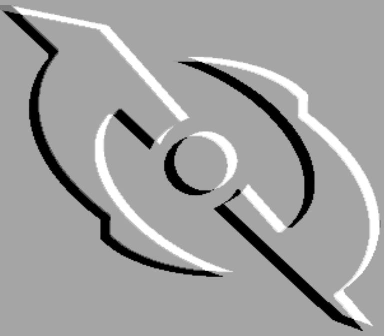

VirusScan Command Line

User's Guide

Version 4.0

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE AGREEMENT

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENTATION DESCRIBES, 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.

Issued June 1999/VirusScan Command Line v4.0.3

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 45,000 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. Network Associates has, however, assembled the world’s largest and most experienced anti-virus research staff within its Anti-Virus Emergency Response Team (A.V.E.R.T)* division. This means that the 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

Introduction

1

What are the VirusScan Command Line scanners?

The VirusScan Command Line* software package is a collection of Network Associates' powerful command line products. You can use it to search for viruses in any drive, folder, or file in your computer—this is known as an ”on-demand” scan. The program can also be set to scan a file any time it is opened or saved to—an ”on-access” scan. The VirusScan scanners include a powerful array of options allow you to set decisive responses to any detected virus: moving the infected files to a quarantine location, cleaning, or deleting the infected data.

When a virus is detected, the VirusScan program will alert you to its presence. You can set the software's alerting features to create an effective alerting system to ensure that not only the user, but *all* key personnel will be notified of a virus infection. You can customize the alert message to include the next steps an employee should take to best protect data and keep downtime to a minimum. A variety of reporting options provide you multiple ways of tracking the results of all scan activity.

The VirusScan scanners, kept current with updated virus data files from Network Associates AVERT labs is the backbone of an aggressive, comprehensive network security program. Network Associates strongly urges you to set up a comprehensive security program for your network, incorporating as many protective measures as possible. (For additional security information and resources, see Appendix A, “Preventing Virus Infection.”)

New engine technology

This release of VirusScan Command Line software is built on a powerful new engine created and backed by the Network Associates, and the world-wide research teams of the McAfee Labs.

Since Network Associates' command line scanners are powered by the same engine, and use the same virus definition files as every product across the McAfee* and Dr Solomon's* product lines, this software offers the same virus detection and cleaning rates as our other award-winning products. These command line scanners can be used alone, or as a powerful tool to back up any

Network Associates' graphical user interface-based scanning software, such as VirusScan for Windows 95/98. These command line scanners is one of the many Network Associates continues to provide network administrators with anti-virus software that offers the highest virus detection and repair rates in the industry.

Administrative impact

With Year 2000 (Y2K) plans in place, many administrators have legitimate concerns about integrating any substantial revisions of any sort into their company's security system at this point in time. To minimize any administrative impact, the integration of the new engine into the VirusScan Command Line software is a transparent change; while the content of the program files has changed, the file names themselves have not. Upgrading to this latest version of our software will not require rewritten scripts, or any other diversion of administrative effort at this critical time in network management.

How VirusScan works

The verbs "scan" and "vshield," in conjunction with myriad options (see Appendix C, page 91 for a complete alphabetical list) are the two commands to use at the command prompt to configure the software's powerful scanning modules. This is the shell around the new VirusScan engine—the engine common to all Network Associates and Dr Solomon's products.

Network Associates is now offering a new utility comprises self-installing upgrades to the scanning engine as well as the virus data (.DAT) files which the engine uses in its virus handling tasks. Both of these updating tasks, which used to be separate maintenance procedures, are now handled efficiently by the SuperDAT* utility. These updates will not change how you configure the scanners; they simply influence the actions of the engine itself, and the data it uses for virus detection and cleaning efforts. Visit the Network Associates website at www.nai.com for further details on this new utility.

The components of the VirusScan Command Line software include:

> **SCAN.EXE—**Scan is the on-demand scanning component of the VirusScan program. It acts as a decision-maker for how the software will operate in a given session. As the VirusScan software runs, SCAN.EXE will dynamically respond to any environmental change or limitation—such as restricted memory—and automatically call one of its "helper" programs to successfully run the scan tasks it is configured to launch. If SCAN.EXE detects a 32-bit environment, it will initialize a scan task itself. If SCAN.EXE determines that it is running in a DOS-based environment, it will assess the resources available, and call either SCAN86 or SCANPM to conduct the scan operation.

Should Scan initiate either SCAN86 or SCANPM, any change will be transparent to you. Only by viewing the online Help file will you learn which particular on-demand scanning component is running. (To view the Help file, type “scan /?” at the command prompt of the directory where you installed these scanners.)

VSHIELD—This on-access scanner for DOS will scan your system automatically every time you access a file—the action of creating a file, copying, renaming, writing to, and saving. The VShield scanner can be configured to launch at system startup. For details on on-access scanning, see Chapter 4, “On-access Scanning.”

Virus data files— Network Associates’ current virus data files (.DAT files), comprised of the three files NAMES.DAT, SCAN.DAT, and CLEAN. DAT, are a complete collection of virus signatures and other information that the VirusScan scanners use for virus detections. Your license agreement includes free weekly updates to these files. Being vigilant about keeping these .DAT files current is the key to keeping your anti-virus software running at peak performance. See pages 71 to 73 for details on updating these files.

Since the command line scanners share the same virus data as other Network Associates products, you can enjoy the same outstanding detection rates as our GUI-based scanners.

Features of the VirusScan product

The VirusScan scanner’s cutting-edge technology includes:

- **Advanced heuristic analysis—**These scanners use both “positive” analysis—searching for possible viral code—and well as “negative” analysis—searching for code that is distinctly *not* a virus. This dual approach allows for incredible detection rates for macro viruses, while nearly eliminating false alarms.

- **Enhanced handling of macro viruses in password-protected documents—**These scanners offer unparalleled advances in how password-protected Microsoft Office files are handled which most macro viruses to be cleaned—even macro viruses which have the ability to set their own passwords. Other new advances include:

    – Macro viruses can now be detected in password-protected Microsoft Word 7.0 files (Word for Office 95) in all languages supported by Word.

    – The scanner’s enhanced password sensitivity allows removal of macro viruses from password-protected Microsoft Excel 95 files without disturbing user passwords.

  - More precise handling of password-protected Microsoft Office files as the scanner searches for macro viruses.
  - The VirusScan software now includes options to detect and remove any and all macros in any Word document or Excel Spreadsheet. (See page 94 for details.)

- **Enhanced scanning of OLE files.**
- **Additional compressed file types now scanned.** (See page 36 for further details on scanning compressed and archived files.).
- **.VBS, .INI, and .HTM file types are now scanned by default.** (For a complete list of file types scanned by default, please see page 35.)

The VirusScan Command Line package

Here is complete list of the files included with your copy of the command-line scanners.

