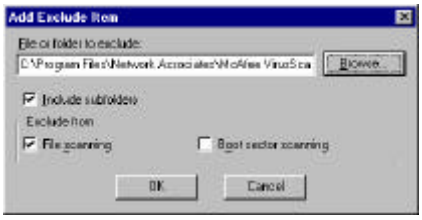

Figure 5-15. Add Exclude Item dialog box

   a. Type the volume, the path to the file, or the path to the folder that you want to exclude from scanning, or click **Browse** to locate a file or folder on your computer.

> **NOTE:** If you have chosen to move infected files to a quarantine folder automatically, VShield will not scan that folder.

b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.

c. Select the **File scanning** checkbox to tell VShield not to look for file-infector viruses in the files or folders you exclude.

d. Select the **Boot sector scanning** checkbox to tell VShield not to look for boot-sector viruses in the files or folders you exclude. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

> **WARNING:** Network Associates recommends that you do *not* exclude your system files from virus scanning.

e. Click **OK** to save your changes and close the dialog box.

f. Repeat steps a. through d. until you have listed all of the files and folders you do not want scanned.

- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.
- **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. VShield will then scan this file or folder during its next scanning operation.

3. Click a different tab to change any of your System Scan settings, or click one of the icons along the side of the System Scan Properties dialog box to choose options for a different module.

   To save your changes in the System Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the E-mail Scan module

VShield's E-mail Scan module can check e-mail messages you receive via a corporate e-mail system such as Microsoft Exchange, Microsoft Outlook, or Lotus cc:Mail, or via POP-3 or SMTP e-mail client programs such as Eudora, Netscape Mail, or Microsoft Outlook Express. VShield will scan any attachments included with your e-mail, examining your mailbox on your mail server, or intercepting your mail before any infecting viruses can cause any harm.

To choose your options, click the E-mail Scan icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield does not enable the E-mail Scan module by default, unless you've already used its configuration wizard to choose your options, because it needs to know which e-mail system you use.

To activate and configure e-mail scanning, follow these steps:

1. Select the **Enable Scanning of e-mail attachments** checkbox.

   The options in the rest of the property page activate (Figure 5-16).

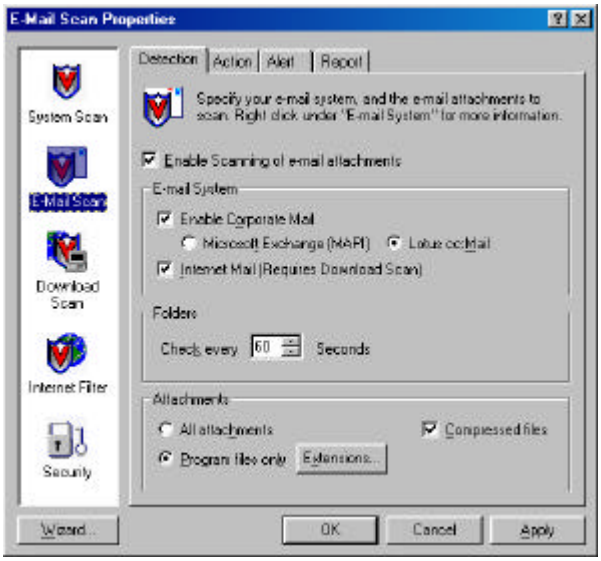

Figure 5-16. E-mail Scan Properties dialog box - Detection page

2. Select the type of e-mail system you use. Your options are:

   - **Enable Corporate Mail.** Select this checkbox to have VShield scan mail you receive via a mail system that runs within your office network. Usually such systems use a proprietary mail protocol and have a central mail server to which you send mail for delivery. Often such systems send and receive Internet mail, but they usually do so through a gateway application. The E-mail Scan module supports two types of corporate e-mail systems:

     – **Microsoft Exchange (MAPI)**. Select this button if you use an e-mail system that sends and receives mail via Microsoft's Messaging Application Programming Interface, a Windows mail protocol. Examples include Microsoft Exchange, Microsoft Outlook 97 and Outlook 98, Lotus cc:Mail 8.0, and cc:Mail 8.01.

     – **Lotus cc:Mail.** Select this button if you use cc:Mail 6.x or 7.x. These systems use a proprietary Lotus protocol to send and receive e-mail. You can also install cc:Mail version 8.0 or later so that it uses the same protocol as earlier cc:Mail versions. To verify which system you use, check with your network administrator.

     NOTE: You can select only one *corporate* e-mail system at a time, but you can have VShield scan both corporate and Internet e-mail systems if you use both.

   - **Internet Mail (Requires Download Scan).** Select this checkbox to have VShield scan Internet mail that you send and receive via the Post Office Protocol (POP-3) or the Simple Mail Transfer Protocol (SMTP). Choose this option if you work from home or through a dial-up Internet service provider with such software as Qualcomm's Eudora Pro, Microsoft's Outlook Express, or Netscape Mail.

     IMPORTANT: Because you receive Internet mail and other files that you download through the same "pipe," VShield uses the detection, action, alerting and reporting options you set in the Download Scan module to determine how to respond to incoming Internet mail. To scan Internet mail, therefore, you must also enable the Download Scan module and use those property pages to choose the settings you want.

3. Tell VShield how often to scan your cc:Mail or MAPI mailbox on your network's mail server.

   In the **Folders** area, enter the number of seconds VShield should wait before it looks for viruses. By default, it checks once every minute. Be sure to set an interval *shorter* than the interval you set to receive your e-mail so that VShield has an opportunity to detect any viruses before they reach your computer.

4. Specify the types of e-mail attachments you want VShield to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have VShield look for viruses in files compressed in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats. Although it does give you better protection, scanning compressed files can lengthen a scan operation, especially when you must process a large volume of mail.

   - **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 when you have a large volume of mail to process.

     To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 5-17).

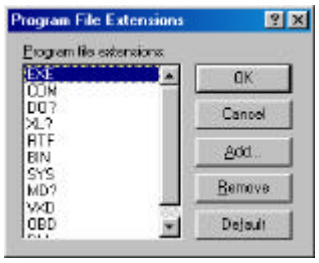

Figure 5-17. Program File Extensions dialog box

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

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

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

- **Scan all attachments.** To have VShield examine any attachment that arrives with any e-mail message, whatever its extension, select the **All attachments** button. This may slow e-mail processing down if you receive a large volume of e-mail, but it will ensure that your mail is virus free.

5. Click the Action tab to choose additional VShield options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield detects a virus in an e-mail attachment, 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 VShield 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 E-mail Scan module to display the correct property page (see Figure 5-18 on page 95).

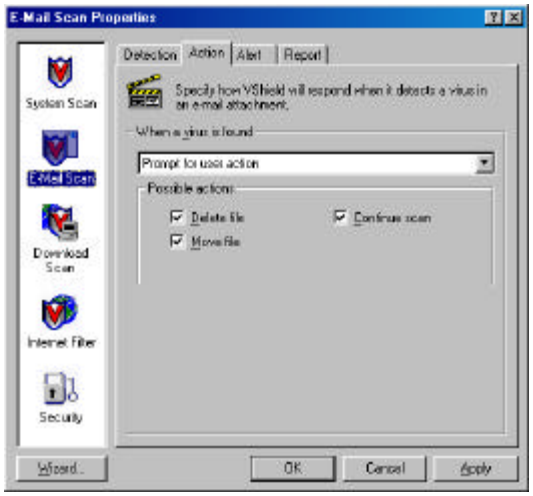

Figure 5-18. E-mail Scan Properties dialog box - Action page

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 choice. Your choices are:

   - **Prompt for user action.** Use this option if you want VShield to ask you what to do when it finds a virus—the program will display an alert message and offer you a range of possible responses. Choose which response options you want to see in that alert message from among these:

     – **Delete file.** This option tells VShield to delete the infected attachment immediately. VShield will, however, preserve the e-mail message it came in.

     – **Move file.** This option tells VShield to move the infected file to a preselected quarantine directory.

     – **Continue scan.** This option tells VShield to continue with its scan, but not take any other actions. If you have its reporting options enabled, VShield records the incident in its log file.

   - **Move infected files to a folder**. Use this option to have VShield move infected files to a quarantine directory as soon as it finds them. By default, VShield moves these files to a folder named INFECTED.

     If you use a corporate e-mail system, VShield will create the INFECTED folder on the network mail server. You cannot designate a different folder or change the folder's name. Depending on the access you have to your mail server through your e-mail client, however, you might be able to see or delete the file in that folder.

If you use an Internet mail client, VShield will create the INFECTED folder at the root level of the drive to which you download your mail. For example, if your mail client's "in box" sits on your D: drive and VShield finds an infected attachment in your e-mail, it will create the directory D:\INFECTED and copy the file to it.

You can change the name and location of the folder into which VShield deposits infected Internet mail, but to do so, you must switch to the Download Scan module and click the Action tab there. See "Choosing Action options" on page 103 for details.

- **Delete infected files.** Use this option to have VShield delete every infected file it detects immediately. Be sure to enable its reporting feature so that you have a record of which files VShield deleted. You will need to restore deleted files from backup copies. See "Choosing Report options" on page 99 for details.
- **Continue scanning.** This tells VShield to continue scanning without taking any action against the virus it finds. If you also activate the VShield reporting feature (see "Choosing Report options" on page 99 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 Alert tab to choose additional VShield options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and remove viruses from your incoming e-mail automatically, as it finds them, with almost no further intervention. If, however, you want VShield to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you and to others in a variety of ways. Use the Alerts property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the E-mail Scan module to display the correct property page (see Figure 5-19 on page 97).

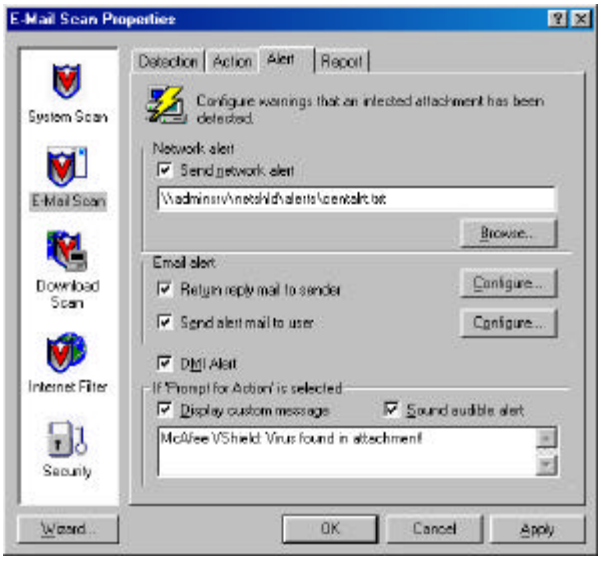

Figure 5-19. E-mail Scan Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

NOTE: The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

---

3. To send an alert message to the person who sent you the infected e-mail attachment, select the **Return reply mail to sender** checkbox. You can then compose a standard reply to send. Follow these steps:

   a. Click **Configure** to open a standard mail message form.

   b. Fill in the subject line, then add any comments you want to make in the body of the message, below a standard infection notice that VShield will supply. You may add up to 1024 characters of text.

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

   d. Click **OK** to save the message.

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

4. To send an e-mail message to warn others about an infected attachment, select the **Send alert mail to user** checkbox. You can then compose a standard reply to send to one or more recipients—a network administrator, for example—each time VShield detects an infected e-mail attachment. Follow these steps:

   a. Click **Configure** to open a standard mail message form.

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

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

   c. Fill in the subject line, then add any comments you want to make in the body of the message below the infection notice. You may add up to 1024 characters of text.

   d. Click **OK** to save the message.

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

5. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

6. If you chose **prompt for user action** as your response in the Action page (see "Choosing Action options" on page 94 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

7. Click the Report tab to choose additional VShield options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's E-mail Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called WEBEMAIL.TXT. You can have VShield write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor.

The WEBEMAIL.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VShield found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Report property page to determine which information VShield will include in its log file.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the E-mail Scan module to display the correct property page (Figure 5-20).

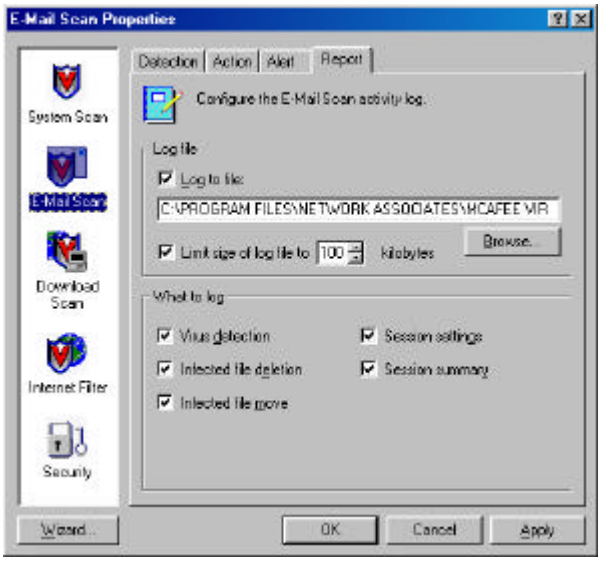

Figure 5-20. E-mail Scan Properties dialog box - Report page

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

   By default, VShield writes log information to the file WEBEMAIL.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.

3. 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, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VShield to record in its log file. You can choose to record this information:

   - **Virus detection.** Select this checkbox to have VShield note the number of infected files it found as it checked your e-mail.
   - **Infected file deletion.** Select this checkbox to have VShield note the number of infected files it deleted as it checked your e-mail.

- **Infected file move.** Select this checkbox to have VShield note the number of infected files it moved to your quarantine directory.
- **Session settings.** Select this checkbox to have VShield list the options you choose in the E-mail Scan Properties dialog box for each scanning session.
- **Session summary.** Select this checkbox to have VShield summarize its actions during each scanning session. Summary information includes the number of files VShield scanned, the number and type of viruses it detected, the number of files it moved or deleted, and other information.

5. Click a different tab to change any of your E-mail Scan settings, or click one of the icons along the side of the E-mail Scan Properties dialog box to choose options for a different module.

   To save your changes in the E-mail Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the Download Scan module

VShield's Download Scan module can check files you download from the Internet as you visit websites, FTP sites, and other Internet sites. This module is also where you set the options you want to use to respond to infected e-mail attachments you receive via POP-3 or SMTP e-mail client programs such as Eudora, Netscape Mail, or Microsoft Outlook Express. To activate this function, you must also choose an appropriate mail system in the E-mail Scan module's Detection page. See "Choosing Detection options" on page 91 for details.

To set VShield to scan files you download, click the Download Scan icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield initially assumes that you want it to scan for viruses each time you download any file susceptible to virus infection from the Internet (see Figure 5-21 on page 102). These default options provide excellent security, but your environment might require different settings.

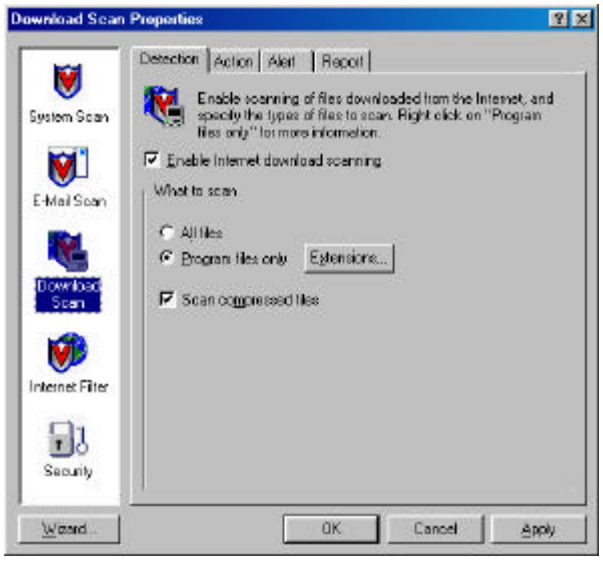

Figure 5-21. Download Scan Properties dialog box - Detection page

To modify these settings, verify that the Enable Internet Download Scanning checkbox is selected, then follow these steps:

1. Specify the types of files you want VShield to examine. You can

   - **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 file downloading, particularly with large files or a large group of files. To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 5-22).

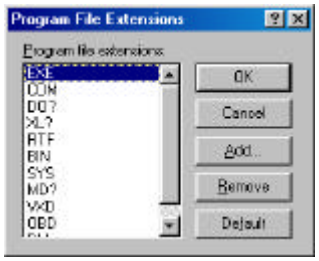

Figure 5-22. Program File Extensions dialog box

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

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

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

- **Scan all files.** To have VShield examine every file that you download, whatever its extension, select the **All files** button. This might slow download operations, but will ensure that your system remains virus free.
- **Scan compressed files.** Select the **Compressed files** checkbox to have VShield look for viruses in files compressed in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats. Although it does give you better protection, scanning compressed files as you download them can lengthen download time.

2. Click the Action tab to choose additional VShield options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield 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 VShield 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 Download Scan module to display the correct property page (Figure 5-23).

Figure 5-23. Download Scan Properties dialog box - 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 choice. Your choices are:

   - **Prompt for user action.** Use this option if you want VShield to ask you what to do when it finds a virus—the program will display an alert message and offer you a range of possible responses. Choose which response options you want to see in the alert message from among these:

     – **Delete file.** This option tells VShield to delete the infected file immediately.

     – **Move file.** This option tells VShield to move the infected file to a quarantine directory you designate.

     – **Continue scan.** This option tells VShield to continue with its scan, but not take any other actions. If you have its reporting options enabled, VShield records the incident in its log file.

   - **Move infected files to a folder**. Use this option to have VShield move infected files to a quarantine directory as soon as it finds them. By default, VShield moves these files to a folder named INFECTED that it creates at the root level of the hard disk onto which you save the files you download.

For example, if VShield found a virus in a file you downloaded to E:\MY DOWNLOADS and you specified INFECTED as the quarantine directory, VShield would copy the file to E:\INFECTED.

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

- **Delete infected files.** Use this option to have VShield delete every infected file you download. Be sure to enable its reporting feature so that you have a record of which files VShield deleted.
- **Continue scanning.** This tells VShield to continue scanning without taking any action against any virus it detects. If you also activate the VShield reporting feature (see "Choosing Report options" on page 107 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 Alert tab to choose additional VShield options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and remove viruses as it detects them in files you download, with almost no further intervention. If, however, you want VShield to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you or to others in a variety of ways. Use the Alerts property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the Download Scan module to display the correct property page (Figure 5-24 on page 106).

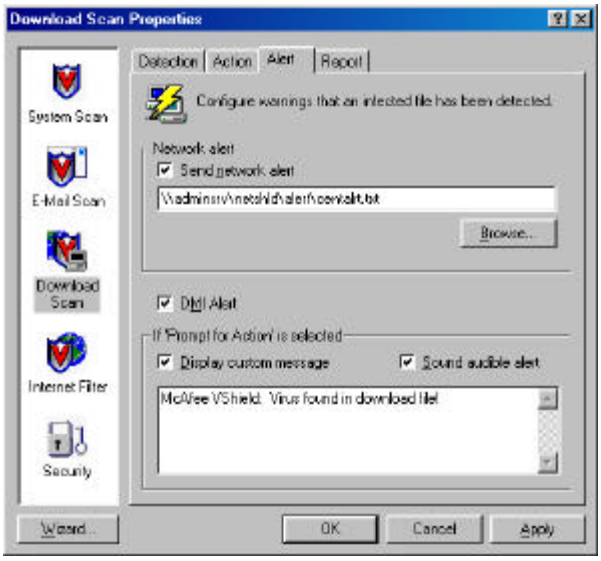

Figure 5-24. Download Scan Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

   NOTE: The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

4. If you chose **prompt for user action** as your response in the Action page (see "Choosing Action options" on page 103 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. Click the Report tab to choose additional VShield options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's E-mail Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called WEBINET.TXT. You can have VShield write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor. Use the Report property page to determine which information VShield will include in its log file.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the Download Scan module to display the correct property page (Figure 5-25).

