McAfee VirusScan for
Windows 95 and Windows 98

User's Guide

Version 5.0

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES, INC. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

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

(i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the Documentation's proprietary notices.

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

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

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

4. **Ownership Rights.** The Software is protected by United States copyright laws and international treaty provisions. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

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

6. **Warranty and Disclaimer**

   a. **Limited Warranty.** McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be free from defects in materials and workmanship.

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

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

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

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

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

   IN ADDITION, YOU SHOULD BE AWARE OF THE FOLLOWING: EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE.

SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY PERSONAL OR BUSINESS USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION TO, OR IMPORTATION OF, ENCRYPTION BY: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE IT IS YOUR ULTIMATE RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS AND THAT MCAFEE HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

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

11. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. This Agreement supersedes any other communications with respect to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee or a duly authorized representative of McAfee. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

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

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

Table of Contents

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.

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.

About McAfee VirusScan 1

What is VirusScan?

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

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

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

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

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

What comes with VirusScan?

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

- **Common Components.** This set consists of data files and other support files that many of the VirusScan programs share. These files include VirusScan .DAT files, default configuration files, validation files, the Virus List and similar common files.

- **Command Line Scanners.** This set consists of two powerful scanning agents—SCAN.EXE and BOOTSCAN.EXE, both of which allow you to initiate targeted scan operations from the MS-DOS Prompt window. Ordinarily, you'll use VirusScan's graphical user interface (GUI) to perform most scanning operations, but if you have trouble starting Windows or if the VirusScan GUI components will not run in your environment, you can use the command-line programs as backups.

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

- **VirusScan.** This component gives you unmatched control over your scanning operations. You can initiate a scan operation at any time—a feature known as "on-demand" scanning—specify local and network disks as scan targets, choose how VirusScan will respond to any infections it finds, and see complete reports on its actions. You can get started quickly with VirusScan's basic configuration mode, or move to its advanced mode for maximum flexibility. See the "McAfee VirusScan Advanced Options User Guide" for details.

- **VirusScan Central**. This component features a simple but dynamic interface that serves as the heart of the VirusScan program suite. Use it to start each of the other components, to see statistics, reports and other information, and to update your VirusScan data files. See "Using VirusScan Central" on page 65 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 77 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 v7.x or earlier. See “Scanning cc:Mail” on page 198 for details.

- **MAPI Scanner**. This component allows you to scan, at your initiative, the Inbox or other mailbox for e-mail client applications that adhere to Microsoft’s Messaging Applications Programming Interface (MAPI). Use it to supplement the continuous background scanning VShield provides for MAPI clients such as Microsoft Exchange and Microsoft Outlook. See “Scanning Microsoft Exchange and Outlook mail” on page 185 for details.

- **McAfee ScreenScan**. This optional component scans your computer as your screen saver runs during idle periods. See “Using ScreenScan” on page 199 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 157 for details.

- **Safe & Sound**. This component lets you create automatic or interactive backups of selected drives, directories, files or file types. You can back up to a protected volume file (a separate area on the drive). A protected volume file contains information about each file in every sector to ensure that files can be recovered even if the hard drive's directories and data are severely damaged or lost. You can also create mirror backups that instantly back up data as you save it, make backups after a time delay when the PC is idle, or create manual backups. See "Using Safe & Sound" on page 205 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, select Help in the upper right-hand corner of the window.

    VirusScan also includes context-sensitive online help. To see help topics, right-click buttons, lists or other elements within dialog boxes, or click **Help** buttons where you see them.
  - A README.TXT file. This file contains last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and often describes new product features incorporated into incremental product updates. You'll find the README.TXT file at the root level of your VirusScan CD-ROM—you can open and print it from Windows Notepad, or from nearly any word-processing software.

– A README.1ST file. This file outlines the terms of your license to use VirusScan. Read it carefully—by installing VirusScan you agree to its terms.

Deciding when to scan for viruses

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

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

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

Even the most diligent scanning can miss new viruses, however, if your scanning software is not up to date. Your VirusScan purchase entitles you to free virus updates for the life of your product, so you can update frequently to keep current. VirusScan will even tell you when you should update your data files and offer to download them for you.

Recognizing when you don't have a virus

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

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

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

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

Installing McAfee VirusScan 2

Before You Begin

Network Associates distributes McAfee VirusScan in two ways: as an archived file that you can download from the Network Associates website or other electronic services; and on CD-ROM. Once you have downloaded a VirusScan archive or placed your VirusScan installation disc in your CD-ROM drive, the installation steps are the same. Review the system requirements shown below to verify that VirusScan will run on your system, then follow the installation steps on page 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 80486 or later. Network Associates recommends at least an Intel Pentium-class or compatible processor.
- A CD-ROM drive. If you downloaded your copy of VirusScan, this is an optional item.
- At least 20 MB of free hard disk space.
- At least 16MB of random-access memory (RAM).
- Microsoft Windows 95 or Microsoft Windows 98.

Other recommendations

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

- **NOTE:** Network Associates does *not* provide Internet connections. To obtain an Internet connection, contact a local Internet service provider.

Installation Steps

Select from the following:

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

  E **IMPORTANT:** If you suspect that your computer has a virus infection, download and install the VirusScan installation files onto a computer that is ***not*** infected. Then use the McAfee Rescue Disk utility during setup to make a disk that you can use to boot your infected computer and remove the virus. For more information, see "If you suspect you have a virus..." on page 49.

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

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

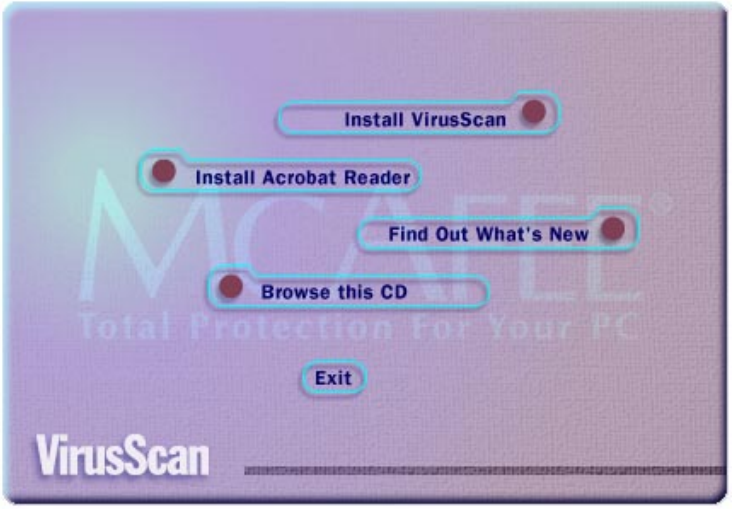

Figure 2-1. McAfee VirusScan welcome screen

To install VirusScan immediately, click **Install VirusScan**. Then, skip to Step 7 on page 35 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. Select **Run** from the **Start** menu.

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

Figure 2-2. The Run dialog box

2. Type <X>:\SETUP.EXE and click **OK**.

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

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

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

Figure 2-3. The Welcome to Setup wizard panel

3. Click **Next>**.

If Setup detects an existing version of VirusScan on your computer, Setup will detect and offer to remove it (Figure 2-4). Otherwise, continue to Step on page 34.

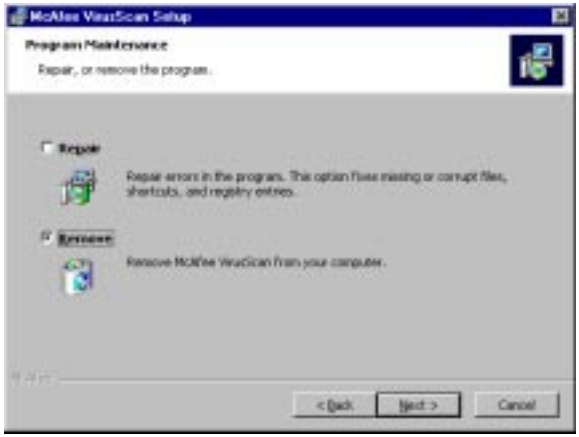

Figure 2-4. Found Current Version Installed panel

4. Select Remove and click **Next>**.

   Setup prompts you to continue.

5. Click **Remove**.

   VirusScan begins removing the existing version from your computer. When finished, Setup will prompt you to reboot your computer.

6. Click **Yes**.

   After your computer restarts, run Setup again.

   If Setup does not find an existing version of VirusScan, it will display the License Agreement panel (Figure 2-5). Read this agreement carefully—if you install VirusScan, you agree to abide by the terms of the license.

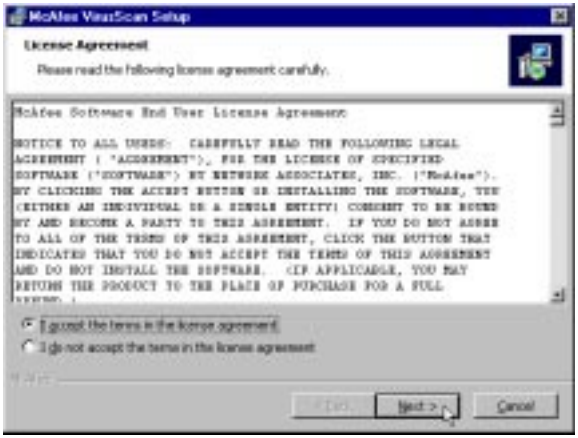

Figure 2-5. The Welcome to Setup wizard panel

7. If you do not agree to the license terms, select **No** and click **Next>**. Setup will quit immediately. Otherwise, select **Yes** and click **Next>**.

   The Setup Type panel appears (Figure 2-6).

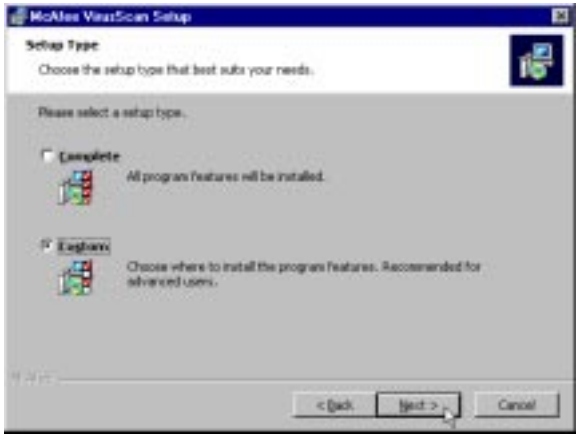

Figure 2-6. The Setup Type panel

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

   - **Complete.** Select this option to install all VirusScan options using the default installation options. Network Associates recommends this installation for most users.
   - **Custom.** Select this option to select a custom installation location.

9. If you selected Complete, continue to Step 11 on page 36. If you selected Custom, the Custom Setup page appears. Click **Browse** to locate the folder you want to use for the installation. By default, Setup installs VirusScan in this path:

   C:\Program Files\McAfee\McAfee VirusScan

10. After choosing a destination, click **Next>**.

    The Configuration Setup panel appears.

Figure 2-7. The Configuration Setup panel

11. Select from the following:

    - To configure the VirusScan Scheduler to scan your local hard drives every Monday, select the Schedule Weekly Scan checkbox.
    - To configure VShield to automatically scan your computer for viruses at startup, select the Scan at Startup checkbox.

    When you are finished, click **Next>**.

    The Ready to Install the Program panel appears.

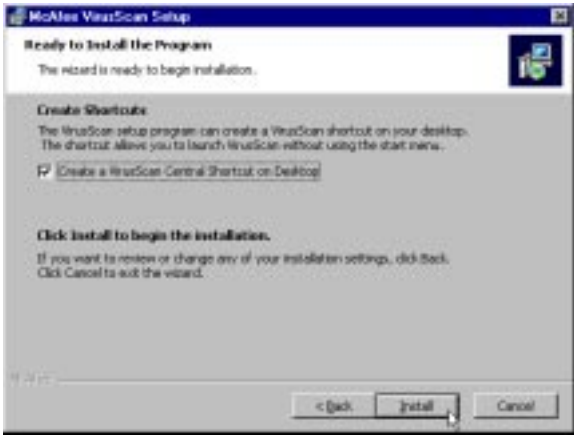

Figure 2-8. The Ready to Install the Program panel

12. To create a VirusScan Console shortcut on your desktop, select the Create Shortcuts checkbox.

    When you are ready to install VirusScan, click **Install**. To change installation options, click **<Back**. To exit without installing VirusScan, click **Cancel**.

    Setup begins copying files. When it is finished, the Configuration Setup panel appears.

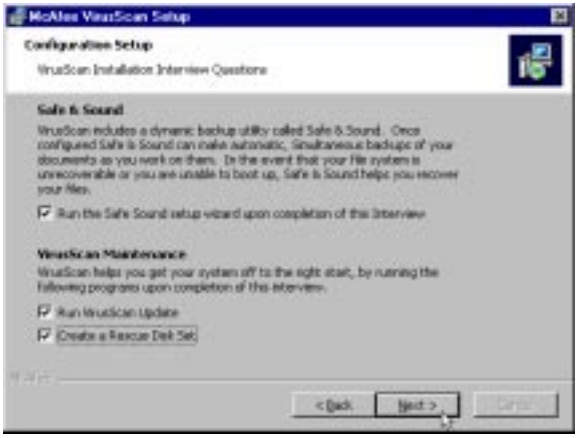

Figure 2-9. The Configuration Setup panel

13. Select from the following:

- Safe & Sound is a backup utility that automatically saves files as you work with them. For more information, see "What comes with VirusScan?" on page 26. To enable Safe & Sound, select the Safe & Sound checkbox.
- To offer you the best protection possible, Network Associates continually updates data files that detect new viruses and other harmful agents. To configure VirusScan to automatically update its virus data files after installation, select the Run VirusScan Update checkbox.

NOTE: This option requires an Internet connection.

- The VirusScan Emergency Disk enables you to boot your computer safely should your system become seriously infected. To create an Emergency Disk, select the Create a Rescue Disk Set checkbox.

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, do *not* create an Emergency Disk on the infected computer.

When you are finished choosing configuration options, click **Next>**.

The Launch Readme panel appears.

14. The Readme file contains important last minute information that did not make it into the user manual. To view the Readme file, select the View Readme File checkbox and click **Next>**.
15. If you did not select the Safe & Sound option, continue to Step 23 on page 42. If you did select the Safe & Sound option, the first Safe & Sound Wizard panel appears (Figure 2-10).

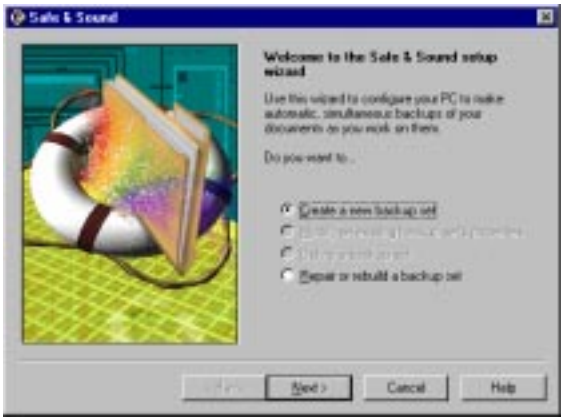

Figure 2-10. Safe & Sound: First Wizard Panel

16. Select Create a New Backup Set and click **Next >**. The second panel of the Safe & Sound Wizard appears.

17. Select whether to back up to a Protected Volume File or a Directory. Then click Next >.

    Protected Volume File–The Protected Volume File is the preferred backup type. A protected volume file is a sectioned off portion on the drive. It has special characteristics to ensure that even if organizational structures, such as the file allocation table on the drive is corrupted or lost, or the data becomes scrambled, the files in the backup set can be reconstructed. Safe & Sound stores extra information (in each sector for each file and also in a separate directory) to provide this level of protection. For details, see "Protected Volume Files (The Ultimate Backup Protection)" on page 205.