SCAN.EXE = VirusScan Command Line program for 32-bit environments

SCANPM.EXE = VirusScan Command Line program for protected mode environments

SCAN86.EXE = VirusScan Command Line program for real-mode environments

README.1ST = Network Associates license document

PACKING.LST = Packing list

VALIDATE.EXE = Authenticity validation program

SCAN.DAT = Virus detection data

LICENSE.DAT = Virus definition data

MCSCAN32.DLL = 32-bit scanning engine

MESSAGES.DAT = List the error messages a user might encounter using the VirusScan scanners.

NAMES.DAT = Virus names definition data

CLEAN.DAT = Virus clean definition data

EMSCAN.DAT = Virus definition data for boot disk

EMNAMES.DAT = Virus definition data for boot disk

EMCLEAN.DAT = Virus definition data for boot disk

BOOTSCAN.EXE = Scanner for boot disk

WHATSNEW.TXT = Release documentation including installation instructions

RESELLER.TXT = Network Associates authorized resellers

RWABS16.DLL = VirusScan 32-bit / 16-bit support file

RWABS32.DLL = VirusScan 32-bit / 16-bit support file

VSHIELD.EXE = VirusScan on-access scan component included with the installable version of this software.

Documentation included with the VirusScan software

The documentation you received with this software includes:

- 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 the VirusScan Command Line software, and includes other useful background information and advanced configuration options. Acrobat .PDF files are flexible online documents that contain hyperlinks, outlines, and other aids for easy navigation and information retrieval.

NOTE: For best results when opening and printing the *User's Guide,* Network Associates recommends using Acrobat Reader 3.0; Reader version 3.0.1 has difficulty correctly printing graphics included in the .PDF file.

- A WHATSNEW.TXT file. This file contains last-minute additions or changes to the documentation, lists any known behavior or other issues with the product release, and often describes new product features incorporated into incremental product updates. You'll find the WHATSNEW.TXT file at the root level of your VirusScan CD-ROM; you can open and print it from Windows Notepad, or from nearly any word-processing software.
- A README.1ST file. This file outlines the terms of your license to use the VirusScan software. Read it carefully—by installing this software you agree to its terms.

Installing Your Scanning Software

2

Before you start

It’s important to minimize the risk of spreading viruses that may already be present on your system before you install the VirusScan software. Before installation:

1. Review the system requirements below.
2. Ensure that your system is virus-free.
3. Confirm that your Date / Time settings are accurate.

System requirements

- A 386 or later IBM-compatible personal computer running DOS version 5.0 or later.
- At least 4MB of memory and 4MB of free hard drive space.

Installation instructions

Follow the instructions in the next section,“The installable version of VirusScan” if you are using the installable version of the VirusScan Command Line software. See the section, “Manual installation of VirusScan” on page 32 if you are manually installing the program.

NOTE: If you suspect your system is already infected, see “If you suspect you have a virus ...” on page 67 before installing the VirusScan software.

The installable version of VirusScan

This version of the software includes VirusScan’s installation program, Install. Install will search your system for previous versions of the VirusScan software. If this is the first time you are installing the program, Install will create an installation directory, and complete the installation according to the options you choose.

To use Install:

1. Complete either a, b or c, depending on the source of your VirusScan program files:

    a. **If you are installing from compact disc,** insert the compact disc containing the VirusScan program into your CD-ROM drive.

    b. **If you are installing from floppy disks:**

    - Insert the first VirusScan floppy disk into your A: drive.
    - Use the cd command to change to the A: drive.

    c. **If you are installing from VirusScan files you downloaded from the Network Associates website:**

    - Decompress the zipped files into a temporary directory on your hard drive.

    > **NOTES:** Network Associates recommends using the -d switch to restore directory structure.
    >
    > Decompression software such as PKUNZIP is widely available; download it at no charge from the Network Associates website, www.nai.com.

    - Use the cd command to change to the folder where the VirusScan files are located.

2. Type `install.bat` at the command prompt to launch Install.

    The first Install dialog box appears.

    > **NOTE:** The action of DOS-based dialog boxes is different from making dialog box or wizard selections in Windows. Use the tab keys instead of using the mouse to move from text fields and options. To select an option, clicking **ENTER** replaces the mouse-click.

3. Select **`Next`** to begin the installation, or select **`Cancel`** to cancel the installation.

4. If you are running Install from Windows 3.1, Windows 95, or Windows NT, the following appears onscreen:

```
Install has detected that it is being run from a
DOS shell. VShield will not function in a Windows
95/NT environment.  However, VShield will
function properly in Windows 3.1x.
Do you wish to install VShield?
```

Select either **`Yes`** or **`No`**.

5. Install then displays the default installation directory, C:\NETA\SCAN. Complete one of the following:
   - **If you want Install to use this default directory,** select **`Next`**.
   - **If you prefer Install to load the files to a different installation directory:**
     a. Type the full path name to the installation directory you prefer in the space provided. Select **`Next`** to continue the installation.
     b. If the directory you specify does not yet exist, Install will ask if it can create it. Choose one of the following:
        - Select **`Yes`** to create the directory.
        - Select **`No`** to return to the installation location screen. You may then specify a different directory. Select **`Next`** to continue the installation.
6. Install then browses your system files for an existing installation of the VirusScan software, or any of its components.
   - **If no previously installed VirusScan files are found,** Install creates the installation directory you have just specified, and begins the installation of the VirusScan package.
     – Select **`Next`** to continue the installation. If you are installing from floppy disks, follow the prompts to insert the correct disks.
     – Select **`Back`** to choose a different installation directory. Type the full pathname to the location you prefer in the space provided.
     – Select **`Cancel`** to exit Install.
   - **If Install discovers a previous version of VirusScan on your system,** you are prompted to select **`OK`** to allow the overwriting of each older file.
7. Install will prompt you for permission to modify the AUTOEXEC.BAT. Choose one of the following:

- Select **`Yes`** to continue. Install modifies your AUTOEXEC.BAT, configuring the VShield scanner to launch at system startup.
- Select **`No`** if you do not want the AUTOEXEC.BAT modified. Install then creates a copy of the proposed revisions, named AUTOEXEC.NAI, for reference in case you want to modify your autoexec.bat in the future.

8. Select one of these three options:
   - **`System`** to scan your C: drive.
   - **`Full`** to scan all local hard drives.
   - **`Cancel`** to close Install. No scan will take place at this time.

   Whether you initiate a scan at this point, or choose to wait until a later time, the VirusScan software is now fully installed on your system.

Manual installation of VirusScan

Follow the directions below if your copy of the VirusScan software does not include INSTALL.BAT. (See "The installable version of VirusScan" on page 29 if you have an installable version of the software, and would like to use the installation utility.)

To manually install the VirusScan software:

1. Make a directory for the VirusScan software named "NETA" on your hard drive.
2. Complete a, b, or c, depending on the source of your VirusScan program files:
   a. **If you are installing from a compact disc:**
      - Insert the compact disc containing the VirusScan software into your CD-ROM drive.
      - Copy the VirusScan files from the compact disc to the directory you created for them, C:\NETA.

   b. **If you are installing from floppy disks:**
      - Insert the first VirusScan floppy disk into the A: drive.
      - Copy the VirusScan program files from the floppy disk to the directory you created for them on your system, C:\NETA.

c. **If you are installing from VirusScan files you downloaded from the Network Associates website,** decompress the zipped files into the C:\NETA directory you created.