Figure 5-25. Download Scan Properties dialog box - Report page

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

   By default, VShield writes log information to the file WEBINET.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.

3. 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, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want VShield to record in its log file. You can choose to record this information:

   - **Virus detection.** Select this checkbox to have VShield note the number of infected files it found as you downloaded them.
   - **Infected file deletion.** Select this checkbox to have VShield note the number of infected files it deleted as you downloaded them.
   - **Infected file move.** Select this checkbox to have VShield note the number of infected files it moved to your quarantine directory.
   - **Session settings.** Select this checkbox to have VShield list the options you choose in the Download Scan Properties dialog box for each scanning session.
   - **Session summary.** Select this checkbox to have VShield summarize its actions during each scanning session. Summary information includes the number of files VShield scanned, the number and type of viruses it detected, the number of files it moved or deleted, and other information.

5. Click a different tab to change any of your Download Scan settings, or click one of the icons along the side of the Download Scan Properties dialog box to choose options for a different module.

   To save your changes in the Download Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the Internet Filter module

Although both Java and ActiveX objects include safeguards designed to prevent harm to your computer system, determined programmers have developed objects that exploit arcane Java or ActiveX features to cause various sorts of harm to your system.

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

VShield allows a more judicious approach. It uses an up-to-date database of objects known to cause harm to screen Java classes and ActiveX controls you encounter as you browse.

To set VShield to block harmful objects and filter dangerous Internet sites, click the Internet Filter icon at the left side of the VShield Properties dialog box to display the property pages for this module. The next sections describe your options.

Choosing Detection options

VShield starts by blocking all of the harmful objects and sites listed in its database, in order to prevent you from accidentally encountering them (Figure 5-26).

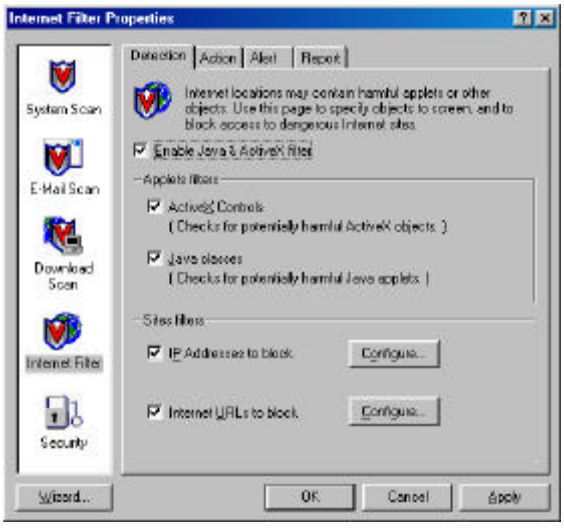

Figure 5-26. Internet Filter Properties - Detection page

To change these default options, verify that the Enable Java & ActiveX filter checkbox is selected, then follow these steps:

1. Tell VShield which objects to filter. Your options are:

   - **ActiveX Controls.** Select this checkbox to have VShield look for and block harmful ActiveX or .OCX controls.
   - **Java classes.** Select this checkbox to have VShield look for and block harmful Java classes, or applets written in Java.

   VShield will compare the objects you encounter as you visit Internet sites with an internal database that lists the characteristics of objects known to cause harm. When it finds a match, VShield can alert you and let you decide what to do, or it can automatically keep the object from downloading. See "Choosing Action options" on page 113 more details.

2. Tell VShield which sites to filter. The program uses a list of dangerous Internet sites to decide which ones to prevent your browser from visiting. You can enable this function and add to the list of "banned" sites in two ways:

   - **IP Addresses to block.** Select this checkbox to tell VShield to identify dangerous Internet sites by using their Internet Protocol (IP) addresses. To see or designate which addresses you want VShield to ban, click **Configure** to open the Banned IP Addresses dialog box (Figure 5-27).

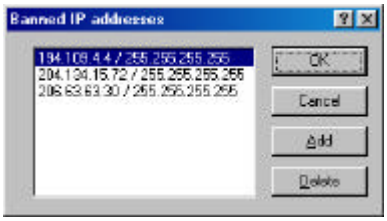

Figure 5-27. Banned IP addresses dialog box

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

123.456.789.101

VShield can use this number to identify a specific computer or network of computers on the Internet and prevent your browser from connecting to it. In Figure 5-27, each address has two sets of IP numbers. The first is the banned site's domain address—the number you use to find it on the Internet—and the second is a "subnet mask."

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

– To add to the banned list, click **Add**, then type the addresses you want VShield to block in the dialog box that appears (Figure 5-28).

Figure 5-28. Add IP address dialog box

Be sure to enter each address carefully in the correct form. If you know the subnet mask value for the site you want to avoid, enter it in the text box below. Otherwise, leave the default value shown. Click **OK** to save your address and return to the Banned IP Addresses dialog box. To add another address to the list, repeat these steps.

– To remove an address from the banned list, select it, then click **Delete**.

When you have finished editing the list, click **OK** to save your changes and and return to the Internet Filter Properties dialog box. Click **Cancel** to close the dialog box without saving your changes.

- **Internet URLs to block.** Select this checkbox to tell VShield to identify dangerous Internet sites by using their Uniform Resource Locator designation. To see or choose which addresses you want VShield to ban, click **Configure** to open the Banned URLs dialog box (Figure 5-29).

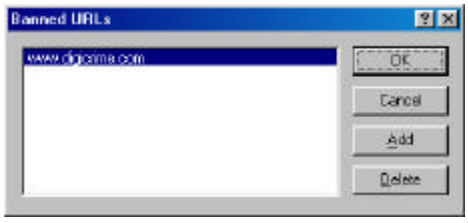

Figure 5-29. Banned URLs dialog box

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

http://www.dangerdomain.com

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

– To add to the banned list, click **Add**, then type the addresses you want VShield to block in the dialog box that appears (Figure 5-28).

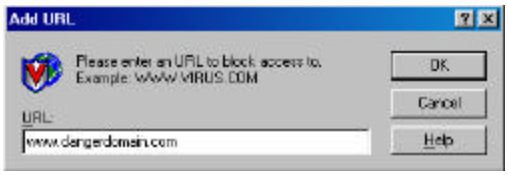

Figure 5-30. Add URL dialog box

Be sure to enter each address carefully in the correct form. To ban a website, you can enter *only the domain name*, VShield will assume you mean the HyperText transport protocol. Click **OK** to save your address and return to the Banned IP Addresses dialog box. To add another address to the list, repeat these steps.

– To remove an address from the banned list, select it, then click **Delete**.

When you have finished editing the list, click **OK** to save your changes and return to the Internet Filter Properties dialog box. Click **Cancel** to close the dialog box without saving your changes.

3. Click the Action tab to choose additional VShield options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When VShield encounters a dangerous object or a banned site, it can respond either by asking you whether it should block the object or site, or by automatically blocking it. Use the Action property page to specify which of these courses you want VShield to take.

By default, VShield lets you decide what you want to do (Figure 5-31).

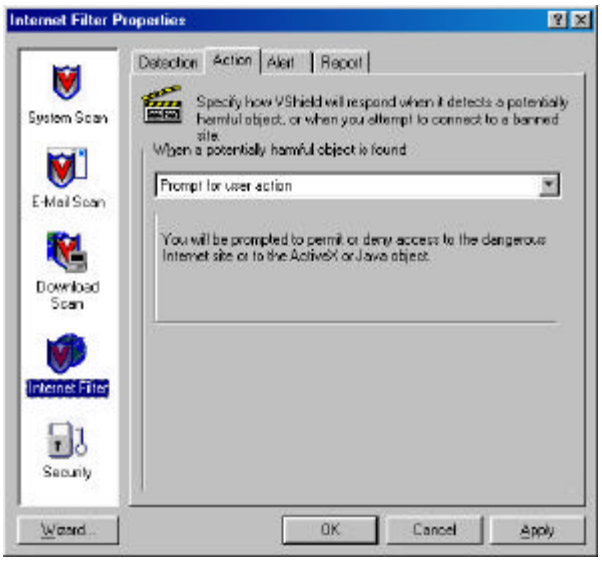

Figure 5-31. Internet Filter Properties dialog box - Action page

Choose a response from the **When a potentially harmful object is found** list. Your choices are:

- **Prompt for user action.** Choose this to have VShield ask you whether to block a harmful object or site, or to permit access to it.
- **Deny access to objects.** Choose this to have VShield block harmful objects or sites automatically. The program will do so based on the contents of its own database, plus whatever site information you added. See “Choosing Detection options” on page 109 for details.

Click the Alert tab to choose additional VShield options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let VShield look for and block harmful objects or Internet sites, with almost no further intervention. If, however, you want VShield to inform you immediately when it encounters such an object or site so you can take appropriate action, you can configure it to send an alert message to you or to others in a variety of ways. Use the Alerts property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the Internet Filter module to display the correct property page (Figure 5-32).

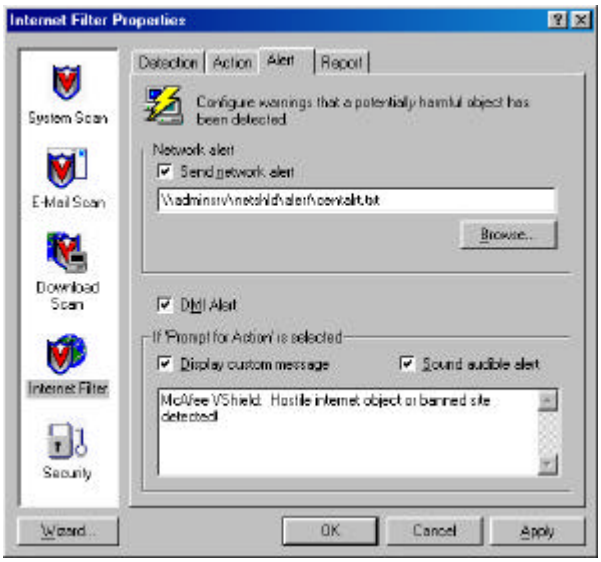

Figure 5-32. Internet Filter Properties dialog box - Alert page

2. To tell VShield to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VShield and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To have VShield send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, consult your network administrator.

4. If you chose **Prompt for user action** as your response in the Action page (see "Choosing Action options" on page 113 for details), you can also tell VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. Click the Report tab to choose additional VShield options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

VShield's Internet Filter module records how many Java and ActiveX objects it scanned, and how many it blocked from access to your computer in a log file called WEBFLTR.TXT. The same file records the number of Internet sites you visited while VShield was active, and how many dangerous sites the program kept your browser from visiting.

You can have VShield write its log to its default file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor. Use the Report property page to designate the file you want to serve as VShield's Internet Filter log, and to determine that file's permissible size.

To set VShield to record its actions in a log file, follow these steps:

1. Click the Report tab in the Internet Filter module to display the correct property page (Figure 5-25).

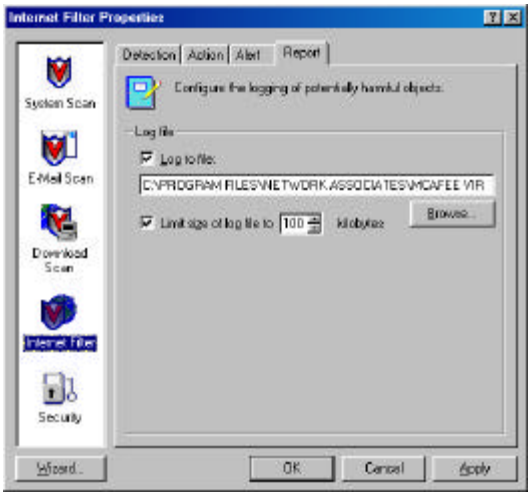

Figure 5-33. Internet Filter Properties dialog box - Report page

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

   By default, VShield writes log information to the file WEBFLTR.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.

3. 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, VShield limits the file size to 100KB. If the data in the log exceeds the file size you set, VShield erases the existing log and begins again from the point at which it left off.

4. Click a different tab to change any of your Internet Filter settings, or click one of the icons along the side of the Internet Filter Properties dialog box to choose options for a different module.

   To save your changes in the Internet Filter module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the Security module

To keep the settings you chose for each VShield module safe from unauthorized changes, you can protect any or all module property pages with a password. If you are a system administrator, you can use this feature in conjunction with VShield's ability to save its settings in a .VSH file to replicate your configuration options across all client computers on your network. If you prevent VShield from being disabled (see Step 4 on page 82 for details), then protect that setting with a password, you can enforce a strict anti-virus security policy for all network users, easily and effectively.

Use the Security module to assign a password and to choose which pages to protect.

Enabling password protection

VShield does not enable the Security module by default, because it needs to know which password you want to assign to your settings.

To activate and configure VShield password protection, follow these steps:

1. Select the **Enable password protection** checkbox.

   The options in the rest of the property page activate (Figure 5-34).

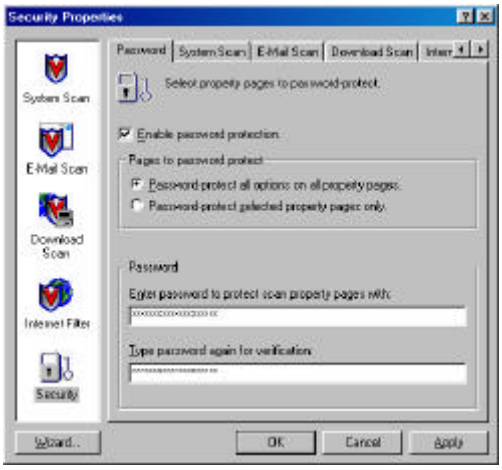

Figure 5-34. Security Properties dialog box - Password page

2. Decide whether to protect the property pages for all VShield modules, or whether to protect individual pages. Your choices are:

   - **Password-protect all options on all property pages.** Select this button to lock everything all at once.
   - **Password-protect selected property pages only.** Select this button to choose which property pages in individual modules you want to lock. The other tabs in the Security Properties dialog box let you designate individual pages.

3. Enter a password to use to lock your settings. Type any combination of up to 20 characters in the upper text box in the **Password** area, then enter the exact same combination in the text box below to confirm your choice.

   IMPORTANT: VShield's password protection is different from the password protection you can assign to VirusScan. Choosing a password for one component does not assign that password to the other component—you must choose passwords for each independently.

4. Click any of the other Security module tabs to protect individual property pages. To save your password without closing the Security Properties dialog box, click **Apply**. If you chose to protect all property pages in all modules and want to close the dialog box, click **OK**. To close the dialog box without saving any changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Once you have protected your settings with a password, VShield will ask you to enter that password whenever you open the VShield Properties dialog box (Figure 5-35).

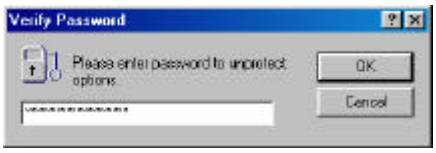

Figure 5-35. Verify Password dialog box

Enter the password you chose in the text box provided, then click **OK** to get access to the VShield Properties dialog box.

Protecting individual property pages

If you chose Password-protect selected property pages only in the Security module's Password page, you can choose which configuration options you want to lock.

Follow these steps:

1. Click the tab for the *module* whose settings you want to protect. If you don't see the tab you want, click ◀ or ▶ to bring it into view. A representative page appears in Figure 5-36.

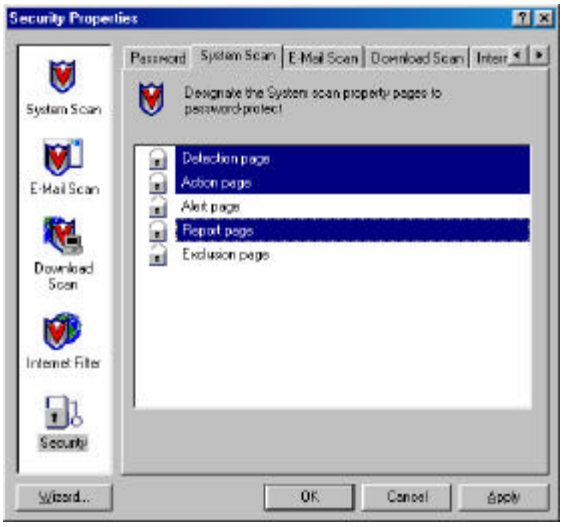

Figure 5-36. System Scan security options

2. Select the settings you want to protect in the list shown.

   You may protect any or all of a module's property pages. Protected property pages display a locked padlock icon in the security list shown in Figure 5-36. To remove protection from a property page, click the locked padlock icon to unlock it .

3. Select as many property pages as you want protected in each module.

4. To save your password without closing the Security Properties dialog box, click **Apply**. to save your changes close the dialog box, click **OK**. To close the dialog box without saving any changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

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.
- **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.
- **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.
- **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.

Tracking VShield status information

Once activated and configured, VShield operates continuously in the background, watching for and then scanning e-mail you receive, files you run, or download, or Java and ActiveX objects you encounter.

To enable or disable its scanning activity, or to see a summary of its progress

1. Double-click the VShield system tray icon to open the VShield Status dialog box.
2. Click the tab that corresponds to the program component you want to enable or disable, or whose progress you want to check.

   For the System Scan module, VShield reports the number of files it has scanned, the number of infected files it found, and the number it cleaned, moved or deleted. For the E-mail Scan and Download Scan modules, it reports the number of files it scanned, the number of infections it found, and the number it moved or deleted. For Java and ActiveX applets or Internet sites, VShield reports the number of items it has scanned and the number it has "banned," or kept you from encountering.

If you have activated its reporting feature, VShield also records the same information in the log file for each module.

3. Click **Enable** to start the program component. To disable it, click **Disable**.
4. Click **Properties** to open the VShield Properties dialog box, where you can set options that tell VShield how to perform each type of scan.
5. Click **Close** to close the VShield Status dialog box.

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 "Setting VShield properties" on page 78 for details).

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 120 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 5-37).

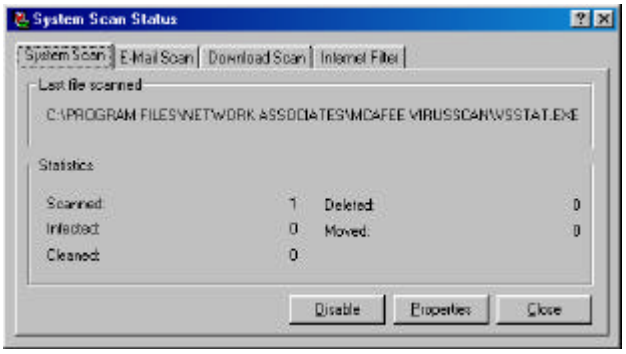

Figure 5-37. VShield status dialog box

For each module 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.** Click **VShield** in the VirusScan Central window, or right-click the VShield icon in the Windows system tray, point to **Properties**, then choose **System Scan** from the shortcut menu that appears. Either method will display the VShield Properties dialog box (see Figure 5-38 on page 122).

