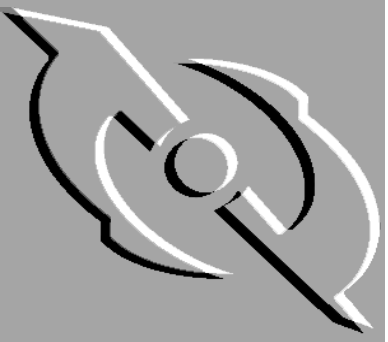

VirusScan for OS/2

User's Guide

Version 4.0.2

COPYRIGHT

LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

6. **Warranty and Disclaimer**

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

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

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

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

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

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

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

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

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

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”). Network Associates 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. The Agreement set forth here is advisory in nature and does not supersede the provisions of any Agreement set forth in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the README.1ST or the LICENSE.TXT document, the text document will constitute the terms of your license grant to use the Software. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Network Associates. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Network Associates or a duly authorized representative of Network Associates. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

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

Table of Contents

Preface

What happened?

If you've ever lost important files stored on your hard disk, watched in dismay as your computer ground to a halt only to display a prankster's juvenile greeting on your monitor, or found yourself having to apologize for abusive e-mail messages you never sent, you know first-hand how computer viruses and other harmful programs can disrupt your productivity. If you haven't yet suffered from a virus "infection," count yourself lucky. But with more than 24,000 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 small proportion 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 cost 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 "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. Some estimates have placed the total worldwide cost in time and lost productivity for merely 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 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. As further catalyst, 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 virus 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. Many Network Associates anti-virus products anticipate 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 other vendors, 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. But most existing anti-virus software easily kept pace with updates that detected and disposed 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, the 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.

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. The chat client sends script viruses as plain text, which would ordinarily preclude them from infecting systems, 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

Network Associates anti-virus software 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. Anti-virus software, moreover, is only as good as its latest update. Because as many as 200 to 300 viruses and variants appear each month, the data (.DAT) files that enable Network Associates software to detect and remove viruses can get quickly outdated. If you have not updated the files that originally came with your software, you could risk infection from newly emerging viruses. Because Network Associates has assembled the world's largest and most experienced anti-virus research staff within its McAfee Labs division, however, the updated files you need to combat new viruses appear as soon as—and often before—you need them.

Most other security 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. Network Associates anti-virus software distributions include VALIDATE.EXE, a verfication utility, to prevent this type of manipulation. Neither it nor any anti-virus software, however, can detect when someone substitutes an as-yet unidentified Trojan horse or other malicious program for one of your favorite shareware or commercial utilities.

Web and Internet access poses its own risks. 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.

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

How to contact Network Associates

Customer service

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

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

Technical support

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

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

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

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

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

For corporate-licensed customers:

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

For retail-licensed customers:

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

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

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

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

Network Associates training

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

Comments and feedback

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

Reporting new items for anti-virus data file updates

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

virus_research@nai.com	Use this address to send questions or virus samples to our North America and South America offices
vsample@nai.com	Use this address to send questions or virus samples gathered with Dr Solomon's Anti-Virus Toolkit software to our offices in the United Kingdom

To report items to our European research offices, use these e-mail addresses:

virus_research_europe@nai.com	Use this address to send questions or virus samples to our offices in Western Europe
virus_research_de@nai.com	Use this address to send questions or virus samples gathered with Dr Solomon's Anti-Virus Toolkit software to our offices in Germany

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

virus_research_japan@nai.com	Use this address to send questions or virus samples to our offices in Japan and East Asia
virus_research_apac@nai.com	Use this address to send questions or virus samples to our offices in Australia and South East Asia

International contact information

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

Network Associates Australia

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

Network Associates Austria

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

Network Associates Belgium

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

Network Associates do Brasil

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

Network Associates Canada

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

Network Associates People's Republic of China

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

NA Network Associates Oy

Sinikalliontie 9, 3rd Floor
02630 Espoo
Finland
Phone: 358 9 5270 70
Fax: 358 9 5270 7100

Network Associates France S.A.

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

Network Associates Deutschland GmbH

Ohmstraße 1
D-85716 Unterschleißheim
Deutschland
Phone: 49 (0)89/3707-0
Fax: 49 (0)89/3707-1199

Network Associates Hong Kong

19th Floor, Matheson Centre
3 Matheson Way
Causeway Bay
Hong Kong 63225
Phone: 852-2832-9525
Fax: 852-2832-9530

Network Associates Srl

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

Network Associates Japan, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku
Tokyo 105-0001 Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0780

Network Associates
Latin America

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

Network Associates
de Mexico

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

Network Associates
International B.V.

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

Network Associates
Portugal

Av. da Liberdade, 114
1269-046 Lisboa
Portugal
Phone: 351 1 340 4543
Fax: 351 1 340 4575

Net Tools Network Associates
South Africa

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

Network Associates
South East Asia

78 Shenton Way
#29-02
Singapore 079120
Phone: 65-222-7555
Fax: 65-220-7255

Network Associates
Spain

Orense 4, 4ª Planta.
Edificio Trieste
28020 Madrid
Spain
Phone: 34 91 598 18 00
Fax: 34 91 556 14 04

Network Associates
Sweden

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

Network Associates AG

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

Network Associates International Ltd.

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

Network Associates Taiwan

Suite 6, 11F, No. 188, Sec. 5
Nan King E. Rd.
Taipei, Taiwan, Republic of China
Phone: 886-2-27-474-8800
Fax: 886-2-27-635-5864

Introducing VirusScan for OS/2 1

What is VirusScan?

VirusScan for OS/2 is the first complete scanning package for the OS/2 environment. This version of VirusScan combines its new graphical interface version of VShield, the on-access scanner, with an updated on-demand scanner to provide you with complete and powerful anti-virus protection for your OS/2 desktop.

In today's computing world, 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.

System Requirements

VirusScan for OS/2 runs under both Warp 3 and Warp 4. The system requirements below list the particular configurations necessary to run VirusScan under each OS/2 version.

WARP 4:

To install and run VirusScan for OS/2 on Warp 4 systems, your computer must:

- Run OS/2 Warp 4 with IBM's Security Enabling System component installed and enabled.

> **NOTE:** Please see "SES enabling" on page 7 for details on SES.

- Have OS/2 FixPak 4 or later installed.
- Have a minimum of 16MB of RAM.
- Have at least 5MB free disk space.
- FAT16 or HPFS partition.

WARP 3

To install and run VirusScan's VShield component on Warp 3 systems, your computer must:

- Run OS/2 Warp 3 with the Security Enabling System (SES) component installed and enabled.
- The SES component, in turn, requires OS/2 FixPak 17 (XR_W017). (You can obtain both SES and FixPak 17 from IBM, or download it from the IBM website at ftp://ftp.software.ibm.com.)

> **NOTE:** If you have FixPak versions later than FixPak 17 installed, you must remove them, install FixPak 17 and the SES FixPak, then reinstall later-version FixPaks in order to correctly enable SES.

- Have OS/2 FixPak 26 or later installed. You must install FixPak 26 or any later FixPak *after* you install the SES component. You can obtain the necessary FixPak software from IBM, or download it from the IBM website at ftp://ftp.software.ibm.com.

What comes with VirusScan?

Files included in your copy of VirusScan for OS/2 include:

- **VirusScan.** VirusScan's new engine, created and backed by the combined efforts of the McAfee Labs and Dr Solomon anti-virus research teams, is at the heart of this powerful on-demand scanner. Use the updated graphical user interface to initiate a scan operation at any time. You can specify local and network drives as scan targets, choose how VirusScan will respond to any infections it finds, and see complete reports on its actions. See Chapter 4, "On-Demand Scanning," page 27, for details.

- **OS2SCAN.EXE**, the command line on-demand scanner for the OS/2 environment. Ordinarily, you'll use VirusScan's graphical user interface (GUI) to perform most scanning operations, but if you have trouble getting to the OS/2 desktop, or prefer to initiate on-demand scans from the command line, use OS2SCAN.EXE. See Chapter 5, "On-Demand Scanning at the Command Line," page 37, for details.

- **VShield.** This component gives you continuous anti-virus protection from viruses borne on floppy disks, brought in from your network, or loaded into memory. VShield starts when you start your computer, and stays in memory until you shut down. A flexible set of property pages allows you to tell VShield what parts of your system to scan, when to scan them, which to leave alone, and how to respond to any infected files it finds. In addition, VShield can alert you when it finds a virus, and can generate reports that summarize each of its actions. Chapter 3, "On-Access Scanning," page 19, for details.

- **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.

- **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 most basic scan operation.

  - 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 3.0.2 —Reader version 3.0.1 has difficulty correctly printing graphics included in the .PDF file.

– An online help file.

– A WHATSNEW.TXT file. This file contains last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and often describes new product features incorporated into incremental product updates. You'll find the WHATSNEW.TXT file at the root level of your VirusScan CD-ROM—you can open and print it from the OS/2 View program, 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 access a floppy disk in 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.

If you suspect you have a virus...

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

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

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 VirusScan for OS/2 2

Before you install

Congratulations! You have chosen VirusScan for OS/2, the most complete virus protection available for the OS/2 platform. In this chapter you will find details on installing the complete VirusScan for OS/2 package, which will allow you to manage on-access scan tasks through VShield's native OS/2 user interface, and handle on-demand scans via an easy-to-use user interface, or at the command line.

The three components you may install are:

- **VirusScan for OS/2,** the user interface and command-line on-demand scanners
- **VShield for OS/2,** the on-access scanning module
- **Enable SES,** which prepares your system for using VShield.

Installation options

There are situations where not every component of VirusScan for OS/2 needs to be installed on a system. For example:

You may not need to enable SES
While most users will elect to install all components, you may not need all of them. If you are certain you are already running SES on your system, you will not need to re-enable the SES components.

You don't have SES components installed
If you do not have SES installed, and have no plans to do so, your system will not be able to run VShield. You may still, however, install all the program files necessary for on-demand scanning, by selecting the VirusScan for OS/2 component only.

SES enabling

IBM's Security Enabling Services (SES) are a set of extensions to the OS/2 operating system that VShield uses in order to gain the full file access it needs to scan properly. You can select the VirusScan component which enables SES at installation (Step 5 on page 9), or directly edit the CONFIG.SYS file to enable SES. Directions for editing the CONFIG.SYS can be found in Appendix C, "SES Enabling," page 77.