NOTE: Decompression software such as PKUNZIP is widely available; download it at no charge from the Network Associates website, www.nai.com.

---

3. Add the VirusScan directory you created to the path statement in your AUTOEXEC.BAT file.
4. Make a clean start-up disk. See "Creating an emergency disk" on page 78 for more information.

To run the VirusScan program from a NetWare login script without running out of memory, follow these steps immediately after installation:

1. Rename LOGIN.EXE to LOGIN1.EXE, then remove any references to the VirusScan software from the file.
2. Create a batch file named LOGIN.BAT.
3. Use the first line of the batch file to run the VirusScan software with whatever options you want to include.
4. Use the second line of the batch file, to run LOGIN1.EXE.

These steps prevent LOGIN.EXE and SCAN.EXE from loading into memory at the same time. This allows the VirusScan scanners to run before your computer tries to get access to the network. Your login script should then run without complications.

Validating your files

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

You can protect yourself from this possibility by ensuring that you:

- Download your files only from the Network Associates website or other approved electronic source such as AOL or CompuServe; and
- Validate the files that you download.

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

How to validate your copy of the VirusScan software

To ensure that you have exactly the same files as did the engineers who packaged your copy of the VirusScan software, you need to compare the validation codes that VALIDATE.EXE generates against the packing list supplied with your copy of the software. The packing list is a text file that contains the validation codes that Network Associates engineers generated from independent cyclical redundancy check (CRC) processes when they packaged the software for delivery.

To validate your files, follow these steps:

1. Install the VirusScan software as described in "Installation instructions" on page 29.
2. Click **Start** in the Windows taskbar, point to **Programs,** then choose **MS-DOS Prompt.**
3. In the window that appears, change your command prompt to point to the directory that contains the VirusScan files. If you chose the default installation options, you'll find the files in this path:

   C:\PROGRAM FILES\NETA\SCAN
4. Run VALIDATE.EXE. To do so, type `validate *.*` at the command prompt.

   VALIDATE.EXE scans all of the files stored in your VirusScan program directory, then generates a file list that includes:

   - each file name
   - its size in bytes
   - its creation date and time
   - two validation codes in separate columns.

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

---

5. Network Associates recommends that you redirect the output from VALIDATE.EXE to your printer so that you can review it easily. Complete one of the following steps to do this:

    - If you have set your printer to capture output from MS-DOS programs, type `validate >prn` at the MS-DOS prompt. To learn how to set your printer to print from MS-DOS programs, consult your Windows documentation.

    - Alternatively, you can direct the output to a file that you designate on your hard drive. You can then print the file directly from any text editor, such as Microsoft Notepad. To direct the output to a file, type `validate *.* > c:\<directory name>\<filename>` at the command line prompt.

    To finish the validation process, you will need to compare the output from VALIDATE.EXE that you just generated against the unique packing list codes included in your copy of the VirusScan Command Line software. Complete the sequence below to generate the packing list.

To generate the packing list and complete your comparison, follow these steps:

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

2. Complete one of the following steps to print the contents of the packing list:

    - Type `type packing.lst>prn` at the DOS prompt to redirect the output from PACKING.LST to your printer.

    - Alternatively, you can direct the output to a file that you designate on your hard drive. You can then print the file directly from any text editor, such as Microsoft Notepad. To direct the output to a file, type `validate *.* > c:\<directory name>\<filename>` at the command line prompt.

3. Compare the output from VALIDATE.EXE to that from PACKING.LST.

The sizes, creation dates and times, and validation codes for each file name should match *exactly*. If they do not, delete the file immediately. Do not open the file or examine it with any other utility; doing so can risk virus infection.

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

Testing your installation with the Eicar Standard Anti-Virus Test File

Users often have the need to test that their installations function correctly. The anti-virus industry, through the European Institute for Computer Anti-virus Research (EICAR), has adopted this standard to facilitate this need.

The Eicar Standard Anti-Virus Test File is the result these efforts. To test your installation of the VirusScan software, copy the following line into its own file, name it EICAR.COM, and save it as a text file. It will be saved as a 68- to 70-byte file.

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

NOTE: The characters in this text file must all appear on one line.

When this file is scanned, it will report,

```
"Found the EICAR test file, not a virus."
```

Because the Eicar Standard Anti-Virus Test File is not a *true* virus infection, you can not clean or repair this "infected" file. Network Associates recommends deleting this file when you are finished testing your installation, so unsuspecting users are not unnecessarily alarmed.

IMPORTANT: Please note that VirusScan products that operate through a graphical user interface do *not* return this same EICAR identification message.

On-demand Scanning 3

What is on-demand scanning?

An on-demand scan is a scan operation that the user initiates. You can use the software's powerful options to scan any file you have administrative rights to at any time.

As an administrator, you maintain full control over the scope of the scans, how users will be notified if a virus in found, and how you want the VirusScan software to handle possibly corrupted files. This chapter explains how to use the program's on-demand scan features to search specific files, directories, or drives for known boot, file, multi-partite, stealth, encrypted, polymorphic, and macro viruses.

Remember, while you are learning how to configure basic scan tasks, and beginning to customize scans to meet your specific needs, the VirusScan scanners are quietly running *on-access* protections through its VShield component, which runs with a default set of options at system startup. See Chapter 4, page 59, for further details. (See "How VirusScan works" on page 22 for details on the various components of the program.)

When should you scan?

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.

The VirusScan scanners are built to operate with minimal use of system resources. The program also includes options that administrators can use to help ensure that the VirusScan software is being used most efficiently. For example, you can take advantage of the scanner's /FREQUENCY option, which sets a mandatory time period between scans, to help minimize resources during peak periods of network activity. A full list of options begins on page 46 of this chapter.

What can you scan?

File types scanned by default

VBS, INI and HTM file types have been added to the list of file types scanned by default. The VirusScan software also scan these file types as well: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD.

Archived and compressed files recognized by the VirusScan scanners

Compressed and archive file formats which the VirusScan program can scan now include RAR, TAR and GZIP format files. The software can also scan .ARC, .ARJ, .CAB, Diet, LZEXE, .LZH, PKLite, .TD0, .??_, and .ZIP files.

The VirusScan software detects and reports any infections found in any compressed or archive file it scans. The VirusScan software currently can not clean infections found in compressed or archived files. If you have access to Windows, Network Associates does have GUI versions of the VirusScan software with the ability to clean infections found in compressed files. Visit the Network Associates website, www.nai.com for detailed product information.

NOTES: The switches /UNZIP and /NOCOMP can be used to help configure how the VirusScan scanner handles compressed files. Find these and other target-related scan options in the tables from pages 47 to 50.

The VirusScan software cannot scan compressed files in low-memory (16-bit) environments.

The basics of an on-demand scan

Here are the basics of an on-demand scan. Once you master the fundamentals of how the VirusScan software functions, more advanced examples explore how to specify different targets for scan tasks.