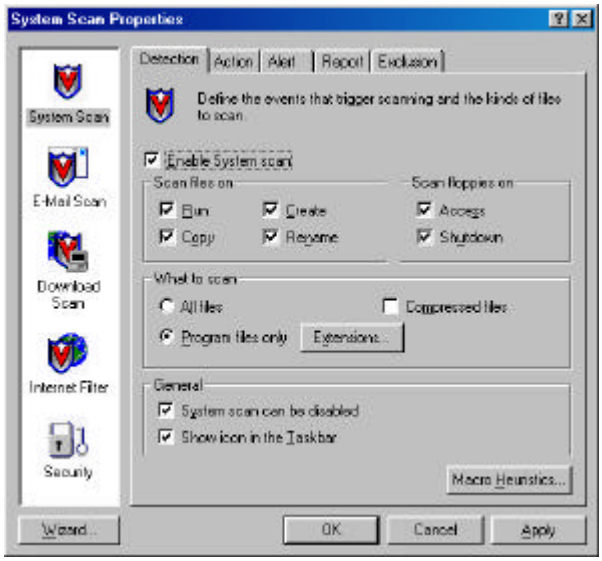

Figure 5-38. VShield Properties dialog box

For each module 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 **Scheduler** in the VirusScan Central window to open the Scheduler window (Figure 5-39).

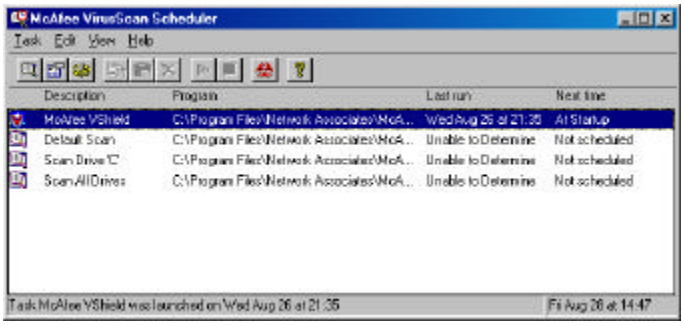

Figure 5-39. VirusScan Scheduler window

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 6

What is VirusScan?

The VirusScan name applies both to the entire set of desktop anti-virus program components described in this *User's 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 scanning operation concurrently.

This chapter describes how to use VirusScan in both its Classic and Advanced modes.

Why run on-demand scan operations?

Because its VShield component provides background scanning protection, using VirusScan to scan your system might seem redundant. But good anti-virus security measures incorporate complete, regular system scans because:

- **Background scanning checks files as they execute.** VShield looks for virus code as executable files run or when you read a floppy disk, but VirusScan can check for code signatures in files stored on your hard disk. If you rarely run an infected file, VShield might not detect the virus until it deploys its payload. VirusScan, however, can detect a virus as it lies in wait for an opportunity to run.
- **Viruses are sneaky.** Accidentally leaving a floppy disk in your drive as you start your computer could load a virus into memory before VShield loads, particularly if you do not have VShield configured to scan floppy disks. Once in memory, a virus can infect nearly any program, including VShield.

- **Scanning with VShield takes time and resources.** Scanning for viruses as you run, copy or save files can delay software launch times and other tasks—time you might rather devote to important work. Although the impact is very slight, you might be tempted to disable VShield if you need every bit of available power for demanding tasks. In that case, performing regular scan operations during idle periods can guard your system against infection without compromising performance.
- **Good security is redundant security.** In the networked, web-centric world in which most computer users operate today, it takes only a moment to download a virus from a source you might not even realize you visited. If a software conflict has disabled background scanning for that moment, or if background scanning is not configured to watch a vulnerable entry point, you could end up with a virus. Regular scan operations can often catch infections before they spread or do any harm.

VirusScan Classic comes with a single, default scan operation preconfigured 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 preconfigured scan operation, which scans all of your local hard disks.

Starting VirusScan

To start VirusScan, either

- Start VirusScan Central, then click **Scan** at the left side of the window. To learn how to start and use VirusScan Central, see Chapter 4, "Using VirusScan Central."
- 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 (Figure 6-1).

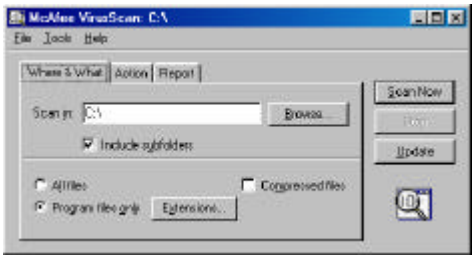

Figure 6-1. VirusScan Classic window

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 Classic 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. VirusScan will ask you whether you want to replace the file that records the default settings. Click **Overwrite** to continue. If you make changes to the default settings but decide that you want to return to the default settings, choose **Restore Default** from the **File** menu.

NOTE: Once you save new settings as default settings, choosing **Restore Default** from the **File** menu will restore the new settings you saved, not the original settings that came with the program. To preserve the original settings, use Windows Explorer to locate the file DEFAULT.VSC in the VirusScan program directory, then make a copy of it. Next, to restore the original program settings, delete the existing copy of DEFAULT.VSC and rename your backup copy to DEFAULT.VSC. To learn about the .VSC file format, see Appendix C, "Understanding the .VSC File Format."

- **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 as a .VSC file. 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 129 or "Configuring VirusScan Classic" on page 129 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 6-2). 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 143.

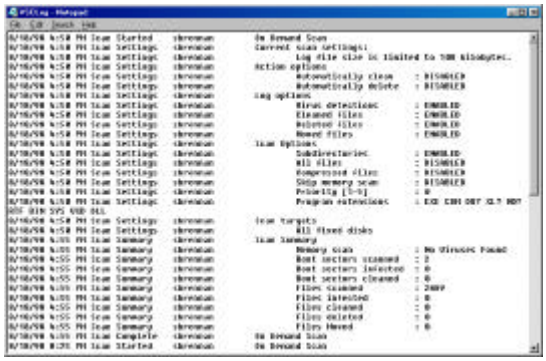

Figure 6-2. VirusScan Activity Log

- **Update VirusScan data or program files.** Choose **Update VirusScan** from the **File** menu or click the **Update** button at the right of the VirusScan window to start the Network Associates SecureCast wizard that will guide you through updating your data (.DAT) files or your product version. See "Using SecureCast to Update Your Software" on page 179 to learn how to use the wizard.

- **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.** To switch from VirusScan Classic to VirusScan Advanced, choose **Advanced** from the **Tools** menu. To switch from VirusScan Advanced to VirusScan Classic, choose **Classic** from the **Tools** menu.

- **Activating password protection.** VirusScan Advanced gives you the ability to lock your settings to prevent unauthorized changes. Choose **Password Protect** from the **Tools** menu to open a dialog box where you can choose which settings to protect. See "Enabling password protection" on page 147 for details.

- **Open the Virus List.** Choose **Virus List** from the **Tools** menu to information about the viruses that VirusScan detects and cleans. To learn more about the information available in the Virus List, see "Viewing the Virus List" on page 149.

- **Start VirusScan Scheduler.** VirusScan Advanced gives you a link to VirusScan Scheduler, a utility that lets you configure and run unattended scan operations. Choose **Scheduler** from the **Tools** menu to open the Scheduler window. To learn how to use the Scheduler, see "Scheduling Scan Tasks" on page 153.
- **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.
- **Link to the Network Associates Virus Information Library.** Choose **On-line Virus Info** from the **Help** menu to connect to the Network Associates website. To use this service, you must have a web browser installed on your computer and have a dial-up or network connection to the Internet. To learn more about what information the Virus Information Library has, see "Connecting to the Online Virus Information Library" on page 151.

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 6-3).

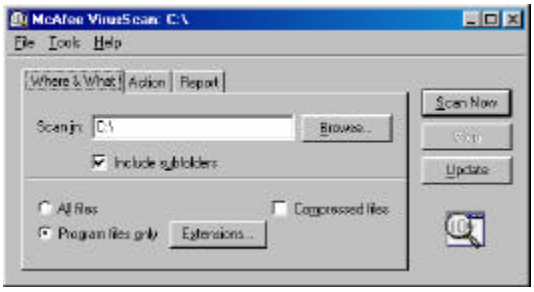

Figure 6-3. VirusScan Classic window - Where & What page

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 6-4).

Figure 6-4. 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 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 in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats. 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 6-5).

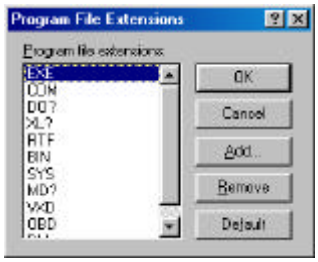

Figure 6-5. The Program File Extensions dialog box

By default, VirusScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, 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 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 **Delete**.
  - 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. 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 6-6).

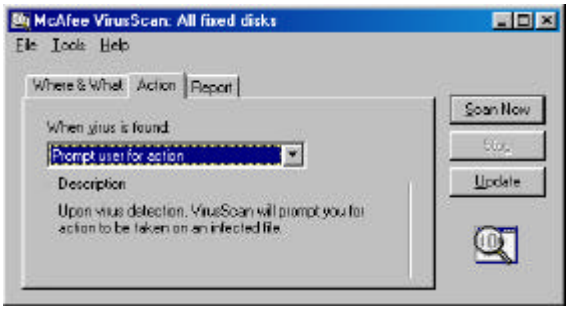

Figure 6-6. VirusScan Classic window - Action page

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 choice. Your choices are:

   - **Prompt User for Action.** Use this option 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 responses.
   - **Move infected files automatically**. Use this option 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.** Use this option 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 notify you in its message area and, if you have its reporting features enabled, will note the incident in its log file. See "Choosing Report options" on page 143 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.
- **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 143 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. 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 a 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 6-7).

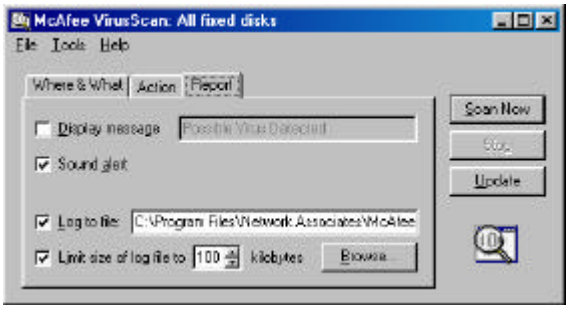

Figure 6-7. VirusScan Classic window - Report page

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 custom 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 140 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 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. 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**.

Configuring VirusScan Advanced

VirusScan Advanced offers you more flexibility in your configuration options than does VirusScan Classic, including the ability to run more than one scan operation concurrently, the ability to exclude items from scan operations, and the ability to set a sensitivity level for VirusScan's macro virus detection function.

Starting VirusScan from VirusScan Central opens VirusScan Classic first. To switch VirusScan from Classic mode to Advanced mode, choose **Advanced** from the **Tools** menu in the VirusScan Classic window. As with VirusScan Classic a series of property pages controls the options for each task in VirusScan Advanced. Click each tab in the VirusScan Advanced window to set up VirusScan for your task.

Choosing Detection options

VirusScan initially assumes that you want to scan all hard disks on your computer, including those mapped from network drives, and to restrict the files it scans only to those susceptible to virus infection (Figure 6-8).

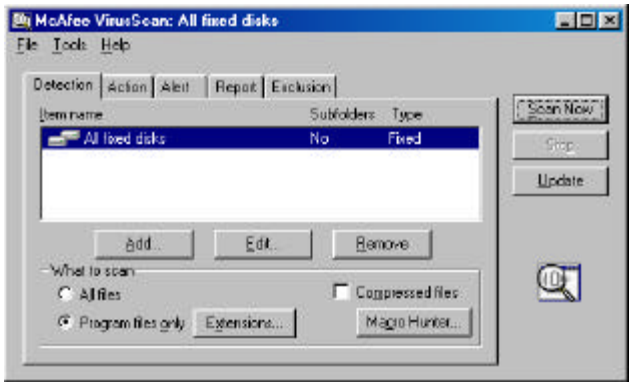

Figure 6-8. VirusScan Advanced window - Detection page

To modify these options and add others, follow these steps:

1. Choose which parts of your system or your network that you want VirusScan to examine for viruses. You can

   - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 6-9).

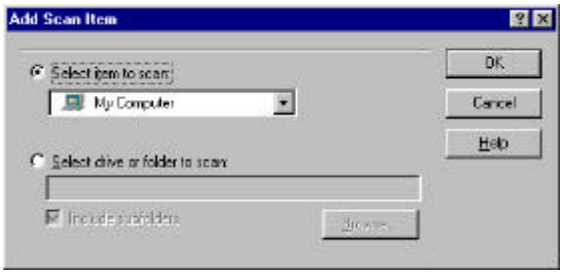

Figure 6-9. The Add Scan Item dialog box

To have VirusScan examine your entire computer or a subset of the drives on your system or your network, click the **Select item to scan** button, then choose the scan target from the list provided. Your choices are:

– **My Computer.** This tells VirusScan to scan all drives physically attached to your computer or logically mapped via Windows Explorer to a drive letter on your computer.

– **All Removable Media.** This tells VirusScan to scan only CD-ROM discs, Syquest and Iomega cartridges, or similar storage devices physically attached to your computer.

– **All Fixed Disks.** This tells VirusScan to scan hard disks physically connected to your computer.

– **All Network Drives.** This tells VirusScan to scan all drives logically mapped via Windows Explorer to a drive letter on your computer.

To have VirusScan examine a particular disk or folder on your system, click the **Select drive or folder to scan** button. Next, type in the text box provided the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer. Select the **Include subfolders** checkbox to have VirusScan also look for viruses in any folders inside your scan target. Click **OK** to close the dialog box.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Item to Scan dialog box (Figure 6-10).

Figure 6-10. The Edit Item to Scan dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

2. 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 in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats. 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 6-11).

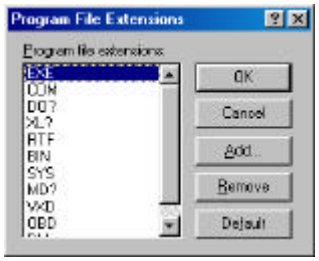

Figure 6-11. The Program File Extensions dialog box

By default, VirusScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, 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 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 **Delete**.
- 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.

- **Turn on heuristic scanning**. Click **Macro Heuristics** to open the Macro Heuristics Scan Settings dialog box (Figure 6-12).

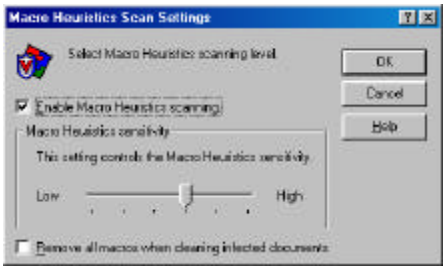

Figure 6-12. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables VirusScan to recognize new macro viruses based on their resemblance to similar viruses it already knows. To do this, VirusScan first identifies all Microsoft Word, Microsoft Excel, and other Microsoft Office files that have embedded macros, then it compares the macro code to its virus signature database. Exact matches it identifies with the virus name; code signatures that resemble existing viruses cause VirusScan to tell you it has found a “probable” macro virus. Unless you know that the file does not contain a virus, you should treat “probable” infections with the same caution you would confirmed infections.

To activate heuristic scanning, follow these steps:

a. Select the **Enable macro heuristics scanning** checkbox.

b. Set the sensitivity level you want VirusScan to use when it looks for macro viruses. Drag the slider to the left to set a low level of sensitivity—this causes VirusScan to look for as close a match as possible between the macros it finds in the file and existing virus code signatures before it labels a file as infected.

   Drag the slider to the right to set a high level of sensitivity—this causes VirusScan to look with suspicion at nearly all macro code and to identify a wider range of files as potentially infected.

   NOTE: Higher levels of sensitivity can cause VirusScan to falsely identify a file as infected, but it does so out of caution. Until virus researchers have examined the suspicious file and positively eliminated any possibility of infection, the potential exists for nearly all macro code to harbor new viruses. The sensitivity setting exists for you to choose the level that works best for your environment.

c. Determine how you want to treat infected macro files. Select **Remove all macros when cleaning infected documents** to eliminate all infectable code from the document and leave only data. To try to remove only the virus code from the document's macros, leave this checkbox clear.

   NOTE: Use this feature with caution: removing all macros from a document can cause it to lose data or to become corrupted and unusable.

d. Click **OK** to save your settings and return to the VirusScan Properties dialog box.

3. 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. 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 Advanced window to display the correct property page (Figure 6-13).

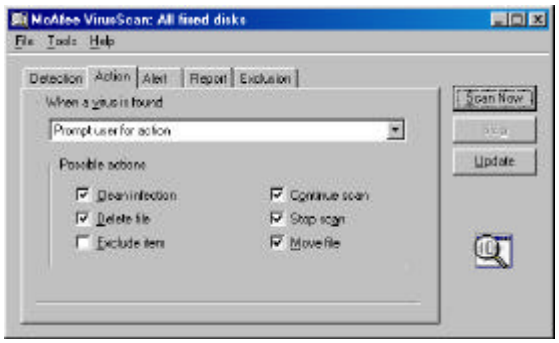

Figure 6-13. VirusScan Advanced - Action page

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 choice. Your choices are:

   - **Prompt User for Action.** Use this option if you expect to be at your computer when VirusScan examines your disk—the program will display an alert message when it finds a virus and offer you a range of possible responses. Choose which response options you want to see from among these:

     – **Clean infection.** This option tells VirusScan to try to remove the virus code from the infected file.

     – **Delete file.** This option tells VirusScan to delete the infected file immediately.

     – **Exclude item.** This option tells VirusScan to skip the file during later scan operations. This is the only option not selected by default.

     – **Continue scan.** This option tells VirusScan to continue with its scan, but not take any other actions. If you have its reporting options enabled, VirusScan records the incident in its log file.

  - **Stop scan.** This option tells VirusScan to stop the scan operation immediately. To continue, you must click **Scan Now** to restart the operation.
  - **Move file.** This option tells VirusScan to move the infected file to a quarantine folder.

- **Move infected files automatically**. Use this option 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.** Use this option 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 notify you in its message area and, if you have its reporting features enabled, will note the incident in its log file. See "Choosing Report options" on page 143 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.

- **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 143 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 Alert 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. 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 Alert options

Once you configure it with the response options you want, you can let VirusScan look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want VirusScan to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you in a variety of ways. Use the Alerts property page to choose which alerting methods you want to use.