There are two important issues surrounding SES enablement and the installation of VirusScan. **It is critical that the status of SES on a system is correctly ascertained prior to installing VirusScan.**

First, it is your responsibility to determine if SES is installed on a system prior to installing VirusScan. This is because VirusScan's INSTALL.EXE has no way of determining if SES is installed prior to beginning to enable SES.

By not being clear on the status of SES, and proceeding with the installation, you run the risk of possibly destabilizing your system by attempting to enable components that do not exist.

Please refer to your IBM documentation for full details on OS/2 operating systems and the SES extensions. (Information is also available at the IBM website, http://www.software.ibm.com/os/warp.)

Installing VirusScan

After ensuring that your computer meets the system requirements for running VirusScan, complete the instructions below to install VirusScan on your system.

To install VirusScan for OS/2, complete these steps:

1. Verify that the SES components (see "SES enabling" on page 7) are already installed on your computer.

   WARNING: Attemping to enable SES when the SES extensions are not, in fact, installed could corrupt your system.

2. Complete either of the following steps, depending on the media you are installing from:

   - Insert the compact disc with your copy of VirusScan for OS/2 into your CD-ROM drive.
   - If you downloaded a compressed copy of VirusScan for OS/2 from the Network Associates website or other electronic service, create a temporary directory on your hard disk or on a disk available on your network, then extract the files you downloaded into that directory.

3. Complete either of the following:

   - Click the drive icon from the OS/2 desktop. When the folder opens, click the INSTALL.EXE icon from the folder.

- **If you extracted files that you downloaded** to your hard disk or to a disk on your network, be sure to specify the path to the correct directory. For example, type:

  `C:\DOWNLOAD\INSTALL.EXE.`

4. The VirusScan installation will begin with the **Welcome** page (Figure 2-1). Click **Continue** to proceed with the installation.

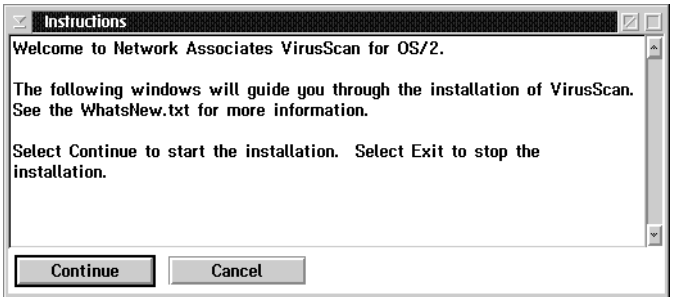

Figure 2-1. Install - Instructions page

5. Select the components you want to install at the **Install - directories** page (Figure 2-2 on page 10) by clicking **Select all.** To view descriptions of the components, highlight the component's name, and click **Descriptions**

   By default, the program files will be installed to C:\NETA\VSCANOS2. If you prefer Install to use a different location, enter the location you want the VirusScan for OS/2 components installed to in the **File directory:** text box.

TIP: If you need to check available disk space before finalizing your installation decision, click **Disk Space.** You will be told of the space available on the drive currently listed in the **File Directory** text box.

Figure 2-2. Install - directories page

6. When you have finalized your installation choices, click **Install.** The installation will begin, and the **Install - progress** page (Figure 2-3), will open.

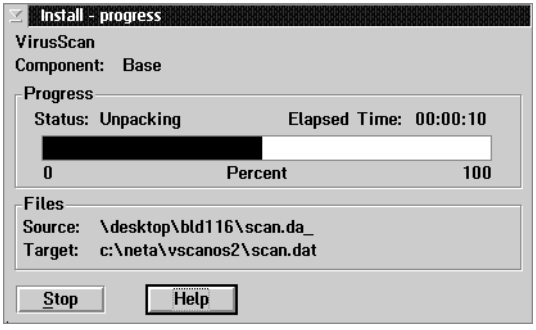

Figure 2-3. Install - progress page

7. The status bar on the **Install - progress page** shows the percentage of the installation which has been completed. The page also lists:

   - which VirusScan component is being installed at any given time
   - the source of the program file currently being installed
   - the target directory of the program file being installed.

To stop the installation at any time, click **Stop.**

8. VirusScan will notify you when the installation is complete by displaying the **Installation completed** page (Figure 2-4). Click **OK** to close this page.

   As with most programs new to your system, you will need to reboot immediately following installation to properly use VirusScan.

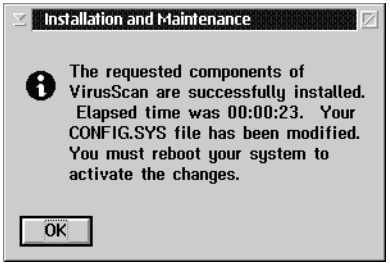

Figure 2-4. Installation completed page

Uninstalling VirusScan

You can uninstall either the entire VirusScan for OS/2 program, or selected components.

To uninstall VirusScan, follow these steps:

1. Open the folder where VirusScan is installed. (VirusScan installs this folder to the OS/2 desktop by default.)

2. Double-click the UNINSTALL.EXE icon. The Uninstall utility will open. (See Figure 2-5.)

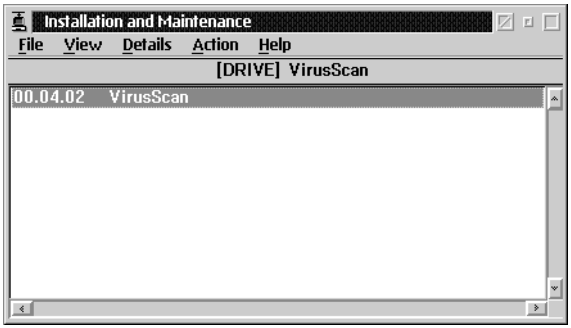

Figure 2-5. First Uninstall page

3. VirusScan is already displayed and highlighted in the window. To begin uninstalling the program, Select **Delete** from the **Action** menu. The **Delete** page (Figure 2-6) opens.

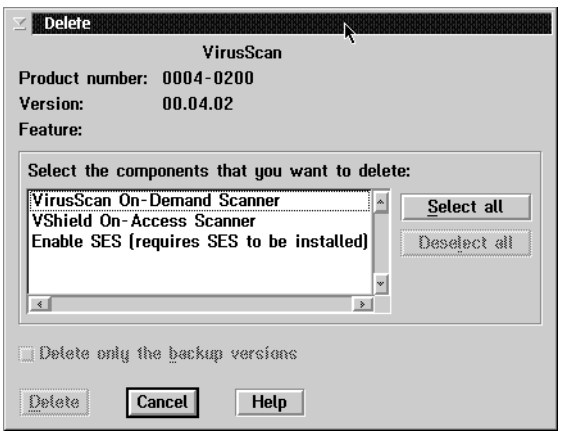

Figure 2-6. Delete page

4. If you want to delete all VirusScan components, click **Select all.** If you only want to delete selected components, click on the name of the component(s) you want to delete.

5. Click **Delete.** The components you have selected will be deleted. You will be notified when the uninstall utility has finished.

Keeping the .DAT files current

What are .DAT files?

DAT files contain up-to-date virus signatures and other information that Network Associates anti-virus products use to protect your computer against the thousands of computer viruses in circulation. New .DAT files are released regularly to provide protection against the 200 to 300 new viruses that appear each month. To ensure that you are protected against the latest virus threats, download and install the latest .DAT files.

The 4009 .DAT files included with this release of VirusScan for OS/2 are compatible with Network Associates anti-virus products that use scan engine versions 4.0.xx only. These .DAT files will NOT work with v3.x or v2.x scan engines.

Why would I need to update my data files?

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

As a registered user, you can continue to receive .DAT file updates for the life of your product. Network Associates cannot, however, guarantee compatibility between future .DAT file updates and older product versions. By keeping both your copy of VirusScan for OS/2 and the .DAT files current, you ensure complete virus protection for the term of your software subscription or maintenance plan.

Updating the .DAT files

VirusScan for OS/2 needs to be kept current with the latest Virus Definition Files (.DAT files) in order to keep your system efficiently protected from the network to the desktop. New viruses and other harmful agents appear at a rate of more than 200 per month—don't risk letting your data disintegrate or your network become inaccessible simply because you forgot to update these files.

Updating the .DAT files is a three-step process:

- The .DATs need to be downloaded to a temporary directory, and unzipped (see page 13).
- VShield needs to be disabled (see "Disabling VShield," pages 14 to 15)

- The three .DAT files which VirusScan for OS/2 uses need to be copied to the \NETA (or other installation) directory (see pages 15 to 16).
- VShield must be enabled.

Disabling VShield

Since VShield uses the .DAT files in its continuous on-access scanning activities, it must be disabled in order for you to successfully update the .DAT files. It is not possible to update a data file which is in use.

VShield can be temporary disabled by editing the CONFIG.SYS and SECURE.SYS files.

To disable VShield, follow these steps:

1. Locate the CONFIG.SYS file on your system. It can be found in the root directory of the OS/2 boot drive.
2. Open the CONFIG.SYS with OS/2's editing program "E" by typing,

   ```
   E CONFIG.SYS
   ```

   at the command prompt. The CONFIG.SYS file is displayed.
3. Type the letters REM followed by a single space before the following two lines in the CONFIG.SYS file. These should be at or close to the end of the file.

   ```
   BASEDEV=VSHIELD.FLT
   RUN=C:\NETA\VSCANOS2\GDDAEMON.EXE
   ```

   NOTE: These examples assume VirusScan was installed to the default installation directory of \NETA\VSCANOS2. If you selected a different installation directory, the alternate location will be reflected in your system's CONFIG.SYS file.
4. Save these changes by selecting **Save** from E's **File** menu.
5. Close the edited CONFIG.SYS by clicking on the Close Window icon in the upper right corner of the toolbar.
6. Locate the SECURE.SYS file on your system. This can be found in the \OS2\SECURITY\SESDB directory on the OS/2 boot drive.
7. Open the SECURE.SYS with OS/2's editing program "E" by typing,

   ```
   E SECURE.SYS
   ```

   at the command prompt. The SECURE.SYS file is displayed.