    - **NOTE:** You can copy files into a protected volume file manually using My Computer or Windows Explorer to add them to your backup set and instantly protect them.

    There are two drawbacks to using a protected volume file backup type. The first drawback is that three percent more storage space is required for the extra information that will be used to reconstruct the files in the event of a problem. The second drawback is that a protected volume file is slightly slower because it has to manipulate more information in more areas on the disk and more disk accesses are required. This is a marginal performance degradation, which you can eliminate by also selecting a Write-behind Delay of seconds or minutes.

Directory–The Directory backup type makes another copy of the files and directories selected for backup in a different location. This type of backup creates no performance drain on the system and it's simple to manage the backup area. You can use My Computer or Windows Explorer to cut or copy files in or out of the backup location or delete the files. The drawback of selecting a directory backup type is that the files are no more protected than if you had created a backup copy yourself.

The third panel of the Safe & Sound Wizard appears.

18. Specify the target destination where the backup set will be created and click Next >.

    The fourth panel of the Safe & Sound Wizard appears.

19. Click the Settings button if you want to customize any of the settings for this backup set.

    Volume Settings

    - **Backup Type**–Displays the currently selected backup type (Protected Volume File or Directory).
    - **Enable Automatic Backup**–While this check box is selected, Safe & Sound automatically updates this backup set as you update the files it contains based on the time delay you specify.
    - **Name of Backup Set**–If you are saving this backup set to a non-Windows 95/98 or NT drive (such as to a UNIX server on your network) be sure to follow the 8.3 naming convention for this name.
    - **Backup Delay**–Select the Mirror (0) write-behind delay if you want your backup set to remain in constant synchronization with the original files as you change them. Select a write-behind delay in seconds or minutes if you want your backup to be created during times when your PC is idle starting at any time after the time delay you select.

      A write-behind delay in seconds or minutes is recommended if you are using the protected volume file backup type and want to eliminate the slight speed reduction caused by extra disk accesses in more locations on the drive.
    - **View Drive As**–(*available only for backup sets stored as a Protected Volume File*). The drive letter you want to use for the Protected Volume File backup set.
    - **Keep Deleted Files For**–Select how long you want the backup set to keep files whose original counterparts have been deleted from your system.

- **Limit Size of Backup Volume**–Drag the slider left to reduce the backup volume size limit or right to increase the backup volume size limit.

Drives

Drive and Directory Folders appear in the Backup Drive list so you can select any of the ones you want to add to your backup set. Click folders to open and close them. Click the check boxes to place a check mark beside the drives or directories that you want to back up.

File Types

You can select groups of files that you want to include in your backup set by selecting their file type. The file type, such as TXT (for a text file), indicates the file's purpose. Safe & Sound displays a list of all the registered file types in Windows 95/98. The file types with check marks show the types of files that will be included in your backup set.

Safe & Sound obtains its list of registered file types from Windows. You can view or add registered file types in My Computer or Windows Explorer.

If you are not yet familiar with file types and want to see them, you can open My Computer or Windows Explorer, choose the Options command from the View menu, and click the File Types tab.

In the Options dialog box you can examine the list of the registered file types on your system. These are the file types that will be available to you in Safe & Sound. You can add new registered file types in the Options dialog box to make them available to Safe & Sound the next time you run it.

Many file types are standard, such as BMP and PCX which are used by paint applications like Microsoft Paint, or TIF which is a standard file type for TIFF graphic images. Each application's documents typically have a file type (which may or may not be registered in Windows). For example, Microsoft Word documents may be stored using registered file types of DOC, RTF or TXT, depending on the file type selected when saving the document.

- **NOTE:** You can also view file types directly in My Computer or Windows Explorer. Choose the Options command from the View menu, click the View tab, and make sure the HIDE MS-DOS FILE EXTENSIONS FOR FILE TYPES THAT ARE REGISTERED check box is deselected. Registered file types are also listed in the File Types tab in the Options dialog box. The other place where file types appear is in the Save As dialog box of Windows applications.

20. To apply the changes, click **Apply**. When you are finished, click **OK**. The fifth panel of the Safe & Sound Wizard appears.
21. Enter a backup volume name and click **Next >**. Safe & Sound begins backing up files.
22. When it is finished, click **Finish**.
23. If you did not select the Create a Rescue Disk Set option, you are prompted to reboot the computer. Select **Yes**. Installation is complete. If you did select the Create a Rescue Disk Set option, the first Emergency Disk Wizard panel appears.

Figure 2-11. First Emergency Disk Wizard panel

24. Click **Next>**.
25. The second Emergency Disk Wizard panel appears.

Figure 2-12. Second Emergency Disk Wizard panel

26. Select from the following:

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

      You are prompted to insert a disk.

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

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

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

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

         The Format dialog box appears.

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

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

         You are returned to the Emergency Disk Wizard.

      d. Click **Next>**.

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

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

  You are prompted to insert a disk.

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

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

27. 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** and click **Finish**. Otherwise, select **Yes, I want to restart my computer now** and click **Finish** to reboot your system.

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

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 44.
2. Click **Start** in the Windows taskbar, point to **Programs**, then choose **MS-DOS Prompt**.
3. In the window that appears, change your command-line prompt to point to the directory that contains the VirusScan files you installed. If you chose the default installation options, you'll find the files in this path:

   C:\Program Files\McAfee\McAfee VirusScan

   To get to this directory, type `cd progra~1\mcafee\mcafee~1` at the command prompt, then press ENTER. If you installed VirusScan in a different directory, type the correct path to that directory.
4. Run VALIDATE.EXE. To do so, type `validate *.*` at the command-line prompt.

   VALIDATE.EXE scans all of the files stored in your VirusScan program directory, then generates a file list that includes the file name, its size in bytes, its creation date and time, and two validation codes in separate columns. To use VALIDATE.EXE to examine individual files, simply follow `validate` with the name of the file you want to verify at the prompt, or use the DOS wildcards `?` and `*` to specify a range of files.

   - **NOTE:** Network Associates recommends that you redirect the output from VALIDATE.EXE to your printer so that you can review it easily. If you have set your printer to capture output from MS-DOS programs, simply type `validate *.* >lpt1` at the command-line prompt. To learn how to set your printer to print from MS-DOS programs, consult your Windows documentation.

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

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

- **NOTE:** Network Associates again recommends that you redirect the output from PACKING.LST to your printer. To do so, type `type packing.lst >lpt1` at the command-line prompt.

---

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

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

Testing Your Installation

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

To test your installation, follow these steps:

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

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

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

2. Save the file with the name EICAR.COM. The file size will be 69 or 70 bytes.
3. Start VirusScan and allow it to scan the directory that contains EICAR.COM. When VirusScan examines this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

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

Removing Infections From Your System 3

If you suspect you have a virus...

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

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

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

As it installs itself, VirusScan will examine your computer's memory and your hard disk's boot sectors to verify that it can safely copy its files to your hard disk without risking their infection. If VirusScan reports during setup that your system appears virus-free, continue with the installation, then perform a full system scan as soon as you restart your computer—file-infector viruses that don't load into your computer's memory or hide in your hard disk's boot blocks might still be lurking somewhere on your system. See Chapter 2, "Installing McAfee VirusScan," to learn about virus scanning during setup. 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 50.

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

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

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

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

2. Insert the McAfee Emergency Disk that came with your copy of VirusScan into your floppy drive.

   - **NOTE:** If your VirusScan copy did not come with a McAfee Emergency Disk, or if you have misplaced your Emergency Disk, you must create a new disk on an *uninfected* computer. Locate a computer that you know is virus-free, then follow the steps outlined in "Creating an emergency disk" on page 51.

3. Start your computer again.

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

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

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

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

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

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

   - **Return to working with your computer.** If Scan did not find a virus, or if it cleaned any infected files it did find, remove the Emergency Disk from your floppy drive, then restart your computer normally. If you had planned to install VirusScan on your computer but stopped when Setup found an infection, you can now continue with your installation.
   - **Try to clean or delete infected files yourself.** If Scan found a virus, but could not remove the virus code from the file, it will identify the infected file and tell you that it could not clean the file, or that it does not have a current remover for the infecting virus.

     As your next step, you can:

     – **Locate and delete the infected file or files.** You will need to restore any files you delete from backup files. Be sure to check your backup files for infections also.

     – **Try to remove the infection yourself.** Network Associates supplies information that can help you remove a virus from an infected file. To learn how, visit the Network Associates website at http://www.nai.com/vinfo. Look for one of these documents in the online Virus Information Library:

     #0013 #0319 #0322 #0323 #0327 #1145

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

Creating an emergency disk

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

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

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

1. Insert a blank 1.44MB disk into your floppy drive.
2. Start VirusScan Central.
3. Click **Options**, point to **Tools**, and Select **Emergency Disk**. The Emergency Disk Wizard opens. (Figure 3-13). Click **Next>**.
4. If you did select the Create a Rescue Disk Set option, the first Emergency Disk Wizard panel appears.

Figure 3-13. First Emergency Disk Wizard panel

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

Figure 3-14. Second Emergency Disk Wizard panel

7. Select from the following:

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

  You are prompted to insert a disk.

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

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

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

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

     The Format dialog box appears.

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

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

     You are returned to the Emergency Disk Wizard.

  d. Click **Next>**.

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

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

  You are prompted to insert a disk.

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

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

- **NOTE:** A write-protected floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position. Because software cannot write to a write-protected disk, viruses cannot infect it.

Creating an Emergency Disk without the utility

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

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

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

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

   Next, press **ENTER** to format the floppy disk you inserted, to overwrite any existing information on it, to copy DOS system files to it, and to have DOS prompt you to enter a volume label for it.
4. When DOS prompts you for a volume label, enter “E-disk” or another name up to 11 characters long that distinguishes this disk from others.
5. If you have VirusScan installed on your computer and in its default program directory, change to the correct directory by typing this command at the MS-DOS prompt:

   ```
   cd\progra~1\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 77 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 (Figure 3-15).

Figure 3-15. System Scan response options

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

- **Stop.** Click this to tell VShield to take no action. Normally, you would use this option to bypass files that you know do not have viruses. VShield will note each incident in its log file.
- **Clean.** Click this to tell VShield to try to remove the virus code from the infected file. If VShield succeeds, it will restore the file to its original state. If VShield cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will note this result in its log file, but will take no other action. In most cases, you should delete such files and restore them from backups.
- **Delete.** Click this to tell VShield to delete the infected file attachment from the e-mail message you received. By default, VShield notes the name of the infected attachment in its log file so that you can restore it from a backup copy.
- **Move File to.** Click this to tell VShield to move infected files to a quarantine directory as it finds them. By default, VShield moves these files to a folder named INFECTED that it creates at the root level of the drive on which it found the virus. For example, if VShield found an infected file in T:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VShield would copy the file to T:\INFECTED.
- **Exclude file.** Click this to tell VShield not to scan the file from now on. Unless you know the file is not infected, this option is not recommended.

E-mail Scan module

This module looks for viruses in e-mail messages you receive via corporate e-mail systems such as cc:Mail and Microsoft Exchange. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-16). A fourth option provides you with additional information.

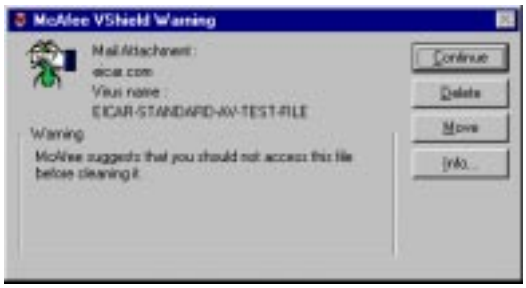

Figure 3-16. E-mail Scan module response options

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

- **Continue.** Click this to tell VShield to take no action and to resume scanning. Normally, you would use this option to bypass files that you know do not have viruses, or if you plan to leave your computer unattended as you download e-mail. VShield will note each incident in its log file.
- **Delete.** Click this to tell VShield to delete the infected file attachment from the e-mail message you received. By default, VShield notes the name of the infected attachment in its log file so that you can restore it from a backup copy.
- **Move.** Click this to tell VShield to create a quarantine directory where it found the virus, then move the infected file to it. If you use Microsoft Exchange, Microsoft Outlook or other MAPI mail clients, for example, the quarantine directory will appear as a folder called INFECTED in your mailbox on the mail server. If you use a POP-3 or similar mail client, the quarantine folder will appear at the root level of your hard disk as soon as you download an infected file.
- **Info.** Opens the Virus Information Center where you can view information about the virus (requires Internet connection). This choice does not cause the program to take any action against the virus it detected. See "Opening the Virus Information Center" on page 73 for more details.

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

Download Scan module

This module looks for viruses in e-mail messages and other files you receive over the Internet via a web browser or such e-mail client programs as Eudora Light, Netscape Mail, Outlook Express, and others. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-17). A fourth option provides you with additional information.

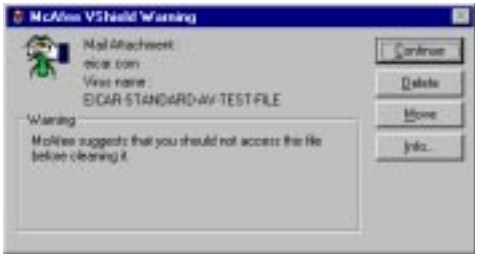

Figure 3-17. Download Scan response options

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

- **Delete.** Click this to tell VShield to delete the infected file or e-mail attachment you received. By default, VShield notes the name of the infected file in its log so that you can restore the file from a backup copy.
- **Move.** Click this to tell VShield to create a quarantine directory where it found the virus, then move the infected file to it. If you use a POP-3 or SMTP mail client, the quarantine folder will appear as a folder called INFECTED at the root level of your hard disk as soon as you download an infected file.
- **Continue.** Click this to tell VShield to take no action and to resume scanning. Normally, you would use this option to bypass files that you know do not have viruses, or if you plan to leave your computer unattended as you download e-mail or other files. VShield will note each incident in its log file.
- **Info.** Opens the Virus Information Center where you can view information about the virus (requires Internet connection). This choice does not cause the program to take any action against the virus it detected. See “Opening the Virus Information Center” on page 73 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 3-18).

Figure 3-18. 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 3-19).

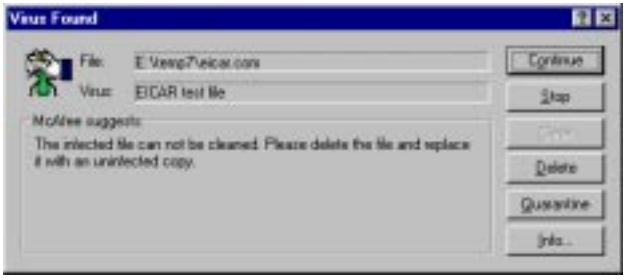

Figure 3-19. VirusScan response options

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

- **Continue.** VirusScan will proceed with its scan operation, list each infected file in the lower portion of its main window (Figure 3-20), 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.

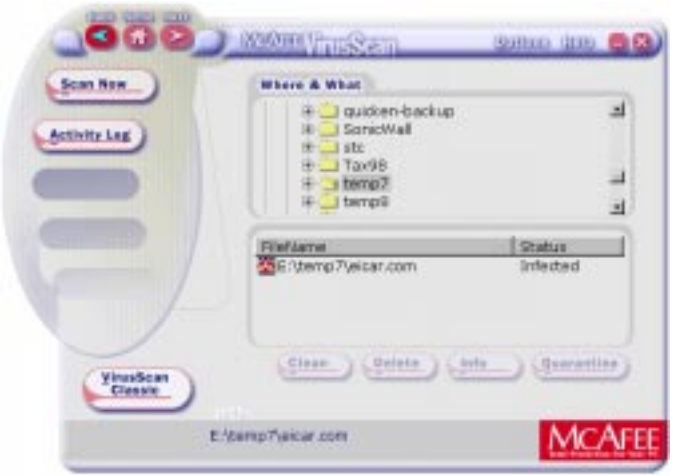

Figure 3-20. VirusScan main window

- **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 3-20) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.
- **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 3-19, VirusScan failed to clean the Eicar Test Virus—a mock "virus" written specifically to test whether your anti-virus software installed correctly. Here, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.
- **Delete.** VirusScan will immediately delete the file from your system. By default, VirusScan will record the name of the infected file in its log so that you can restore the file from a backup copy.

- **Move file to.** VirusScan will open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Info.** Opens the Virus Information Center where you can view information about the virus (requires Internet connection). This choice does not cause the program to take any action against the virus it detected. See "Opening the Virus Information Center" on page 73 for more details.

Responding when E-Mail Scan detects a virus

VirusScan's E-Mail Scan program component lets you scan incoming Microsoft Exchange or Microsoft Outlook e-mail messages for viruses at your initiative. You can start it from within either e-mail client and use it to supplement VShield's continuous e-mail background scanning. E-Mail Scan also offers the ability to clean infected file attachments or stop the scan operation, capabilities that VShield lacks. In its initial configuration, E-Mail Scan will prompt you for a response when it finds a virus (Figure 3-21).

Figure 3-21. 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 3-22 on page 62), 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 3-22 on page 62) 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.

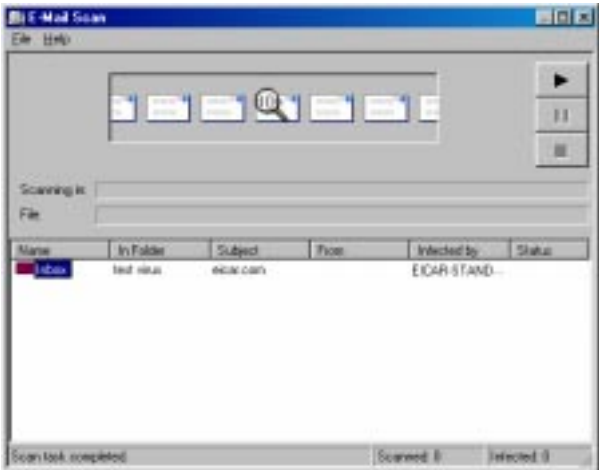

Figure 3-22. E-Mail Scan window

- **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 3-21, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.
- **Delete.** E-Mail Scan will immediately delete the file from your system. By default, the program will record the name of the infected file in its log so that you can restore the file from a backup copy.
- **Move file to.** E-Mail Scan will open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Info.** Opens the Virus Information Center where you can view information about the virus. This choice does not cause the program to take any action against the virus it detected. See "Opening the Virus Information Center" on page 73 for more details.

Understanding false detections

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

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

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

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

Using VirusScan Central 4

What is VirusScan Central?

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

Starting VirusScan Central

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

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

Figure 4-1. VirusScan Central window

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

Starting VirusScan program components

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

Starting VirusScan

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

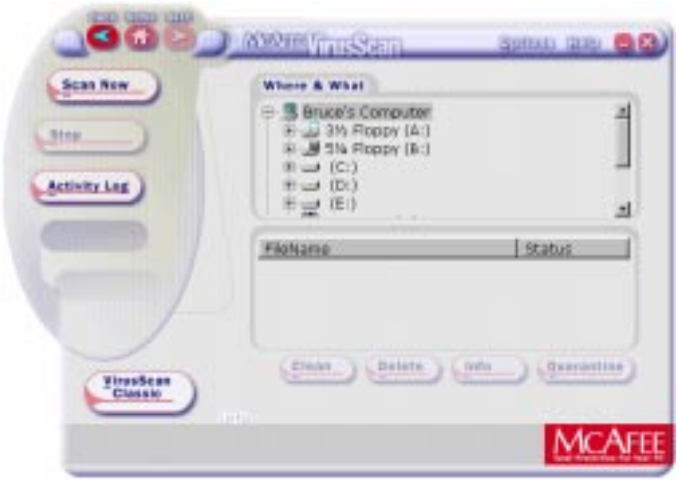

Figure 4-2. VirusScan window

NOTE: If you are a previous user of VirusScan products and would like to access the VirusScan Classic or VirusScan Advanced interfaces, see Chapter 6, "Using McAfee VirusScan."

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

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

VirusScan will start to look for viruses immediately. A reporting area at the bottom of the window allows you to track its progress and respond to any infected files it finds. See “Responding when VirusScan detects a virus” on page 59 to learn what to do when you have a virus on your system.

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

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

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

Figure 4-3. VShield Configuration dialog box

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

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

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

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

- **E-mail Scan.** Select the **Enable Scanning of E-mail attachments** checkbox to start this module. E-mail Scan does not have default settings, so you will need to configure it to work in your environment. See "Using VShield" on page 77 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 Pro, Netscape Navigator, and other POP-3 e-mail clients.

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

- **Security.** Select the **Enable password protection** checkbox to activate this module. The Security module does not have any default settings, so you will need to choose a password and decide which of the VShield property pages you want to protect from unauthorized changes. See "Using VShield" on page 77 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

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

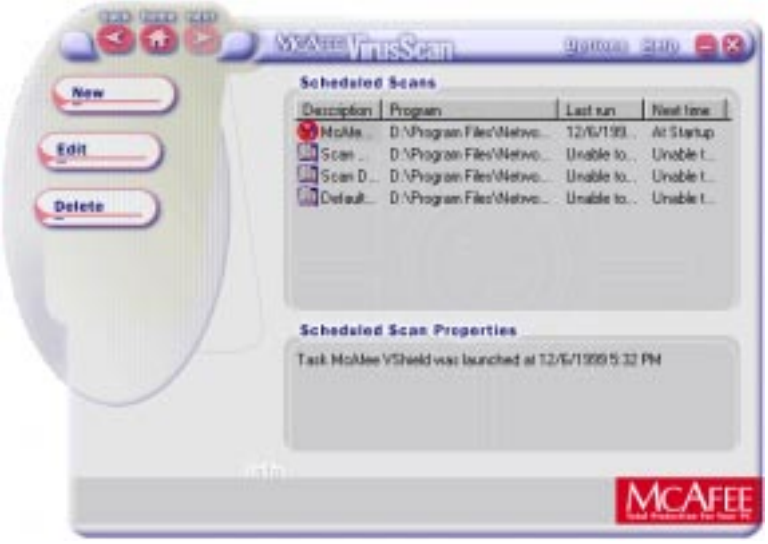

Figure 4-4. VirusScan Scheduler window

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

The Scheduler comes with four pre-configured scan tasks, which provide basic protection for your system. 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 Quarantine Explorer

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

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

Figure 4-5. Quarantine Explorer window

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

Using VirusScan Tools

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

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

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

Using Safe & Sound

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

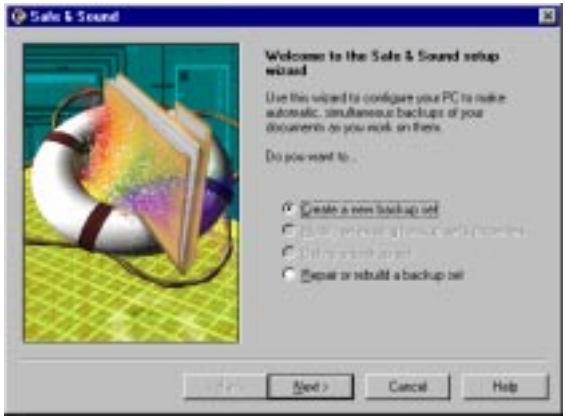

Figure 4-7. Safe & Sound: First Wizard Panel

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

You can also create mirror backups that instantly back up data as you save it or when the PC is idle. See "Using Safe & Sound" on page 205 to learn how to use the utility.

Creating an Emergency Disk

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

Figure 4-8. Emergency Disk Creation Utility dialog box

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

This disk is similar to the Emergency Disk that comes with your copy of VirusScan. However, to create an emergency disk with the utility, you will need a floppy disk formatted with bootable DOS system files. See "Creating an emergency disk" on page 51 to learn how to use the utility.

Opening the Virus Information Center

To open the Virus Information Center (Figure 4-9), click **Options**, point to Tools, and click **Virus Info**.

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

Figure 4-9. 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, click the first letter of the virus name in the Find Viruses Alphabetically area. Then, scroll through the list until you find the virus that you want to know about and click the virus name.

A Virus Information window for the virus you selected will appear (Figure 4-10).

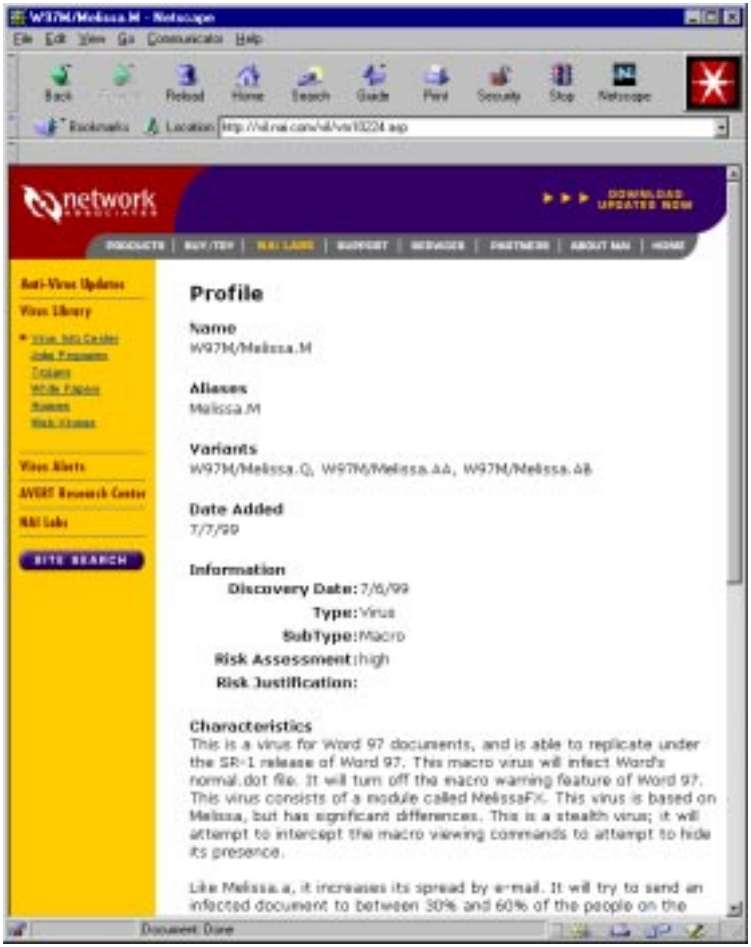

Figure 4-10. Virus Information window

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.

Updating VirusScan

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

Using VShield 5

What does VShield do?

VShield acts as your system guardian, protecting each point-of-entry as you work with files from diskettes, work with files from the network, open e-mail attachments, and as your system loads programs into memory.

VShield loads when you start your computer and stays active 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.** 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 provides 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 79 or "Setting VShield properties" on page 83 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
- Microsoft Internet Explorer v5.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, v4.0, and v5.0

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 and begins working with default 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 provide increased security, you should configure VShield to work with your e-mail client software and to closely examine your Internet traffic for viruses and malicious software. VShield's configuration wizard can help you set up many of these options right away. Later, as you become more familiar with VShield and your system's susceptibility to harmful software, you can tailor the program to work better in your environment.

To start the VShield configuration wizard, either:

- Start VirusScan Central, then click the **Options** button in the upper-right hand corner of the VirusScan Central window. To learn how to start and use VirusScan Central, see "Starting VirusScan Central" on page 65.
- Locate the VShield icon in the Windows system tray. Right-click it, point to **Properties**, and click **System Scan**.

The VShield Properties dialog box opens (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**. Otherwise, select **No**. Click **Next>** to continue.

The E-mail Scan wizard panel appears (Figure 5-4).

Figure 5-4. VShield configuration wizard - E-mail Scan panel

Select from the following:

- **I do not use e-mail**. If you do not use e-mail or do not have an Internet connection, select this option. Otherwise, select the checkbox that corresponds to the type of e-mail client you use.
- **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.
- **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. 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 panel contains 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 panel contains options for VShield's Internet Filter module (Figure 5-6).

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

To have VShield block Java applets and ActiveX controls that it knows can cause your system harm, select **Yes, enable hostile applet protection**, then click **Next>**. 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 the **Options** button in the upper-right hand corner of the VirusScan Central window. To learn how to start and use VirusScan Central, see "Starting VirusScan Central" on page 65.
- Locate the VShield icon in the Windows system tray. Right-click it, point to **Properties**, and click **System Scan**.

The VShield Properties dialog box opens (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 configure System Scan options, click the System Scan icon on the left side of the VShield Properties dialog box.

Choosing Detection options

By default, VShield scans 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 84). 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. Choose when and where VShield will look for viruses. Select from the following:

   - **Scan files as you work with them.** Each time you open, copy, save, rename, or otherwise use files on your hard disk, viruses can execute and spread infections to other files. To prevent this, select any combination of the **Run**, **Copy**, **Create** and **Rename** checkboxes. Although 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. Select from the following:

   - **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. Therefore, you can safely speed up scan operations by narrowing the scope of your scan operations to file types most susceptible to virus infection. To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions**. The Program File Extensions dialog box opens (Figure 5-9).

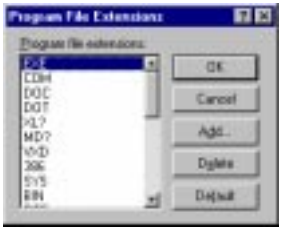

Figure 5-9. Program File Extensions dialog box

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 both 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 have VShield scan 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 an extension to the list, click **Add** and enter the extensions you want VShield to scan.

  – To remove an extension from the list, select it and click **Delete**.

  – To restore the list to its original form, click **Default**.

  When you are finished, click **OK**.

- **Scan all files.** To have VShield examine all files types on your system that you use in any way, select **All files**. Although this will ensure that it is virus free, it will slow your system down considerably.

3. Select whether you want to enable Heuristic scanning. To open the Macro Heuristics Scan Settings dialog box, click **Heuristics** (Figure 5-10).

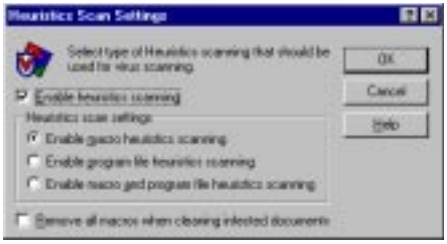

Figure 5-10. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables VShield to recognize new viruses based on their resemblance to similar viruses it already knows. To do this, VShield scans all files and compares them to its virus signature database. If it finds an exact match, it identifies the virus by name. If the code signatures resemble existing viruses, VShield informs you that it has found a "probable" 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. Select whether you want VShield to scan for macro viruses, program file viruses, or both.

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, deselect this checkbox.

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