Follow these steps:

1. Click the Alert tab in the VirusScan Advanced window to display the correct property page (Figure 6-14).

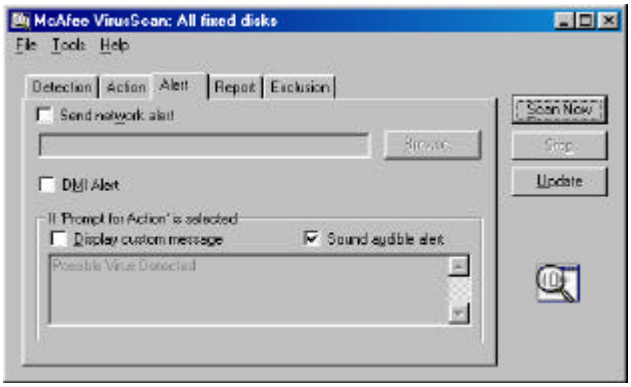

Figure 6-14. VirusScan Advanced - Alert page

2. To tell VirusScan to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VirusScan and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

3. To have VirusScan send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, see your network administrator.

4. If you chose **Prompt user for action** as your response in the Action page (see "Choosing Action options" on page 140 for details), you can also tell VirusScan to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

5. 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. 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

VirusScan 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 a text editor.

The VSCLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VirusScan found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Reports property page to determine which information VirusScan will include in its log file.

To set VirusScan to record its actions in a log file, follow these steps:

1. Click the Report tab in the VirusScan Advanced window to display the correct property page (Figure 6-15).

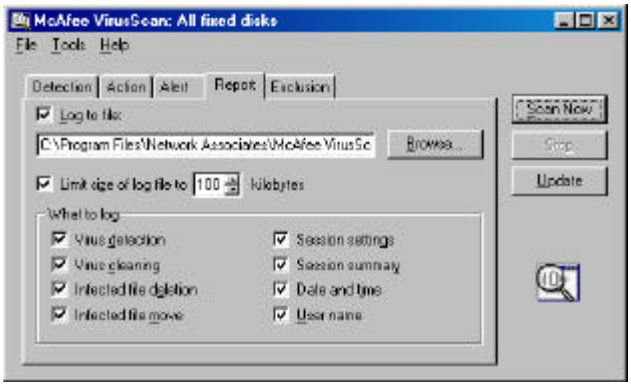

Figure 6-15. VirusScan Advanced - Report page

2. 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 in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. 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.

4. Select the checkboxes that correspond to the information you want VirusScan to record in its log file. You can choose to record this information:

   - **Virus detection.** Select this checkbox to have VirusScan note the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VirusScan note the number of infected files from which it removed the infecting virus.
   - **Infected file deletion.** Select this checkbox to have VirusScan note the number of infected files it deleted from your system.
   - **Infected file move.** Select this checkbox to have VirusScan note the number of infected files it moved to your quarantine directory.

- **Session settings.** Select this checkbox to have VirusScan list the options you choose in the McAfee VirusScan Properties dialog box for each scanning session.
- **Session summary.** Select this checkbox to have VirusScan summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information.
- **Date and time.** Select this checkbox to have VirusScan append the date and time to each log entry it records.
- **User name.** Select this checkbox to have VirusScan append the name of the user logged in to your computer at the time it records each log entry.

To see the contents of the log file, start VirusScan, then choose **View Activity Log** from the **File** menu. For more information, see "Using VirusScan menus" on page 127.

5. Click the Exclusion 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. 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 Exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling VirusScan to look only at susceptible file types (see "Choosing Detection options" on page 135 for details), or you can tell VirusScan to ignore entire files or folders that you know will not get infected.

Once you scan your system thoroughly, you can exclude the files and folders that do not change or that are not normally vulnerable to virus infection. You can also rely on VShield to provide you with protection in between scheduled scan operations. Regular scan operations that examine all areas of your computer, however, provide you with the best virus defense.

To exclude files or folders from scan operations, follow these steps:

1. Click the Exclusion tab in the VirusScan Advanced window to display the correct property page (Figure 6-15).

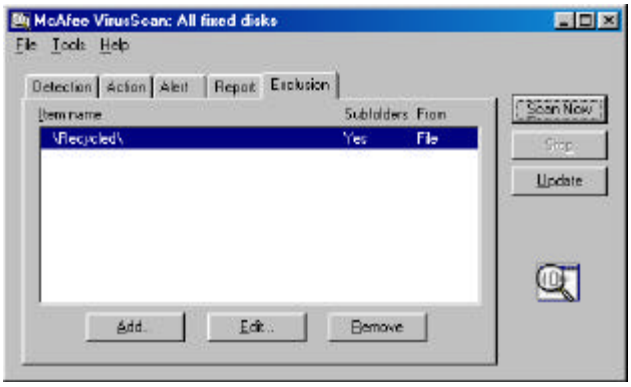

Figure 6-16. VirusScan Advanced window - Exclusion page

The Exclusion page will initially list only your Recycle Bin. VirusScan excludes the Recycle Bin from scan operations because Windows will not run files stored there.

2. Specify the items you want to exclude. You can

   - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 6-17).

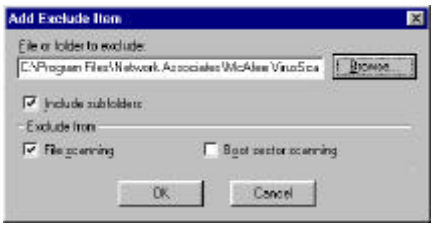

Figure 6-17. Add Exclude Item dialog box

   a. Type the volume, the path to the file, or the path to the folder that you want to exclude from scanning, or click **Browse** to locate a file or folder on your computer.

> **NOTE:** If you have chosen to move infected files to a quarantine folder automatically, the program excludes that folder from scan operations.

b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.

c. Select the **File scanning** checkbox to tell VirusScan not to look for file-infector viruses in the files or folders you exclude.

d. Select the **Boot sector scanning** checkbox to tell VirusScan not to look for boot-sector viruses in the files or folders you exclude. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

> **WARNING:** Network Associates recommends that you do *not* exclude your system files from virus scanning.

e. Click **OK** to save your changes and close the dialog box.

f. Repeat steps a. through d. until you have listed all of the files and folders you do not want scanned.

- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.
- **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. VirusScan will then scan this file or folder during its next scanning operation.

3. 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. 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**.

Enabling password protection

VirusScan lets you set a password to protect the settings you choose in each property page from unauthorized changes. This feature is particularly useful for system administrators who need to keep users from tampering with their security measures by changing VirusScan settings. Use the Security property page to lock your settings.

To enable password protection for VirusScan Advanced, follow these steps:

1. Choose **Password Protect** from the **Tools** menu in the VirusScan Advanced window to open the Password Protection dialog box (Figure 6-18).

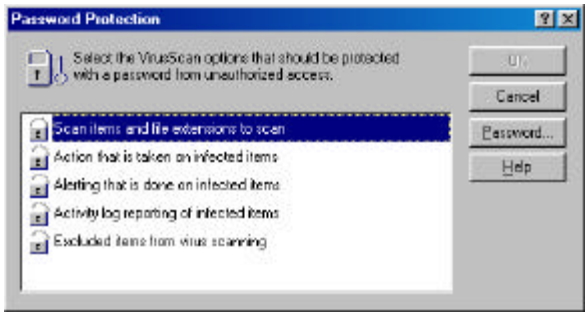

Figure 6-18. Password Protection dialog box

2. Select the settings you want to protect in the list shown.

   You may protect any or all VirusScan property pages. Protected property pages display a locked padlock icon in the security list shown in Figure 6-18. To remove protection from a property page, click the locked padlock icon to unlock it .

3. Click **Password** to open the Specify Password dialog box (Figure 6-19).

Figure 6-19. Specify Password dialog box

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

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

4. Click **OK** to return to the VirusScan Advanced window.

Viewing the Virus List

Choose **Virus List** from the **Tools** menu in either VirusScan Classic or VirusScan Advanced to open the Virus List window (Figure 6-20).

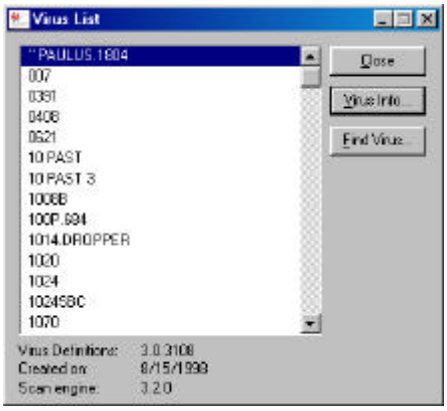

Figure 6-20. Virus List window

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, scroll through the list to locate the one you want to know about, select it, then click **Virus Info** at the right edge of the window. If you know the name of a particular virus you want to locate, click **Find Virus**, then enter the virus name in the text box provided. The Virus List will scroll immediately to the name you entered. Click **Close** in the Find What Virus box, select the virus name in the list, then click **Virus Info**.

A Virus Information window for the virus you selected will appear (Figure 6-21). Click >> or << to move backward or forward in the Virus List.

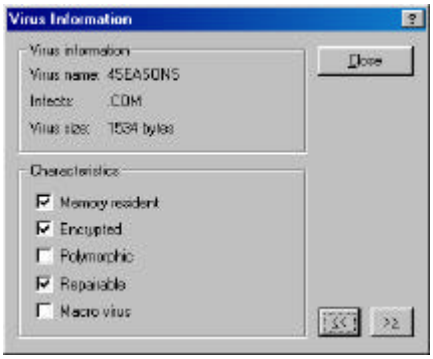

Figure 6-21. Virus Information window

The Virus Information page tells you this about each virus:

- **Virus Name.** The name given to the virus usually results from agreement among anti-virus vendors who follow certain naming conventions, but occasionally different vendors will call the same virus by different names.
- **Infects.** Most viruses infect either executable files or the master boot record and boot blocks of your hard disk. Some rare virus strains infect other file types, such as mIRC script files or Java language files.
- **Virus Size.** This is the size of the virus code itself, in bytes. In some cases, a change in a file's size by the number of bytes listed here can alert you to an infection.
- **Characteristics.** Virus characteristics can include the types of strategies a virus will use to conceal itself and whether its code can be safely removed from an infected file. The Information page provides these specifics:
  - **Memory Resident.** A checkmark in this box means that the virus copies itself from its location on your hard disk into your computer's memory, where it can then infect any file that you run or save to disk.
  - **Encrypted.** A checkmark in this box means that the virus encrypts its identifying "code signature"—the byte pattern it uses to tell itself which files it has already infected—so that it will not re-infect the same file. This can make identifying the virus much more difficult.
  - **Polymorphic.** A checkmark in this box means that the virus uses a variety of techniques to conceal its code signature. These techniques include: encryption; "mutation," in which the virus alters or scrambles its code signature each time it infects another file; and "stealth," in which the virus redirects system queries that attempt to read its location on disk.
  - **Repairable.** A checkmark in this box means that VirusScan or VShield has a "remover" specifically designed to delete the virus code from the infected file and restore it to its original state.
  - **Macro Virus.** A checkmark in this box means that the virus infects Microsoft Office data files that include code written in Microsoft's Visual Basic for Applications, or other macro languages.

Connecting to the Online Virus Information Library

For more comprehensive information about viruses, visit the online Virus Information Library at the Network Associates website. Choose **Online Virus Info** from the **Help** menu, or use your web browser to connect to this address:

http://www.nai.com/vinfo/

The Virus Information Library contains documents that give an overview of each virus type in much more detail than that available from the Virus List. 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.

Scheduling Scan Tasks 7

What does VirusScan Scheduler do?

VirusScan Scheduler runs scan operations and other tasks on the dates and at the times you choose, or at intervals you set. Use the Scheduler to run a scan operation in your absence, when it causes the least disruption to your work, as part of a series of automated tasks, or in other ways that suit your needs.

Why schedule scan operations?

Although VirusScan includes components that look for viruses continuously or that allow you to scan your system whenever you want, you can schedule regular scan operations and other VirusScan activities to

- **Set a periodic baseline for your system.** If you want to track your system or your network for recurring virus activity, schedule a full scan of your system at regular intervals. VirusScan's reporting features can provide you with a complete report on the number, type, size and other characteristics of any viruses it finds.
- **Supplement or replace on-access scanning.** Network Associates recommends that you use VShield to scan continuously for viruses, but if your environment doesn't permit you to use VShield or if you have other concerns about system performance, schedule frequent scan operations to prevent infections. Even if you do use VShield, scheduling periodic full scans of your system reduces the likelihood that infected files remain undetected.
- **Alternate between scan operations.** Scheduled scanning operations give you the flexibility to choose different operations for different purposes or different times. If, for example, you want to use VShield to scan your own system continuously and scan mapped network drives less frequently, you can schedule a task for this purpose.

The Scheduler comes with a default set of tasks already configured, but not yet scheduled. This set includes tasks that start VShield when you start your computer, that perform a default scan task, that scan your C: drive, or that scan all drives on your system. You can enable one of the default tasks to start, or you can create your own tasks to suit your work habits.

Starting the VirusScan Scheduler

To start the VirusScan Scheduler, either

- Start VirusScan Central, then click **Schedule** at the left side of the window. To learn how to start and use VirusScan Central, see Chapter 4, "Using VirusScan Central."
- Start VirusScan Classic, then choose **Advanced** from the **Tools** menu to switch to VirusScan's advanced mode. Next, choose **VirusScan Scheduler** from the **Tools** menu. To learn how to start VirusScan and use its advanced mode, see Chapter 6, "Using McAfee VirusScan."

Both methods open the Scheduler window (Figure 7-1). Once you start it, the Scheduler also displays a small icon in the Windows system tray. Double-click this icon to bring the Scheduler window to the foreground.

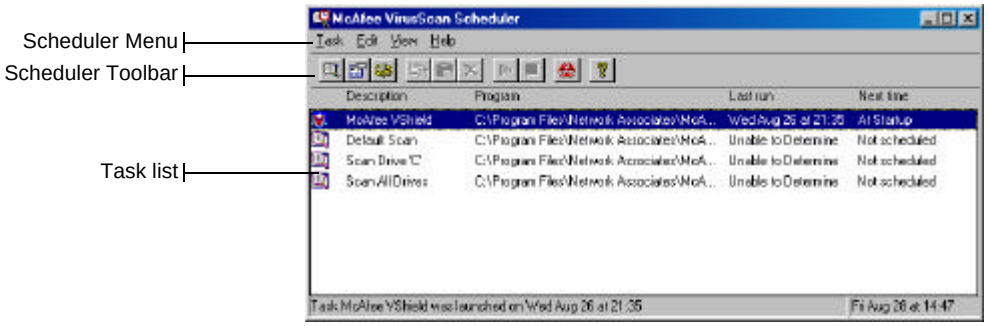

Figure 7-1. VirusScan Scheduler window

The Scheduler window initially shows a set of default tasks that come with the Scheduler, pre-configured and ready to run. A "task" is a set of instructions to run a particular program, in a certain configuration, at a certain time. The Scheduler's task list indicates which program will carry out your task —you'll schedule VShield or SCAN32.EXE for most tasks—displays the time and date when you last ran your task, and shows you when you have it set to run again. Each new task that you create appears at the bottom of the task list.

The toolbar at the top of the Scheduler window gives you quick access to the program's most common commands. Most of those same commands also appear in the menus at the top of the Scheduler window, and in shortcut menus that appear when you click a listed task with your right mouse button.

A status bar at the bottom of the Scheduler window counts the number of listed tasks. When you select a listed task, the status bar tells you when the task last ran. The status bar also shows a brief description of each toolbar button as you pass your mouse cursor over it. Choose **Toolbar**, **Title Bar** or **Status Bar** from the **View** menu to display or hide each window element.

Using the Scheduler window

From the Scheduler window, you can:

- **Create a new task.** Choose **New Task** from the **Task** menu, or click  in the Scheduler toolbar. A Task Properties dialog box will appear. See "Creating new tasks" on page 157 to learn how to specify the actions you want performed.

- **Schedule and enable a task.** Select one of the tasks listed in the Scheduler window, then choose **Properties** from the **Task** menu, or click  in the Scheduler toolbar. A Task Properties dialog box will appear. See "Enabling tasks" on page 158 to learn how to specify the options you want for your task and ready it to run.

- **Configure the task program.** Select one of the tasks listed in the Scheduler window, then click  in the Scheduler toolbar to display a property page for the VirusScan program component that will run the task. How this property page looks depends on which VirusScan component you run. See "Configuring task options" on page 161 to learn how to choose options for the scan program.

  > **NOTE:** You can configure only those programs that you run as part of a scan operation—that is, VShield or VirusScan (SCAN32.EXE).

- **Copy a task.** Select one of the tasks listed in the Scheduler window, then choose **Copy** from the **Edit** menu, or click  in the Scheduler toolbar. This copies the task to the Windows clipboard. Next, click inside the Scheduler window, then choose **Paste** from the **Edit** menu, or click  in the Scheduler toolbar to paste the task copy to the Scheduler list. Use this feature to copy task settings that you want to use as templates for other, similar tasks.

- **Delete a task.** Select one of the tasks listed in the Scheduler window, then choose **Delete** from the **Task** menu, or click  in the Scheduler toolbar. The Scheduler will ask you to confirm that you want to delete the selected task. Click **Yes** to delete the task, or click **No** to keep it.

  > **NOTE:** You can delete only tasks that you create—you may not delete any of the tasks from the default set that come with the Scheduler. You can, however, disable any default task you don't want to run. See "Enabling tasks" on page 158 for details.

- **Start a task.** Select one of the tasks listed in the Scheduler window, then choose **Start** from the **Task** menu, or click  in the Scheduler toolbar. The task you selected will start immediately and will run with the options you've chosen. To enable VShield's scanning functions, select McAfee VShield in the task list, then choose **Enable** from the **Task** menu. To start VShield and load it into memory, select the VShield task, then click  in the Scheduler toolbar.
- **Stop a task.** Select one of the tasks listed in the Scheduler window, then choose **Stop** from the **Task** menu, or click  in the Scheduler toolbar. To stop VShield from running, select McAfee VShield in the task list, then click  in the Scheduler toolbar. To simply disable VShield, select the VShield task, then choose **Disable** from the **Task** menu.
- **See the Virus List.** Choose **Virus List** from the **View** menu, or click  in the Scheduler toolbar. The Virus List will appear in a separate window. When you have finished with the list, click **Close** to close the dialog box. See "Viewing the Virus List" on page 149 to learn more about what information the list contains.
- **Open the online help file.** Choose **Help Topics** from the **Help** menu, or click  in the Scheduler toolbar to see a list of VirusScan help topics.

Working with default tasks

As soon as you install VirusScan on your computer and reboot, VShield will immediately begin scanning your system, using a default configuration that provides you with a basic range of protection for your system. The other tasks listed in the Scheduler window also have default configurations set up, but these tasks remain dormant until you activate them. See "Enabling tasks" on page 158 for details.

The default tasks are:

- **VShield.** By default, this task runs automatically as soon as you start your computer. You cannot schedule VShield to run any other time, but you can choose different scan options. See Chapter 5, "Using VShield," to learn which options you have available.
- **Default Scan.** This task serves as a template that you can use to create other tasks. By default, it scans your C: drive, your RAM and the boot sectors of your disk. You must activate this task to get it to run.
- **Scan Drive C:.** This task scans your C: drive, your RAM and the boot sectors of your hard disk by default. You must activate it to get it to run.
- **Scan All Drives.** This task scans all fixed disks and all removable media on your system, along with your RAM and hard disk boot sectors. You must activate this task to get it to run.

Creating new tasks

Although the tasks that come in the default set can provide your system with adequate protection, you will probably want to create and run your own tasks after you have some experience with VirusScan and a good idea of what and when you want it to scan.