8. Type the letters REM followed by a single space before the following two lines in the SECURE.SYS file .

```
C:\NETA\VSCANOS2\GDDAEMON.EXE  /SCA='OS2GUARD'  /SPA
/LOCALUSER=NO
C:\NETA\VSCANOS2\CRYER.EXE  /SCA='OS2GUARD'  /SPA
/LOCALUSER=YES  /START
```

9. Save these changes by selecting **Save** from E's **File** menu.
10. Close the edited SECURE.SYS by either clicking on the Close Window icon in the upper right corner of the toolbar.
11. Reboot your system. VShield is no longer active.

Updating the .DAT files

To update the .DAT files:

1. Download the latest .DAT files from any of these four electronic sources:
   - **WWW:** http://www.nai.com/download/updates/updates.asp
   - **FTP:** ftp.nai.com/pub/antivirus/datfiles
   - **CompuServe:** GO McAfee
   - **AOL Keyword:** McAfee

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

2. Unzip the .DAT file into a temporary directory.
3. Copy the three .DAT files NAMES.DAT, SCAN.DAT and CLEAN.DAT into the directory where VirusScan for OS/2 is installed. By default, this is C:\NETA\VSCANOS2, unless you chose a different location during Step 5 on page 9 of this Installation chapter.

   The zipped .DAT files you download include:

   NAMES.DAT—includes virus names and other details that the user sees when viewing the Virus List.

   SCAN.DAT—includes detection string data for all viruses detected.

   CLEAN.DAT—includes removal string data for all viruses cleaned.

   INTERNET.DAT—VirusScan for OS/2 does not use this .DAT file; you may safely delete it.

Re-enabling VShield

You are now ready to reactivate VShield. When you have completed this procedure, VShield will reboot with the new .DAT files loaded.

To re-enable VShield after updating the .DAT files, follow these steps:

1. Locate and open your system's CONFIG.SYS file with OS/2's editing program "E" by typing,

   ```
   E CONFIG.SYS
   ```

   at the command prompt. The CONFIG.SYS file is displayed.

2. Delete the text, "REM" (followed by a single space) preceding the following two lines in the CONFIG.SYS file. These should be at or close to the end of the file.

   ```
   BASEDEV=VSHIELD.FLT
   RUN=C:\NETA\VSCANOS2\GDDAEMON.EXE
   ```

   NOTE: These examples assume VirusScan was installed to the default installation directory of \NETA\VSCANOS2. If you selected a different installation directory, the alternate location will be reflected in your system's CONFIG.SYS file.

3. Save these changes by selecting **Save** from E's **File** menu.

4. Close the edited CONFIG.SYS by clicking on the Close Window icon in the upper right corner of the toolbar.

5. Locate and open the SECURE.SYS with OS/2's editing program "E" by typing,

   ```
   E SECURE.SYS
   ```

   at the command prompt. The SECURE.SYS file is displayed.

6. Delete the text, "REM" (followed by a single space) preceding the following two lines in the SECURE.SYS file.

   ```
   C:\NETA\VSCANOS2\GDDAEMON.EXE  /SCA='OS2GUARD'  /SPA
   /LOCALUSER=NO
   C:\NETA\VSCANOS2\CRYER.EXE  /SCA='OS2GUARD'  /SPA
   /LOCALUSER=YES  /START
   ```

7. Save these changes by selecting **Save** from E's **File** menu.

8. Close the edited SECURE.SYS by clicking on the Close Window icon in the upper right corner of the toolbar.

9. Reboot your system. VShield is now active, and the current .DAT files are loaded.

On-Access Scanning 3

What is VShield?

VShield is the on-access scanning component of VirusScan for OS/2. With this release of VShield, you can now configure this powerful on-access scanner through a native OS/2 graphical user interface.

Once configured, and the system rebooted, VShield launches on system startup, and remains active in the background, silently scanning all program and data files as they are opened or written to—"on-access." This powerful scanning protection does not require any user input, although VShield can be reconfigured and redeployed at any time to better respond to changing security needs.

Once VShield locates a possible infection, it responds according to the settings you have chosen. This chapter provides instructions on configuring the on-access scanner to best protect the challenges of your computing environment.

NOTE: SES must be installed *and enabled* in order for VShield to scan correctly. For details on enabling SES, please see Chapter 2, "SES enabling" on page 7

Configuring VShield

VShield's default settings provide powerful protection with an eye toward using minimal system resources.

You may, however, prefer to configure the on-access scanner to more precisely meet your needs. Follow the procedures in this chapter to set various scanning options to best meet your needs.

The remaining sections in this chapter cover each of the five VShield property pages, in the order they appear onscreen.

The Detection page

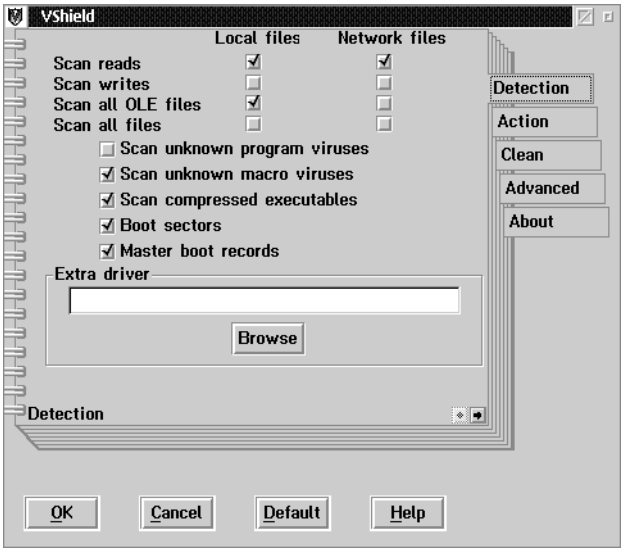

Figure 3-1. VShield Detection page

To set what files are included in on-access scanning, follow these steps:

1. Locate the VShield icon on the OS/2 desktop or in the minimized window viewer.
2. Double-click the icon to open the VShield property pages. The **VShield Detection page** (Figure 3-1) opens.
3. Select the checkboxes for either **Local Files, Network Files,** or both, for the following on-access scanning options:
   - **Scan Reads** VShield will scan all files as they are opened.
   - **Scan Writes** VShield will scan all files as they are saved—"written"— to.
   - **Scan All OLE Files** VShield will scan files which include links to data stored outside the file, using Microsoft's OLE technology.
   - **Scan All Files** By default, VShield scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD.

NOTE: VShield will not scan network drives if you are running a DOS or Windows session within OS/2 — you must return to the OS/2 graphical user interface or command line for VShield to scan drives over a network.

4. Select the **Scan unknown program viruses** checkbox to enable heuristic scanning for possible program viruses.
5. Select the **Scan compressed executables** checkbox if you want VShield to include zipped program files in its scans.
6. Select the **Boot Sectors** checkbox to set scanning of the boot sectors on system startup.
7. Select the **Master Boot Record** checkbox to set scanning of the partition tables.
8. If for any reasons Network Associates furnishes you with a specialized driver for use with VirusScan, you will need to load it here. Click **Browse.** The **Open File** dialog box (Figure 3-2) will open.

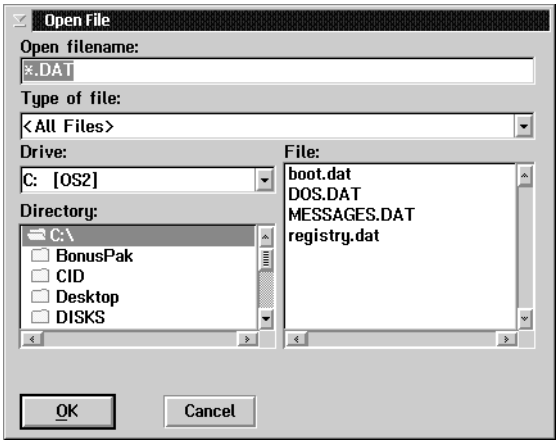

Figure 3-2. VShield Open File dialog box

9. Locate the driver for VShield to use, and click **OK.** You will be returned to VShield's **Scanning** page.
10. Click **OK** to save your settings from the VShield **Scanner** page.

The Action page

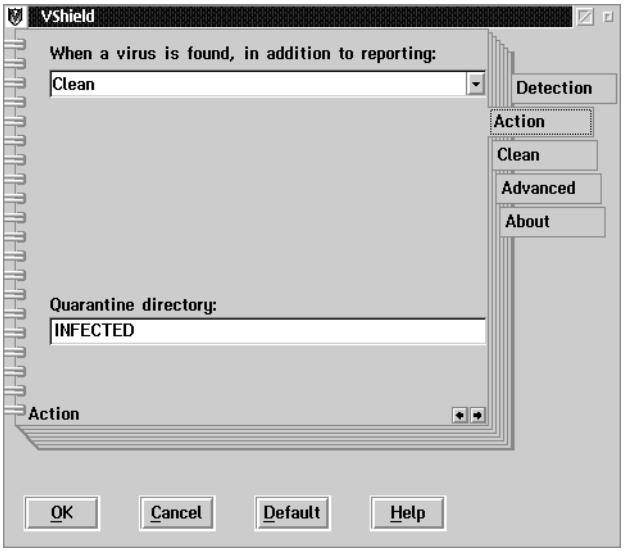

Figure 3-3. VShield Action page

To set how VShield handles detected viruses, follow these steps:

1. Click the Action tab to open the **Action** page (Figure 3-3).
2. Select one of the following options from the **When a virus is found, in addition to reporting:** text box:
   - **Deny access—**Users will be blocked from opening the file.
   - **Delete—**The file will be deleted.
   - **Quarantine—**The file will be moved to the quarantine directory. To change the quarantine director, see Step 3 below.
   - **Clean**—VShield will clean the file according to the setting you have selected from the tabbed **Clean** page (Figure 3-4 on page 23).
3. The default quarantine directory VShield uses for quarantined files, INFECTED, is shown in the **Quarantine Directory:** text box. If you want VShield to use a different directory for quarantining, enter the name of the alternate directory here. If the directory you specify does not exist, VShield will create it for you.

The Clean page

Figure 3-4. VShield Clean page

To configure the actions VShield will take upon discovering an infected file, follow these steps:

1. Click the Clean tab to open the **Clean** page (Figure 3-4).
2. To set a backup directory for infected files, select the **Backup files before disinfecting** checkbox, and type the name of the directory you want used for backup in the **Backup Directory** text box. If this directory does not already exist, VShield will create it for you.
3. Set the action VShield should take with a file if it cannot be cleaned in the **If file cannot be disinfected:** box. Select one of the following choices:
   - **Deny Access** to lock the file without moving it from its current location
   - **Delete** to delete the file.
   - **Quarantine** to send uncleanable files to the Quarantine directory. (To change the Quarantine directory, see Step 3 on page 22.)
4. By default, VShield alerts users after a file has been successfully cleaned. If you do not want this alert shown, select the **Do not show alert dialog if disinfection is successful** checkbox.
5. Click **OK** to save your settings.