To perform a basic scan:

1. From the command prompt, use the `cd` command to change to the directory where the VirusScan program was installed. (For example, if the software was installed on the C: drive, in directory “Scan,” type `cd scan` at the C: prompt.)
2. The following examples are general scan options. See the tables in pages 46 to 53 for a complete list of on-demand scan options at your disposal.

   NOTE: As you become more familiar with the capabilities of these scanners, you can create “scanning profiles,” which capture scan tasks for future use. See “Configuring a scan to run at system startup” on page 45, for details.

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

  ```
  scan 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:

  ```
  scan /adl /all
  ```

  where:

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

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

  ```
  scan a:
  ```

3. The VirusScan software can 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. The following information is a sample of what the program reports after scanning a floppy disk in the A: drive:

```
McAfee VirusScan for Win32 v4.0.3
Copyright (c) 1992-1999 Network Associates, Inc. All
rights reserved.
(408) 988-3832  LICENSED COPY - Nov 23 1998


Scan engine v4.0.25 for Win32.
Virus data file v4021 created 04/12/99
Scanning for 42497 viruses, trojans and variants.




05/04/99  15:12:13



Options:
A: /REPORT 40.TXT

Scanning A: []
Scanning A:\*.*
```

```
Summary report on A:\*.*
File(s)
        Total files: ...........      14
        Clean: .................       5
        Not scanned: ...........       9
        Possibly Infected: .....       0
Master Boot Record(s): .........       2
        Possibly Infected: .....       0
Boot Sector(s): ................       1
        Possibly Infected: .....       0



Time: 00:00.03
```

You may want to redirect these onscreen reports to a report file. See "Advanced scanning: an overview" on page 40 for details on scan reports.

After you initiate a scan task, one of two results occurs: If VirusScan reports that no viruses were found—as in the example above—your system is most likely virus-free. You should still maintain common-sense practices such as backing up your system, to protect your data from a possible virus infection in the future.

NOTE: The VirusScan software's ability to detect viruses must be maintained through regular updates of the VirusScan data files. For more information about updating this software, see "Updating the data (.DAT) files" on page 71.

If the VirusScan scanners find 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: The VirusScan program 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. Do not run any other programs. Turn to “If the VirusScan software detects a virus” on page 67 for details on how to manage a virus infection of your system.

Advanced scanning: an overview

Once you have mastered the basics of how the VirusScan Command Line software operates, you can take advantage of the myriad options available to build instructions for comprehensive scans of your network, generate reports of scan results, and configure scan tasks to meet various needs unique to your computing environment. In the final example in this section (page 42), you can learn how to save scans you find particularly useful as scanning "profiles." Using these profiles is an efficient means to handle multiple or repetitive scanning tasks, and they are also used as templates for new scans as your needs evolve.

This section includes a series of examples to show how to use many of the software's advanced options, create and use scanning profiles, and generate reports.

Remember: whether you are going through the following examples, or configuring custom scans on your own, you must have administrative rights to the file you target in order for a scan operation to be successful.

Example #1: Determining scan targets

The first step in building a scan command is to determine which files or directories you are targeting. You may easily scan one file or folder at a time; there are, however, many scan options which make targeting specific directories or drives easy. A complete table of such options can be found on page 47.

To initiate a scan task from the command line, complete the following steps:

1. If necessary, use the cd command to change to the directory where VirusScan is installed.
2. At the command prompt, type

   ```
   scan /adn
   ```

3. Click ENTER to initiate the scan.

   VirusScan scans all network drives, and generates an on-screen report of the results.

Example #2 Creating a scan report

Next, we'll build upon this one-step task, by asking the VirusScan program to create a report file containing the results of the scan. The report is named "WEEK40.TXT". By default, the program stores this report in the folder you are currently working from: the VirusScan installation folder.

To configure this scan task to also include a report:

1. If necessary, use the cd command to change to the directory where VirusScan is installed.
2. At the command prompt, type

   ```
   scan /adn /report /week40.txt
   ```

3. Click ENTER to initiate the scan.

   The VirusScan program scans all network drives and generates a text file of the scan results. The contents of the report are identical to what you see on-screen as the scan task is running.

Example #3 Creating an appended scan report

Perhaps it would be more useful to use this report file as a running log of the VirusScan program's ongoing scans of your network. Use the /APPEND option to append any scan results to an existing text file. When using /APPEND, if the text file you tell the software to report to—in this example, "WEEK40.TXT"— does not already exist, the program creates it for you.

To configure this scan to add scan results to an existing report file:

1. If necessary, use the cd command to change to the directory where VirusScan is installed.
2. At the command prompt, type

   ```
   scan /adn /report /append /week40.txt
   ```

3. Click **ENTER** to initiate the scan.

The VirusScan program scans all network drives, and appends the results of the scan to a preexisting report file, called WEEK40.TXT.

Example #4 Changing the location of the reports

By default, VirusScan stores any reports it generates in the folder it was installed to. Perhaps you need to share details of virus scanning activity with other members of your department. Your options are to copy the resultant text file WEEK40.TXT to a shared folder on the network, or setting VirusScan to handle this for you. The following example builds on the scan task above by asking the program to also save the report file directly to your shared network folder.

NOTE: When specifying the location the report file will be saved to, you can specify only one local and one network location.

To configure the program to save report files to different location:

1. If necessary, use the cd command to change to the directory where VirusScan is installed.
2. At the command prompt, type

```
scan a: /report /append d:\temp\week40.txt
/report /append
\\<your computer>\<shared directory>\weekly.40.txt
```

3. Click **ENTER** to initiate the scan.
4. The VirusScan program scans your A: drive, and appends the appropriate report file in two locations: your local D: drive, as well as the existing report file in the shared directory.

Example #5 Capturing this scan task in a scanning profile

Use the VirusScan software's ability to capture this scan operation in a text file. By referencing a scanning profile at the command prompt, your command-line text is greatly minimized.

To capture this customized scan task in a profile, follow these steps:

1. Using any text editor, such as Windows Notepad, open a new file.
2. Copy the command-line instructions from Step 2 above in to this file. Save the file to the VirusScan directory with the title "SAMPLE.TXT."

   NOTE: You may choose any filename for your scanning profile, and you may use any text editor to create the profile, keeping the following in mind: a true text editor such as Edit (in MS-DOS), or Notepad, saves characters to a file without additional formatting. Most word processing programs, however, add additional information which can render a file unusable as a .txt file. If you use a program such as Word or Wordpad to create text files, *be certain to save them in .txt format.*

3. To execute this scan, type the following at the command prompt:

```
scan /load sample.txt
```

The VirusScan scanners will complete the scan task as specified in the profile.

Using scanning profiles

By default, VirusScan runs with the most common scanning options enabled. For more complex scans, you may find it most efficient to save scan configurations you find useful as “scanning profiles”--text files containing your chosen settings for a particular task. (Example #5, above, used a scanning profile.) Instead of recreating a particular scan at the command line, you can load these profiles with a single command and quickly execute the preconfigured scan of your choice.

Building a complex scan operation? If you have saved a similar scan’s profile, use that profile as a template for the new scan task you are building.

In the following example, a user will use VirusScan--installed locally--to scan local data using a scanning profile stored in a common area on the network. The profile includes instructions for creating a report, titled WEEK39.TXT, to be generated to both a local destination, and to a shared network destination for group use.

In this example, the scanning profile SAMPLE.TXT contains the following scan options:

```
a: /report week39.txt
```

- Sets the a: drive as the target for the scan
- A report of this scan WEEKLY39.TXT will be generated. The content of this text file is identical to the scan results which show onscreen as the scan as in process.
- By default, VirusScan saves report files to the folder which VirusScan is installed to. In this example, the report named WEEK39.TXT is stored in a shared network folder.

NOTE: Remember, if you are saving scanning profiles to a network drive, you must have access to that drive or the scan operation will fail.

Follow these steps to load the scanning profile and initiate the scan:

1. At the command prompt, use the cd command to change to the directory VirusScan is installed.
2. To initiate a scan from a profile named SAMPLE.TXT, type the following at the command prompt:

```
scan /load sample.txt
```

While scanning profiles can be called from any local directory, by default, VirusScan saves generated reports to the folder where it was installed to.

3. Type ENTER. VirusScan will load the scanning profile and begin the scan. When the scan is complete, a report file named WEEK39.TXT can be found in the VirusScan directory. It reads:

```
McAfee VirusScan for Win32 v4.0.3

Copyright (c) 1992-1999 Network Associates, Inc. All
rights reserved.

(408) 988-3832  LICENSED COPY - Nov 23 1998


Scan engine v4.0.25 for Win32.

Virus data file v4021 created 04/12/99

Scanning for 42497 viruses, trojans and variants.




05/04/99  15:41:03



Options:

/LOAD D:\TEMP\SAMPLE.TXT


Scanning A: []

Scanning A:\*.*


Summary report on A:\*.*

File(s)

        Total files: ...........      14

        Clean: .................       5

        Not scanned: ...........       9

        Possibly Infected: .....       0

Master Boot Record(s): .........       2

        Possibly Infected: .....       0

Boot Sector(s): ................       1

        Possibly Infected: .....       0
```

Configuring a scan to run at system startup

Configuring your computer to have a VirusScan scanner automatically load at startup, and run with the options you find most helpful, is one of the best security measures you can put in place.

To add a scanning profile to run at system startup, complete the following steps:

1. Change to the root directory by typing `cd c:\`
2. Type the following:

   ```
   edit autoexec.bat
   ```

   The Edit program starts.
3. Locate the first line which references VShield. Insert one space between the word “VShield” and the first option.
4. After the single space, type:

   ```
   /load <filename>
   ```

   where <*filename*> is the name of the scanning profile you want VirusScan to run at system startup. To add additional scanning profiles, continue with Steps 5 and 6. When you are finished editing your AUTOEXEC.BAT, please skip to Step 7 below.
5. Type a single space.
6. Repeat Steps 4 and 5 until all the scanning profiles you want the VirusScan program to load at startup are entered.
7. To save your changes to the AUTOEXEC.BAT, type **ALT+F** to open the File menu, **ALT + S** to save, then type **X** to exit.

On-demand scanning options

General options

The following table lists the VirusScan scanner'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 the program creates. To do this, type /? /report *<filename>* at the command prompt. The results of your scanning report are appended with the full set of options available for that scan task.
/ANALYZE	Extended memory required.	Sets the program 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.
/LOAD *<filename>*	None.	Load scanning options from the named file, or "scanning profile." Scanning profiles can be called from any local directory.
/MANALYZE	Extended memory required.	Sets VirusScan's heuristic scanning features to target macro viruses. *Note:* /PANALYZE targets program viruses only; /ANALYZE targets both program and macro viruses.
/NOEXPIRE	None.	Disables the "expiration date" message if the VirusScan data files are out of date. See Chapter 6, page 71 for details on these files.
/PANALYZE	Extended memory required.	Sets the VirusScan program to heuristically scan for program viruses. *Note:* /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.

Target options

The following table lists VirusScan's target-related scanning options.

❑ **NOTE:** To configure on-demand scans, you must note a target location for the scan (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, the program only scans files with the following extensions: .BIN, .COM, .DLL, .DOC, .DOT, .EXE, .INI, .HTM, HTML, .OVL, .RTF, .SYS, .XLA, .XLS, .XLT, .VBS and .VXD. These are the file types that are most susceptible to viruses.
/BOOT	None.	Scan boot sector and master boot record only.
/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 ?

Target Command-Line Option	Limitations	Description
/MANY	None.	Scans multiple disks consecutively in a single drive. The program prompts you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run the VirusScan program from a boot disk and you have only one floppy drive.
/MAXFILESIZE *<xxx.x>*	None.	Scan only files no 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, the program 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 the scanners from accessing the boot record. This feature was added to allow the software to run under Windows NT. You might need to use this option on some device-driven drives. Using /NODDA with the /ADN or /ADL switches can 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.
/NOMEM	None.	Does not scan memory for viruses. This greatly reduces scan time. Use /NOMEM only when you are absolutely certain that your computer is virus-free.

Target Command-Line Option	Limitations	Description
/SUB	None.	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, the VirusScan scanners 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 specify an entire drive as a target.
/UNZIP	Extended memory required.	Scan inside compressed files.

Response and notification options

The following table lists the VirusScan program'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 the NetShield program.	Designates the directory *<dir>* as a network path to a remote NetWare volume or Windows NT directory, monitored by Centralized Alerting*.
		The VirusScan program sends 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 which is sent 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 if a single infection is found. *Note:* This option deletes all macros, 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.
/DAM		A repair switch: deletes all macros in the event an infected macro is found. If used with /FAM, like in this example: scan <filename> /fam /dam this option can be used to pre-emptively delete *all* macros in a file.
/DEL	None.	Deletes infected files permanently.
/FAM		Find all macros: not just macros suspected of being infected. It causes any macro found to be treated as a possible virus detection. When used in conjunction with the option /DAM, as in this example: scan <filename> /fam /dam. this option finds and deletes *all* macros upon first detection of a macros virus in a file.
/DEL	None.	Deletes infected files permanently.

Response and Notification Command Line Option	Limitations	Description
/LOCK	Not available in low-memory environments.	With the /LOCK option enabled, VirusScan halts and locks your system if it finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. Network Associates recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if the VirusScan program locks the system.
/MOVE *<dir>*	None.	*/MOVE <directory>:* Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. *Note:* This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.
/NOBEEP	None.	Disables the tone that sounds whenever the VirusScan scanners find 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.
- **To capture a VirusScan report to a text file,** /REPORT must be used, along with any additional switches as needed.

For additional examples of using VirusScan's reporting options, see "Advanced scanning: an overview" on page 40.

Report Command-Line Option	Limitations	Description
/ALERTPATH *<dir>*	None.	Designates the directory *<dir>* as a network path monitored by Centralized Alerting.
/APPEND *<filename>*	None.	Used with /REPORT to append the results of a scan to the specified report *<filename>* instead of overwriting the existing content.
/PAUSE	None.	Enables screen pause. The "Press any key to continue" prompt will appear when the VirusScan program fills a screen with messages. Otherwise, by default, the program fills and scrolls a screen continuously without stopping. This allows the VirusScan software to run on PCs with multiple drives or that have severe infections, without needing your input. Network Associates recommends omitting /PAUSE when using the report options (/REPORT, /RPTALL, /RPTCOR, and /RPTERR).

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 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. Network Associates recommends omitting /PAUSE when using any report option.
/RPTALL	None.	Includes the names of all scanned files in the /REPORT file. You can use /RPTCOR with /RPTERR on the same command line. Network Associates recommends omitting /PAUSE when using any report option.
/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 that the VirusScan scanners find 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). Network Associates recommends omitting /PAUSE when using any report option.

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. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. 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. Network Associates recommends omitting /PAUSE when using any report option.
/VIRLIST	None.	Displays the name of each virus that the VirusScan software can detect. Because the VirusScan program can detect many viruses, this file is over 250 pages long. This is too large for the MS-DOS “Edit” program to open; Network Associates recommends using Notepad or another text editor to open the virus list.

Viewing the Virus List

The Virus List is a comprehensive list of viruses detected by the VirusScan scanners. This list provides information for each known virus which the software can detect, including what type of virus it is, its characteristics, size, and whether or not it can be "cleaned," leaving the infected file intact.

Monthly updates to this list are available from Network Associates, and should be updated in a timely manner; please see "Updating the data (.DAT) files" on page 71 for details.

To view the on-screen list of viruses detected by VirusScan:

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

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

   where <*filename*> is the name you chose for the text file. You can use any name you want to use. This redirects the output of the current Virus List to <*filename*>.txt.
3. Since the Virus List is over 250 pages long, it is too large a file for Edit to open. To view this file, open it in Notepad or another text editor of your choice. For instructions on printing the file, see below.

To print the list of viruses detected by the VirusScan software, complete the following steps:

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

   ```
   scan /virlist /report filename.txt
   ```

   where <*filename*> is the name you chose for the text file. You can use any name you want to use. This redirects the output of the current Virus List to <*filename*>.txt.
3. If your printer is set to capture output from MS-DOS programs, type `<filename>.txt>prn` at the MS-DOS prompt to redirect the output of <*filename*>.txt to your printer.

NOTE: To learn how to set your printer to print from MS-DOS programs, please consult your Windows documentation.

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.

Preparing your system

The VirusScan software needs to run from your hard drive in order to scan floppy disks inserted into the A: drive. This means that if you have the program running from floppy disks, and you have only one floppy drive on your computer, you must install and run the VirusScan software from your hard drive in order to scan floppy disks in the A: drive. (See Chapter 2, “Installing Your Scanning Software.” for installation instructions.)

How to scan floppy disks

To scan floppy disks:

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

   ```
   scan 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.