To create a new task, follow these steps:

1. Choose **New Task** from the **Task** menu in the Scheduler window, or click  in the Scheduler toolbar.

   The Task Properties dialog box will appear (Figure 7-2).

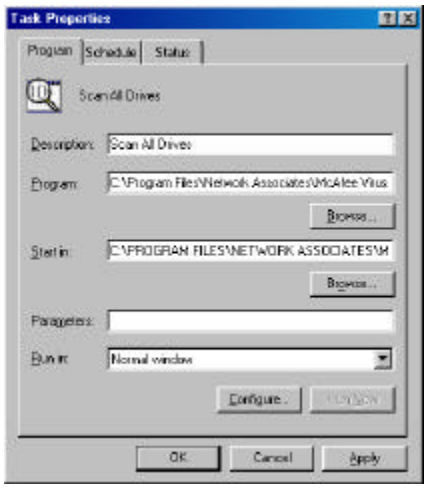

Figure 7-2. Task Properties dialog box - Program page

2. Type a name for the task in the **Description** text box. Be sure that your name describes the task so that you can distinguish it from others in the Scheduler window and so that you can tell at a glance what it does.

3. Type the full path and file name for the program you want to carry out your task in the **Program** text box, or click **Browse** to locate the program on your hard disk.

   By default, the Scheduler chooses VirusScan as the program that will run your task, and locates it in the following path:

   C:\Program Files\Network Associates\McAfee VirusScan\SCAN32.EXE

   You can run any executable program from within the VirusScan Scheduler, but you can configure program options only for VirusScan and VShield. See "Configuring task options" on page 161 for details.

4. To have the program you chose in Step 3 look in a particular folder for its data files, .INI files, or other items it needs to start, type the path to the correct folder in the **Start In** text box, or click **Browse** to locate it on your hard disk. Ordinarily, a program will look in its own folder for necessary files.

5. Type any parameters you want your program to use when it starts. For most programs, allowable parameters include any options available from the command line, or any files you want the program to open when it starts.

6. Choose **Normal** from the **Run In** list to have the program appear in its default window when it starts. Choose **Maximized** to expand the window to its largest size. Choose **Minimized** to shrink the window to a taskbar icon.

At this point you have entered enough information to create your task, but you have not yet scheduled it to run or chosen program options. You can

- Click **Apply** to save your changes without closing the Task Properties dialog box, then click the Schedule tab. To learn how to set a task schedule, see "Enabling tasks."
- Click **OK** to save your changes and return to the VirusScan Scheduler window. You will need to set a task schedule later to get it to run. To do so, select the task from the list in the Scheduler window, then click  to open the Task Properties dialog box.
- Click **Cancel** to close the dialog box without creating a task.

Enabling tasks

Enabling a task means choosing a schedule for it and activating that schedule so that the task runs when you need it. To run tasks that use VirusScan—not VShield—to scan your system, you'll also need to configure the scan operation to start automatically. See Step 4 on page 166 for more details.

To enable a task, follow these steps:

1. If you do not already have the Task Properties dialog box open, double-click one of the listed tasks in the Scheduler window, or select a task, then click  in the Scheduler toolbar.

   The Task Properties dialog box will appear (see Figure 7-2 on page 157).

2. Click the Schedule tab to display the correct property page (see Figure 7-3 on page 159).

Figure 7-3. Task Properties dialog box - Schedule page

3. Select the **Enable** checkbox. The options in the **Run** and the **Start At** areas will become active.

4. Choose how often you want the task to run in the **Run** area. Depending on which interval you select, the **Start At** area gives you a different set of choices for your task schedule. The choices are:

   - **Once.** This runs your task exactly once on the date and at the time you specify. Enter the time in the leftmost text box in the **Start At** area, then select a month from the list to the right. Next, enter the date and the year in the text boxes provided.
   - **Hourly.** This runs your task each hour as long as your computer is on and the Scheduler is running. Specify in the text box provided how many minutes the Scheduler should wait after each hour to run your task.
   - **Daily**. This runs your task once at the time you specify on the days you indicate. Enter the time in the text box provided, then select the checkboxes for each day that you want the task to run.
   - **Weekly.** This runs your task once each week on the day and at the time you specify. Enter the time in the text box provided, then choose a day from the list to the right.
   - **Monthly.** This runs your task once each month on the day and at the time you specify. Enter the time in the leftmost text box, then enter the day of the month on which you want the task to run.

   NOTE: Enter all scheduled times, except for the hourly time interval, using a 24-hour clock. If you want the task to run at 9:30 p.m., for example, enter 21:30.

5. You have now set a schedule for your task and readied it to run at the scheduled time. Click **OK** to close the Task Properties dialog box, or click **Apply** to save your settings without closing the dialog box. Click **Cancel** to close the dialog box without saving your changes.

> **NOTE:** To start your task, your computer must be on and the VirusScan Scheduler must be running. If your computer is off or if the Scheduler is not running at the time your task should start, the task will start at the next scheduled time. You can minimize the Scheduler so that appears only as an icon in the Windows taskbar. If your task will run VirusScan, you must also configure the program to start its scan operation automatically. See Step 4 on page 166 for details.

Checking task status

The VirusScan Scheduler window summarizes the time and date when your tasks last ran and when you have scheduled them to start again—look for this information to the right of each listed task. To see the results for each task—how many files it scanned, whether it found any infected files, and what actions it took to respond to the infections—follow these steps to open the Task Properties dialog box to its Status page.

1. If you do not already have the Task Properties dialog box open, double-click one of the listed tasks in the Scheduler window, or select a task, then click  in the Scheduler toolbar.

2. The Task Properties dialog box will appear (see Figure 7-2 on page 157). Click the Status tab to display the correct property page (Figure 7-4).

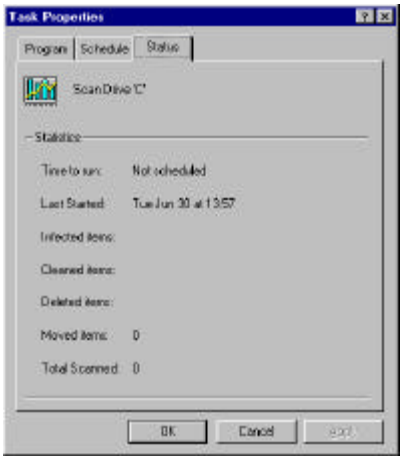

Figure 7-4. Task Properties dialog box - Status page

The property page will list the time your task last ran, the results of that scan operation, and when you have it scheduled to run again. Click **OK** or **Cancel** to close the dialog box.

Configuring task options

When you first create and schedule a task, the VirusScan Scheduler will run the program that you specify in the Task Properties dialog box with a default set of options. In most cases, the default set will provide your computer with sufficient protection from viruses and other malicious software, but you can choose custom options that better reflect your work habits and security needs.

NOTE: You can use the Scheduler to configure VirusScan program components only. To configure any other software you want to run from within the Scheduler, you must use the tools appropriate for that software to configure it separately. Consult the documentation for your other software for details.

Normally, you'll use VirusScan to perform your scheduled scan tasks. Although you can configure VShield to perform various scan tasks, you cannot specify when it will run—VShield runs when you start your computer and stops running when you shut your computer down. You can disable and re-enable VShield from within the Scheduler, but you cannot create a second VShield task.

Configuring VirusScan for scheduled scanning

To perform a scheduled scan, VirusScan needs to know what you want it to scan and what you want it to ignore, 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 and prevent others from changing your settings. A series of property pages controls the options for each task—click each tab in the McAfee VirusScan Properties dialog box to set up VirusScan for your task.

To work with the VirusScan property pages, follow these steps:

1. Select one of the scan tasks listed in the Scheduler window, then click  in the Scheduler toolbar.

   NOTE: The task you select must be configured to run VirusScan. You can modify one of the default tasks, or configure a task you created. See "Creating new tasks" on page 157 to learn how to specify the program that will run your scan task.

The McAfee VirusScan Properties dialog box will appear (Figure 7-5).

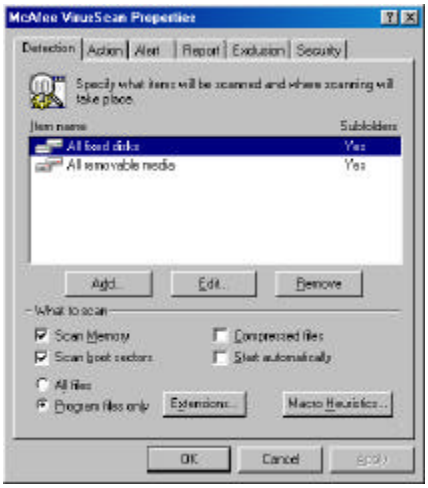

Figure 7-5. VirusScan Properties dialog box - Detection page

Choosing detection options

VirusScan initially assumes that you want to scan your C: drive and your computer's memory, to look for boot sector viruses, and to restrict the files it scans only to those susceptible to virus infection.

To modify these options, follow these steps:

1. Choose which parts of your system or your network that you want VirusScan to examine for viruses. You can

   - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 7-6).

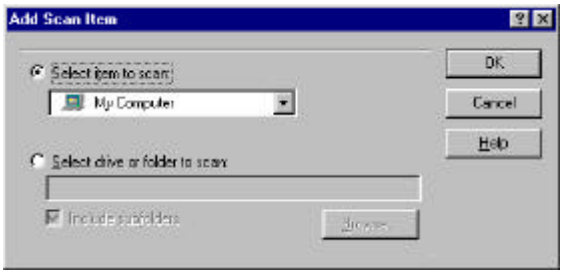

Figure 7-6. The Add Scan Item dialog box

To have VirusScan examine your entire computer or a subset of the drives on your system or your network, click the **Select item to scan** button, then choose the scan target from the list provided. Your choices are:

- **My Computer.** This tells VirusScan to scan all drives physically attached to your computer or logically mapped via Windows Explorer to a drive letter on your computer.
- **All Removable Media.** This tells VirusScan to scan only CD-ROM discs, Syquest and Iomega cartridges, or similar storage devices physically attached to your computer.
- **All Fixed Disks.** This tells VirusScan to scan hard disks physically connected to your computer.
- **All Network Drives.** This tells VirusScan to scan all drives logically mapped via Windows Explorer to a drive letter on your computer.

To have VirusScan examine a particular disk or folder on your system, click the **Select drive or folder to scan** button. Next, type in the text box provided the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer. Select the **Include subfolders** checkbox to have VirusScan also look for viruses in any folders inside your scan target. Click **OK** to close the dialog box.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Item to Scan dialog box (Figure 7-7).

Figure 7-7. The Edit Item to Scan dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

2. 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 in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats. 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 7-8).

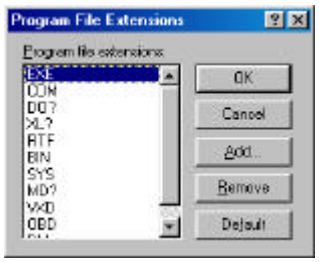

Figure 7-8. The Program File Extensions dialog box

By default, VirusScan looks for viruses in files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .BIN, .SYS, .MD?, .VXD, .OBD, and .DLL. Files with .DO?, .XL?, .RTF, 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 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 **Delete**.
- 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.

- **Turn on heuristic scanning**. Click **Macro Heuristics** to open the Macro Heuristics Scan Settings dialog box (Figure 7-9).

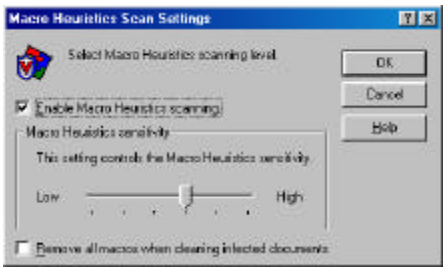

Figure 7-9. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables VirusScan to recognize new macro viruses based on their resemblance to similar viruses it already knows. To do this, VirusScan first identifies all Microsoft Word, Microsoft Excel, and other Microsoft Office files that have embedded macros, then it compares the macro code to its virus signature database. Exact matches it identifies with the virus name; code signatures that resemble existing viruses cause VirusScan to tell you it has found a “probable” macro virus. Unless you know that the file does not contain a virus, you should treat “probable” infections with the same caution you would confirmed infections.

To activate heuristic scanning, follow these steps:

a. Select the **Enable macro heuristics scanning** checkbox.

b. Set the sensitivity level you want VirusScan to use when it looks for macro viruses. Drag the slider to the left to set a low level of sensitivity—this causes VirusScan to look for as close a match as possible between the macros it finds in the file and existing virus code signatures before it labels a file as infected.

   Drag the slider to the right to set a high level of sensitivity—this causes VirusScan to look with suspicion at nearly all macro code and to identify a wider range of files as potentially infected.

> **NOTE:** Higher levels of sensitivity can cause VirusScan to falsely identify a file as infected, but it does so out of caution. Until virus researchers have examined the suspicious file and positively eliminated any possibility of infection, the potential exists for nearly all macro code to harbor new viruses. The sensitivity setting exists for you to choose the level that works best for your environment.

c. Determine how you want to treat infected macro files. Select **Remove all macros when cleaning infected documents** to eliminate all infectable code from the document and leave only data. To try to remove only the virus code from the document's macros, leave this checkbox clear.

> **NOTE:** Use this feature with caution: removing all macros from a document can cause it to lose data or to become corrupted and unusable.

d. Click **OK** to save your settings and return to the VirusScan Properties dialog box.

3. Choose other scanning options. Boot-sector viruses load themselves into your computer's memory and conceal themselves in the boot blocks or master boot record on your hard drive. To detect these viruses, select the **Scan Memory** and **Scan boot sectors** checkboxes.

4. If you have scheduled scan operations that you want to run in your absence, select the **Start automatically** checkbox to tell VirusScan to begin scanning as soon as it launches. If you do not select this checkbox, the Scheduler will start VirusScan, but VirusScan will wait for you to click **Scan Now** to start scanning. Leaving the checkbox clear gives you a chance to cancel the scan operation if it will interfere with your work.

5. Click the Action tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

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. To start from the Scheduler window, select the task you created in the task list, then click  in the Scheduler toolbar.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 162). Click the Action tab to display the correct property page (Figure 7-10).

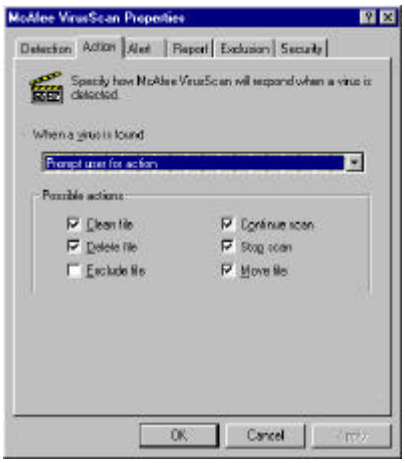

Figure 7-10. VirusScan Properties dialog box - Action page

3. To tell VirusScan what to do when it finds a virus, 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 choice. Your choices are:

   - **Prompt User for Action.** Use this option if you expect to be at your computer when VirusScan examines your disk—VirusScan will display an alert message when it finds a virus and offer you a range of possible responses. Choose which response options you want to see from among these:

     – **Clean file.** This option tells VirusScan to try to remove the virus code from the infected file.

     – **Delete file.** This option tells VirusScan to delete the infected file immediately.

     – **Exclude file.** This option tells VirusScan to skip the file during later scan operations.

     – **Continue scan.** This option tells VirusScan to continue with its scan, but not take any other actions. If you have its reporting options enabled, VirusScan records the incident in its log file.

  - **Stop scan.** This option tells VirusScan to stop the scan operation immediately. To continue, you must restart the operation, either from the Scheduler, or from VirusScan itself.
  - **Move file.** This option tells VirusScan to move the infected file to a quarantine folder.

- **Move infected files automatically**. Use this option 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.** Use this option 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 notify you in its message area and, if you have its reporting features enabled, will note the incident in its log file. See "Choosing report options" on page 170 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.
- **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 170 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.

4. Click the Alert tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing alert options

Once you configure it with the response options you want, you can let VirusScan look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want VirusScan to inform you immediately when it finds a virus so that you can take appropriate action, you can configure it to send an alert message to you in a variety of ways. Use the Alerts property page to choose which alerting methods you want to use.

Follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click  in the Scheduler toolbar.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 162). Click the Alert tab to display the correct property page (Figure 7-11).

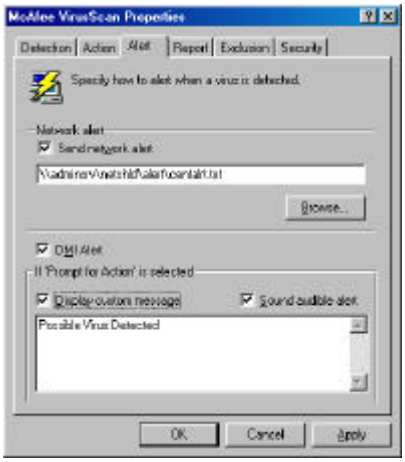

Figure 7-11. VirusScan Properties dialog box - Alert page

3. To tell VirusScan to send an alert message to a server running NetShield, a Network Associates server-based anti-virus solution, select the **Send network alert** checkbox, then enter the path to the NetShield alert folder on your network, or click **Browse** to locate the correct folder.

> **NOTE:** The folder you choose must contain CENTALRT.TXT, the NetShield Centralized Alerting file. NetShield collects alert messages from VirusScan and other Network Associates software, then passes them to network administrators for action. To learn more about Centralized Alerting, see the NetShield *User's Guide*.

4. To have VirusScan send virus alert messages via the DMI Component Interface to desktop and network management applications running on your network, select the **DMI Alert** checkbox.

   NOTE: The Desktop Management Interface is a standard for communicating management requests and alert information between hardware and software components stored on or connected to desktop computers, and the applications used for managing them. To learn more about using this alert method, see your network administrator.

5. If you chose **Prompt user for action** as your response in the Action page (see "Choosing action options" on page 166 for details), you can also tell VirusScan to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox, then enter the message you want to see in the text box provided—you can enter a message up to 225 characters in length. Next, select the **Sound audible alert** checkbox.

6. Click the Report tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing report options

VirusScan 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 a text editor.

The VSCLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections VirusScan found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Reports property page to determine which information VirusScan will include in its log file.

To set VirusScan to record its actions in a log file, follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click  in the Scheduler toolbar.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 162). Click the Report tab to display the correct property page (Figure 7-12).