The Advanced page

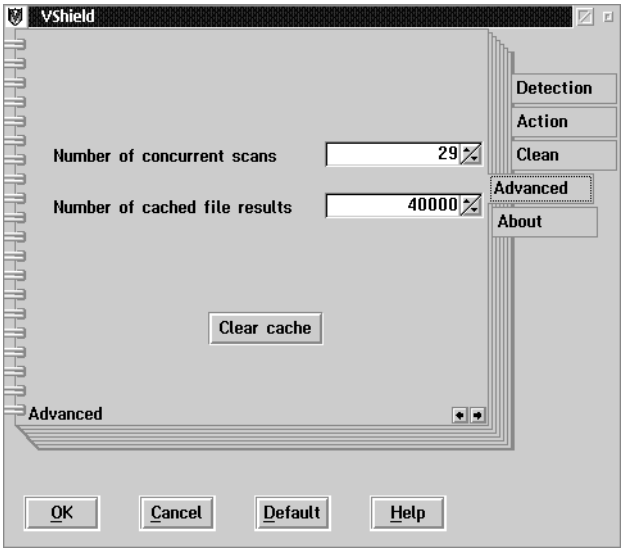

Figure 3-5. VShield Advanced page

To set how VShield works with system memory, follow these steps:

1. Click the Advanced tab to open the **Advanced** page (Figure 3-5).
2. To set a limit on the number of simultaneous scans VShield can execute, click either the up or down arrows in the **Number of concurrent scans** box to select the number you want.
3. To set a limit on how many scanning records VShield retains in memory, click either the up or down arrows in the **Number of cached file results** box to select the number you want.
4. Click **OK** to save your changes.

The About page

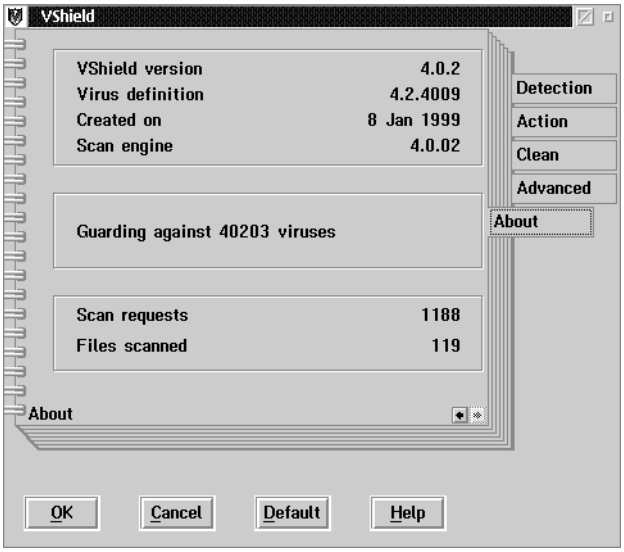

Figure 3-6. VShield About page

This page, Figure 3-6, contains information regarding your copy of VShield and the number of scan results currently saved in memory. Details include:

- **VShield version** The version number of your copy of VShield.
- **Virus definition** The Virus Definition File (.DAT file) version number.
- **Created on** The release date of loaded .DAT file. For VShield to operate at peak performance, this .DAT file should be updated often.
- **Guarding against x viruses** The number of virus definitions the loaded .DAT file contains.
- **Scan requests** The number of times that files subject to on-access scanning have been either opened or saved to. Clicking the **Clear Cache** button on the **Advanced** page (see page 24) will change this number to zero.
- **Files scanned** The number of files which met VShield's criteria for a scan. Clicking the **Clear Cache** button on the **Advanced** page will change this number to zero.

On-Demand Scanning 4

What is on-demand scanning?

On-demand scanning is a scan that you initiate at any time. As it works, VirusScan's on-demand scanner will log its activities, notify the appropriate personnel when a possible infection is found, and isolate, clean or delete infected files, depending on how you have configured the program.

While most users will find it most efficient to run on-demand scans from the VirusScan user interface, on-demand scans can also be run from the command line; see Chapter 5, "On-Demand Scanning at the Command Line," page 37, as well as Appendix B, "Reference: Command-Line Options," page 59, for details.

Using the VirusScan for OS/2 interface

Running a basic scan

You can initiate a basic on-demand scan of any local hard drive or linked network drive from VirusScan's main screen (Figure 4-1), or from the toolbar. As you become more familiar with VirusScan, you may choose to configure scan tasks to meet differing security needs. Instructions for creating and saving custom on-demand scan configurations can be found in "Saving a custom scan" on page 31.

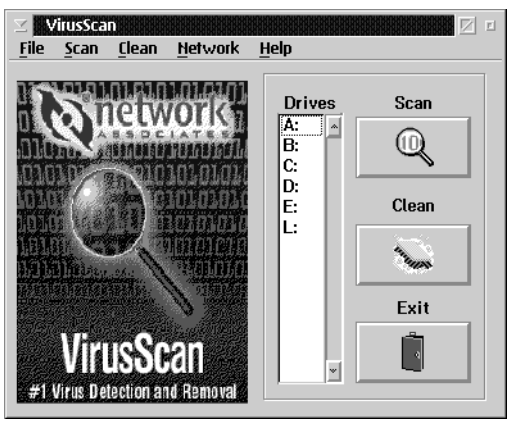

Figure 4-1. VirusScan for OS/2 main page

To initiate a basic scan from VirusScan's main page:

1. To select the target drive for the scan, click on the drive's letter. On networked systems, use the scroll bar to locate the drive.
2. When you have set the target for this scan, click **Scan** to begin the scan. You will be notified if a virus is found.
3. If you have receive a virus detected notice, click **Clean** to clean the infected files. You will be notified when VirusScan has completed disinfecting the files.
4. To exit VirusScan, click **Exit.** If you exit the program during a scan-in-progress, you will be prompted to confirm that you want to close the program. Click **Yes.** VirusScan will close.

NOTE: Any preconfigured scan can be run from this main page (Figure 4-1 on page 27) by first loading the custom .INI file for that scan task; please see "Loading a custom scan" on page 31.

Configuring a basic scan

You can select fundamental scanning options from the **Scan viruses** page. To run an identical scan in the future, you can save any scan configuration you find helpful: see "Saving a custom scan" on page 31 for details.

To configure and start an on-demand scan:

1. Select **Scan Viruses** from VirusScan's **Scan** menu. The **Scan viruses** page (Figure 4-2) opens.

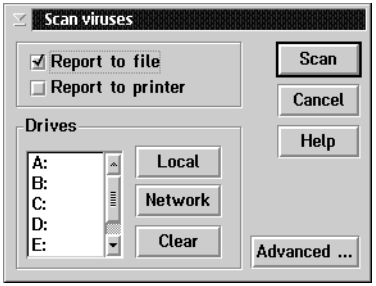

Figure 4-2. VirusScan - Scan viruses page

2. Set your reporting options:

   - Select the **Report to file** checkbox to send the results of this scan to a file. The default filename of a scan report is SCAN.REP. (To change the filename, see the **Advanced Options** page, Step 7 , below.)
   - Select the **Report to printer** checkbox to send the results of this scan to a printed text file.

3. Set your target options:

   - Click on the drives you want scanned. For networked drives, use the scroll bar to view the complete drive list.
   - Click the **Local** or **Network** button to quickly select either all local hard drives or all network drives as a scan target. To change your settings, click **Clear.**

4. Click **Advanced** to open the **Advanced Options** page (Figure 4-3).

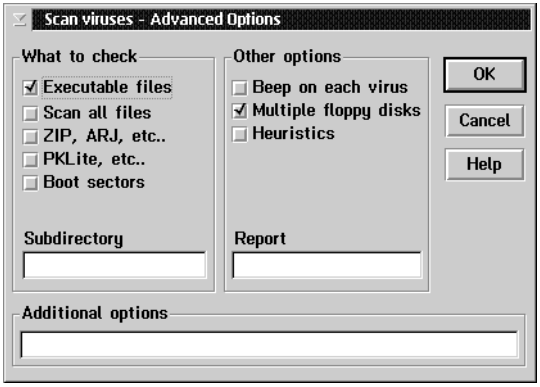

Figure 4-3. The Scan viruses - Advanced Options page

5. Set the actions of the scan by selecting the checkbox for any of the following:

   - **Executable files** to target program files only
   - **Scan all files** to target all files in the specified drive
   - **ZIP, ARJ, etc.** to include archives in the scan
   - **PKLite, etc.** to include compressed files in the scan
   - **Boot sectors** to include the boot sectors of all disks in the target directories

- **Multiple floppy disks** to set VirusScan to scan a series of disks.
- **Beep on each virus** to set VirusScan to beep upon each virus detected during a scan
- **Heuristics** to set VirusScan to use heuristics scanning.

6. To target a certain subdirectory, enter the name in the **Subdirectory** text box. Do not include the drive letter.
7. The default report filename is SCAN.REP. To generate a report file with any other name, enter the name in the **Report** text box. It will be saved to the default program directory, unless you specify a different path. For example,

   ```
   C:\TEMP\WEEKLY.REP
   ```

   creates a report file named, “Weekly” in the Temp directory.
8. List any other command-line options you want to use in the **Additional options** text box. (For a complete list of command-line options, please see Appendix B, “Reference: Command-Line Options,” on page 59.)
9. After you have made your selections, click **OK** to save your settings. The **Advanced Options** page will close, and you will be returned to the **Scan viruses** page (Figure 4-2 on page 28).
10. You are now ready to initiate the scan you have just configured. Alternately, you can save this particular configuration to use later. To do this, follow the procedure in “Saving a custom scan” directly below.

    To start the scan immediately, complete either of the following:

    - Click **Scan** from VirusScan’s main page (Figure 4-1 on page 27).
    - At the VirusScan toolbar, select **Scan viruses** from VirusScan’s **Scan** menu. You will be notified if a virus is found.

Saving a custom scan

You can save any configuration you find useful using VirusScan's **Save Configuration** feature. Scan settings are saved in an .INI file.