d. To save your settings and return to the VShield Properties dialog box, click **OK**.

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 126 and "Tracking VShield status information" on page 126 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.

I **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, deselect this checkbox and protect the settings with a password. This will prevent other users from disabling VShield through VirusScan Scheduler or the VShield Properties dialog box. See "Configuring the Security module" on page 123 for details.

---

5. To configure additional VShield options, click the Action tab. 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 make available when it finds a virus, or which action you want it to take on its own.

Follow these steps:

1. To display the correct property page, click the Action tab in the System Scan module (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.** Select 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. To select which responses you want VShield to make available, select or deselect the following check boxes:

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

  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.** Select this option to configure VShield to automatically remove the virus code from infected files that it finds. If VShield cannot remove the virus, it will notify you in its message area and, if you have its reporting features enabled, will record the incident in its log file. See "Choosing Report options" on page 92 for details.

- **Delete infected files automatically.** Select this option to configure VShield to automatically delete infected files that it finds. 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.** Select this option to configure VShield to mark the file "off limits" and continue 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 92 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete or clean them at your next opportunity.

3. To choose additional VShield options, click the Alert tab. 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

When VShield detects a virus, it can respond to the virus automatically or prompt you for action. The Alert property page enables you to customize how VShield prompts you for action.

Additionally, many network administrators monitor virus infections to prevent virus outbreaks within their companies. The Alert property page enables you to keep your network administrator informed when VShield finds viruses.

Follow these steps:

1. To display the Alert property page, click the Alert tab in the System Scan module (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 88 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 and enter a custom message in the provided text box (up to 225 characters). Next, select the **Sound audible alert** checkbox.

5. To configure additional VShield options, click the Report tab. 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. To display the Report property page, click the Report tab in the System Scan module (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 path and filename in the provided text box or click **Browse** to select a file and location on your hard disk or network.

3. To prevent the log file from becoming too large, select the **Limit size of log file to** checkbox and enter the maximum file size (in kilobytes) in the provided text box.

   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 type of information that you want VShield to record by selecting or deselecting the following checkboxes:

   - **Virus detection.** Select this checkbox to have VShield record the number of infected files it found during this scanning session.
   - **Virus cleaning.** Select this checkbox to have VShield record the number of infected files that it cleaned.
   - **Infected file deletion.** Select this checkbox to have VShield record the number of infected files it deleted from your system.

- **Infected file move.** Select this checkbox to have VShield record 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. To choose additional VShield options, click the Exclusion tab. 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 84 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. To display the Exclusion property page, click the Exclusion tab in the System Scan module (Figure 5-13).

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

By default, the Exclusion page only lists your Recycle Bin. VShield excludes the Recycle Bin from scan operations because Windows does not run files that are 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 automatically move infected files to a quarantine folder, 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 and click **Edit**. The Edit Exclude Item dialog box opens. Make the changes you need and click **OK**.
- **Remove an item from the list.** To delete an exclusion item, select it in the list and click **Remove**. VShield will then scan this file or folder during its next scanning operation.

3. To change any of your System Scan settings, click a different tab. To configure options for a different module, click one of the icons along the left side of the System Scan Properties dialog box.

   To save your changes in the System Scan module without closing this 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 configure e-mail options, click the E-mail Scan icon on 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 on the property page become available (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.

     – **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. 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. Therefore, you can safely speed up scan operations by narrowing the scope of your scan operations to file types most susceptible to virus infection.

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

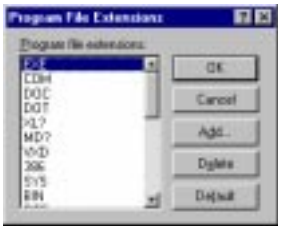

Figure 5-17. Program File Extensions dialog box

  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 both document and template files.

  – To add to the list, click **Add** and enter the extensions you want VShield to scan.

  – To remove an extension from the list, select it and click **Delete**.

  – To restore the list to its original form, click **Default**.

  When you have finished, click **OK**.

- **Scan all attachments.** To have VShield examine any attachment that arrives with any e-mail message, regardless of its extension, select **All attachments**. Although this will ensure your mail is virus free. it might slow your system down considerably.

4. To choose additional VShield options, click the Action tab. 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 make available when it finds a virus, or which action you want it to take on its own.

Follow these steps:

1. To display the correct property page, click the Action tab in the E-mail Scan module (see Figure 5-18 on page 100).

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. These include:

   - **Prompt for user action.** Select 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. To select which responses you want VShield to make available, select or deselect the following checkboxes:

     – **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 pre-selected quarantine directory.

  - **Clean file.** This option tells VShield to try to remove the virus code from the infected file.
  - **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**. Select this option to have VShield move infected files to a quarantine directory as it finds them. By default, VShield moves these files to a folder named INFECTED.

  If you use a corporate e-mail system, VShield creates the INFECTED folder on the network mail server. You cannot designate a different folder or change the folder's name. Depending on your access to the mail server, 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 109 for details.

- **Delete infected files.** Select this option to configure VShield to automatically delete infected files that it finds. 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 104 for details.

- **Continue scanning.** Select this option to configure VShield to continue scanning without taking any action against viruses that it finds. If you choose this option, make sure to also activate the VShield reporting feature (see "Choosing Report options" on page 104 for details). The program will record the names of any viruses it finds and the names of infected files so you can delete them at your next opportunity.

3. To choose additional VShield options, click the Alert tab. 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

When VShield detects a virus, it can respond to the virus automatically or prompt you for action. The Alert property page enables you to customize how VShield notifies you of virus infections.

Additionally, many network administrators monitor virus infections to prevent virus outbreaks within their companies. The Alert property page enables you to keep your network administrator informed when VShield finds viruses.

Follow these steps:

1. To display the correct property page, click the Alert tab in the E-mail Scan module (see Figure 5-19 on page 102).

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

2. To configure 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. 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 and 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. To compose a standard reply, follow these steps:

    a. Click **Configure**. The Return Mail Configuration dialog box appears.

    b. Fill in the subject line and add any comments you want to make in the body of the message (up to 1024 characters). They will appear below a standard infection notice that VShield will supply.

    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. To save the message, click **OK**.

    Whenever it detects a virus, VShield will send this message to the person who sent the infected e-mail attachment, using the recipient's address from the original message header. VShield identifies the virus and the affected file and appends your comments to the end of the message. If you have activated its report feature, VShield also logs each instance when it sends an alert message.

4. To send an e-mail message to warn others (such as a network administrator) about an infected attachment, select the **Send alert mail to user** checkbox. To compose a standard reply to send to one or more recipients each time VShield detects an infected e-mail attachment, follow these steps:

    a. Click **Configure**. The Send Mail Configuration dialog box appears.

    a. 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, address book, or 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.

    ---

b. Fill in the subject line and add any comments you want to make in the body of the message (up to 1024 characters). They will appear below a standard infection notice that VShield will supply.

c. To save the message, click **OK**.

Whenever it detects a virus, VShield sends a copy of this message to each of the addresses that you entered in Step a. VShield identifies the virus and the affected file and appends your comments to the end of the message. If you have activated its report feature, VShield also logs each instance when it sends an alert message.

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.

5. If you chose **Prompt for user action** as your response in the Action page (see "Choosing Action options" on page 100 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 and enter a message in the provided text box (up to 225 characters). Next, select the **Sound audible alert** checkbox.

6. To choose additional VShield options, click the Report tab. 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. To display the Report property page, click the Report tab in the E-mail Scan module (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 select a file and location on your hard disk or the network.

3. To prevent the log file from becoming too large, select the **Limit size of log file to** checkbox and enter a maximum file size (in kilobytes) in the provided text box.

   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. Select from the following:

- **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. To change any of your E-mail Scan settings, click a different tab. To choose options for a different module, click one of the icons on the left side of the E-mail Scan Properties dialog box.

   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 on the E-mail Scan module's Detection page. See "Choosing Detection options" on page 97 for details.

To set VShield to scan files you download, click the Download Scan icon on the left side of the VShield Properties dialog box. 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 107). 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, follow these steps:

1. Select the Enable Internet Download Scanning checkbox.
2. 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. Therefore, you can safely speed up scan operations by narrowing the scope of your scan operations to file types most susceptible to virus infection. To do so, select the **Program files only** button. To see or change the file name extensions VShield will examine, click **Extensions**. The Program File Extensions dialog box opens (Figure 5-22).

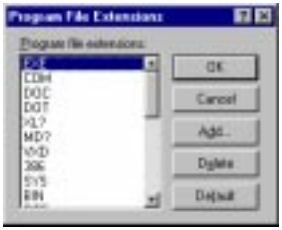

Figure 5-22. Program File Extensions dialog box

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 both document and template files.

- To add to the list, click **Add** and enter the extensions you want VShield to scan.
- To remove an extension from the list, select it and click **Delete**.
- To restore the list to its original form, click **Default**.

When you are finished, click **OK**.

- **Scan all files.** To have VShield examine every file that you download, regardless of its extension, select **All files**. Although this will ensure that you do not download known viruses, this might slow download operations.
- **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.

3. To choose additional VShield options, click the Action tab. 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. To display the Action property page, click the Action tab in the Download Scan module (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.** Select 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. To select which responses you want VShield to make available, select or deselect the following checkboxes:

     – **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**. Select this option to have VShield move infected files to a quarantine directory as it finds them. By default, VShield moves these files to a folder named INFECTED at the root level of the hard disks where the viruses are found.

  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.** Select this option to have VShield automatically delete every infected file that you download. Be sure to enable its reporting feature so that you have a record of which files VShield deleted.

- **Continue scanning.** Select this option to configure VShield to continue scanning without taking any action against viruses it finds. If you select this option, you should also activate the VShield reporting feature (see "Choosing Report options" on page 112 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. To choose additional VShield options, click the Alert tab. 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

When VShield detects a virus, it can respond to the virus automatically or prompt you for action. The Alert property page enables you to customize how VShield notifies you of virus infections.

Additionally, many network administrators monitor virus infections to prevent virus outbreaks within their companies. The Alert property page enables you to keep your network administrator informed when VShield finds viruses.

Follow these steps:

1. To display the Alert property page, click the Alert tab in the Download Scan module (Figure 5-24).

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

2. To configure 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. 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 and 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 109 for details), you can also configure VShield to beep and display a custom message when it finds a virus. To do so, select the **Display custom message** checkbox and enter the message you want to see in the provided text box (up to 225 characters). Next, select the **Sound audible alert** checkbox.
5. To choose additional VShield options, click the Report tab. 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 Download 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. To display the Report property page, click the Report tab in the Download Scan module (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 select a file and location on your hard disk or on your network.

3. To prevent the log file from becoming too large, select the **Limit size of log file to** checkbox and enter a maximum file size (in kilobytes) in the provided text box.

   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. Select from the following:

   - **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 all Java applets or ActiveX controls, 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 on the left side of the VShield Properties dialog box. 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, follow these steps:

1. Select the Enable Java & ActiveX filter checkbox.
2. 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 118 more details.
3. 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**. The Banned IP Addresses dialog box opens (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** and enter the addresses you want VShield to block in the dialog box that opens (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. To save your address and return to the Banned IP Addresses dialog box, click **OK**. To add another address to the list, repeat these steps.

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

When you have finished editing the list, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

- **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**. The Banned URLs dialog box opens (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.nastyviruses.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).

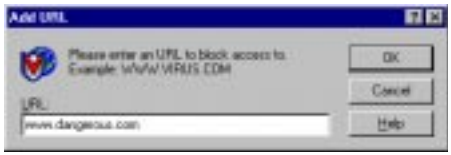

Figure 5-30. Add URL dialog box

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. To save your address and return to the Banned IP Addresses dialog box, click **OK**. To add another address to the list, repeat these steps.

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

When you have finished editing the list, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