   > ☐ **NOTE:** If the VirusScan scanners detect a virus on this disk, it will carry out the command-line option you chose for dealing with the virus. See “Removing a virus found in a file” on page 68 for details on virus removal.

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.

On-access Scanning

4

What is on-access scanning?

The VShield scanner is the on-access scanning component of the VirusScan package. It automatically scans any file on your system as it's opened, or any executable as it's launched. Once you install the VShield scanner, it starts protecting your computer immediately with a default set of options, providing a strong defense against new virus threats. You can further customize on-access scanning by using the options listed in the tables from pages 62 to 63 of this chapter.

You can easily configure the VShield scanner to launch at system startup to ensure continuous on-access protection: see "Editing your AUTOEXEC.BAT file" on page 64 for instructions. The VShield scanner launches and runs silently in the background, terminating when you end your DOS session.

On-access scanning in the Windows NT environment:

On-access scanning is not available for the Windows NT command line environment. To perform on-access scanning in a Windows NT environment, Network Associates recommends the graphical user interface version of VirusScan for Windows NT. See "How to contact Network Associates" on page xiii for further details.

On-access scanning in the OS/2 environment:

Network Associates recommends the new VirusScan for OS/2 for users needing on-access scanning protection in the OS/2 environment.

Users of earlier versions of the VirusScan Command Line software may wish to continue using the VShield scanner in the OS/2 environment. Limitations of this scanner in OS/2 include:

- The VShield scanner does not run directly in the OS/2 environment. You can, however, use its features to scan DOS or FAT partitions on your hard disk by starting a DOS or WINOS2 session in OS/2.
- Some configuration options do not function in an OS/2 environment—this manual notes these exceptions in the descriptions of each option. See the command tables in "Configuring the VShield scanner" on page 61, and in Appendix C, page 91, for details.
- The VShield scanner detects only those viruses that can propagate in the OS/2-DOS environment; a virus in a file with a long filename, for example, is not detected.

Starting the VShield scanner

If you have configured your computer to load the VShield scanner at startup, it will load and remain active in the background when you start your system.

Is the VShield scanner active? Follow either of these steps to find out:

- Type `chkvshld` at the DOS prompt in the the VirusScan program directory. You will receive a message that tells you if the VShield scanner is running, and if so, which of its options are currently selected.
- Check your AUTOEXEC.BAT file for the VShield scanner's command line. (See "Editing your AUTOEXEC.BAT file" on page 64 for instructions.)

Disabling the VShield scanner

At times you may need to temporarily disable the on-access scanner—when updating the virus data (.DAT) files, for example. (See page 71.) Remember, any files you download, or new data files that you open can not be properly scanned if this module is disabled.

To temporarily disable VShield, follow these steps:

1. If necessary, use the cd command to change to the directory where the VirusScan software was installed to.
2. Type VSHIELD /REMOVE at the command prompt. This unloads the VShield scanner from memory.
3. To enable on-access scanning, complete either of the following steps, depending on the how your system is configured:
    - Restart the VShield scanner by typing VSHIELD at the command prompt, followed by the scanning options that you want to use. (See pages 62 to 63 for a complete listing of on-access scanning options.)
    - If you previously configured your AUTOEXEC.BAT file to load the VShield scanner at startup, rebooting your computer will reenable the scanner.

Optimizing the VShield scanner's performance

The VShield scanner is a Terminate-and-Stay-Resident (TSR) program, which remains in memory while you run other programs. The scanner tries to optimize memory usage and minimize conflicts with other TSRs.

If, however, you do encounter problems using on-access scanning, they may be due to conflicts with other TSR programs in your system, or with other programs that monitor disk access. The VShield scanner minimizes the use of conventional memory by attempting to load into extended, expanded, upper memory, or a combination thereof, before using conventional memory. If you have more than 640 KB, the VShield scanner tries to load as much of itself as possible above conventional memory, first into expanded memory (EMS), into extended memory (XMS), then into upper memory blocks (640 KB to 1024 KB, or UMB).

Configuring the VShield scanner

The on-access scanner runs with the most common configuration options enabled by default. Unless you disable the program, or stop it entirely, you never have to worry about starting the VShield scanner, or scheduling tasks for it.