To save settings for a particular on-demand scan task, follow these steps:

1. Select **Save Configuration** from VirusScan's **File** menu. The **Save Configuration** page (Figure 4-4) opens.

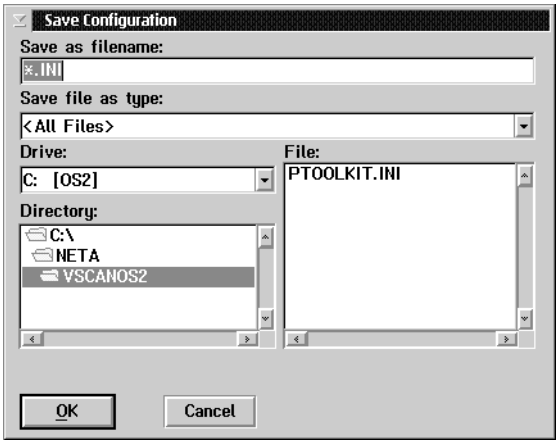

Figure 4-4. VirusScan - Save Configuration page

2. Locate the directory where you want to save the .INI file to by highlighting the appropriate choice in the **Drive:** and **Directory:** boxes.
3. Type the name for this .INI file in the **Open Filename:** box.
4. Click **OK.** Your settings will be saved to the location you specify.

Loading a custom scan

When you save a particular on-demand scan for later use, it it saved as an .INI file. VirusScan uses an .INI file called TOOLKIT.INI by default. You can instead use any preconfigured .INI you wish to run a custom scan at any time.

For instructions on saving scan settings for future use, please see "Saving a custom scan" on page 31. Complete the following procedure to load custom .INI files.

To load saved configurations, follow these steps:

1. Select **Load Configuration** from VirusScan's **File** menu. The **Load Configuration** page (Figure 4-5) opens.

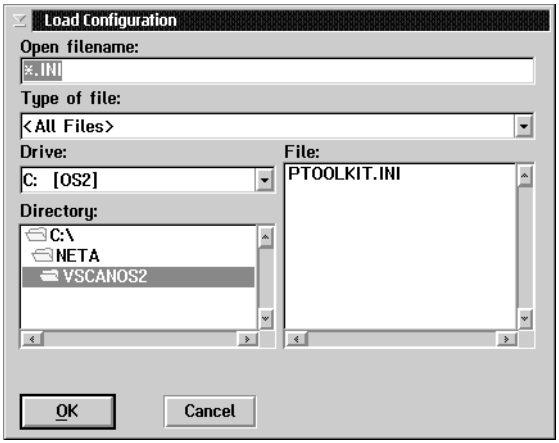

Figure 4-5. VirusScan - Load Configuration page

2. Locate the directory of the .INI file you want VirusScan to use by highlighting the appropriate choice in the **Drive:** and **Directory:** boxes.
3. Either select the file name from the **File:** box, or type the name in the **Open Filename:** box.
4. Click **OK.** The custom configuration you have selected will load.

Configuring cleaning

Configure how you want VirusScan to clean infected files at the **Clean drive** page (Figure 4-6).

To set how VirusScan will clean infected files, follow these steps:

1. Select **Clean Drive** from VirusScan's **Clean** menu to open the **Clean drive** page (Figure 4-6).
   .

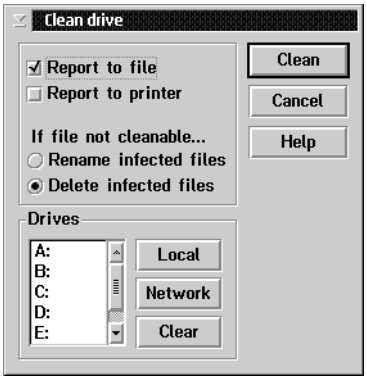

Figure 4-6. VirusScan - Clean drive page

2. Select either the **Report to file** or **Report to printer** checkbox to set how VirusScan will report the results of the cleaning. The default filename for reports is SCAN.REP.
3. Select either the **Rename infected files** or **Delete infected files** option to set the action VirusScan takes if an infection cannot be cleaned.
4. Click on the letter of the drive(s) you want VirusScan to clean. You can also click the **Local** or **Network** button to quickly select either all local or all network drives as a cleaning target. To change your settings, click **Clear.**
5. You can now initiate a cleaning of any infected files VirusScan has detected. To do this, complete either of the following steps::
   - Select **Clean drive** from the **Clean** menu.
   - Click **Clean** from the **Clean Drive** page.

Deleting or “shredding” an infected file

Compared to simply deleting an infected file, VirusScan’s “Shred” utility offers a far more secure way of deleting known infected data.

Shred destroys a file after overwriting it with a series of characters. This is done in order to circumvent various “undelete” programs, which can sometimes successfully recover conventionally deleted files along with any imbedded viruses. A Shred command cannot be undone.

IMPORTANT: Since shredded files cannot be recovered, use this powerful tool with caution.

To delete a file using Shred, follow these steps:

1. Select **Shred – Select File** from VirusScan’s **File** menu. The **Shred File** page (Figure 4-7) will open.

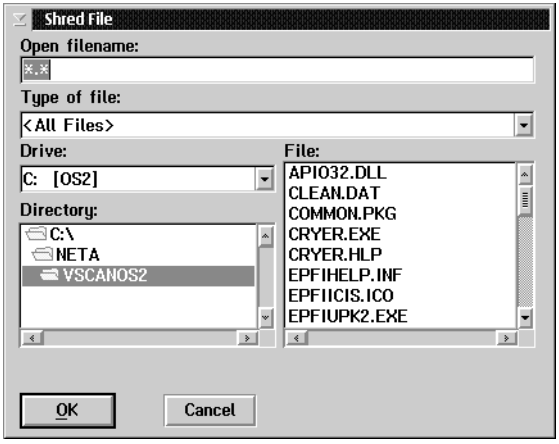

Figure 4-7. VirusScan - Shred page

2. Locate the directory of the file to be shredded by highlighting the appropriate choice in the **Drive:** and **Directory:** boxes.
3. Either select the name of the file to be shredded from the **File:** box, or type the name in the **Open Filename:** box.
4. Click **OK.** You will be prompted again to confirm your decision to shred the selected file.
5. Click **Yes.** The file is then shredded.

Network messaging and alerting

You can enable VirusScan to set a network message at any time—encouraging users to update their Virus Definition Files, for example—or a specific message to be automatically sent upon a virus detection, alerting users to the threat. You can use this message to not only warn your users about a detection, but include instructions on how to handle the situation as well.

IMPORTANT: This release of VirusScan for OS/2 supports network messaging and alerting on Novell servers only.

To configure VirusScan to send a network message, follow these steps:

1. Select **Send Network Message** from VirusScan's **Network** menu.
2. Enter the recipient(s) network login name of the recipient in the **Send message to** box.
3. Enter the text of the message in the **Message** box. This message cannot exceed 32 characters.
4. Click **Send** to send the network message.

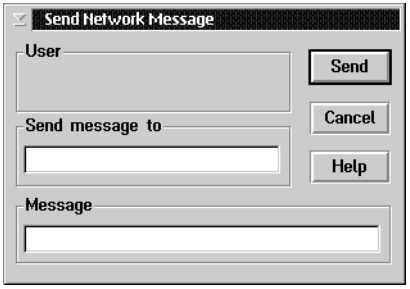

Figure 4-8. VirusScan - Send network message page

To configure VirusScan to send a network alert message upon discovering a virus, follow these steps:

1. Select **Network options** from VirusScan's **Network** menu. The **Network options** page (Figure 4-9 on page 36) will open.
2. Select the **Network alarm on virus** checkbox to activate VirusScan alerting.
3. Enter the text of the message in the **Virus alert message** box.

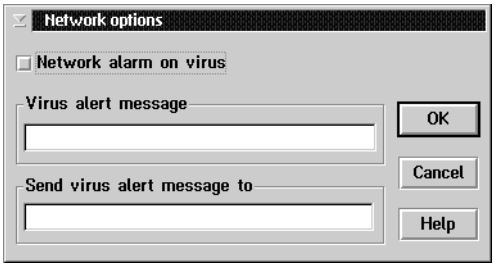

Figure 4-9. VirusScan - Network options page

4. Enter the recipient(s) network login name in the **Send message to** box.
5. Click **OK** to save your settings. Virus alerting is now active.

To disable network alerting, follow these steps:

1. Select **Network options** from VirusScan's **Network** menu. The **Network options** page (Figure 4-9, above) will open.
2. Deselect the **Network alarm on virus** checkbox.
3. Click **OK** to save your changes. Virus alerting is no longer active.

On-Demand Scanning at the Command Line 5

How VirusScan works

At the command line, configuring VirusScan's OS2SCAN.EXE is all you need to do to initiate VirusScan's powerful scanning capabilities.

You can tell VirusScan to conduct a scan operation at any time, on any target drive, directory or file with the scanning options you choose. This chapter explains how to use VirusScan's on-demand scan features to search specific files, directories, or drives for known boot, file, multi-partite, stealth, encrypted, polymorphic, and macro viruses.

You should scan any file new to your system; any newly downloaded or installed files, and, depending on how susceptible your system is to virus infection, as frequently as once a day.

Remember, while you are learning how to configure basic scan tasks, and beginning to customize VirusScan, VirusScan is quietly running *on-access* protections through its VShield component, which runs with a default set of options at system startup. See Chapter 3, page 19, for further details.

Archived and compressed files recognized by VirusScan

32-BIT ENVIRONMENT:

Formats / utilities recognized:

.ARC, .ARJ, .CAB, Diet, LZEXE, .LZH, PKLite, .TD0, .ZIP, .??_

16-BIT ENVIRONMENT:

.CAB files cannot be scanned in low-memory environments.

The switches /UNZIP and /NOCOMP can be used to help configure how VirusScan handles compressed files. Find these and other target-related scan options in the tables from pages 42 to 45.

Basic scanning

To perform a basic scan:

1. From the command prompt, use the `cd` command to change to the directory where VirusScan is installed.
2. The following examples are general scan options. See the tables in pages 40 to 47 for a complete list of on-demand scan options.

   NOTE: As you become more familiar with VirusScan's capabilities, you can create "scanning profiles," which capture scan tasks for future use. See "Creating a scanning profile" on page 50, for details.