4. To choose additional VShield options, click the Action tab. 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 prompts you for action (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 114 for details.

To choose additional VShield options, click the Alert tab. 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

When VShield detects a harmful object or Internet site, it can block access to the object or prompt you for action. The Alert property page enables you to customize how VShield notifies you of virus infections.

Additionally, many network administrators monitor harmful objects and sites to prevent problems within their companies. The Alert property page enables you to keep your network administrator informed when VShield finds harmful objects or Internet sites.

Follow these steps:

1. To display the correct property page, click the Alert tab in the Internet Filter module (Figure 5-32).

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

2. To configure 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. 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 118 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 and enter a custom message in the provided text box (up to 225 characters). Next, select the **Sound audible alert** checkbox.

5. To choose additional VShield options, click the Report tab. 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 87 for details) and protect that setting with a password, you can easily and effectively enforce a strict anti-virus security policy for all network users.

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 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.

   E **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.

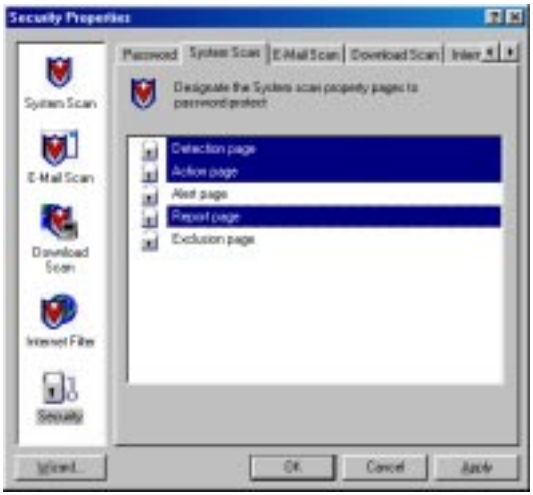

Figure 5-36. System Scan security options

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 keeps several of its common commands in a shortcut menu associated with its system tray icon. To display the VShield Status dialog box, double-click this icon. To display other commands, right-click the icon and select from the following:

- **Status.** Select this to open the VShield Status dialog box.
- **Enable.** Point to this and select one of the VShield modules to activate or deactivate it. Modules preceded by checkmarks are active; those without are inactive.
- **Properties.** Point to this and select one of the VShield modules listed to open the VShield Properties dialog box for that module.
- **About.** Select 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.** Select 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 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. To start the program component, click **Enable**. To disable it, click **Disable**.

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

5. To close the VShield Status dialog box, click **Close**.

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 83 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 126 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 128).

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.

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: the VirusScan "on-demand" scanner. "On demand" means that you can 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 three modes:

- **VirusScan "Standard" interface**—gets you up and running quickly, with a minimum of configuration options.
- **VirusScan "Classic" interface**—provides previous users with the traditional basic VirusScan interface.
- **VirusScan "Advanced" interface**—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 all three 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.

By default, VirusScan is configured to scan all drives on your computer. VirusScan Classic comes with a single, default scan operation pre-configured to look for viruses on your C: drive. VirusScan Advanced comes with a single pre-configured scan operation, which scans all of your local hard disks. Any of these interfaces can be changed to scan specific drives or folders.

Starting and Configuring VirusScan Standard

To start VirusScan:

Start VirusScan Central and click **Scan** at the left side of the window. To learn how to start and use VirusScan Central, see Chapter 4, “Using VirusScan Central.”

The VirusScan window appears (Figure 6-1).

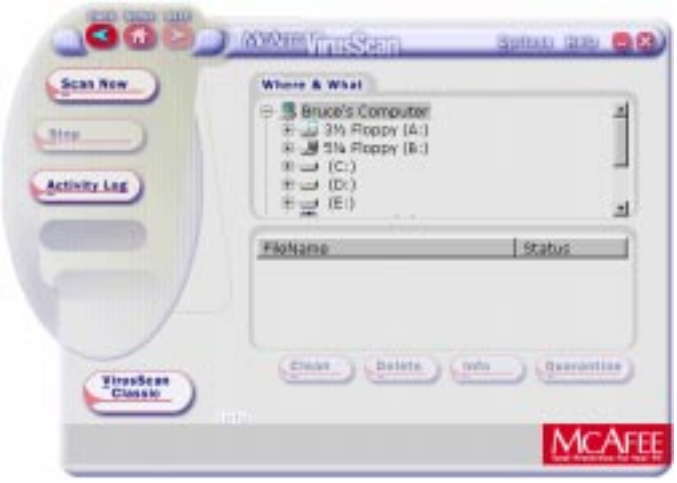

Figure 6-1. VirusScan window

VirusScan initially assumes that you want to scan all drives on your computer.

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.

   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—to choose these items as scan targets, you must switch to VirusScan Advanced. For more information, see "Configuring VirusScan Advanced" on page 142.

2. When you have selected your scan target and are ready to start scanning, click **Scan Now**.

Starting VirusScan Classic or VirusScan Advanced

To start VirusScan:

Start the VirusScan Console and click **Scan**. The VirusScan Window appears.

Click **VirusScan Classic**. The VirusScan Classic window opens (Figure 6-2).

Figure 6-2. VirusScan Classic window

To start the default scan task immediately, click **Scan Now**. To configure a scan task that suits your needs, click the tabs at the top of the window and choose 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, select **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 copy the backup file to the VirusScan program directory. To learn about the .VSC file format, see the "McAfee VirusScan Advanced Options Reference Guide".

- **Save new settings.** If you need different VirusScan configurations in order to run various scan operations, or if you want to run a scan operation with the same configuration on more than one computer, you can save your configuration options 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 136 or "Configuring VirusScan Classic" on page 136 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.** To open the log file VirusScan uses to record its actions and settings, choose **View Activity Log** from the **File** menu.

  The log file opens in a Notepad window (Figure 6-3). 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 149.

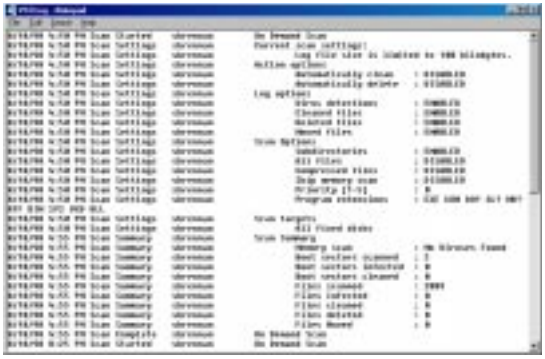

Figure 6-3. VirusScan Activity Log

- **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 and follow the on-screen instructions.

- **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 153 for details.
- **Link to the Network Associates Virus Information Library.** Choose **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 the Virus Information Library, see "Connecting to the Online Virus Information Library" on page 155.
- **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 157.
- **Open the online help file.** Choose **Help Topics** from the **Help** menu to see a list of VirusScan help topics. To see a context-sensitive description of buttons, lists and other items in the VirusScan window, choose **What's this?** from the **Help** menu, then click an item with your left mouse button after your mouse cursor changes to  . You can see these same help topics if you right-click an element in the VirusScan window, then choose **What's This?** from the menu that appears.

Configuring VirusScan Classic

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

Choosing Where & What options

VirusScan initially assumes that you want to scan your C: drive and all of its subfolders, and to restrict the files it scans only to those susceptible to virus infection (Figure 6-4).

Figure 6-4. 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.

   Enter the path of the target volume or folder in the **Scan in** text box or click **Browse** to select a volume or folder (Figure 6-5).

Figure 6-5. 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 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.

After selecting a scan target, click **OK**. You are returned to the VirusScan Classic window.

2. To have VirusScan look for viruses in folders within your scan target, make sure to select the **Include subfolders** checkbox.

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

   - **Scan compressed files.** To have VirusScan look for viruses in files compressed in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats, select the **Compressed files** checkbox. 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. Therefore, you can safely speed up scan operations by narrowing the scope of your scan operations to file types most susceptible to virus infection. To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions**. The Program File Extensions dialog box opens (Figure 6-6).

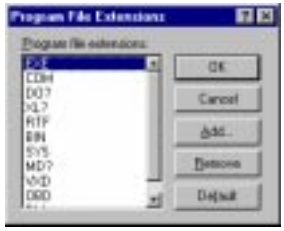

Figure 6-6. The Program File Extensions dialog box

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 both document and template files.

   – To add to the list, click **Add** and enter the extensions you want VirusScan to scan.

   – To remove an extension from the list, select it and click **Delete**.

   – To restore the list to its original form, click **Default**.

When you have finished, click **OK**.

To have VirusScan examine all files on your system, regardless of their extensions, select **All files**. Although this will ensure that it is virus free, it will slow scan operations down considerably.

4. To choose additional VirusScan options, click the Action tab.

   To start a scan operation immediately with the options you chose, 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. To display the Action property page, click the Action tab in the VirusScan Classic window (Figure 6-7).

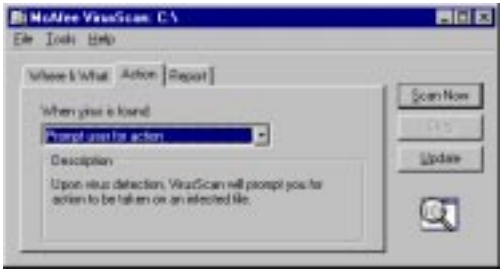

Figure 6-7. VirusScan Classic window - Action page

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.** Select this option if you expect to be at your computer when VirusScan performs scans—VirusScan will display an alert message when it finds a virus and allow you to choose from its available responses.

- **Move infected files automatically**. Select this option to have VirusScan move infected files to a quarantine directory 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.** Select this option to tell VirusScan to remove the virus code from infected files that it finds. 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 149 for details.

- **Delete infected files automatically.** Select this option to have VirusScan delete every infected file it finds. 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 149 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. To choose additional VirusScan options, click the Report tab.

   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, and 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. To display the Report property page, click the Report tab in the VirusScan Classic window (Figure 6-8).

Figure 6-8. 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 and enter the message you want to appear in the provided text box (up to 225 characters).

     - **NOTE:** To have VirusScan display your message, you must select **Prompt user for action** (see "Choosing Action options" on page 146 for details).

   - **Generate an audible alert.** 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 select a file on your hard disk or network.

4. To prevent the log file from becoming too large, select the **Limit size of log file to** checkbox and enter a maximum file size (in kilobytes) in the provided text box.

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. To change any of your VirusScan settings, click another tab.

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

Configuring VirusScan Advanced

VirusScan Advanced offers you more configuration flexibility than VirusScan Classic. These options include the ability to run more than one scan operation concurrently, the ability to exclude items from scan operations, and the ability to configure VirusScan's heuristic virus detection function.

When you start VirusScan, VirusScan Classic opens. To switch VirusScan from Classic mode to Advanced mode, select **Advanced** from the **Tools** menu in the VirusScan Classic window. 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

By default, VirusScan 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 6-9).

Figure 6-9. 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.** To open the Add Scan Item dialog box, click **Add** (Figure 6-10).

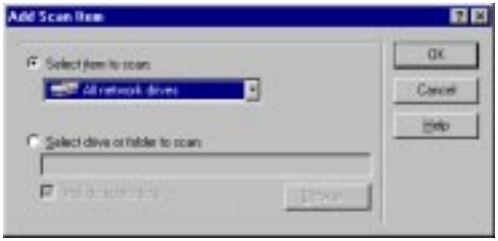

Figure 6-10. The Add Scan Item dialog box

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, choose **Select drive or folder to scan**. Next, enter the path to the drive or folder in the provided list box or click **Browse** to locate the scan target on your computer. To have VirusScan also look for viruses in any folders within the scan target, make sure to select the **Include subfolders** checkbox.

When you are finished, click **OK**. Repeat this step for each target you would like to add.

- **Change scan targets.** Select one of the listed scan targets and click **Edit**. The Edit Item to Scan dialog box opens (Figure 6-11).

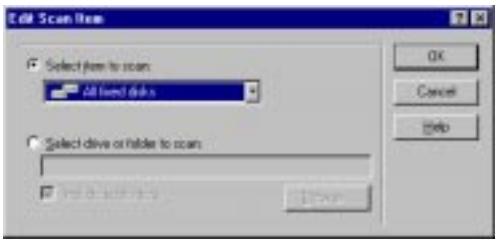

Figure 6-11. Edit Scan Item dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target and click **OK**.

- **Remove scan targets.** To delete a scan target, select a targets and click **Remove**.

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

- **Scan compressed files.** To have VirusScan look for viruses in files compressed in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats, select the **Compressed files** checkbox. 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. Therefore, you can safely speed up scan operations by narrowing the scope of your scan operations to file types most susceptible to virus infection. To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions**. The Program File Extensions dialog box opens (Figure 6-6).

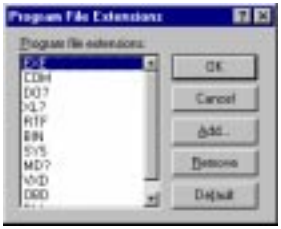

Figure 6-12. The Program File Extensions dialog box

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 both document and template files.

- To add to the list, click **Add** and enter the extensions you want VirusScan to scan.
- To remove an extension from the list, select it and click **Delete**.
- To restore the list to its original form, click **Default**.

When you have finished, click **OK**.

To have VirusScan examine all files on your system, regardless of their extensions, select **All files**. Although this will ensure that it is virus free, it will slow scan operations down considerably.

- **Turn on heuristic scanning**. To open the Macro Heuristics Scan Settings dialog box, click **Macro Heuristics** (Figure 6-13).

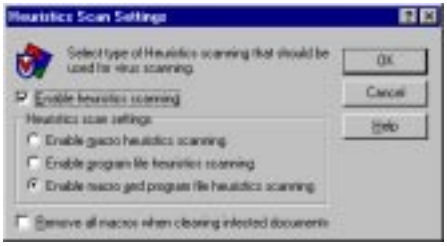

Figure 6-13. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables VirusScan to recognize new viruses based on their resemblance to similar viruses it already knows. To do this, VirusScan scans all files and compares them to its virus signature database. If it finds an exact match, it identifies the virus by name. If the code signatures resemble existing viruses, VirusScan informs you that it has found a “probable” 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. Select whether you want VShield to scan for macro viruses, program file viruses, or both.

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, deselect this checkbox.

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

d. To save your settings and return to the VirusScan Properties dialog box, click **OK**.

3. To configure additional VirusScan options, click the Action tab.

   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, and 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. To display the correct property page, click the Action tab in the VirusScan Advanced window (Figure 6-14).

Figure 6-14. 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.** Select this option if you expect to be at your computer when VirusScan is running. When it finds a virus, VirusScan will display an alert message and offer you a range of possible responses. Select from the following:
     - **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**. Select this option to have VirusScan move infected files to a quarantine directory 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 R:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VirusScan would copy the file to R:\INFECTED.

     You can enter a different name in the provided text box, or click **Browse** to locate a suitable folder on your hard disk.
   - **Clean infected files automatically.** Select this option to tell VirusScan to automatically remove virus code from infected files. 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 149 for details.

- **Delete infected files automatically.** Select this option to have VirusScan automatically delete infected files. Be sure to enable its reporting feature so you have a record of which files VirusScan deleted. You will need to restore deleted files from backup copies.
- **Continue scanning.** Select this option only if you plan to leave your computer unattended while VirusScan checks for viruses. Be sure to also activate the VirusScan reporting feature (see "Choosing Report options" on page 149 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. To choose additional VirusScan options, click the Alert tab.

   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

When VirusScan detects a virus, it can respond to the virus automatically or prompt you for action. The Alert property page enables you to customize how VirusScan prompts you for action.

Additionally, many network administrators monitor virus infections to prevent virus outbreaks within their companies. The Alert property page enables you to keep your network administrator informed when VirusScan finds viruses.

Follow these steps:

1. Click the Alert tab in the VirusScan Advanced window (Figure 6-15).

Figure 6-15. 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. Enter the path to the NetShield alert folder on your network or click **Browse** to locate the 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 146 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 and enter a message in the provided text box (up to 225 characters). Next, select the **Sound audible alert** checkbox.

5. To choose additional VirusScan options, click the Report tab.

   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 (Figure 6-16).

Figure 6-16. 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 provided text box or click **Browse** to select a file on your hard disk or network.

3. To prevent the log file from becoming too large, select the **Limit size of log file to** checkbox. Enter a value for the file size, in kilobytes, in the provided text box.

   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 type of information that you want VShield to record by selecting or deselecting the following checkboxes:

   - **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 and choose **View Activity Log** from the **File** menu. For more information, see "Using VirusScan menus" on page 134.

5. To select additional VirusScan options, click the Exclusion tab.

   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 142 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 6-16).

Figure 6-17. VirusScan Advanced window - Exclusion page

By default, the Exclusion page lists 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**. The Add Exclude Item dialog box opens (Figure 6-18).

Figure 6-18. 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. To change any of your VirusScan settings, click a different tab.

   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. The Password Protection dialog box opens (Figure 6-19).

Figure 6-19. Password Protection dialog box

2. Select the property pages you want to protect.

   You may protect any or all VirusScan property pages. Protected property pages display a locked padlock icon in the security list shown in Figure 6-19. To remove protection from a property page, click the locked padlock icon .

3. Click **Password**. The Specify Password dialog box opens (Figure 6-20).

Figure 6-20. Specify Password dialog box

   a. Enter a password in the first text box. Reenter the password in the text box below to confirm your choice.

   b. To close the Specify Password dialog box and save changes, click **OK**.

4. To save changes and return to the VirusScan Advanced window, click **OK**.

Connecting to the Online Virus Information Library

Choose **Virus List** from the **Tools** menu in either VirusScan Classic or VirusScan Advanced to open the Virus Information Library (Figure 6-21).

Figure 6-21. Virus List window

The Virus Information Library is a comprehensive collection of information about viruses. It can also be accessed by using 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. 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 automatically runs scan operations and other tasks at the times or intervals you specify. You can configure Scheduler to run scan operations when you are away from the computer or whenever it suits your needs.

Why schedule scan operations?

Although VirusScan includes components that look for viruses continuously and others that allow you to scan your system whenever you want, you can schedule regular automated 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

Start VirusScan Central and click **Schedule**. To learn how to start and use VirusScan Central, see Chapter 4, "Using VirusScan Central."

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.

Using the Scheduler window

From the Scheduler window, you can:

- **Create a new task.** Click **New**. A Task Properties dialog box will appear. See "Creating new tasks" on page 160 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 and click **Edit**. A Task Properties dialog box will appear. See "Enabling tasks" on page 161 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 and click **Edit**. A Task Properties dialog box will appear. Click **Configure**. How this property page looks depends on which VirusScan component you run. See "Configuring task options" on page 164 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).

- **Delete a task.** Select one of the tasks listed in the Scheduler window and click **Delete**. The Scheduler will prompt you for confirmation. Click **Yes** to delete the task. Click **No** to keep it.

  - **NOTE:** You can only delete tasks that you create—you may not delete any of the default tasks that come with the Scheduler. However, you can disable any default tasks you don't want to run. See "Enabling tasks" on page 161 for details.

- **Start a task.** Select one of the tasks listed in the Scheduler window and click **Edit**. A Task Properties dialog box will appear. Click **Run Now**. 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 and click **Edit**. A Task Properties dialog box will appear. Click **Enable**.

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 161 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 My Computer.** 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. Click **New** in the Scheduler window.

   The Task Properties dialog box appears (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\McAfee\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 164 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 162 for more details.

To enable a task, follow these steps:

1. If you do not already have the Task Properties dialog box open, click one of the listed tasks in the Scheduler window and click **Edit**.

   The Task Properties dialog box appears (Figure 7-2 on page 160).

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

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 162 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, select a task and click **Edit**.

   The Task Properties dialog box will appear (Figure 7-2 on page 160).

2. Click the Status tab to display the correct property page (Figure 7-4).

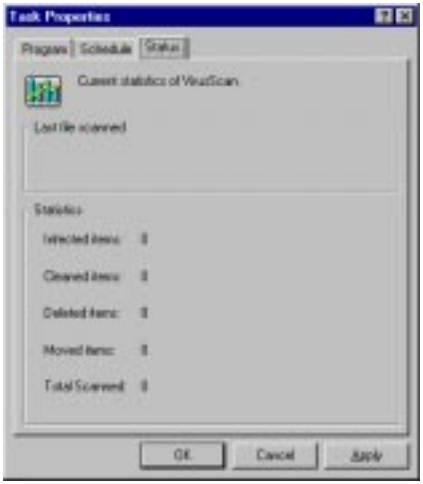

Figure 7-4. Task Properties dialog box - Status page

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 160 to learn how to specify the program that will run your scan task.

   The McAfee VirusScan Properties dialog box appears (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, enter the path to the drive or folder in the provided list box or click **Browse** to locate the scan target on your computer. To have VirusScan also look for viruses in any folders within the scan target, make sure to select the **Include subfolders** checkbox. When you are finished selecting a target, click **OK**.

- **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 and click **OK**.

- **Remove scan targets.** To delete a scan target, select a target and click **Remove**.

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

- **Scan compressed files.** To have VirusScan look for viruses in files compressed in LZH, WinZip or PKZIP, UUENCODE, and Windows Compressed Application Binary (.CAB) archiving formats, select the **Compressed files** checkbox. 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. Therefore, you can safely speed up scan operations by narrowing the scope of your scan operations to file types most susceptible to virus infection. To do so, select the **Program files only** button. To see or designate the file name extensions VShield will examine, click **Extensions**. The Program File Extensions dialog box opens (Figure 7-8).

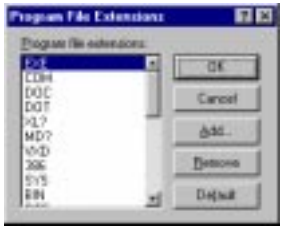

Figure 7-8. The Program File Extensions dialog box

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 both document and template files.

- To add to the list, click **Add** and enter the extensions you want VirusScan to scan.
- To remove an extension from the list, select it and click **Delete**.
- To restore the list to its original form, click **Default**.

When you have finished, click **OK**.

To have VirusScan examine all files on your system, regardless of their extensions, select **All files**. Although this will ensure that it is virus free, it will slow scan operations down considerably.

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

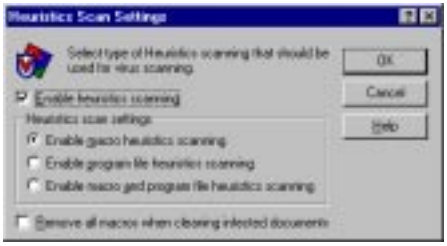

Figure 7-9. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables VirusScan to recognize new viruses based on their resemblance to similar viruses it already knows. To do this, VirusScan scans all files and compares them to its virus signature database. If it finds an exact match, it identifies the virus by name. If the code signatures resemble existing viruses, VirusScan informs you that it has found a “probable” 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. Select whether you want VShield to scan for macro viruses, program file viruses, or both.

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, deselect this checkbox.

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

d. To save your settings and return to the VirusScan Properties dialog box, click **OK**.

3. 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 and click **Edit**. The Task Properties dialog box appears. Click **Configure**.

2. The McAfee VirusScan Properties dialog box appears (Figure 7-5). Click the Action tab (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.** Select this option if you expect to be at your computer when VirusScan is running. When it finds a virus, VirusScan will display an alert message and offer you a range of possible responses. Select from the following:
     - **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**. Select this option to have VirusScan move infected files to a quarantine directory 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 R:\MY DOCUMENTS and you specified INFECTED as the quarantine directory, VirusScan would copy the file to R:\INFECTED.

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

- **Clean infected files automatically.** Select this option to tell VirusScan to automatically remove virus code from infected files. 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 173 for details.

- **Delete infected files automatically.** Select this option to have VirusScan automatically delete infected files. Be sure to enable its reporting feature so you have a record of which files VirusScan deleted. You will need to restore deleted files from backup copies.

- **Continue scanning.** Select this option only if you plan to leave your computer unattended while VirusScan checks for viruses. Be sure to also activate the VirusScan reporting feature (see "Choosing report options" on page 173 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

When VirusScan detects a virus, it can respond to the virus automatically or prompt you for action. The Alert property page enables you to customize how VirusScan prompts you for action.

Additionally, many network administrators monitor virus infections to prevent virus outbreaks within their companies. The Alert property page enables you to keep your network administrator informed when VirusScan finds viruses.

Follow these steps:

1. To start from the Scheduler window, select the task you created in the task list and click **Edit**. The Task Properties dialog box appears. Click **Configure**.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 165). Click the Alert tab (Figure 7-11).

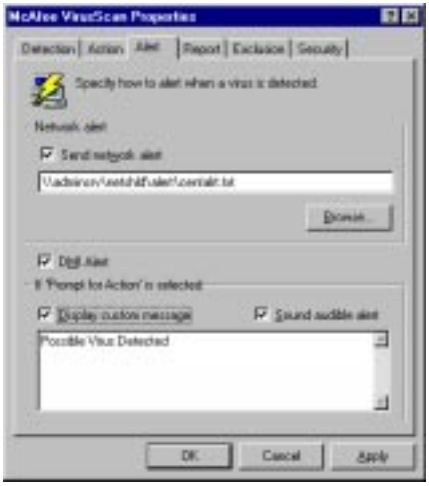

Figure 7-11. VirusScan Properties dialog box - Alert page

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. Enter the path to the NetShield alert folder on your network or click **Browse** to locate the 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 169 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 and enter a message in the provided text box (up to 225 characters). 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 and click **Edit**. The Task Properties dialog box appears. Click **Configure**.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 165). Click the Report tab (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 provided text box or click **Browse** to select a file on your hard disk or network.

4. To prevent the log file from becoming too large, select the **Limit size of log file to** checkbox. Enter a value for the file size, in kilobytes, in the provided text box.

   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 type of information that you want VShield to record by selecting or deselecting the following checkboxes:

   - **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 134.

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 165 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 and click **Edit**. The Task Properties dialog box appears. Click **Configure**.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 165). Click the Exclusion tab (Figure 7-13).

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

By default, the Exclusion page lists 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**. The Add Exclude Item dialog box opens (Figure 7-14).

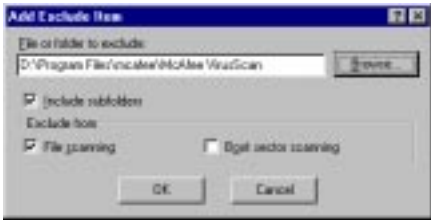

Figure 7-14. Add Exclude Item dialog box

   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 and click **Edit**. The Task Properties dialog box appears. Click **Configure**.

2. The McAfee VirusScan Properties dialog box appears (see Figure 7-5 on page 165). Click the Security tab (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, 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 Specialized Scanning Tools 8

Using Quarantine Explorer

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

Quarantine Explorer provides a convenient interface that enables you to view and respond to all quarantined files on your system.

To start Quarantine Explorer:

1. Start the VirusScan Console.
2. Click Quarantine.

   The Quarantine Explorer window appears (Figure 8-1).

Figure 8-1. Quarantine Explorer window

3. Select an infected file and choose from the following.
   - **Add.** Select this option to quarantine a suspected file.
   - **Clean.** Select this option to remove the virus code from infected file. If the virus cannot be removed, it will notify you in its message area.

- **Restore.** Select this option to restore a file to its original folder. This option does not clean the file. Make sure the file is not infected before using this option
- **Delete.** Select this option to delete the infected file. Make sure to note the file location so you have a record of the deleted files. You will need to restore deleted files from backup copies.
- **Submit to McAfee.** Select this option to submit new viruses to McAfee.

Submitting Possible Viruses

When you click **Submit to McAfee**, the McAfee Labs A.V.E.R.T Response Center wizard starts (Figure 8-2).

Figure 8-2. 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 8-3).

Figure 8-3. 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 8-4).

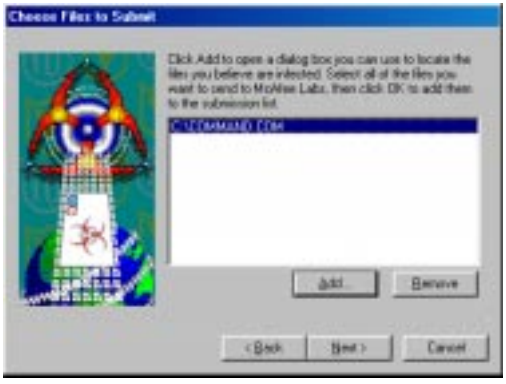

Figure 8-4. A.V.E.R.T Response Center Choose Files to Submit panel

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 8-5 on page 184).

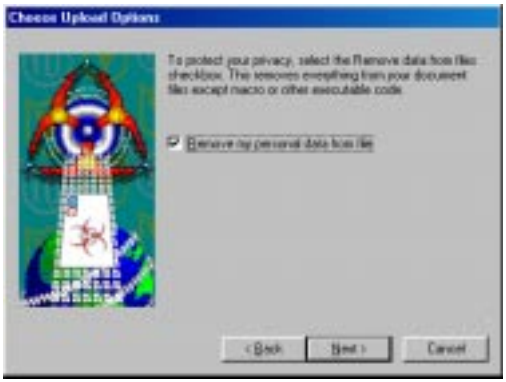

Figure 8-5. A.V.E.R.T. Response Center Choose Upload Options panel

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 8-6).

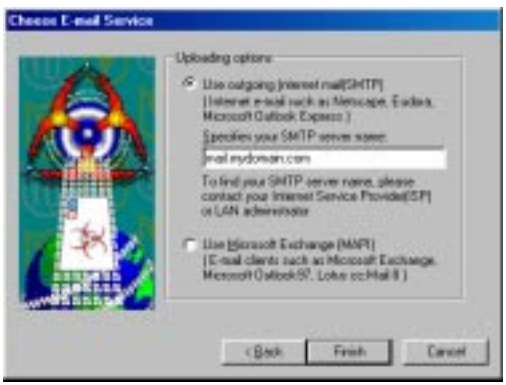

Figure 8-6. A.V.E.R.T. Response Center Choose E-mail Service panel

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.

Scanning Microsoft Exchange and Outlook mail

In addition to the continuous background scanning that VShield provides you with through its E-Mail Scan module, VirusScan includes a full-featured program component designed specifically to look for viruses in your Microsoft Exchange and Microsoft Outlook mailboxes, or on any MAPI-compliant mail server. The E-Mail Scan program component gives you the ability to scan your mail servers at your own initiative, and at times convenient for you. An unobtrusive plug-in architecture gives you access to the scanner from directly within your Exchange or Outlook client application.

If you installed VirusScan with the Typical installation option (see page 35 for details), you already have access to the E-Mail Scan program component.

To use the E-Mail Scan program component with its default settings, simply start your Microsoft Exchange or Microsoft Outlook client software, then

1. Log on to your mail server as you would normally.
2. Choose **Scan for Viruses** from the **Tools** menu, or click  in the Exchange or Outlook toolbar.

- **NOTE:** If you use Microsoft Exchange 5.0, a limitation in the way the program updates its toolbar prevents E-Mail Scan from displaying its buttons immediately. To add the Scan for Viruses button to the toolbar, choose **Customize Toolbar** from the **Tools** menu, then add the E-mail Scan buttons from the list of available buttons in the Customize Toolbar dialog box.

Once you've started it, E-Mail Scan will immediately beginning scanning your Exchange or Outlook mailbox for viruses (see Figure 8-1 on page 186).

By default, E-Mail Scan examines *all* of the mail messages stored in your Inbox on the mail server, looking for attachments susceptible to virus infection. If you have a large number of messages stored there that you have not yet downloaded, this scan operation can take a long time. To pause the operation, click ▮▮. To stop it altogether, click ■. To resume the operation, click ►.

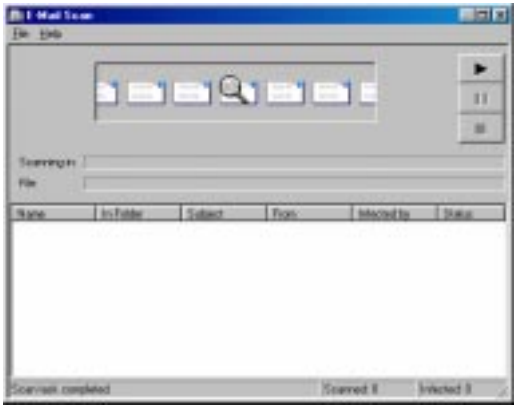

Figure 8-1. E-Mail Scan in progress

If it finds an infected file, E-Mail Scan will ask you how to respond to the virus. See "Responding when E-Mail Scan detects a virus" on page 61 for details.

Configuring the E-Mail Scan program component

Although E-Mail Scan's default settings give you good protection against infections spread via your Exchange or Outlook e-mail, they might not suit your work habits.

To modify E-Mail Scan's configuration options, follow these steps:

1. Start your Exchange or Outlook client software, then log onto your e-mail server.

   - **NOTE:** If you have already logged into the network domain that hosts your e-mail server, you might not need to log into to your e-mail server directly—instead, you can simply start Exchange or Outlook. See your network administrator to learn the log in requirements for your server.

2. Choose **E-Mail Scan Properties** from the **Tools** menu in either program, or click  in the Exchange or Outlook toolbar.

   The E-Mail Scan Properties dialog box will appear (see Figure 8-2 on page 187). The Properties dialog box consists of a series of property pages that controls E-Mail Scan's settings—click each tab to set up the program for your needs.

Figure 8-2. E-Mail Scan Properties dialog box - Detection page

Choosing Detection options

E-Mail Scan initially assumes that you want to scan all e-mail messages stored on your Exchange or Outlook server, and to restrict the files it scans only to those susceptible to virus infection (see Figure 8-2).

To change these settings, follow these steps:

1. Tell E-Mail Scan which e-mail messages you want it to scan. Your choices are:

   - **All messages.** Select this button to have E-Mail Scan look at all messages now stored on your Exchange server. This scan, while thorough, can take a long time if you store your e-mail on the server instead of downloading it to your computer.
   - **Unread messages only.** Select this button to have E-Mail Scan examine only those messages on the server marked "unread." After you scan your entire mailbox, choose this option to speed up scan operations, while maintaining complete anti-virus protection for your computer.

     - **NOTE:** Once you download mail to your computer, VirusScan treats your personal folder or archive file as it would any other file, unless you specifically exclude it from scanning operations. This gives you an added layer of anti-virus security.