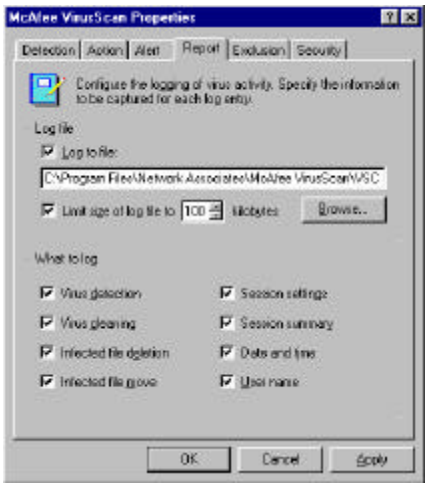

Figure 7-12. VirusScan Properties - Reports page

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 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. Select the checkboxes that correspond to the information you want VirusScan to record in its log file. You can choose to record this information:

   - **Virus detection.** Select this checkbox to have VirusScan note the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VirusScan note the number of infected files from which it removed the infecting virus.
   - **Infected file deletion. Select this checkbox to have VirusScan note the number of infected files it deleted from your system.**
   - **Infected file move.** Select this checkbox to have VirusScan note the number of infected files it moved to your quarantine directory.
   - **Session settings.** Select this checkbox to have VirusScan list the options you choose in the McAfee VirusScan Properties dialog box for each scanning session.
   - **Session summary.** Select this checkbox to have VirusScan summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information.
   - **Date and time.** Select this checkbox to have VirusScan append the date and time to each log entry it records.
   - **User name.** Select this checkbox to have VirusScan append the name of the user logged in to your computer at the time it records each log entry.

   To see the contents of the log file, start VirusScan, then choose **View Activity Log** from the **File** menu. For more information, see "Using VirusScan menus" on page 127.

6. Click the Exclusion tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

   NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling VirusScan to look only at susceptible file types (see "Choosing detection options" on page 162 for details), or you can tell VirusScan to ignore entire files or folders that you know will not get infected.

Once you scan your system thoroughly, you can exclude the files and folders that do not change or that are not normally vulnerable to virus infection. You can also rely on VShield to provide you with protection in between scheduled scan operations. Regular scan operations that examine all areas of your computer, however, provide you with the best virus defense.

To exclude files or folders from scan operations, follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click  in the Scheduler toolbar.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 162). Click the Exclusion tab to display the correct property page. (Figure 7-13).

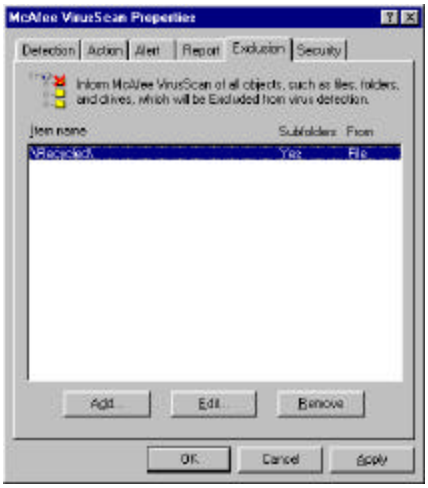

Figure 7-13. VirusScan Properties dialog box - Exclusion page

The Exclusion page will initially list only your Recycle Bin. VirusScan excludes the Recycle Bin from scan operations because Windows will not run files stored there.

3. Specify the items you want to exclude. You can

   - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 7-14).

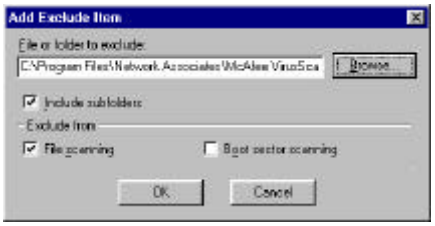

Figure 7-14. Add Exclude Item dialog box

   a. Type the volume, the path to the file, or the path to the folder that you want to exclude from scanning, or click **Browse** to locate a file or folder on your computer.

   NOTE: If you have chosen to move infected files to a quarantine folder automatically, the program excludes that folder from scan operations.

   b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.

   c. Select the **File scanning** checkbox to tell VirusScan not to look for file-infector viruses in the files or folders you exclude.

   d. Select the **Boot sector scanning** checkbox to tell VirusScan not to look for boot-sector viruses in the files or folders you exclude. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

   WARNING: Network Associates recommends that you do *not* exclude your system files from virus scanning.

   e. Click **OK** to save your changes and close the dialog box.

   f. Repeat steps a. through d. until you have listed all of the files and folders you do not want scanned.

   - **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.

- **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. VirusScan will then scan this file or folder during its next scanning operation.

4. Click the Security tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

> **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing security options

VirusScan lets you set a password to protect the settings you choose in each property page from unauthorized changes. This feature is particularly useful for system administrators who need to keep users from tampering with their security measures by changing VirusScan settings. Use the Security property page to lock your settings.

Follow these steps:

1. To start from the Scheduler window, select the task you created in the task list, then click  in the Scheduler toolbar.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 162). Click the Security tab to display the correct property page. (Figure 7-13).

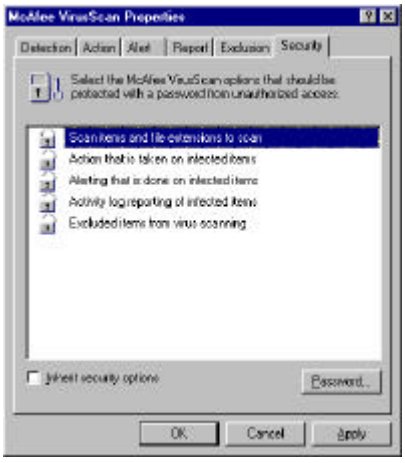

Figure 7-15. VirusScan Properties dialog box - Security page

3. Select the settings you want to protect in the list shown.

   You may protect any or all VirusScan property pages. Protected property pages display a locked padlock icon in the security list shown in Figure 7-15. To remove protection from a property page, click the locked padlock icon to unlock it .

4. Click **Password** to open the Specify Password dialog box (Figure 7-16).

Figure 7-16. Specify Password dialog box

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

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

5. If you want to create other scan tasks by copying this task (see page 155 for details), you can ensure that your security settings will appear by default in the copied task by selecting the **Inherit security options** checkbox. If you configure the Default Scan task with this option, all new tasks you create by choosing **New Task** from the **Scan** menu or by clicking will have the security settings you choose for the Default Scan task.

6. Click a different tab to change any of your VirusScan settings. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Scheduler window, click **OK**. To return to the Scheduler window without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring options for other programs

You can use the Scheduler to run other programs at specific times, but unless the program you want to run is a Network Associates anti-virus product, you cannot use the Scheduler to configure the program to run with particular options. To do that, you must open and pre-configure the program yourself—the Scheduler will simply run the program as you have it configured at the time you specify. You can, however, use the Scheduler to open the VShield Properties dialog box so that you can configure VShield to run with particular scan options. To learn how to do this, see Chapter 5, "Using VShield."

Using SecureCast to Update Your Software A

Introducing SecureCast

The Network Associates SecureCast service conveniently delivers the latest product upgrades and data file updates to your desktop. With it, you can choose to receive updates for your licensed Network Associates software via the Internet, regularly and automatically. To use this option, you must install the SecureCast client software and subscribe to either the Home SecureCast channel (for retail customers) or the Enterprise SecureCast channel (for corporate customers).

If you are a retail customer and would rather decide when to update your system, an option allows you to download new files only when your software reminds you that it's time to update. If you are a corporate customer (but not an administrator), contact your administrator to learn where to update your files, or use the AutoUpdate feature if your product includes it.

Choose one of the update options listed in this appendix to keep your system efficiently protected from the network to the desktop. With SecureCast, you'll get the latest data files and program files as soon as they're available. New viruses and other harmful agents appear at a rate of more than 200 per month—don't risk letting your data disintegrate or your network become inaccessible simply because you forgot to update or upgrade your software.

NOTE: The term "update" refers to data (.DAT) files; the term "upgrade" refers to product version revisions, executables, and data files. Network Associates offers free .DAT file updates for the life of your product. This does not, however, guarantee that .DAT files will be compatible with previous product versions. By upgrading your software to the latest product version and updating to the latest .DAT files regularly via SecureCast, you ensure complete protection for the term of your software subscription or maintenance plan.

Why would I need to update my data files?

To offer you the best protection possible, Network Associates continually updates data files that detect new viruses and other harmful agents. Although your software has technology that allows it to detect previously unknown strains of viruses or malicious code, new virus types and other agents appear frequently. Often, your existing software cannot detect these intruders because the data files that came with it became outdated. Your software periodically notifies you to update these files. For maximum protection, Network Associates strongly recommends that you update your files on a regular basis.

Which data files does SecureCast deliver?

With SecureCast, you'll receive automatic downloads of these common data files:

- NAMES.DAT—includes virus names and other details that the user sees when viewing the Virus List.
- SCAN.DAT—includes detection string data for all viruses detected.
- CLEAN.DAT—includes removal string data for all viruses cleaned.

In addition to the common .DAT files above, you may also receive some of these additional files, depending on which anti-virus or security products you're running:

- WEBSCANX.DAT or INTERNET.DAT—includes detection string data for hostile Java applets and ActiveX controls. WebShieldX and WebScanX use these files.
- MCALYZE.DAT—includes detection string data for complex polymorphic virus detection. Network Associates 32-bit products with engine versions 3.0.0 through 3.1.4 use this file.
- POLYSCAN.DAT—includes detection string data for complex polymorphic virus detection. Network Associates 32-bit products with engine versions 3.1.5 and later use this file.

System requirements

- Windows 95 or later, or Windows NT
- At least 100MB free hard disk space: Home SecureCast (client and channel) 7MB, plus 3–6MB per download. Enterprise SecureCast (client and channel) 15MB, plus 6–65MB per download.
- An active Internet connection—direct or dialup—for a minimum of one hour per week.

SecureCast features

- SecureCast uses client software developed with BackWeb Technologies.
- SecureCast eliminates the need for downloading update files from Network Associates electronic services.
- SecureCast works invisibly in the background, allowing other applications to take priority over it and using your Internet connection when it's idle. You can also configure your desktop client so that SecureCast downloads have a higher priority.
- SecureCast works with most corporate firewalls.
- SecureCast supports 32-bit TCP/IP connections for Enterprise SecureCast and Home SecureCast channel subscribers, and provides non-Internet connections for retail customers using asynchronous modem dialup.
- SecureCast delivers .ZIP, .EXE, and .DAT files to your desktop as BackWeb InfoPaks.

Free services

- Automatic delivery of .DAT files. New .DAT files are usually available mid-month.
- Alerts on newly identified dangerous viruses.
- Announcements of new versions of software and associated products.

Home SecureCast Channel

Retail customers may install SecureCast client software from a Network Associates CD-ROM.

Understanding SecureCast

If you are a retail customer, you can use SecureCast's timely, free delivery service in one of two ways:

- To receive automatic downloads of the latest updates for your licensed Network Associates software via the Internet, install the SecureCast client, then subscribe to the Home SecureCast channel; or
- If you would rather decide when to update your software, use the included update utility when your software reminds you that it's time.

Downloading automatically

Setting up Home SecureCast

Follow these steps to subscribe to the Home SecureCast channel:

1. Install the BackWeb client software from a Network Associates CD-ROM.

   You will receive a Welcome InfoPak that tells you that your connection to the Home SecureCast channel is working. An InfoPak can contain sounds, animations, Web pages, and more. When you receive a new InfoPak from Home SecureCast, it will automatically appear as an animated object on your desktop until you open it. To open an InfoPak, simply double-click it.

2. Complete the channel registration process via the User Registration Information dialog box (which will appear in either the first or second InfoPak you receive), then click **Next**.

   The Online Activity Status dialog box tracks the status of your data transmission.

3. When your user registration is complete, make a note of your registration number, then click **Finish**.

Using Home SecureCast

You are now ready to receive periodic Virus Alerts, plus product updates and upgrades. Within a few days, you should receive additional InfoPaks. Double-click these to extract and set up the updates or upgrades they contain.

Unsubscribing from Home SecureCast

Follow these steps to cancel this service at any time:

1. Double-click the SecureCast client icon in the Windows taskbar status area.

2. Right-click the **Home** channel button.

   A shortcut menu appears.

3. Click **Unsubscribe**, then click **OK** to confirm.

Initiating a Download

Updating registered software

Network Associates software includes a feature that periodically reminds you to update your software. If many months have passed since you first installed your software, Network Associates strongly recommends that you use the update options described in the following sections to ensure that you are using the latest data files and product versions available.

Updating after installation

After you install your anti-virus or security software, the Welcome dialog box (Figure A-1) prompts you to update your software. This dialog box also appears when you start a computer system pre-loaded with Network Associates software for the fifth time. McAfee VirusScan, for example, displays this notice:

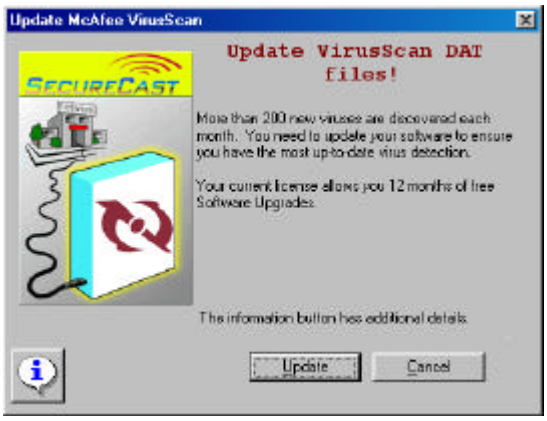

Figure A-1. Welcome dialog box

4. Click **Update** to receive the latest version of the software for free.

The Internet Access dialog box (Figure A-2) appears.

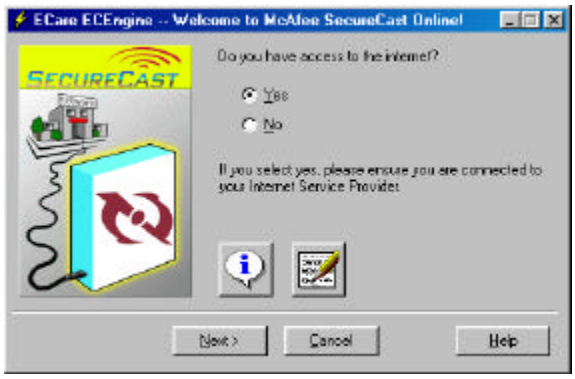

Figure A-2. Internet Access dialog box

5. If you have Internet access, select **Yes**, then click **Next**. If you do not have Internet access, select **No**, then click **Next**.

   - If you selected **Yes**, the User Registration dialog box appears (Figure A-4).

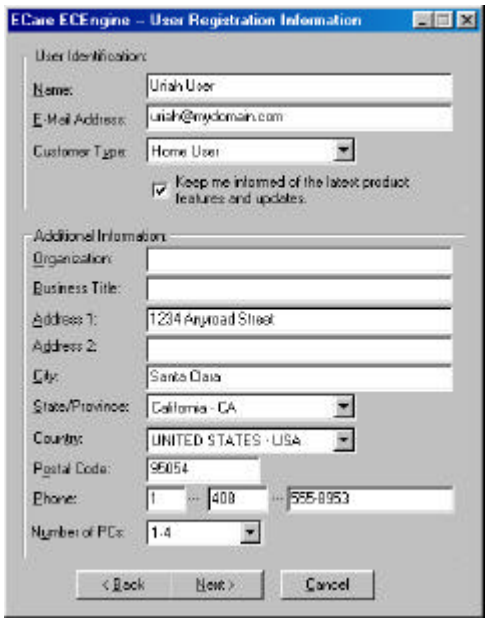

Figure A-3. User Registration dialog box

Fill in the information requested. To move between each text box, press TAB on your keyboard. When you have finished, click **Next>**.

- If you selected **No**, the download server dialog box will appear (Figure A-4). Here, you need to enter or verify your country code and area code, then choose the dial-up server closest to your location.

Figure A-4. Server dialog box

> **NOTE:** Downloading .DAT files from Network Associates dial-up servers might cause you to incur long-distance charges.

When you have finished, click **Next>** to continue.

Your system connects to a Network Associates server.

- If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (Figure A-5) tells you that your files are up-to-date.

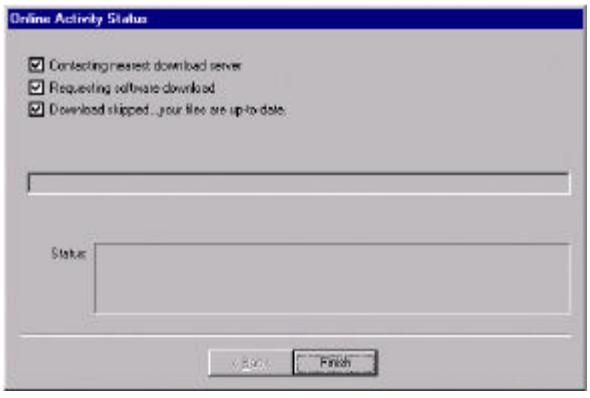

Figure A-5. Online Activity Status dialog box (No Download)

Click **Finish** to disconnect from the server.

- If the server has new .DAT files, the Online Activity Status dialog box (Figure A-6) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.

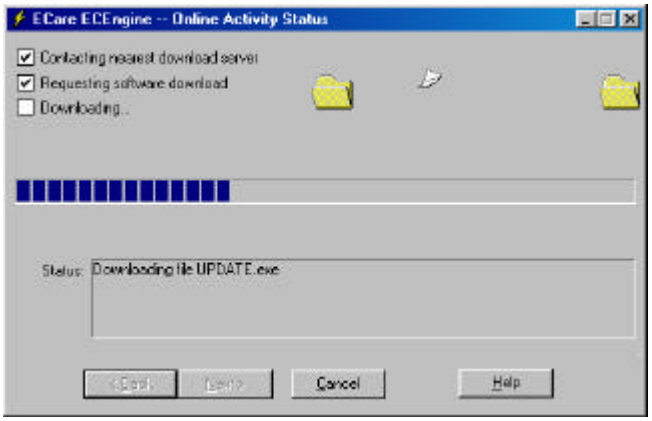

Figure A-6. Online Activity Status dialog box

a. When the download is complete, click **Next**. The Online Activity Complete dialog box (Figure A-7) appears.

Figure A-7. Online Activity Complete dialog box

b. Click **Finish** to install your new .DAT file updates.

- If the server has a product version more recent than yours, the Newer Component Found dialog box (Figure A-8) appears. To download only the latest .DAT files, select **DAT files only**, then click **Next**. To download a new product version, click **Next**.

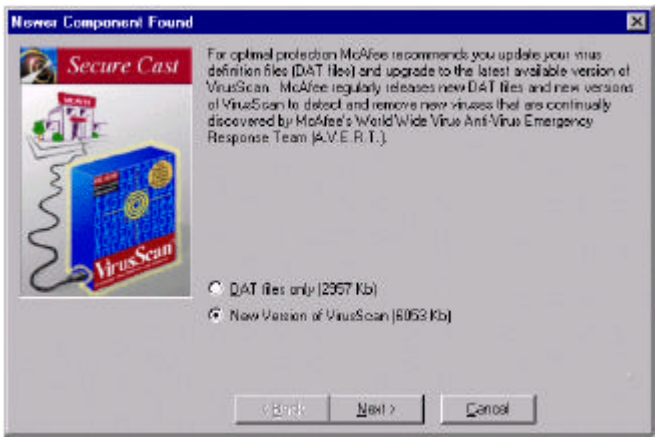

Figure A-8. Newer Component Found dialog box

The Online Activity Status dialog box (see Figure A-6 on page 186) tracks the status of your download. When your download is complete, click **Next** to continue.

The Online Activity Complete dialog box (Figure A-9) confirms that your download is complete.

Figure A-9. Online Activity Complete dialog box

6. Note the name and location of the downloaded file, then click **Finish** to install your software.

Updating at periodic intervals

At 30-day intervals, the Update dialog box (Figure A-10) prompts you to update your software.