   - To scan every file on the C: and D: drives that are susceptible to infection, type:

     ```
     os2scan c: d: /all
     ```

   - To scan every file that is susceptible to infection in all system drives (including compressed drives and PC drives—but not disks), type:

     ```
     os2scan /adl /all
     ```

     where:

     - /ADL specifies all local drives as the target of the scan.
     - /ALL instructs VirusScan to scan all files that are susceptible to infection.

   - To scan a floppy disk in the A: drive, type:

     ```
     os2scan a:
     ```

3. VirusScan might take several minutes to check for viruses in memory and on drives, but will keep you informed of its progress. Read the information on the screen carefully. You may wish to redirect VirusScan's onscreen reports to a report file. See "Report options" on page 47 for options.

   Either of these results will occur:

   If VirusScan reports No Viruses Found, your system is most likely virus-free. Copy important files to fresh disks or tape backup so your current and clean files are maintained should a virus later infect your system.

NOTE: VirusScan's ability to detect viruses must be maintained through regular updates of the VirusScan data files. For more information, please see pages 13 to 16.

If VirusScan finds one or more viruses, a message similar to the following is displayed:

```
Scanning C:
Scanning file C:\DOS\ATTRIB.EXE
Found the Jerusalem Virus!!!
```

NOTE: VirusScan notes any unknown macro virus detected by heuristic scanning by reporting:

```
Could be a new virus!!!
```

Do not panic, even if the virus has infected many files. VirusScan will respond to the suspected infection according to the options you have chosen; see "Response and notification options" on page 45 for details.

Selecting scanning options

Before creating a scanning profile, determine which parameters are necessary for your environment. In this section you will find tables of these various VirusScan options:

- Target options, see page 42
- Response and notification options, see page 45
- Report options, see page 47
- For a complete table of VirusScan command-line options, see Appendix B, page 59.

NOTE: For an onscreen list of scanning options and their usage, use the `cd` command to change to the directory where VirusScan is installed, then type `os2scan /?`

General options

The following table lists VirusScan's general scan options.

General Command-Line Option	Limitations	Description
/? or /HELP	None.	Displays a list of VirusScan command-line options, each with a brief description. You may find it helpful to add a list of scanning options to the report files that VirusScan creates. To do this, type /? /report *<filename>* at the command prompt. The results of your scanning report will be appended with the full set of options available for that scan task.
/ANALYZE	Extended memory required.	Sets VirusScan to scan using its full heuristics, both program and macro. *Note:* /MANALYZE targets macro viruses only; /PANALYZE targets program viruses only.
/FREQUENCY <*n* >	None.	Do not scan <*n*> hours after the previous scan. In environments where the risk of viral infection is very low, use this option to prevent unnecessary scans. Remember, the greater the scan frequency, the greater your protection against infection.

General Command-Line Option	Limitations	Description
/LOAD *<filename>*	None.	Load scanning options from the named file. Use this option to perform a scan you've already configured by loading custom settings saved in an ASCII-formatted file.
/NOEXPIRE	None.	Disables the "expiration date" message if the VirusScan data files are out of date.

Target options

The following table lists VirusScan's target-related scanning options. To configure on-demand scans, you must enter a scan target (e.g. , C:\, A:\, /ADL, /ADN).

Target Command-Line Option	Limitations	Description
/ADL	None.	Scan all local drives—including compressed and PC drives, but not disks—in addition to any other drive specified on the command line. To scan both local and network drives, use the /ADL and /ADN commands together on the same command line. OS/2: /ADL includes the CD-ROM drive in the scan, when used with /NODDA.
/ADN	None.	Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command line. *Note:* To scan both local drives and network drives, use the /ADL and /ADN commands together on the same command line.
/ALL	None.	Overrides the default scan setting by scanning all infectable files—regardless of extension. *Notes:* Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect you have one. By default, VirusScan only scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD. These are the file types that are most susceptible to viruses.
/ANALYZE	Extended memory required.	Use /ANALYZE to set VirusScan to target both program and macro viruses. *Note:* Use /MANALYZE to set VirusScan's heuristic scanning features to target macro viruses only; use /PANALYZE to set VirusScan's heuristic scanning to target only program viruses.
/BOOT	None.	Scan boot sector and master boot record only.
/CHECKLIST *<filename>*	None.	Scan the files listed in *<filename>,* a text list of file names.

Target Command-Line Option	Limitations	Description
/EXCLUDE *<filename>*	None.	Do not scan the files listed in *<filename>*. Use this option to exclude specific files from a scan. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?
/MANALYZE	Extended memory required.	Sets VirusScan's heuristic scanning features to target macro viruses only. *Note:* /PANALYZE targets program viruses only; /ANALYZE targets both program and macro viruses.
/MANY	None.	Scans multiple disks consecutively in a single drive. VirusScan will prompt you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run VirusScan from a boot disk and you have only one floppy drive.
/MAXFILESIZE *<xxx.x>*	None.	Do not scan files larger than *<xxx.x>* megabytes.
/NOBREAK	None.	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress with /NOBREAK in use.
/NOCOMP	Extended memory required.	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. This reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for virus signatures.
/NODDA	None.	No direct disk access. This prevents VirusScan from accessing the boot record. You might need to use this option on some device-driven drives. Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.
/NODOC	None.	Does not scan Microsoft Office files.

Target Command-Line Option	Limitations	Description
/PANALYZE	Extended memory required.	Sets VirusScan to scan using program heuristics. *Note:* /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.
/SUB	None.	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories within any directories you have specified. It is not necessary to use /SUB if you are scanning an entire drive.

Response and notification options

The following table lists VirusScan's response and notification options after a virus has been detected.

Response and Notification Command Line Option	Limitations	Description

/ALERTPATH *<dir>*	Can only be used on networks whose servers are running the correct version of NetShield.	Designates the directory *<dir>* as a network path to a remote NetWare volume or NT directory, monitored by Centralized Alerting.
		VirusScan will send an .ALR text file to the server when it detects an infected file.
		From this directory, NetShield will, through its Centralized Alerting feature broadcast or compile the alerts and reports according to its established configuration.
		Requirements:
		• These remote NetWare or Windows NT servers running NetShield for Windows NT v2.5.3 and later, or NetShield for NetWare v2.3.3 and later.
		• You must have write access to the *<directory>* you specify.
		• *<directory>* must contain the NetShield-supplied CENTALRT.TXT file.
		Add these variables to your AUTOEXEC.BAT file to ensure that the .ALR file VirusScan sends identifies the infected system and its user:
		`Set COMPUTERNAME=<name of computer>`
		`Set USERNAME=<user name>`

/CLEAN	None.	Clean viruses from all infected files and system areas.
/CLEANDOCALL	None.	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. *Note:* This option deletes all macros from infected files, including macros not infected by a virus.

Response and Notification Command Line Option	Limitations	Description
/CONTACTFILE *<filename>*	None.	Display the contents of *<filename>* when a virus is found. It is an opportunity to provide contact information and instructions to the user when a virus is encountered. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. *Note:* Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.
/DEL	None.	Deletes infected files permanently.
/MOVE *<dir>*	None.	Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. *Note:* This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.
/NOBEEP	None.	Disables the tone that sounds whenever VirusScan finds a virus.

Report options

The following table lists the available options for configuring how VirusScan displays the results of scanning activity.

- **To view the results of a scan task onscreen**, none of the options below are necessary to add to the command line.

  For example,

  ```
  os2scan a: /ONLY WEEKLY
  ```

  will result in the scan results of a floppy disks' directory "Weekly" appearing onscreen.

- **To capture a VirusScan report to a text file,** /REPORT must be used, along with any additional switches as needed.

  In the following example, the results of the above scan will not appear onscreen; they are instead redirected to a text file named, "rpt1.txt" in the C: drive directory, "Scans."

  ```
  os2scan a: /ONLY WEEKLY /REPORT> c:\scans\rpt1.txt
  ```

  The resultant text file can be viewed with any text editor.

You may find it helpful to add a list of scanning options to the report files VirusScan creates. To do this, type /? /report <*filename*> at the command prompt. The results of your scanning report will be appended with the full set of options available for that scan task.

Report Command-Line Option	Limitations	Description
/ALERTPATH <*dir*>	None.	Designates the directory <*dir*> as a network path monitored by Centralized Alerting.
/APPEND	None.	Used with /REPORT to append report message text to the specified report file instead of overwriting it.

Report Command-Line Option	Limitations	Description
/REPORT *<filename>*	None.	Creates a report of infected files and system errors, and saves the data to *<filename>* in ASCII text file format. If *<filename>* already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: VirusScan will add report information to the end of the file, instead of overwriting it. You can also use /RPTALL, /RPTCOR, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report. You may find it helpful to add a list of scanning options to the report files VirusScan creates. To do this, add /? to the command. The results of your scanning report will include the full set of options available for that scan task. You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive.
/RPTALL	None.	Include all scanned files in the /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. You can use /RPTCOR with /RPTERR on the same command line.
/RPTCOR	None.	Include corrupted files in /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files which VirusScan finds may have been damaged by a virus. You can use /RPTCOR with /RPTERR on the same command line. There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).

Report Command-Line Option	Limitations	Description
/RPTERR	None.	Include errors in /REPORT file. When used with /REPORT, this option adds a list of system errors to the report file. You can use /RPTERR with /RPTCOR on the same command line. System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.
/VIRLIST	None.	Displays the name of each virus that VirusScan detects.

Creating a scanning profile

Before creating a scanning profile, select the scanning options best suited to your computing environment and needs. See “Selecting scanning options” on page 40 for a complete options list. Once you have made your choices, you are ready to construct a “scanning profile,” a text file of instructions and options VirusScan will use to execute a specific scan task.

Like other text files, you may update these scan profiles at any time, and create as many specialized scan tasks as you need.

To create a scanning profile, follow these steps:

1. Using the `cd` command, change to the VirusScan directory.

   (For example, if VirusScan was installed on directory “Scan” on your C: drive, type `cd \scan` at the command prompt.)

2. Type the following:

   ```
   e profile.txt
   ```

   > **NOTE:** You may choose any filename for your scanning profile, and you may use any text editor to create the profile.

   The OS/2 text program “E” opens.

3. Enter a scanning option (e.g. /ADL, /ADN, etc.).

4. Press **ENTER.**

   The cursor is moved to the next line.