2. Tell E-Mail Scan which types of attachments you want it to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have E-Mail Scan look for viruses in attachments compressed in the 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 attachments 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 E-Mail Scan will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 8-3).

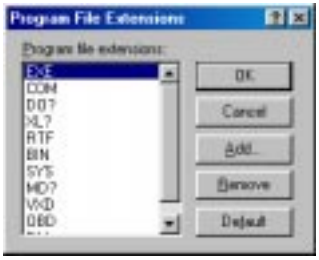

Figure 8-3. Program File Extensions dialog box

By default, E-Mail Scan 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 E-Mail Scan to scan document and template files.

- To add to the list, click **Add**, then type the extensions you want E-Mail Scan 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 E-Mail Scan examine all files on your system, whatever their extensions, select the **Scan all file attachments** 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 8-4).

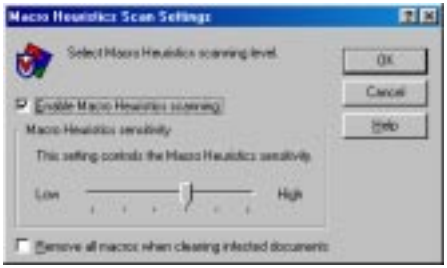

Figure 8-4. Macro Heuristics Scan Settings dialog box

Heuristic scan technology enables E-Mail Scan to recognize new macro viruses based on their resemblance to similar viruses it already knows. To do this, E-Mail Scan 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 E-Mail Scan 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 E-Mail Scan to use when it looks for macro viruses. Drag the slider to the left to set a low level of sensitivity—this causes E-Mail Scan 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. Dragging the slider all the way to the left will turn off heuristic scanning altogether.

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

   Dragging the slider all the way to the right will flag any file that contains macro code as potentially infected.

   • **NOTE:** Higher levels of sensitivity can cause E-Mail Scan 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.

+ **WARNING:** 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 E-Mail Scan Properties dialog box.

3. Click the Action tab to choose additional E-Mail Scan 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 E-Mail Scan 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 E-Mail Scan 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 Properties dialog box to display the correct property page (Figure 8-5).

Figure 8-5. 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 expect to be at your computer when E-Mail Scan 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 file.** This option tells E-Mail Scan to try to remove the virus code from the infected file.

     – **Delete file.** This option tells E-Mail Scan to delete the infected file immediately.

     – **Move file.** This option tells E-Mail Scan to move the infected file to a quarantine folder.

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

     – **Stop scan.** This option tells E-Mail Scan to stop the scan operation immediately. To continue, you must click **Scan Now** to restart the operation.

- **Move infected attachment automatically**. Use this option to have E-Mail Scan move infected files to a quarantine directory named INFECTED. E-Mail Scan will create the INFECTED folder on the Exchange or Outlook mail server.

  You cannot designate a different folder or change the folder's name, but the infected folder will appear under your mailbox folder. You can open the folder and view the message if you wish, but note that doing so could expose your computer to virus infection.

- **Clean infected attachment automatically.** Use this option to tell E-Mail Scan to remove the virus code from the infected attachment as soon as it finds it. If E-Mail Scan 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 196 for details.

- **Delete infected attachment automatically.** Use this option to have E-Mail Scan delete every infected attachment it finds immediately. Be sure to enable its reporting feature so that you have a record of which attachments E-Mail Scan deleted. You will need to restore deleted files from backup copies.

  + **WARNING:** E-mail Scan will *not* try to break any encrypted messages to scan them. If an infected attachment includes a digital signature, E-Mail Scan will *remove* the digital signature in order to clean or delete the infected file.

- **Continue scanning.** Use this option only if you plan to leave your computer unattended while E-Mail Scan checks for viruses. If you also activate the E-Mail Scan reporting feature (see "Choosing Report options" on page 196 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 E-Mail Scan 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 E-Mail Scan look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. If, however, you want E-Mail Scan 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 E-Mail Scan Properties dialog box to display the correct property page (Figure 8-6).

Figure 8-6. E-Mail Scan Properties dialog box - Alert page

2. To tell E-Mail Scan 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 E-Mail Scan 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 E-Mail Scan 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, E-Mail Scan 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 report feature, E-Mail Scan 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 E-Mail Scan 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 have access to a MAPI-compliant user directory. If you are working offline and have not yet logged onto your e-mail system, E-Mail Scan asks you to choose a user profile it can use to log onto your system. 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, E-Mail Scan 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 report feature, E-Mail Scan also logs each instance when it sends an alert message.

5. To have E-Mail Scan 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.

---

6. If you chose **Prompt user for action** as your response in the Action page (see page 192 for details), you can also tell E-Mail Scan 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 E-Mail Scan 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

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

Use the Reports property page to determine which information E-Mail Scan will include in its log file.

To set E-Mail Scan to record its actions in a log file, follow these steps:

1. Click the Report tab in the E-Mail Scan Properties dialog box to display the correct property page (Figure 8-7).

Figure 8-7. E-Mail Scan Properties dialog box - Report page

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

   By default, E-Mail Scan writes log information to the file MAILSCAN.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, E-Mail Scan limits the file size to 100KB. If the data in the log exceeds the file size you set, E-Mail Scan 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 E-Mail Scan to record in its log file. You can choose to record this information:

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

- **Infected file deletion.** Select this checkbox to have E-Mail Scan note the number of infected files it deleted from your e-mail server.
- **Infected file move.** Select this checkbox to have E-Mail Scan note the number of infected files it moved to the quarantine directory on your mail server.
- **Session settings.** Select this checkbox to have E-Mail Scan list the options you choose in the E-Mail Scan Properties dialog box for each scanning session.
- **Session summary.** Select this checkbox to have E-Mail Scan 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 E-Mail Scan append the date and time to each log entry it records.
- **User name.** Select this checkbox to have E-Mail Scan append the name of the user logged in to your e-mail server at the time it records each log entry.

5. Click a different tab to change any of your E-Mail Scan settings. 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**.

Scanning cc:Mail

VirusScan includes native support for later-generation e-mail client software based on Microsoft's MAPI standard, including Microsoft's own Exchange and Outlook clients, and version 8.0 and later of Lotus Development's cc:Mail product. If you use earlier cc:Mail versions—v6.0 or v7.0—you will need to install VirusScan's cc:Mail Scan component to have it look for viruses in your Inbox.

IMPORTANT: To use the cc:Mail Scan component, you must choose the Custom installation option during Setup—VirusScan does not install this component by default. See page 35 for details.

Once installed, cc:Mail Scan logs on to your cc:Mail system, then operates unobtrusively in the background, polling your cc:Mail Inbox to check for new mail. When new mail arrives, cc:Mail Scan calls VirusScan to examine it any infected attachments before your client software takes delivery on your computer.

The only real interaction you will have with cc:Mail Scan is with the login screen it presents to you in order to get access to your cc:Mail server. VirusScan uses your identity and password to log on to the system and scan your Inbox. Enter your cc:Mail user name and password, just as if you were logging directly into cc:Mail, then click **OK** to continue. Next, start your cc:Mail client application, then set the interval for the client to poll your cc:Mail server to a period longer than five minutes. This gives cc:Mail Scan a chance to examine your mail before your client software retrieves it.

The cc:Mail component logs off from your e-mail server when you quit your client software.

Using ScreenScan

VirusScan's ScreenScan component provides you with background virus scanning as your computer's screen saver runs. With it, you can turn otherwise idle computer time to productive use by allowing your machine to check itself for virus infections. ScreenScan will not take any action against viruses it detects, but it will record the results of its scan operations in a log file that you can review at your leisure.

To use ScreenScan, you must choose the Custom installation option during Setup—VirusScan does not install this component by default. See page 35 for details. Once installed, ScreenScan displays a property page in the Windows Display Properties dialog box. Here you can choose the detection and report options that you want ScreenScan to use.

To configure ScreenScan, follow these steps:

1. Click **Start** in the Windows taskbar, point to **Settings**, then choose **Control Panel**.

2. Locate and double-click the Display control panel in the window that appears to open the Display Properties dialog box. Next, click the McAfee ScreenScan tab to display the correct property page (see Figure 8-8 on page 200).

Figure 8-8. Display Properties dialog box - McAfee ScreenScan page

3. Select the **Enable scanning while in screen saver mode** checkbox to activate the options in the rest of the property page.

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

   - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 8-9).

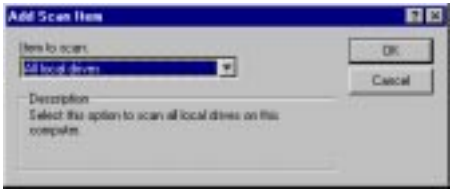

Figure 8-9. The Add Scan Item dialog box

Next, choose the scan target from the list provided. Your choices are:

   – **All local drives.** This tells ScreenScan to scan all drives, both hard disks and floppy disks, either physically attached to your computer or inserted in a floppy drive. This is the safest and most comprehensive option available in ScreenScan.

   – **All fixed drives.** This tells ScreenScan to scan only hard disks physically connected to your computer.

– **Drive or folder.** This tells ScreenScan to scan a particular disk or folder on your computer. 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. Click **OK** to close the dialog box.

> **IMPORTANT:** To scan all of the subfolders in your scan target, be sure to select the **Include subfolders** checkbox in the **What to Scan** area in the ScreenScan property page.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Item to Scan dialog box (Figure 8-10).

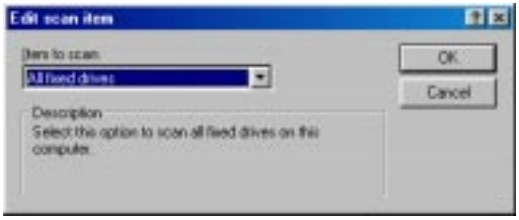

Figure 8-10. The Edit Scan Item dialog box

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 ScreenScan to examine. You can

   - **Scan compressed files.** Select the **Compressed files** checkbox to have ScreenScan look for viruses in files compressed in LZH, WinZip or PKZIP archiving formats.

   - **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 8-11).

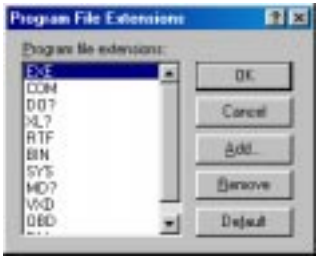

Figure 8-11. The Program File Extensions dialog box

By default, ScreenScan 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 ScreenScan to scan document and template files.

- To add to the list, click **Add**, then type the extensions you want ScreenScan 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 ScreenScan 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.

3. Determine how you want ScreenScan to balance its scan operations against other work priorities for your computer. Click **Advanced** to open the Advanced Scanner Settings dialog box (Figure 8-12).

Figure 8-12. Advanced Scanner Settings dialog box

Drag the slider to the left to give ScreenScan a lower priority relative to other programs running on your computer—including your screen saver. This causes ScreenScan to take longer to scan your system, but allows your other programs to run smoothly. Drag the slider to the right to give ScreenScan a relatively high priority for its scanning tasks. It will complete its scan operation more quickly, but other programs running at the same time will not run as smoothly.

4. Enable ScreenScan's report feature.

   Select the **Enable logging of ScreenScan activities to file** checkbox. By default, ScreenScan records its actions in a text file named SCREENSCAN ACTIVITY LOG.TXT. To choose a different text file to use as ScreenScan's report file, enter its path and file name in the text box provided, or click **Browse** to locate a suitable file on your hard disk.

   - **NOTE:** ScreenScan does not create new report files. To have the program use a different log file, you must choose an existing text file that ScreenScan can open and write to.

   Click **OK** to save your changes and close the dialog box. To close the dialog box without saving your changes, click **Cancel**.

5. To have ScreenScan start scanning from the point at which it left off when interrupted, select the **Resume Scanning where ScreenScan left off** checkbox. If you do not select this checkbox, ScreenScan will begin its scan operation with the first item listed in your chosen scan target, whether or not it has already completed a scan operation on that target.

6. Click **Apply** to save your changes without closing the Display Properties dialog box. 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.**

ScreenScan will run the next time your current screen saver does. If you change screen savers, you should reconfigure your ScreenScan options also.

Using Safe & Sound 9

The most important asset on your computer is the information, or *data*, you create and store there. Over time, this data grows in size and value. The storage devices where you keep this information are vulnerable to a wide range of environmental and human factors that can damage or destroy all or part of the data stored there.

Valuable and vulnerable disk organizational structure information is also stored in various places on a hard drive. This includes the boot sector, partition tables, directories, the FAT (file allocation table), and other structural components. These structural components are used by Windows to find data on the drive, organize it, and so on. If any one of these components is damaged or destroyed, you will not be able to access the data you've stored on the drive.

The FAT, your drive's roadmap, points to the locations where your files are physically stored on the drive. Files can either be stored in contiguous locations or scattered in pieces in different places. Since files are not always stored contiguously, the FAT information becomes even more indispensable than if files were stored one after another, end to end. If a drive's file allocation table becomes corrupt or scrambled (such as may be caused by a virus), your computer will be unable to find and assemble all the pieces of your files. This is true even if all the files' data still exists.

Protected Volume Files (The Ultimate Backup Protection)

McAfee Utilities' Safe & Sound lets you create backup sets in protected volume files, which is the safest and preferred type of backup, and is unique to McAfee Utilities. A *protected volume file* is a sectioned-off area of the drive, sometimes called a logical drive. Safe & Sound's protected volume files have some very special characteristics that let Safe & Sound reconstruct backup files sector by sector, even if the drive's standard FAT is damaged or completely lost. In fact, files can be largely reconstructed even if large parts of the drive are unreadable or erased.

The protected volume file also includes enough information in each directory entry to completely reconstruct a file's entire directory tree even if all its parent nodes are erased.

Safe & Sound provides internal redundancy in the protected volume file backups you create. It does this by marking each sector of each file that it backs up with identifying information about the sector's contents and the file that sector belongs to. Each sector in a protected volume file contains enough information to allow files to be reconstructed from their individual sectors.

Why You Should Make Regular Backups With Safe & Sound

Your data is very valuable and costly to recreate. This means that making frequent or even mirror backup copies of the important data on your drives is *crucial*. A *mirror* backup copy is always identical to the original information on the source drive.

Safe & Sound automates the back-up process, doing the time-consuming and repetitive work for you. It lets you decide which types of files to back up, how often to save them, and where you want the backup set located (on the same drive, another local drive, or on a shared network drive). With Safe & Sound, you can create mirror backup sets that are, at any given time, an exact replica of the files you've selected to back up on the source drive. You can also specify a short time delay in the backup, or back up manually by copying files to the backup set on your drive if you prefer.

All forms of data storage are susceptible to losing the information they hold. The most common types of data storage—hard drives, 3.5-inch disks, ZIP disks or SyQuest tapes—are often called *permanent storage* (thus differentiating them from the volatile storage in your computer's RAM, random access memory). Permanent storage means the information remains intact even when you turn off your computer. Permanent storage does not mean *eternal* storage.