As you become more familiar with how on-access scanning can best help guard your system, you can edit your AUTOEXEC.BAT file to tailor the VShield scanner to best meet your needs.

To customize the VShield scanner, follow these steps:

1. Choose the on-access scanning options most suitable for your work environment. Either of these sources provides a complete list of these options:
   - The tables starting on page 62 of this chapter
   - An on-screen list of scanning options and their usage. To open this list:
     a. Use the `cd` command to change to the VirusScan directory
     b. Type `vshield /?` at the command prompt.

        A complete list of on-access scanning options appears. This list is also reprinted in the tables on page 62.
2. After choosing your on-access scanning options, continue with the instructions on page 64 to add these options to the VShield scanner line in your AUTOEXEC.BAT file.

VShield options

General options

Command-line Option	Limitations	Description
/? or /HELP	None.	Displays a list of the VirusScan program's command-line options, each with a brief description.
/NOREMOVE	None.	Prevents the VShield scanner from being removed from memory with the /REMOVE switch.
/RECONNECT	None.	Restores the VShield scanner after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	None.	Unloads the VShield scanner from memory.
/SAVE	None.	Saves the command-line options to the VSHIELD.INI file.

Memory options

Memory Command-line Option	Limitations	Description
/MEMEXCL	Not available for Windows.	Excludes the memory address A0000:0000 from scanning.
/NOEMS	None.	Keeps the VShield scanner from using expanded memory (EMS).
/NOMEM	None.	Does not scan memory for viruses. This greatly reduces scan time. Use /NOMEM only when you are absolutely certain that your computer is virus-free.
/XMSDATA	None.	Loads VShield data files into XMS memory.

Target options

Target Command-line Option	Limitations	Description
/ANYACCESS	None.	Scans: • the boot sector whenever a disk is either read or written to • executables • any newly created files.
/BOOTACCESS	None.	Scans a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/FILEACCESS	None.	Scans executable files on access as well as execution. *Note:* This scan does *not* check the boot sector.
/IGNORE *<drive(s)>*	None.	Does not check any files loaded from the specified drive(s).
/NODISK	None.	Does not scan boot sector while loading the VShield scanner.
/NOWARMBOOT	None.	Does not check the disk boot sector of the floppy disk in drive A: for viruses during warm boot (system reset or CTRL+ALT+DEL).

Notification options

Notification Command-line Option	Limitations	Description
/CONTACT *<message>*	None.	Displays the specified message when a virus is detected. This message cannot exceed 255 characters.
/CONTACTFILE *<filename>*	None.	Displays the contents of *<filename>* if a virus is detected.
/LOCK	Not available in low-memory environments.	With this /LOCK option enabled, the program halts and locks your system if it finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. Network Associates recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if the VirusScan program locks the system.

Editing your AUTOEXEC.BAT file

After selecting the on-access scanning configuration options best suited to your environment and operating system (see "Configuring the VShield scanner" on page 61 for a list of options), you are ready to edit your AUTOEXEC.BAT file.

To edit your AUTOEXEC.BAT file, follow these steps:

1. Change to the root directory by typing `cd c:\`
2. Type:

   ```
   edit autoexec.bat
   ```

   The Edit program starts.
3. Locate the first VSHIELD line. Insert one space between the word "VShield" and the first option.
4. Type a scanning option (such as /ANYACCESS or /BOOTACCESS).

   NOTE: For DOS sessions in OS/2:
   —The /BOOTACCESS option, *is not valid* since the VShield scanner only scans files stored on floppy disks, but does not scan the boot sectors of floppy disks.
   —The /ANYACCESS option, while functional, scans only floppy disk files.

5. Type a single space.
6. Repeat steps 4 and 5 until all of your chosen options are entered.
7. To save your revisions, press **ALT+F.** The **File** menu appears; press **S** to save.
8. To exit and return to the DOS prompt, press **ALT+F** to open the **File** menu, then press **X** to exit.

Removing Infections From Your System

5

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 helps eliminate one potential cause of your computer problems.

If you have or suspect that you have a virus, and you haven't yet installed the VirusScan software, follow these steps to clean your system:

1. Turn off your computer.

   ✸ **WARNING:** Do not reboot using the reset button or **CTRL+ALT+DELETE;** if you do, some viruses might remain intact or drop destructive payloads.

2. Place a clean start-up disk into the floppy disk drive. If you do not have a clean start-up disk, see "Creating an emergency disk" on page 76.
3. Turn on your computer.
4. At the command prompt, type `scan /ADL /ALL /CLEAN`.

5. **If viruses were removed:**

    Shut down your computer and remove the disk. Begin the installation procedure described in Chapter 2, “Installing Your Scanning Software.”

    To find and eliminate the source of infection, scan your disks immediately after installation. For information on scanning your disks, see “Scanning your floppy disks” on page 57.

    If viruses were not removed:

    If VirusScan cannot remove a virus, you will see one of the following messages:

    ```
    Virus could not be removed.
    ```

    ```
    There is no remover currently available for the
    virus.
    ```

    If the VirusScan scanners finds a virus in a file and cannot remove it, your only choice is to delete the infected file and restore from backups. If the virus was found in the Master Boot Record, refer to documents on the Network Associates website related to manually removing viruses.

If the VirusScan software detects a virus

Viruses attack computer systems by infecting files—usually executable program files or Microsoft Word documents and templates. The VirusScan software can safely remove most common viruses from infected files and repair any damage they may have caused.

Some viruses, however, are designed to damage your files beyond repair. These irreparably damaged files, called “corrupted” files, can be moved by the VirusScan program to a quarantine directory or deleted permanently to prevent further infection of your system.

Removing a virus found in memory

If the VirusScan scanners discover a memory-resident virus, complete the following steps to remove it:

1. Turn off your computer.

   NOTE: Do not reboot using the reset button or **CTRL+ALT+DELETE;** if you do, some viruses might remain intact or drop their destructive payloads.

2. Place a clean start-up disk into the floppy disk drive. If you do not have a clean start-up disk see “Creating an emergency disk” on page 76.
3. Turn on your computer.
4. At the command prompt, type `scan /ADL /ALL /CLEAN`
5. **If viruses were removed:**

   If VirusScan successfully removes all the viruses, shut down your computer and remove the clean start-up disk. Begin the installation procedure again, as described in Chapter 2, “Installing Your Scanning Software.”

   To find and eliminate the source of infection, scan your disks immediately after installation. For information on scanning your disks, see “Scanning your floppy disks” on page 57.

   If viruses were not removed:

   If the VirusScan software cannot remove a virus, you will receive the message:

   ```
   Virus could not be removed.
   ```

```
There is no remover currently available for the
virus.
```

If the virus was found in a file and cannot be removed by the VirusScan program, you should delete the file and repeat the steps described in "If you suspect you have a virus ..." on page 65. If the virus was found in the Master Boot Record, refer to documents on the Network Associates website related to manually removing viruses. For more information, see "How to contact Network Associates" on page xiii.