5. Repeat steps 3 and 4 until all options are entered, one per line.

6. To save the file, press **ALT+F** to access the **File** menu then press **S** to save.

7. To exit and return to the command prompt, press **ALT+F** to access the **File** menu, then press **X** to exit.

   The file is created. To run the file, see “Running a scanning profile,” below.

Running a scanning profile

To run a scanning profile, complete the following steps:

1. Using the `cd` command, change to the VirusScan directory.
2. Type the following:

   `os2scan /load <filename>`

   where <*filename*> is the name of the scanning profile that contains the instructions for the scan task of your choice.

   VirusScan will execute the scan as detailed in the scanning profile you've just loaded.

Viewing the Virus List

The Virus List is a comprehensive list of viruses detected by VirusScan. Monthly updates to this list are available from Network Associates, and should be updated in a timely manner; please see "Keeping the .DAT files current" on page 13 for details.

To view the list of viruses detected by VirusScan onscreen:

1. Using the `cd` command, change to the VirusScan directory.
2. Type the following command:

   ```
   os2scan /virlist /report <filename>.txt
   ```

   where <*filename*> is the name you have chosen for the text file. You may use any name you wish. This will redirect the output of the current Virus List to <*filename*>.txt.

Scanning your floppy disks

Why floppy disks pose a threat

Since many viruses invade computers when systems boot from an infected disk, or when users copy, run, or install programs or files that are infected, scanning all new floppy disks *before first use* will go a long way toward stopping the introduction of new viruses into any computing environment.

You should always take the proactive precaution of scanning all floppy disks you use. Even disks received from friends, co-workers, and other people you know should not be assumed to be virus-free.

Though it may be hard to believe, floppy disks pose a threat even if they are not bootable. To help address this threat, Network Associates recommends that you get in the habit of checking to make sure that your disk drives are empty before you turn on your computer: that way, your system will not pick up a boot sector virus from an infected floppy disk that is lying in one of your disk drives.

How to scan floppy disks

To scan floppy disks:

1. Using the `cd` command, change to the directory where VirusScan was installed.
2. Type:

   ```
   os2scan a: /many
   ```

3. Insert the first disk to scan into the A: drive, and press **ENTER**.

   The disk is scanned and the names of any infected files are displayed.

4. Remove the scanned floppy disk from the A: drive.
5. Insert the next disk and press **ENTER.** Repeat Steps 3 - 4 for all floppy disks needing to be scanned.

Network Associates Support Services

A

Choosing Network Associates anti-virus and security software helps to ensure that the critical information technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from three levels of extended support under the Network Associates PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Personal Support program.

PrimeSupport Options for corporate customers

The Network Associates PrimeSupport program offers a choice of Basic, Extended, or Anytime options. Each option has a range of features that provide you with cost-effective and timely support geared to meet your needs.

PrimeSupport Basic

PrimeSupport Basic gives you telephone access to essential product assistance from experienced Network Associates technical support staff members. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport Basic as part of the package for two years from your date of purchase. If you purchased your Network Associates product with a perpetual license, you can renew your PrimeSupport Basic plan for an annual fee.

PrimeSupport Basic includes these features:

- Telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website.

PrimeSupport Extended

PrimeSupport Extended gives you personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products. By calling in advance, your PrimeSupport Extended representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Extended gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Extended on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Extended includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within one hour to pages, within four hours to voice mail, and within 12 hours to e-mail
- Telephone access to technical support from Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Time
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to five people in your organization as customer contacts

PrimeSupport Anytime

PrimeSupport Anytime offers round-the-clock, personalized, proactive support for Network Associates products deployed in the most business-critical information systems. PrimeSupport Anytime delivers the features of PrimeSupport Extended 24 hours a day, seven days a week, with shorter response time commitments. You may purchase PrimeSupport Anytime on an annual basis when you purchase a Network Associates product, either with a subscription license or a perpetual license.

PrimeSupport Anytime includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within half an hour to pages, within one hour to voice mail, and within four hours to e-mail
- Telephone access to technical support 24 hours a day, seven days a week
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to 10 people in your organization as customer contacts

Table A-1. PrimeSupport At a Glance

Feature	Basic	Extended	Anytime
Technical support via telephone	Monday–Friday 8:00 a.m.–8:00 p.m.	Monday–Friday 7:00 a.m.–7:00 p.m.	24 hours a day, 7 days a week
Technical support via website	Yes	Yes	Yes
Software updates	Yes	Yes	Yes
Assigned support engineer	—	Yes	Yes
Proactive support contact	—	Yes	Yes
Designated customer contacts	—	5	10
Committed response time	—	Pager: 1 hour Voicemail: 4 hours E-mail: 12 hours	Pager: 30 mins. Voicemail: 1 hour E-mail: 4 hours

Ordering PrimeSupport

To order PrimeSupport Basic, PrimeSupport Extended or PrimeSupport Anytime for your Network Associates products:

- Contact your sales representative; or
- Call Network Associates Support Services at 1-800-988-5737 or 1-650-473-2000 from 6:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday.

NOTE: The PrimeSupport program described in this guide is available in North America only. To learn about PrimeSupport options available outside North America, contact your regional sales office. Contact information appears near the front of this guide.

Support services for retail customers

If you purchased your Network Associates product through a retail vendor or from the Network Associates website, you also receive some support services as part of your purchase. The specific level of included support depends on the product that you purchased. Examples of the services you receive include:

- Free data (.DAT) file updates for the life of your product via the Network Associates website. You can also update your data files by using your web browser to visit

  http://www.nai.com/download/updates/updates.asp

- Free program (executable file) upgrades for one year via the Network Associates website. If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your web browser to visit:

  http://www.nai.com/download/upgrades/upgrades.asp

- Free access 24 hours a day, seven days a week to online or electronic support through the Network Associates voice and fax system, the Network Associates website, and though such other electronic services as America Online and CompuServe.

To contact Network Associates electronic services, choose one of these options:

- Automated voice and fax system: (408) 988-3034
- Network Associates website: http://support.nai.com
- CompuServe: GO NAI
- America Online: keyword MCAFEE

- Ninety days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

After your complimentary support period expires, you can take advantage of a variety of personal support options geared toward your needs. Contact Network Associates Customer Care at (972) 278-6100 to learn more about the options available, or visit the Network Associates website at:

http://www.nai.com/services/support/support.asp.

Network Associates consulting and training

Network Associates provides expert consulting and comprehensive education that can help you maximize the security and performance of your network investments through the Network Associates Total Service Solutions program.

Professional Consulting Services

Network Associates Professional Consulting Services is ready to assist during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert supplemental resource and independent perspective to resolve your problems. You'll get help integrating Network Associates products into your environment, along with troubleshooting assistance or help in establishing baselines for network performance. Network Associates consultants also develop and deliver custom solutions to help accomplish your project goals—from lengthy, large-scale implementations to brief problem-solving assignments.

Total Education Services

Network Associates Total Education Services builds and enhances the skills of all network professionals through practical, hands-on instruction that you can take right back to your job. The Total Education Services technology curriculum focuses on network fault and performance management and covers problem solving at all levels. Network Associates also offer modular product training so that you understand the features and functionality of your new software.

You can enroll in Total Education Services courses year-round at Network Associates educational centers, or you can learn from customized courses conducted at your location. All courses follow educational steps along a learning path that takes you to the highest levels of expertise. Network Associates is a founding member of the Certified Network Expert (CNX) consortium.

To learn more about these programs, contact your sales representative or call Total Service Solutions at 1-800-395-3151.

Reference: Command-Line Options B

VirusScan for OS/2 command-line options

The following table lists all of the VirusScan switches in alphabetical order. (For tables of options grouped by type, see pages 40 to 47.)

IMPORTANT: When typing commands, remember that if you name a file which resides *outside* the directory where VirusScan is installed, you must include the full path to that file. If you are specifying a file in an external directory, you must have rights to that file or your command will fail.

Command-Line Option	Description
/? or /HELP	Displays a list of VirusScan command-line options, each with a brief description. You may find it helpful to add a list of scanning options to the report files that VirusScan creates. To do this, type /? /report *<filename>* at the command prompt. The results of your scanning report will be appended with the full set of options available for that scan task.
/ADL	Scan all local drives—including compressed drives and PC cards, but not disks—in addition to any other drive(s) specified on the command line. To scan both local and network drives, use the /ADL and /ADN commands together in the same command line. OS/2: /ADL includes the CD-ROM drive in the scan, when used with /NODDA.
/ADN	Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command line. *Note:* To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command line.

Command-Line Option	Description

/ALERTPATH *<dir>*
Can only be used on networks whose servers are running the correct version of NetShield.
	Designates the directory *<dir>* as a network path to a remote NetWare volume or NT directory, monitored by Centralized Alerting.
	VirusScan will send an .ALR text file to the server when it detects an infected file.
	From this directory, NetShield will, through its Centralized Alerting feature, broadcast or compile the alerts and reports according to its established configuration.
	Requirements:
	• These remote NetWare or Windows NT servers running NetShield for Windows NT v2.5.3 and later, or NetShield for NetWare v2.3.3 and later.
	• You must have write access to the *<directory>* you specify.
	• *<directory>* must contain the NetShield-supplied CENTALRT.TXT file.
	Add these variables to your AUTOEXEC.BAT file to ensure that the .ALR file VirusScan sends identifies the infected system and its user:
	`Set COMPUTERNAME=<name of computer>`
	`Set USERNAME=<user name>`

/ALL	Overrides the default scan setting by scanning all infectable files—regardless of extension. *Notes:* Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect that you have one. By default, VirusScan only scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD. These are the file types that are most susceptible to viruses.
/ANALYZE Extended memory required.	Sets VirusScan to scan using its full heuristics, both program and macro. *Note:* /MANALYZE targets macro viruses only; /PANALYZE targets program viruses only.
/APPEND	Used with /REPORT to append report message text to the specified report file instead of overwriting it.
/BOOT	Scan boot sector and master boot record only.

Command-Line Option	Description
/CHECKLIST *<filename>*	Scan list of files contained in *<filename>*.
/CLEAN	Clean viruses from all infected files and system areas.
/CLEANDOCALL	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. *Note:* This option deletes all macros, including macros not infected by a virus.
/CONTACTFILE *<filename>*	Display the contents of *<filename>* when a virus is found. It is an opportunity to provide contact information and instructions to the user when a virus is encountered. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. *Note:* Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.
/DEL	Deletes infected files permanently.
/EXCLUDE *<filename>*	Do not scan the files listed in *<filename>*. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?
/FREQUENCY <*n* >	Do not scan <*n*> hours after the previous scan. In environments where the risk of viral infection is very low, use this option to prevent unnecessary scans. Remember, the greater the scan frequency, the greater your protection against infection.
/HELP or /?	Displays a list of VirusScan command-line options, each with a brief description. You may find it helpful to add a list of scanning options to the report files VirusScan creates. To do this, type /? /report *<filename>* at the command prompt. The results of your scanning report will be appended with the full set of options available for that scan task.