Figure A-10. Update dialog box

If you are a registered user, complete the following steps to receive the latest version of the software for free. Repeat these steps every month when your software suggests that you do in order to keep your files updated.

NOTE: As a registered user, you can continue to receive .DAT file updates for the life of your product. Network Associates cannot, however, guarantee compatibility between future .DAT file updates and older product versions. By purchasing the latest software upgrades via SecureCast, you ensure complete virus protection for the term of your software subscription or maintenance plan.

---

1. Click **Update** to receive the latest version of the software for free.

   The Internet Access dialog box (see Figure A-2 on page 184) appears.

2. If you have Internet access, select **Yes**, then click **Next**. If you do not have Internet access, select **No**, then click **Next**.

   The Server dialog box (see Figure A-4 on page 185) appears. If you selected **Yes**, then the dialup-number box will be unavailable; if you selected **No**, then the dialup-number box will be available.

3. If you have Internet access, verify your Country Code and Area Code, then click **Next**. If you don't have Internet access, verify your Country Code and Area Code, select a modem dialup number, then click **Next**.

Your system connects to a Network Associates server.

- If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (see Figure A-5 on page 185) tells you that your files are up-to-date. Click **Finish** to disconnect from the server.
- If the server has new .DAT files, the Online Activity Status dialog box (see Figure A-6 on page 186) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.

  When the download is complete, click **Next**. The Online Activity Complete dialog box (see Figure A-7 on page 186) appears.

4. Click **Finish** to install your new .DAT file updates.

If the server has a *product* version more recent than yours, the Newer Component Found dialog box (see Figure A-8 on page 187) appears.

1. To download only the latest .DAT files instead of the entire product, select **DAT files only**, then click **Next**. To download a new product version, click **Next**.
2. The Online Activity Status dialog box (see Figure A-6 on page 186) tracks the status of your download. When your download is complete, click **Next** to continue.

   The Online Activity Complete dialog box (Figure A-11) confirms that your download is complete.

Figure A-11. Online Activity Complete dialog box

3. Note the name and location of the downloaded file, then click **Finish** to install your software.

Registering evaluation software

If you are using a 30-day evaluation version of Network Associates software, the Purchase dialog box (Figure A-12) appears. This dialog box also appears when you choose **Purchase** from the **File** menu in your Network Associates software product.

Figure A-12. Purchase dialog box

If you continue to use evaluation copies of Network Associates software after their 30-day licenses expire, you will see increasingly frequent reminders to register your software. Network Associates strongly recommends that you follow these steps to ensure that you are using the newest data files and product versions available:

1. In the Purchase dialog box (Figure A-12), click **Purchase** to begin registering your evaluation copy of anti-virus software electronically.

   The Internet Access dialog box (see Figure A-2 on page 184) appears.

2. If you have Internet access, select **Yes**, then click **Next**. If you do not have Internet access, select **No**, then click **Next**.

   The Server dialog box (see Figure A-4 on page 185) appears. If you selected **Yes**, then the dialup-number box will be unavailable; if you selected **No**, then the dialup-number box will be available.

3. If you have Internet access, verify your Country Code and Area Code, then click **Next**. If you don't have Internet access, verify your Country Code and Area Code, select a modem dialup number, then click **Next**.

   Your system connects to a Network Associates server.

- If the server has no new .DAT file updates or software upgrades, the Online Activity Status dialog box (see Figure A-5 on page 185) tells you that your files are up-to-date. Click **Finish** to disconnect from the server.
- If the server has new .DAT files, the Online Activity Status dialog box (see Figure A-6 on page 186) tells you that the .EXE file containing the .DAT files is automatically downloading to your system.

  When the download is complete, click **Next**. The Online Activity Complete dialog box (see Figure A-7 on page 186) appears.

4. Click **Finish** to install your new .DAT file updates.

If the server has a product version more recent than yours, the Newer Component Found dialog box (see Figure A-8 on page 187) appears. To download only the latest .DAT files instead of the entire product, select **DAT files only**, then click **Next**. To download a new product version, follow these steps:

1. Click **Next** to obtain the newer version of the software.

   If you are no longer entitled to free software upgrades, a second Newer Component Found dialog box (Figure A-13) appears.

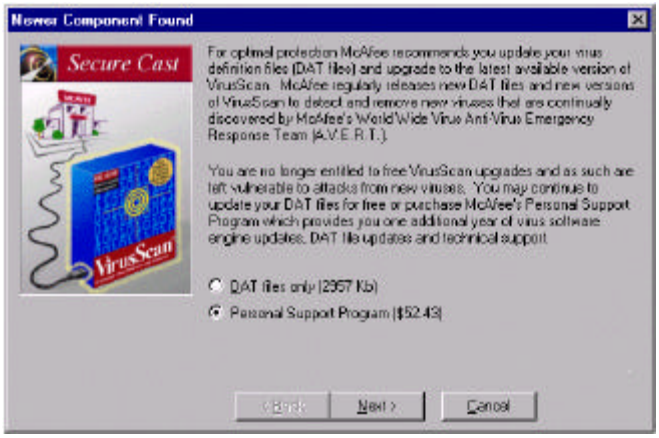

Figure A-13. Newer Component Found dialog box #2

> **NOTE:** File sizes and support pricing are dynamically generated. What you see when you download your purchase, therefore, might vary from what you see in Figure A-13 .

2. Click **Next>** to continue with the download.

The Enter Credit Card Information dialog box (Figure A-14) appears.

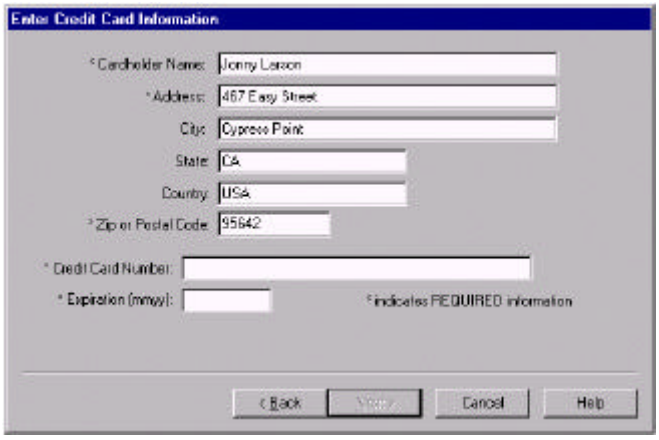

Figure A-14. Enter Credit Card Information dialog box

3. Enter your credit card billing address, account number, and expiration date. Click **Next>** to continue.

> **NOTE:** Your credit card details are safely transmitted in a secure transaction.

The Online Purchase Authorization dialog box (Figure A-15) appears.

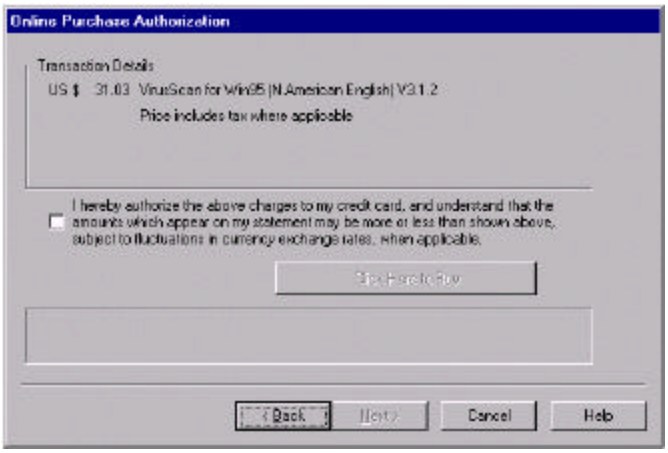

Figure A-15. Online Purchase Authorization dialog box

4. Select the check box to authorize the transaction charges to your credit card, and click Click Here to Buy to begin the download process.

   NOTE: Network Associates will not charge your credit card unless you complete the download successfully.

   The Online Activity Status dialog box (see Figure A-6 on page 186) tracks the status of your download.

5. When your download is complete, note the resulting transaction number for your purchase, then click **Next>** to continue.

   The Online Activity Complete dialog box (see Figure A-9 on page 187) confirms that your transaction is complete.

6. Note the name and location of the downloaded file, then click **Finish** to install your software.

Enterprise SecureCast Channel

If you manage a corporate network, you may download BackWeb's client software from the Network Associates corporate site (http://www.nai.com) and install it on a network server. Enterprise SecureCast is for use by administrators only, not by corporate end users.

NOTE: When the first InfoPak arrives, double-click it to open it, then complete the channel registration process via the Customer Registration Information dialog boxes. When you receive subsequent InfoPak files from Enterprise SecureCast, Network Associates strongly recommends that you distribute them to individual desktops as needed, in order to conserve network bandwidth.

Benefits

- Ease of use

  You no longer have to search for and download updates from Network Associates electronic distribution services. The updates you need will be delivered to you in a zipped format, ready for onsite testing and installation.

- Timely protection

  Network Associates provides you with timely protection by regularly delivering .DAT file updates and product upgrades directly to your desktop. As soon as the updates are released to the SecureCast server, they start to transfer to your site.

- Virus Alerts

  You will receive Virus Alerts that notify you of threatening viruses and suggest the best way to prevent infection. In addition, alerts that distinguish between hoaxes and serious threats will save you valuable time and prevent unnecessary concern.

- Upgrades for multiple platforms

  A subscription to Enterprise SecureCast allows you to receive upgrades and updates to your products for multiple platforms. Data file updates and product upgrades for Network Associates products that run under Windows 95, Windows 98, Windows NT, Windows 3.*x*, DOS, OS/2, and the Mac OS can be delivered to your desktop.

- Localized language versions

  With your subscription, you receive .DAT file updates not only across multiple platforms, but also in the languages of your choice.

- HTTP support in client software

  Enterprise SecureCast supports HTTP (Hypertext Transfer Protocol) for file transmission through your firewall to the SecureCast servers.

> **NOTE:** Firewall considerations: If you have a firewall in place, use HTTP. If you do not, use UDP. If you are using Check Point's Firewall-1™ software, you'll notice that BackWeb is a predefined transmission type.

Setting up Enterprise SecureCast

To obtain the BackWeb client, corporate customers must first have a grant number (product license serial number) to enroll for Enterprise SecureCast.

- If you do not have a grant number, please contact your purchasing agent, your Value Added Reseller, or Network Associates Customer Care at (408) 988-3832 for assistance.
- If you are already a registered Network Associates customer and do not know your grant number, submit the grant-number request form online:

  http://www.nai.com/products/securecast/esc/grantreq.asp

OR

Send an e-mail message to the appropriate address:

ESCRegistration@nai.com (United States)

ESC-Registration-Europe@nai.com (Europe)

ESC-Registration-Asia@nai.com (Asia)

Follow these steps to set up Enterprise SecureCast:

1. Download the Enterprise SecureCast BackWeb client (about 2MB). This client software is specially configured to function in the corporate environment, supporting HTTP file transmission.
2. Install the Enterprise SecureCast client software.

   You will receive a Welcome InfoPak that tells you that your connection to the Enterprise SecureCast channel is working.

3. Begin the channel registration process by entering data about your company in the Customer Registration Information dialog boxes (which will appear in either the first or second InfoPak you receive).

   After you click **Next** on the last registration dialog box, the Online Activity Status dialog box tracks the status of your data transmission.

4. When your user registration is complete, make a note of your registration number, then click **Finish**.

   Your web browser launches showing a product signup form.

5. Select the software, the platforms, and the languages for which you want to receive upgrades and updates.

6. Submit your product signup form.

Using Enterprise SecureCast

You are now ready to receive periodic Virus Alerts, plus product updates and upgrades. Within a few days, you should receive additional InfoPaks. An InfoPak can contain sounds, animations, Web pages, and more. When you receive a new InfoPak from Enterprise SecureCast, it will automatically appear as an animated object on your desktop until you open it. To open an InfoPak, simply double-click it.

Once the updates are on your system, you must distribute them to the workstations on your network. The InfoPaks you receive work well as distribution packages for McAfee Enterprise (Me!) With Me!, you can manage software updates, inventory, distribution, usage metering, and centralized alerting. Contact your Network Associates sales representative for more information about Me!

Troubleshooting Enterprise SecureCast

Registration problems

If you try to register during a busy time of day on the Web, you may encounter a delay when the server tries to process your registration request. If you receive the error message “1105 Error” or “Database Error: Unable to connect to the data source,” this means that there is a database problem on the SecureCast server. Try submitting the form again, or try to register later. If you continue to have problems subscribing to the Enterprise SecureCast channel, please contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central Time) at (972) 278-6100 for assistance.

Firewall problems

Most firewalls that allow web-browsing traffic will also allow you to receive SecureCast InfoPaks. Some firewalls, however, can cause some problems for connections to the SecureCast server. When you complete the registration form and download the software, you will initially download a SecureCast client built with BackWeb version 1.2. Because version 1.2 does not support certain communication protocols, you might see an error similar to "no network connection" when you use it. To correct this problem, download the latest SecureCast client, which was developed with BackWeb version 3.0.

> **NOTE:** You must install the client software that uses BackWeb version 3.0 over the client that uses the 1.2 version of BackWeb. *Do not* uninstall the older version first. This ensures that the new SecureCast client will retain your channel preferences.

Follow these steps to install and configure the newer SecureCast client software:

1. Install BackWeb version 3.0 over BackWeb version 1.2.
2. Start the SecureCast client.
3. To configure the SecureCast client's Communication Method with your own network information, choose **Global Options** from the **Preferences** menu.
4. Change the setting for how BackWeb navigates through your proxy server from **Polite Agent** to **HTTP**. Next, click **HTTP Proxy Setup**, then enter the requested information about your network.

   > **NOTE:** Your proxy server information is specific to your network. If you have further questions, consult your system administrator.

Unsubscribing from Enterprise SecureCast

Follow these steps to cancel this service at any time:

1. Double-click the SecureCast client icon in the Windows taskbar status area.
2. Right-click the **Enterprise** channel button.

   A shortcut menu appears.
3. Click **Unsubscribe**, then click **OK** to confirm.

Support Resources

SecureCast

If you have additional questions about SecureCast, consult the SecureCast FAQ:

http://www.nai.com/products/securecast/esc/enterprise_faq.asp

BackWeb

- For a general description of BackWeb and InfoPaks, read the BackWeb Overview:

  http://www.nai.com/products/securecast/securedetail.asp

- For a comprehensive guide to BackWeb (including additional troubleshooting advice), bookmark the BackWeb User's Manual:

  http://www.backweb.com/doc/version20/Client95/

OR

download the .PDF file:

http://www.backweb.com/doc/version20/bwuser.pdf

- For solutions to serious problems with the operation of BackWeb, please contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central Time) at (972) 278-6100.

Network Associates Support Services B

Choosing Network Associates anti-virus and security software helps to ensure that the critical information technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from three levels of extended support under the Network Associates PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Personal Support program.

PrimeSupport Options for Corporate Customers

The Network Associates PrimeSupport program offers a choice of Basic, Extended, or Anytime options. Each option has a range of features that provide you with cost-effective and timely support geared to meet your needs.

PrimeSupport Basic

PrimeSupport Basic gives you telephone access to essential product assistance from experienced Network Associates technical support staff members. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport Basic as part of the package for two years from your date of purchase. If you purchased your Network Associates product with a perpetual license, you can renew your PrimeSupport Basic plan for an annual fee.

PrimeSupport Basic includes these features:

- Telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Extended

PrimeSupport Extended gives you personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products. By calling in advance, your PrimeSupport Extended representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Extended gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Extended on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Extended includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within one hour to pages, within four hours to voice mail, and within 12 hours to e-mail
- Telephone access to technical support from Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to five people in your organization as customer contacts

PrimeSupport Anytime

PrimeSupport Anytime offers round-the-clock, personalized, proactive support for Network Associates products deployed in the most business-critical information systems. PrimeSupport Anytime delivers the features of PrimeSupport Extended 24 hours a day, seven days a week, with shorter response time commitments. You may purchase PrimeSupport Anytime on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Anytime includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within half an hour to pages, within one hour to voice mail, and within four hours to e-mail
- Telephone access to technical support 24 hours a day, seven days a week
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to 10 people in your organization as customer contacts

Table B-1. PrimeSupport At a Glance

Feature	Basic	Extended	Anytime
Technical support via telephone	Monday–Friday 8:00 a.m.–8:00 p.m.	Monday–Friday 7:00 a.m.–7:00 p.m.	24 hours a day, 7 days a week
Technical support via website	Yes	Yes	Yes
Software updates	Yes	Yes	Yes
Assigned support engineer	—	Yes	Yes
Proactive support contact	—	Yes	Yes
Designated customer contacts	—	5	10
Committed response time	—	Pager: 1 hour Voicemail: 4 hours E-mail: 12 hours	Pager: 30 mins. Voicemail: 1 hour E-mail: 4 hours

Ordering PrimeSupport

To order PrimeSupport Basic, PrimeSupport Extended or PrimeSupport Anytime for your Network Associates products:

- Contact your sales representative; or
- Call Network Associates Support Services at 1-800-988-5737 or 1-650-473-2000 from 6:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday.

NOTE: The PrimeSupport program described in this guide is available in North America only. To learn about PrimeSupport options available outside North America, contact your regional sales office. Contact information appears near the front of this guide.

Support Services for Retail Customers

If you purchased your Network Associates product through a retail vendor or from the Network Associates website, you also receive some support services as part of your purchase. The specific level of included support depends on the product that you purchased. Examples of the services you receive include:

- Free data (.DAT) file updates for the life of your product via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see Appendix A, "Using SecureCast to Update Your Software" for details). You can also update your data files by using your web browser to visit http://www.nai.com/download/updates/updates.asp.
- Free program (executable file) upgrades for one year via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see Appendix A, "Using SecureCast to Update Your Software" for details). If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your web browser to visit:

  http://www.nai.com/download/upgrades/upgrades.asp.

- Free access 24 hours a day, seven days a week to online or electronic support through the Network Associates voice and fax system, the Network Associates website, and though such other electronic services as America Online and CompuServe.

To contact Network Associates electronic services, choose one of these options:

- Automated voice and fax system: (408) 988-3034
- Network Associates website: http://support.nai.com
- CompuServe: GO NAI
- America Online: keyword MCAFEE

- Ninety days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

After your complimentary support period expires, you can take advantage of a variety of personal support options geared toward your needs. Contact Network Associates Customer Care at (972) 278-6100 to learn more about the options available, or visit the Network Associates website at:

http://www.nai.com/services/support/support.asp.

Network Associates Consulting and Training

Network Associates provides expert consulting and comprehensive education that can help you maximize the security and performance of your network investments through the Network Associates Total Service Solutions program.

Professional Consulting Services

Network Associates Professional Consulting Services is ready to assist during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert supplemental resource and independent perspective to resolve your problems. You'll get help integrating Network Associates products into your environment, along with troubleshooting assistance or help in establishing baselines for network performance. Network Associates consultants also develop and deliver custom solutions to help accomplish your project goals—from lengthy, large-scale implementations to brief problem-solving assignments.

Total Education Services

Network Associates Total Education Services builds and enhances the skills of all network professionals through practical, hands-on instruction that you can take right back to your job. The Total Education Services technology curriculum focuses on network fault and performance management and covers problem solving at all levels. Network Associates also offer modular product training so that you understand the features and functionality of your new software.