Many things can cause the data on disks, tapes or drives to become garbled or lost: hardware malfunctions, worn out media, electrical storms, excessive heat, static electricity, magnets, loose cable or power cord connections, and so on. CD discs, though durable, can become scratched enough to damage their data. Human actions can also cause lost data, such as deleting the wrong folder or formatting the wrong drive. Even a well-designed application can sometimes cause its own files to become corrupt.

With so much at risk, you have everything to gain by letting McAfee Utilities' Safe & Sound automatically make backup copies for you. You simply decide what information is important to you, how you want it to be backed up, and where you want the backup copy to be stored. Safe & Sound takes care of the rest!

How Safe & Sound Creates Automatic Backups

When you select to have Safe & Sound automatically create a backup set for you, it creates the first backup set while you are stepping through the Safe & Sound Wizard. Thereafter, while the Enable Automatic Backup option is selected, it continues to update your backup set at the time delay you've specified. If you chose to make Mirror backups, Safe & Sound updates your backup set at the same time that you resave the original source files.

If you select a write-behind delay longer than zero seconds (a Mirror backup), Safe & Sound updates the backup set at any time after the specified time delay when your PC is idle. This allows Safe & Sound to work in the background so that it does not interrupt the work you are doing. This is a good option to use with the protected volume file backup type since it eliminates any speed loss due to more frequent disk accesses and larger file sizes associated with the protected volume file backup type.

Defining Your Backup Strategy

After you decide which backup type you want to use (either a protected volume file or a directory backup set), the most important questions you must answer when defining your own backup strategy are:

- Where will you store the backup set?
- What files are important (which files must be backed up)?
- How often should you or Safe & Sound make these backups?

Where Will You Store the Backup Set?

If the survival of your business depends upon your PC being up and running at all times (and if money is not an object), the ultimate way to protect the data on your PC would be to set up a redundant PC with identical sized drives. This backup PC's only job would be to mirror the data on your primary PC. It would be waiting in the wings should your first PC fail for any reason. And if that happened, you could simply switch your work to the second PC while the first one is repaired.

Often money is a consideration in deciding where you'll store your backup sets. The least expensive way of making backups has traditionally been to copy data to 3.5-inch disks, though this is the most labor intensive way of storing backups because it requires you to switch disks by hand.

In today's computer marketplace, you may discover that it is as cost effective to acquire a separate backup hard drive where you can keep a current mirror backup copy of one or more other drives that you use on your PC.

In addition, you may want the backup copy to be stored at a remote location, for increased protection. As long as Safe & Sound can access a logical drive mapped on your PC, it can store the backup set there. That is, the backup set can be stored on a shared network drive.

- **NOTE:** You can use the Map Network Drive command, available by Right-clicking My Computer, to assign (map) a drive letter to a location on a network drive. This makes that location a “logical drive” on your PC. For more details, see your Windows online Help.

Even if you cannot invest in another drive or disks for storing your backups, you can still create a backup copy of your data on the same drive. This offers the least protection should that drive fail, but the potential for data recovery is increased by having two sets of your most important information stored there. It is further enhanced if you select the protected volume file backup type, which allows recovery in many circumstances even with the drive physically damaged.

- **NOTE:** If your data usually resides on a server, you can make a local copy so you can access data even when the server goes down.

What Files are Important to You?

Safe & Sound automatically selects files that are typically important to include in a backup set. However, you can select other files or types of files to include in your backup set.

In addition, you can create multiple backup sets of data for particular purposes. Each of these backup sets can be created when and where you specify. They can each include exactly the files or types of files that you choose. For example, you might create individual backup sets for each of your clients if you produce data for clients that is stored on your computer, such as advertising layouts, graphic images, books, or accounting data.

How Often Should You or Safe & Sound Make Backups?

The more recent your backup set, the happier you’ll be if your PC does encounter a problem that compromises the data on your primary drives. However, you may want to keep the default Write-behind Delay of 20 minutes to give you time to recover a previous version of a file if you ever need to.

I **TIP:** Save early, save often. While working in applications, you can almost always press **CTRL-S** to save your work as you go. The more often you save your work, the less you have to lose at any given point in time. You may also want to be sure the auto-save option is selected in your applications for more frequent backups.

Creating a Backup Set

Creating a backup set, either manually or to be updated automatically, in Safe & Sound is very easy. Safe & Sound's default choices should work fine, though you may want to add additional folders or file types to your backup list.

To create a backup set:

1. Start the VirusScan Console.
2. Click **Options**, point to Tools, and click **Safe & Sound**. The first panel of the Safe & Sound Wizard appears (Figure 9-1).

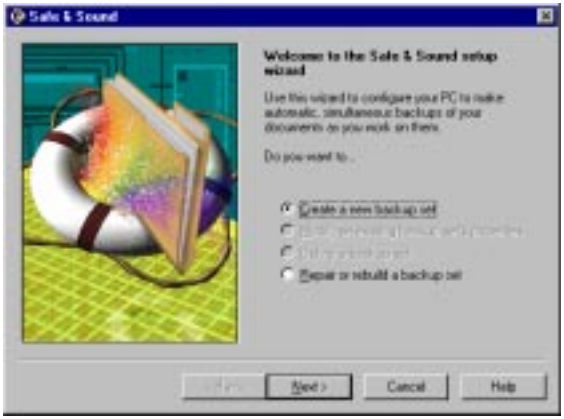

Figure 9-1. Safe & Sound: First Wizard Panel

3. Select Create a New Backup Set and click **Next >**. The second panel of the Safe & Sound Wizard appears.
4. Select whether to back up to a Protected Volume File or a Directory. Then click Next >.

   Protected Volume File–The Protected Volume File is the preferred backup type. A protected volume file is a sectioned off portion on the drive. It has special characteristics to ensure that even if organizational structures, such as the file allocation table on the drive is corrupted or lost, or the data becomes scrambled, the files in the backup set can be reconstructed. Safe & Sound stores extra information (in each sector for each file and also in a separate directory) to provide this level of protection. For details, see <xref>Protected Volume Files (The Ultimate Backup Protection) on page 205.

- **NOTE:** You can copy files into a protected volume file manually using My Computer or Windows Explorer to add them to your backup set and instantly protect them.

There are two drawbacks to using a protected volume file backup type. The first drawback is that three percent more storage space is required for the extra information that will be used to reconstruct the files in the event of a problem. The second drawback is that a protected volume file is slightly slower because it has to manipulate more information in more areas on the disk and more disk accesses are required. This is a marginal performance degradation, which you can eliminate by also selecting a Write-behind Delay of seconds or minutes.

Directory–The Directory backup type makes another copy of the files and directories selected for backup in a different location. This type of backup creates no performance drain on the system and it's simple to manage the backup area. You can use My Computer or Windows Explorer to cut or copy files in or out of the backup location or delete the files. The drawback of selecting a directory backup type is that the files are no more protected than if you had created a backup copy yourself.

The third panel of the Safe & Sound Wizard appears.

5. Specify the target destination where the backup set will be created and click Next >.

   The fourth panel of the Safe & Sound Wizard appears.

6. Click the Settings button if you want to customize any of the settings for this backup set.

   Volume Settings

   - **Backup Type**–Displays the currently selected backup type (Protected Volume File or Directory).
   - **Enable Automatic Backup**–While this check box is selected, Safe & Sound automatically updates this backup set as you update the files it contains based on the time delay you specify.
   - **Name of Backup Set**–If you are saving this backup set to a non-Windows 95/98 or NT drive (such as to a UNIX server on your network) be sure to follow the 8.3 naming convention for this name.

- **Backup Delay**–Select the Mirror (0) write-behind delay if you want your backup set to remain in constant synchronization with the original files as you change them. Select a write-behind delay in seconds or minutes if you want your backup to be created during times when your PC is idle starting at any time after the time delay you select.

  A write-behind delay in seconds or minutes is recommended if you are using the protected volume file backup type and want to eliminate the slight speed reduction caused by extra disk accesses in more locations on the drive.

- **View Drive As**–(*available only for backup sets stored as a Protected Volume File*). The drive letter you want to use for the Protected Volume File backup set.

- **Keep Deleted Files For**–Select how long you want the backup set to keep files whose original counterparts have been deleted from your system.

- **Limit Size of Backup Volume**–Drag the slider left to reduce the backup volume size limit or right to increase the backup volume size limit.

Drives

Drive and Directory Folders appear in the Backup Drive list so you can select any of the ones you want to add to your backup set. Click folders to open and close them. Click the check boxes to place a check mark beside the drives or directories that you want to back up.

File Types

You can select groups of files that you want to include in your backup set by selecting their file type. The file type, such as TXT (for a text file), indicates the file's purpose. Safe & Sound displays a list of all the registered file types in Windows 95/98. The file types with check marks show the types of files that will be included in your backup set.

Safe & Sound obtains its list of registered file types from Windows. You can view or add registered file types in My Computer or Windows Explorer.

If you are not yet familiar with file types and want to see them, you can open My Computer or Windows Explorer, choose the Options command from the View menu, and click the File Types tab.

In the Options dialog box you can examine the list of the registered file types on your system. These are the file types that will be available to you in Safe & Sound. You can add new registered file types in the Options dialog box to make them available to Safe & Sound the next time you run it.

Many file types are standard, such as BMP and PCX which are used by paint applications like Microsoft Paint, or TIF which is a standard file type for TIFF graphic images. Each application's documents typically have a file type (which may or may not be registered in Windows). For example, Microsoft Word documents may be stored using registered file types of DOC, RTF or TXT, depending on the file type selected when saving the document.

- **NOTE:** You can also view file types directly in My Computer or Windows Explorer. Choose the Options command from the View menu, click the View tab, and make sure the HIDE MS-DOS FILE EXTENSIONS FOR FILE TYPES THAT ARE REGISTERED check box is deselected. Registered file types are also listed in the File Types tab in the Options dialog box. The other place where file types appear is in the Save As dialog box of Windows applications.

---

7. To apply the changes, click **Apply**. When you are finished, click **OK**. The fifth panel of the Safe & Sound Wizard appears.
8. Enter a backup volume name and click **Next >**. Safe & Sound begins backing up files.
9. When it is finished, click **Finish**.

Restoring Files from a Backup Set

If you encounter a problem with the information on your drive, you can restore one or more of the files in your Safe & Sound backup sets.

- **NOTE:** Unless you create a backup set containing the entire contents of a drive, you *should never* drag and drop or copy / paste the contents of a Safe & Sound backup set's <drive letter> folder into a drive icon or window. Though the folder names match between a Directory type backup set and the folders on the drive, the files inside are most likely very different. By default, Safe & Sound only backs up files it considers essential, such as INI, TXT, RTF, DOC and WRI files. It backs them up using the original hierarchical directory structure from the source drive. You will know where to restore each file, if you need to, based on its location in the backup set. It does not automatically back up application or DLL files, nor does it back up the Windows directory without your explicit instructions to do so.

I **TIP:** You can use the bootable disk created by Rescue to restore files from a backup set located on a damaged drive.

To restore a backup set:

1. Open Windows Explorer or My Computer and open the backup set.

   If the backup set is a Directory type backup, the folder name (by default) is Backup_1, Backup_2, and so on. If the backup set is a Protected Volume File, it is located at the same level as your physical drives.

2. Find the files to restore and use Drag and Drop or Copy / Paste to copy files from your backup set to the location where you want them.

Modifying or Deleting Backup Sets

You can modify the properties for a backup set, or delete backup sets using Safe & Sound. If you created a backup as a protected volume file, you can only delete it using Safe & Sound.

Modifying an Existing Backup Set

To modify a backup set:

1. Click the Start button and do one of the following:

   - Choose the McAfee Utilities command from the Start menu and click the Safe & Sound button.
   - Choose the Programs > McAfee Utilities > Safe & Sound command.

2. Select the backup set to modify and click the Properties button.
3. Change the settings and click OK when you are done. Click Finish.

Deleting a Backup Set

If you created a Safe & Sound backup set as a protected volume file, you cannot delete it in My Computer or Windows Explorer. You can *only delete the protected volume file* using Safe & Sound.

If you created a Safe & Sound backup set as a directory, you should still delete it using Safe & Sound; however, you can also delete the backup directory via My Computer or Windows Explorer.

To delete a backup set:

1. Start Safe & Sound.
2. Click Next > while the Delete a Backup Set radio button is selected.
3. Select the backup set to delete and click Finish. Then click Yes to confirm the deletion.

Repairing and Rebuilding a Backup Set

If you encounter a problem with the backup set itself, you can repair or rebuild it. For example, if your computer crashes while the backup is being created or updated automatically, the backup's contents may be incomplete or damaged. Safe & Sound automatically checks the backup's integrity when you start Windows. If it is damaged, Safe & Sound starts and asks if you want to repair the backup set.

To repair or rebuild a backup set:

1. Start McAfee Utilities' Safe & Sound and click Next > while the Repair or Rebuild Backup Set radio button is selected.
2. Do one of the following:
   - Click the Repair button and click Next > if you can see the backup set in My Computer or Windows Explorer, but the information is somehow damaged. For example, if a backup was not finished due to a power outage or computer crash.

- Click the Rebuild button and click Next > if you can no longer see the backup set (for example if the protected volume file is no longer visible in My Computer or Windows Explorer).

- **NOTE:** Performing a Rebuild is a time-consuming process because Safe & Sound searches your entire system to find all backup sets that are stored there.

---

3. Select the drives that contain a protected volume file you want to restore. Then click Next >.

   The Restore utility searches the selected drives for protected volume files or backup directories. If it finds a protected volume file, a message appears asking if you want to Save As, Ignore, or Ignore All.

4. Click the Save As button and select where you want the restored volume file to be placed. Then click Save.

Product Support A

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

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

How to Contact McAfee

Customer service

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

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

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

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

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

To inquire about a promotion: mcafeepromotions@beyond.com

Technical support

Support via the web

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

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

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

Support forums and telephone contact

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

Table A-1.

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

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

Table A-1.

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

McAfee training

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

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

Download Information (License ID #: VSF500R) B

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

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

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

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

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

Internet Access

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

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

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

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

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

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

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

Index

C

D

E

F

N

O

P

Q

R

S

T

U

V

W