Command-Line Option	Description
/LOAD *<filename>*	Load scanning options from the named file. Use this option to perform a scan you've already configured by loading custom settings saved in an ASCII-formatted file.
/MANALYZE	Sets VirusScan's heuristic scanning features to target macro viruses only. *Note:* /PANALYZE targets program viruses only; /ANALYZE targets both program and macro viruses.
/MANY	Scans multiple disks consecutively in a single drive. VirusScan will prompt you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run VirusScan from a boot disk and you have only one floppy drive.
/MAXFILESIZE *<xxx.x>*	Scan only files no larger than *<xxx.x>* megabytes.
/MOVE *<dir>*	Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. *Note:* This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.
/NOBEEP	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress with /NOBREAK in use.
/NOCOMP Extended memory required.	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. This reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for virus signatures. VirusScan will still check for modifications to compressed executables if they contain VirusScan validation codes.

Command-Line Option	Description
/NODDA	No direct disk access. This prevents VirusScan from accessing the boot record. You might need to use this option on some device-driven drives. Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.
/NODOC	Does not scan Microsoft Office files.
/NOEXPIRE	Disables the “expiration date” message if the VirusScan data files are out-of-date.
/PANALYZE Extended memory required.	Sets VirusScan to scan using program heuristics. *Note:* /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.
/REPORT *<filename>*	Creates a report of infected files and system errors, and saves the data to *<filename>* in ASCII text file format. If *<filename>* already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: VirusScan will instead add report information to the end of the file, instead of overwriting it. You can also use /RPTALL, /RPTCOR, and /RPTERR to add scanned files, corrupted files, and system errors to the report. You may find it helpful to add a list of scanning options to the report files VirusScan creates. To do this, add /? to the command. The results of your scanning report will include the full set of options available for that scan task. You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive.
/RPTALL	Include all scanned files in the /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. You can use /RPTCOR with /RPTERR on the same command line.

Command-Line Option	Description
/RPTCOR	Include corrupted files in /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files that VirusScan finds may have been damaged by a virus. You can use /RPTCOR with /RPTERR on the same command line. There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).
/RPTERR	Include errors in /REPORT file. When used with /REPORT, this option adds a list of system errors to the report file. You can use /RPTERR with /RPTCOR on the same command line. System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.
/SUB	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories within any directories you have specified. It is not necessary to use /SUB if you are scanning an entire drive.
/VIRLIST	Displays the name of each virus that VirusScan detects.

VirusScan error levels

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

NOTE: See your OS/2 documentation for more information.

VirusScan can return the following error levels:

Errorlevel	Description
0	No errors occurred; no viruses were found.
2	Data file integrity check failed.
6	A general problem.
8	Could not find a data file.
10	A virus was found in memory.
13	One or more viruses or hostile objects were found.
15	VirusScan self-check failed; it may be infected or damaged.
20	Scanning prevented due to the /FREQUENCY switch.
102	User quit via ESC-X, ^C or Exit button. *Note:* This can be disabled with the /NOBREAK command-line option.

SES Enabling C

What is SES?

IBM's Security Enabling Services (SES) are a set of OS/2 extensions used by security software for procedures such as user login, or restricting access to data. VirusScan's on-access scanning component VShield uses SES to get the complete file access it needs to thoroughly check for viruses.

Since VShield cannot run without SES being enabled, taking these two critically important steps *before installing VirusScan* will minimize the chance of a failed VirusScan installation:

- Make certain that the SES extensions are installed on your system. (For further details, please visit visit IBM's website at http://www.software.ibm.com.
- Make certain you select SES enablement as part of the VirusScan installation process. (See Chapter 2, "Installing VirusScan for OS/2." Step 5 on page 9.)

Editing the CONFIG.SYS file

VirusScan can edit the CONFIG.SYS for you at installation, if you selected the Enable SES component at the time you install the program. (See Step 5 on page 9.) If, however, you prefer to update the CONFIG.SYS file without using the VirusScan utility, complete the procedure here. While Network Associates recommends keeping manual editing of the CONFIG.SYS file at a minimum, this section includes a model CONFIG.SYS file for use as an example of how to directly edit your CONFIG.SYS file to enable SES.

IMPORTANT: Network Associates supplies this file ONLY as an example of the configuration required to enable SES extensions for OS/2 systems. Network Associates does NOT guarantee the accuracy or effectiveness of this information for particular computing environments.

For complete configuration information, consult IBM documentation for this product or visit IBM's website at http://www.software.ibm.com.

To enable SES on your system:

1. Install SES on your OS/2 system, together with all necessary FixPak versions. (See the WHATSNEW.TXT file for VShield for OS/2, or consult your IBM OS/2 documentation for more details.)
2. Locate the CONFIG.SYS file on your system. It can be found in the root directory of the OS/2 boot drive.
3. Open the CONFIG.SYS with OS/2's editing program "E" by typing,

   ```
   E CONFIG.SYS
   ```

   at the command prompt. The CONFIG.SYS file is displayed.
4. Next, copy the lines from "A model CONFIG.SYS file" below that appear after this notation:

   ```
   **** INCLUDE THESE LINES TO CONFIGURE SES ****
   ```

   into your existing CONFIG.SYS file, making sure to adjust any parameters necessary for your environment.You might, for example, need to change the path information included here to reflect the correct path information for your own environment. The line

   ```
   **** END OF SES-RELATED MATERIAL ****
   ```

   marks the end of each excerpt.

   (Other notes and related configuration information appear after this line:

   ```
   ***** NOTE *****)
   ```
5. Save these changes by selecting **Save** from E's **File** menu.
6. Close the edited CONFIG.SYS by clicking on the Close Window icon in the upper right corner of the toolbar.
7. Reboot your system for the changes to take effect.

A model CONFIG.SYS file

```
REM             Model CONFIG.SYS File
REM          to enable Security Enabling System
REM            in OS/2 Warp 3 and OS/2 Warp 4
REM            for use with VShield for OS/2
```

```
REM **** INCLUDE THESE LINES TO CONFIGURE SES ****

BASEDEV=SESDD32.SYS

CALL=C:\OS2\SECURITY\SES\SESSTART.EXE
C:\OS2\SECURITY\SES\SESDMON.EXE

REM **** END OF SES-RELATED MATERIAL ****


REM ***** NOTE *****

REM The line that begins with IFS= appears in your
REM CONFIG.SYS file only if youhave formatted your disk
REM with OS/2's High Performance File System (HPFS). If
REM you have an HPFS partition on your computer and you
REM are running OS/2 Warp 4, leave this line as it
REM appears. If you are running OS/2 Warp 3, change the
REM value following CACHE: to 64 instead of 2048.

REM ***** END OF NOTE *****

IFS=C:\OS2\HPFS.IFS /CACHE:2048 /CRECL:4 /AUTOCHECK:CD

REM ***** NOTE *****

REM Remove or remark out the following line in order to
REM install SES.
```

```
REM PROTSHELL=C:\OS2\PMSHELL.EXE

REM ***** END OF NOTE *****


REM **** INCLUDE THIS LINE TO CONFIGURE SES ****

PROTSHELL=C:\OS2\SECURITY\SES\SESSHELL.EXE

REM **** END OF SES-RELATED MATERIAL ****

SET USER_INI=C:\OS2\OS2.INI
SET SYSTEM_INI=C:\OS2\OS2SYS.INI
SET OS2_SHELL=C:\OS2\CMD.EXE

***** NOTE *****

REM The "SET AUTOSTART=" can take different values depending
REM on which version of OS/2 you have installed. To run OS/2
REM with SES, you should remove the value "PROGRAMS" from
REM this line. On some systems, you might also need to remove
REM TASKLIST.

***** END OF NOTE *****


REM The following line appears only in OS/2 Warp 4 files
```

```
SET AUTOSTART=WARPCENTER,CONNECTIONS,TASKLIST,FOLDERS

REM The following line appears only in OS/2 Warp 3 files

SET AUTOSTART=LAUNCHPAD,CONNECTIONS,TASKLIST,FOLDERS


REM ***** NOTE *****

REM REMOVE OR REMARK OUT THIS LINE FOR SES INSTALLATION:

REM SET RUNWORKPLACE=C:\OS2\PMSHELL.EXE

REM ***** END OF NOTE *****


REM **** INCLUDE THESE LINES TO CONFIGURE SES ****

SET RUNWORKPLACE=C:\OS2\SECURITY\SES\PSSDMON.EXE
SET SESDBPATH=C:\OS2\SECURITY\SESDB
SET AUTOGUEST=NO
SET GUESTNAME=GUEST
SET TRUSTEDPATH=NO
SET USERSHELL=C:\OS2\PMSHELL.EXE
SET RESTARTUSERSHELL=YES

REM **** END OF SES-RELATED MATERIAL ****
```

```
SET COMSPEC=C:\OS2\CMD.EXE


REM ***** NOTE *****

REM THE PATH STATEMENTS "LIBPATH=" AND "SET PATH=" ADD THE
REM PATH "C:\OS2\SECURITY\SES;". AN EXAMPLE OF THE CORRECT
REM ADDITIONS APPEARS AT THE END OF EACH PATH STATEMENT
REM IN THE FOLLOWING TEXT.

REM ***** END OF NOTE *****

LIBPATH=C:\OS2\SECURITY\SES;

SET PATH=C:\OS2\SECURITY\SES;

REM ***** NOTE *****

REM THE CHANGES SHOWN ABOVE ARE THOSE NECESSARY TO
ENABLE
REM SES ON YOUR OS/2 SYSTEM. THIS EXAMPLE FILE DOES NOT
REM SHOW THE REMAINING LINES FOUND IN A TYPICAL CONFIG.SYS
REM FILE.

REM ***** END OF NOTE *****
```

```
REM ***** END OF EXAMPLE FILE *****
```

Index

D

E

F

H

I

L

M

N

O

P

Q

R

S

T

U

V

W