You can enroll in Total Education Services courses year-round at Network Associates educational centers, or you can learn from customized courses conducted at your location. All courses follow educational steps along a learning path that takes you to the highest levels of expertise. Network Associates is a founding member of the Certified Network Expert (CNX) consortium.

To learn more about these programs, contact your sales representative or call Total Service Solutions at 1-800-395-3151.

Understanding the .VSC File Format C

Saving VirusScan task settings

When you save VirusScan configuration options in a .VSC file, you are saving a text file formatted in a manner similar to the Windows .INI file that outlines VirusScan's settings. The file consists of variables that have a name followed by an equal (=) sign and a value. The values define which settings you selected for VirusScan configuration. The variables are arranged in eight groups: ScanOptions, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, ScanItems, SecurityOptions, and ExcludedItems. The tables on the following pages list each option, along with its default and possible values.

You can distribute .VSC files to other VirusScan users at other computers, overwrite the existing .VSC files on those computers, and thereby copy VShield's System Scan settings for another user to run. To edit the .VSC file, open it with a text editor, such as Notepad.

NOTE: Boolean variables can have only 0 and 1 as possible values. The 0 value tells VShield to disable the setting, while 1 enables the setting.

ScanOptions

Variable	Description
bAutoStart	Type: Boolean (0/1) Instructs VirusScan to automatically start scan when launched Default Value: 0
bAutoExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning if no viruses were found Default Value: 0
bAlwaysExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning even if viruses were found Default Value: 0

Variable	Description
bSkipMemoryScan	Type: Boolean (0/1) Instructs VirusScan to skip memory scan Default Value: 0
bSkipBootScan	Type: Boolean (0/1) Instructs VirusScan to skip boot sector scanning Default Value: 0
bSkipSplash	Type: Boolean (0/1) Instructs VirusScan to skip display of the VirusScan splash screen on startup Default Value: 0

DetectionOptions

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

AlertOptions

Variable	Description
bNetworkAlert	Type: Boolean (0/1) Instructs VirusScan to send an alert (.ALR) file to a network path being monitored by NetShield for Centralized Alerting when a virus is found Default Value: 0
bSoundAlert	Type: Boolean (0/1) Instructs VirusScan to sound an audible alert when a virus is detected Default Value: 1
szNetworkAlertPath	Type: String Specifies the network alert path being monitored by NetShield for Centralized Alerting. The folder this path points to should contain the Centralized Alerting file, CENTALRT.TXT Default Value: None

ActionOptions

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

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

ReportOptions

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

Variable	Description
bLogUserName	Type: Boolean (0/1) Instructs VirusScan to log user name Default Value: 1
szLogFileName	Type: String Specifies path to log file Default Value: C:\Program Files\McAfee\Viruscan\VSCLOG.TXT

ScanItems

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

SecurityOptions

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

ExcludedItems

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

Understanding the .VSH File Format D

Saving VShield task settings

When you choose configuration options for VShield's System Scan module, the program saves its settings in a .VSH file in the VirusScan program directory. The .VSH file is a configuration text file, formatted similarly to the Windows .INI file, which outlines VShield's settings. Each variable in the file has a name followed by an equal (=) sign and a value. The values define which settings you selected for VShield configuration. The variables are arranged in seven groups: General, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, SecurityOptions, and ExclusionOptions. The tables on the following pages list each option, along with its default and possible values.

You can distribute .VSH files to other VShield users at other computers, overwrite the existing .VSH files on those computers, and thereby copy VShield's System Scan settings for another user to run. To edit the VSH file, open it with a text editor, such as Notepad.

NOTE: Boolean variables can have only 0 and 1 as possible values. The 0 value tells VShield to disable the setting, while 1 enables the setting.

General

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

DetectionOptions

Variable	Description
szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO? XL?
szDefaultProgramExtensions -	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO? XL?
bScanOnExecute	Type: Boolean (1/0) Instructs VShield to scan when files are run Default value: 1
bScanOnOpen	Type: Boolean (1/0) Instructs VShield to scan when files are opened Default value: 1
bScanOnCreate	Type: Boolean (1/0) Instructs VShield to when files are created Default value: 1
bScanOnRename	Type: Boolean (1/0) Instructs VShield to when files are renamed Default value: 1
bScanOnBootAccess	Type: Boolean (1/0) Instructs VShield to scan the boot record of a disk drive the first time it is accessed Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs program to scan inside all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs program to scan inside compressed files (PkLite, LZEXE) Default value: 1

AlertOptions

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

ActionOptions

Variable	Description
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: `Possible Virus Detected`
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: `\Infected`
uVshieldAction	Type: Integer (1-5) Instructs VShield to take the action specified when a virus is detected Possible values: 1 - Prompt for action 2 - Move infected files to a folder 3 - Clean infected files automatically (Deny access if files can't be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files Default value: 1
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1

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

ReportOptions

Variable	Description
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\McAfee\Viruscan\Vshlog.txt
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1

Variable	Description
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Defines if scanning results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1
bLogSettings	Type: Boolean (1/0) Defines if session settings should be logged on shutdown Default value: 1
bLogSummary	Type: Boolean (1/0) Defines if session summary should be logged on shutdown Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1

SecurityOptions

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

ExclusionOptions

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

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

Using VirusScan Command-Line Options E

Running VirusScan Command line

You can run VirusScan Command Line either from a Windows MS-DOS Prompt window, or by restarting your computer in DOS mode. Network Associates recommends restarting in DOS mode for best results. To learn how to restart your computer in DOS mode, see your Microsoft Windows documentation.

To run VirusScan Command line, follow these steps:

1. Open an MS-DOS Prompt window from within Windows, or restart your computer in DOS mode.
2. Change to the VirusScan program directory. If you installed VirusScan with its default options, type this line at your command prompt to locate the correct directory:

   ```
   C:\progra~1\networ~1\mcafee~1
   ```

3. Type `scan`, followed by the scan options you want to use, at the command prompt.

   VirusScan Command Line will start immediately and begin scanning your system with the options you choose. When it has finished, it will display the results of its scan operation, then return to the command prompt.

4. To run another scan operation, repeat Step 3. To close the MS-DOS Prompt window, type `exit` at the command prompt. If you restarted your computer in DOS mode, type `win` to start Windows, or restart your computer as you would normally.

The tables on the following pages list all of the VirusScan options available.

NOTE: When you specify a filename as part of a command-line option, you must include the full path to the file if it is not located in the VirusScan program directory.

Command line options

Command-line Option	Description
/? or /HELP	Displays a list of VirusScan command-line options, each with a brief description. To open the “Help” list, use either of these options alone on the command line.
/ADL For OS/2, includes CD-ROM when used with /NODDA	Scan all local drives-including compressed and PCMCIA drives, but not diskettes--in addition to any other drive specified on the command line. Note: To scan both local and network drives, use the /ADL and /ADN commands together in the same command line.
/ADN For OS/2, use /ADL, above, plus /NODDA for CD-ROM	Scan all network drives--including CD-ROM--for viruses, in addition to any other drive(s) specified on the command line. Note: To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command line.

Command-line Option	Description
/AF <filename>	Inserts validation code which VirusScan uses in virus detection tasks into the file you specify. /AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves. Notes: * To use /AF, you must specify a [filename], including the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. * The /AF option will not store any information about the Master Boot Record or boot sector of the drive being scanned. * Use of the /AF option will increase your scanning time by about 300%. * This validation code increases the size of each file by 98 bytes.
/ALERTPATH <dir>	Designates a directory as a network path monitored by Centralized Alerting.
/ALL	Overrides the default scan setting by scanning all infectable files—regardless of extension. Note: * Using the /ALL option substantially increases the scanning time required. Use it if you find a virus or suspect you have one. * By default, VirusScan only scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD. These are the file types that are most susceptible to viruses.

Command-line Option	Description
/ANYACCESS	Scans only floppy disk files and executables in VirusScan for OS/2. Scans: * the boot sector whenever a diskette is either read or written to * executables * any newly created files. Note: /ANYACCESS cannot be used with /POLY.
/APPEND	* This command, used with /REPORT, will append report message text to the specified report file. * If the /REPORT option is used without /APPEND, the /REPORT option will overwrite the specified report file.
/AV	/AV Adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL) which VirusScan uses in virus detection tasks. Notes: * To update files on a shared network drive, you must have update access rights. * The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned. * This validation code increases the size of each file by 98 bytes. * To exclude self-modifying or self-checking files, or damaged files that might cause false alarms, use the /EXCLUDE option. * Using any of the /AV, /CV, or /RV options together in the same command line returns an error.
/BOOT	Scan boot sector and master boot record only.

Command-line Option	Description
/BOOTACCESS This option not valid for VirusScan Command Line for Windows NT	Scans a diskette's boot sector for viruses whenever the diskette is accessed (including read/write operations).
/CERTIFY This option not valid for VirusScan Command Line for Windows NT	Prevents your system from running files that do not have VirusScan validation codes.
/CF filename	Checks the validation data stored by the /AF option in [filename] as a means of detecting new or unknown viruses. If VirusScan finds that a file or system area has changed, VirusScan will report that a viral infection may have occurred. Notes: * Use of the /CF option increases scanning time by about 250%. * Using any of the /AF, /CF, or /RF options together in a command line returns an error. * Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF on these systems, VirusScan will continuously report boot sector modifications even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.
/CLEAN	Cleans viruses from infected files and system areas.
/CLEANDOC	Cleans viruses from infected Microsoft Word and Office document files only
/CLEANDOCALL	Cleans all macros from Microsoft Word and Office documents. This option deletes all macros, including macros not infected by a virus.

Command-line Option	Description
/CLEAN	Clean viruses from all infected files and system areas.
/CLEANDOC	Cleans viruses from infected Microsoft Word and Office document files only.
/CLEANDOCALL	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. Note: This option deletes all macros, including macros not infected by a virus.
/CONTACT <message>	This option not valid for VirusScan Command Line for Windows NT Displays specified message when a virus is detected.
/CONTACTFILE filename	Display the contents of <filename> when a virus is found. It is an opportunity to provide contact information and instructions to the user when a virus is encountered. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. Note: Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.

Command-line Option	Description
/CV	Check validation codes added to files by /AV to help detect new or unknown viruses. For more information, see “Configuring Validation Options” on page 37. If a file is modified, VirusScan reports that a viral infection may have occurred. Note: * Using the /CV option will increase scanning time by about 50%. * The /CV option does not check the boot sector for changes. * Using any of the /AV, /CV, or /RV options together in the same command line returns an error.
/DEL	Deletes infected files permanently.
/EXCLUDE <filename or directory> This option not available with VirusScan for OS/2	Use this option to: * Exclude specific files from a scan. List the complete path to each file you want to exclude on its own line. You may use wildcards * and ? * Exclude directories and multiple files; e.g., /EXCLUDE c:\dos excludes all directories and files beginning with c:\dos. * Exclude specific files from both /AF and /AV validation and /CF and /CV checking.
/FAST	* Speeds up the scan by asking VirusScan to examine a smaller portion of each file for viruses. * Because it limits virus detection activities, do not use this option if you have found a virus or suspect one. * Use of this option will reduce scanning time by about 15%.
/FILEACCESS This option not valid for VirusScan Command Line for Windows NT	Scans executable files when they are accessed on a diskette, but does not check the boot sector.

Command-line Option	Description
/FORCE	* VirusScan will replace an infected Master Boot Record (MBR) or boot sector with a generic MBR or boot sector if cleaning fails. * VirusScan will use its generic Master Boot Record when cleaning partition table viruses. * Cleans infected boot sectors of diskettes. * Works even if a remover is not yet available for the boot sector virus.
/FREQUENCY hours	Do not scan [n] hours after the previous scan. * In environments where the risk of viral infection is very low, use this option to prevent unnecessary scans. * Remember, the greater the scan frequency, the greater your protection against infection.
/? or /HELP	Displays a list of VirusScan command-line options, each with a brief description. To open the “Help” list, use either of these options alone on the command line.
/IGNORE drive(s) This option not valid for VirusScan Command Line for Windows NT.	Does not check programs loaded from the specified drive(s).
/LOAD filename	* Load scanning options from the named file. * Use this option to perform a scan you’ve already configured by loading custom settings saved in an ASCII-formatted file.

Command-line Option	Description
/LOCK This option not available with VirusScan for OS/2 or VirusScan Command Line for Windows NT.	* With this /LOCK option enabled, VirusScan will halt and lock your system if VirusScan finds a virus. * We recommend using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system. * /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs.
/LOG	VirusScan will log the date and time of the current scan by updating or creating a file called SCAN.LOG in the root of the target drive.
/LONGYEAR	* Display years in four-digit format. * By default, VirusScan reports dates in two-digit format.
/MACROHEUR x	Allows you to adjust the level of sensitivity used when performing heuristic scanning for macro viruses in Microsoft Word documents. When using this command, substitute 0, 1, 2, 3, 4, 5, or 100 for the letter x. * Choosing 0 turns off the heuristic scanning feature. * Choosing 1 (minimum) through 5 (maximum) turns on heuristic scanning at varying levels of sensitivity. * Choosing 100 causes VirusScan to detect all macros, including those not found to be viral or probably viral. Such detections are reported as: “This file contains macros.”

Command-line Option	Description
/MANY	* Scans multiple diskettes consecutively in a single drive. VirusScan will prompt you for each diskette. * Use this option to check multiple diskettes quickly. * You cannot use the /MANY option if you run VirusScan from a boot diskette and you have only one floppy drive. For example, if you are running VirusScan from a diskette in the A: drive, and attempt to use the A: drive to scan other diskettes, VirusScan will become unavailable as soon as you remove the VirusScan diskette. The following command will cause an error during execution: a:\scan a: /many
/MAXFILESIZE xxx.x	Scan only files no larger than xxx.x megabytes.
/MEMEXCL hhhh[-hhhh] Not valid for OS/2 or Windows NT This option not available with VirusScan for OS/2 or VirusScan Command Line for Windows NT.	Does not allow VShield to use UMB address specified. Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.) This will prevent VirusScan from checking areas in upper memory which may contain memory-mapped hardware capable of causing false alarms.

Command-line Option	Description
/MOVE <dir> or *.???	/MOVE directory: Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. Note: This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files. /MOVE*.???: VirusScan will change the extension of infected files, but not move them. For example, using the /MOVE*.BAD option will result in any infected files being simply renamed with the extension .BAD but not physically moved.
/NOBEEP	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	Disables CTRL-C and CTRL-BREAK during scans. * Users will not be able to halt scans in progress with /NOBREAK in use. * Use this option with /LOG to create a meaningful audit trail of regularly scheduled scans
/NOCOMP	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. * This reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files by decompressing each file in memory and checks for virus signatures. * VirusScan will still check for modifications to compressed executables if they contain VirusScan validation codes.

Command-line Option	Description
/NODDA	No direct disk access. This prevents VirusScan from accessing the boot record. * This feature has been added to allow VirusScan to run under Windows NT. * You might need to use this option on some device-driven drives. * Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.
/NODISK This option not valid for VirusScan Command Line for Windows NT.	Does not scan boot sector while loading VShield.
/NODOC	Does not scan Microsoft Office files.
/NOEXPIRE	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMDB This option valid only for VirusScan Command Line for Windows NT.	Does not scan MDB files.
/NOMEM This option not available with VirusScan for OS/2 or VirusScan Command Line for Windows NT.	Does not scan memory for viruses. * This greatly reduces scan time. * Use /NOMEM only when you are absolutely certain that your computer is virus-free.
/NOREMOVE	Prevents VShield from being removed from memory with the /REMOVE switch
/NOUMB	Does not use upper memory blocks (UMB).
/NOWARMBOOT This option not valid for VirusScan Command Line for Windows NT.	Does not check the diskette boot sector for viruses during a warm boot (system reset or CTRL+ALT+DEL).

Command-line Option	Description
/NOXMS This option not valid for VirusScan Command Line for Windows NT.	Does not use extended memory (XMS).
/ONLY drive(s)	Checks only programs loaded from the specified drive(s).
/PAUSE	Enables screen pause. The “Press any key to continue” prompt will appear when VirusScan fills a screen with messages (for example, when you’re using the /SHOWLOG or /VIRLIST options).Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with muultiple drives or that have severe infections without needing your input. We recommend omitting /PAUSE using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR)
/PLAD Not valid for ScanPM or VirusScan Command Line for Windows NT.	Preserve Last Access Dates on Novell NetWare drives. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.
/POLY	Checks for polymorphic viruses. Note: /ANYACCESS cannot be used with /POLY.
/RECONNECT	Restores on-access scanning after certain drivers or TSRs have disabled it.
/REMOVE	Unloads VShield from memory.

Command-line Option	Description
/REPORT <filename>	Creates a report of infected files and system errors, and saves the data to [filename] in ASCII text file format. * If [filename] already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: VirusScan will instead add report information to the end of the file, instead of overwriting it. * You can also use /RPTALL, /RPTCOR, /RPTMOD, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report. * You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive.
/RF <filename>	Removes recovery and validation data created by the /AF option. from [filename] * If filename resides on a shared network drive, you must be able to delete files on that drive. * Using any of the /AF, /CF, or /RF options together in the same command line returns an error.
/RPTALL	Include all scanned files in the /REPORT file. * When used with /REPORT, this option adds the names of corrupted files to the report file. * You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.

Command-line Option	Description
/RPTCOR	Include corrupted files in /REPORT file. * When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files which VirusScan finds may have been damaged by a virus. * You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line. * There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).
/RPTERR	Include errors in /REPORT file. * When used with /REPORT, this option adds a list of system errors to the report file. * System errors can include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. * You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.
/RPTMOD	Include modified files in /REPORT file. * When used with /REPORT, this option adds a list of modified files to the report file. * VirusScan defines a modified file as one including unmatching validation codes (using the /CF or /CV options). * You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.

Command-line Option	Description
/RV	Removes validation and recovery data from files validated with the /AV option. * To update files on a shared network drive, you must have access rights to update them. * Using any of the /AV, /CV, or /RV options together in the same command line returns an error.
/SAVE	Saves the command-line options to the VSHIELD.INI file.
/SHOWLOG	Displays the contents of SCAN.LOG. * SCAN.LOG stores the time and date of previous VirusScan activity. You can create a VirusScan log file by using the /LOG option. * The SCAN.LOG file contains text and some special formatting. You may use the /PAUSE option to read the log data one screen at a time.
/SUB	Scans subdirectories inside a directory. * By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. * Use /SUB to scan all subdirectories within any directories you have specified. * It is not necessary to use /SUB if you are scanning an entire drive.
/SWAP This option not valid for VirusScan Command Line for Windows NT.	Loads VShield kernel (9.2KB) only; swaps the rest to [pathname]

Command-line Option	Description
/VIRLIST	Displays the name and a brief description of each virus that VirusScan detects. * You may use the /PAUSE option to read the virus list one screen at a time. You can use /VIRLIST with /PAUSE on the command line. * You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, enter: * scan /virlist > filename.txt * Because VirusScan can detect many viruses, this file is more than 250 pages long.
/XMSDATA This option not valid for VirusScan Command Line for Windows NT.	Loads VShield data files into XMS memory.

Index

A

B

C

D

E

F

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Index