Removing a virus found in a file

If the VirusScan software detects a virus in a file, it displays the path names of infected files and takes the action specified in either the loaded scanning profile or command-line options. (See Chapter 3, page 35 for details on creating scanning profiles.) For example:

- If you selected /MOVE, the VirusScan program will automatically move the infected files to the specified quarantine directory.
- If you selected /CLEAN, the VirusScan program will attempt to repair the file.
- If you selected /DEL, the VirusScan program will delete and permanently overwrite the infected file.

Additional virus cleaning tasks

Cleaning macro viruses from password-protected files

NOTE: The VirusScan scanners detect macro virus infections in password-protected Microsoft Word 95 (Word 7.0) files in at least six languages.

The VirusScan software is designed to respect users' passwords and leave them intact as often as possible. For example, in password-protected Microsoft Excel 95 files, the program removes macro viruses without disturbing users' passwords.

Macro viruses that infect Microsoft Word files, however, sometimes plant their own passwords. Depending on the capabilities of the particular virus, the VirusScan software will take one of the following actions when it is instructed to clean a password-protected file:

- **If the macro virus cannot plant its own password: the** VirusScan software notes the infection but does not remove the password.

- **If the macro virus can plant its own password: the** VirusScan software cleans the file, removing the planted password along with the virus itself.

Windows NT hard disks:

To clean the Master Boot Record (MBR) on a hard disk formatted with the Windows NT file system (NTFS), follow these steps:

1. Start the computer that has the NTFS file system partition from a virus-free DOS boot disk.
2. Start the VirusScan program with the options /BOOT /CLEAN. Be sure to run the VirusScan program from a floppy disk that you know is free from viruses.

   This will clean the NTFS file system Master Boot Record, but the VirusScan software cannot read the rest of the NTFS file system partition when you boot into a DOS environment.
3. To scan the rest of the NTFS file system partition, reboot into Windows NT, then run the VirusScan program again.

Understanding false alarms

A false alarm is a report of a virus found in a file or in memory when a virus does not actually exist. You are more likely to see false alarms if you are using more than one brand of virus protection software, because some anti-virus programs store their virus signature strings unprotected in memory. As a result, the VirusScan software may “detect” these unprotected strings falsely as a virus.

It is safest to assume that any virus reported by the VirusScan program is a genuine virus threat, and take steps to remove it from your system. If, however, you have reason to believe that the software is generating a false alarm—for example, flagging a file as infected when you have been using it safely for years—review these potential sources for the false detection before contacting Network Associates.

- **You may have more than one anti-virus program running.** If so, the VirusScan program might think that unprotected virus signatures that the other product uses in its own detection efforts are viruses. To solve this problem, configure your system to run only one virus program. When you’ve completed reconfiguring your system, shut down your computer, and turn off the power. Wait a few seconds before turning it on again so that your system can clear the other program’s virus signatures from its memory.

- **You have a BIOS chip with anti-virus features.** Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer's reference manual for details on how its anti-virus features work, and how to disable them if necessary.

- **You have an older Hewlett-Packard or Zenith PC.** Some older models from these manufacturers modify the boot sector each time the system is booted. The VirusScan software may detect these modifications as a possible infection. Check your computer's reference manual to determine if your PC has self-modifying boot code.

- **You have copy-protected software.** There are types of copy protection that may trigger VirusScan to report viruses in the boot sector or Master Boot Record on some floppy disks or other media.

- **Operating system security issues may be limiting how you can scan for viruses.** Because of operating system security, when the VirusScan program scans PAGEFILE.SYS, registry hive files, or user profiles, the system may beep, and a "Read Access Denied" non-critical error message may be displayed.

- **You do not have the correct administrative rights to scan correctly.** Within the Windows NT environment, VirusScan is not be able to access the boot sectors and the Master Boot Record unless you have administrative rights.

If none of these situations apply, contact Network Associates technical support (see page xiv for contact information), or e-mail AVresearch@nai.com with a detailed explanation of your situation.

Using the Virus Definition (.DAT) Files

6

What are the .DAT files?

Between 200 to 300 new viruses are discovered each month. The data files that came with your copy of the VirusScan software might not be able to help the software detect a virus discovered months after you first bought the product.

The files named CLEAN.DAT, NAMES.DAT, and SCAN.DAT all provide virus information to your VirusScan software. These are the data files we’re referring to in this User’s Guide.

To offer the best virus protection possible, you must regularly download and install updates to these three virus data files that VirusScan uses. Network Associates continually updates these files. Weekly updates of .DAT files are available to licensed VirusScan software users at the Network Associates website (www.nai.com) and other electronic services.

If 90 days pass since you last updated the .DAT file, the software notifies you that an update is needed. (This feature can be turned off by using the /NOEXPIRE option. See page 97 for details.) This release of the VirusScan Command Line software includes the 4025 .DAT files. Please see “Updating the data (.DAT) files” on page 71 for instructions on updating the .DATs.

NOTE: Since the VirusScan scanners use the same virus data files as other VirusScan products that may be installed in your network, you can be assured that with current .DAT files in place, command line scanners offer identical protection to other Network Associates anti-virus software.

Updating the data (.DAT) files

The 4025 .DAT files are compatible with Network Associates anti-virus products that use scan engine versions 4.0.xx only. The .DAT files included with this release of the software does *not* work with any VirusScan product that uses a 3.x or v2.x scan engine.

Please note that your ability to download updated .DAT files is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the VirusScan software, and detailed in the software license agreement. See page 71 for more information.

To update .DAT files for the VirusScan Command Line software, follow these steps:

1. Download the data file (for example, DAT-4026.ZIP) from any of these sources:
   - Network Associates' website, http://www.nai.com
   - Network Associates ftp site, at ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
   - Network Associates downloads are also available in the anti-virus area of AOL and CompuServe.

   > **IMPORTANT:** As you are selecting the latest .DATs, you will find references to self-installing .DAT files. Installable .DAT files cannot be used with the VirusScan Command Line scanners.

2. Create a temporary directory on your hard disk.
3. Copy the .DAT file .zip archive you downloaded to that temporary directory.
4. If you have the VShield scanner running on your system, you will need to unload it from memory by typing VSHIELD /REMOVE at the command prompt. This step is not necessary if you have not started the VShield scanner.
5. Locate the directories on your hard drive where your VirusScan software is currently loaded. Typically, the files are stored in C:\NETA\SCAN.
6. The updated .DAT file you just downloaded is in a compressed "ZIP" format. Unzip the file using any PKUNZIP-compatible decompression software. If you don't have the decompression software, you can download PKUNZIP (shareware) from any of the Network Associates electronic sites.
7. You can unzip the files directly to the VirusScan Command Line program directory. Allow the updated files to overwrite the existing .DAT files.

   > **NOTE:** If other VirusScan products are loaded on your system, or if you chose custom installation options, there may be .DAT files located in more than one directory. If so, save these updated .DAT files to each directory.

8. Restart the on-access scanner. To do so, type VSHIELD, followed by the scanning options you want to use, at the command-line prompt. (See pages 62 to 63 for a complete listing of on-access options.)

    NOTE: If you previously configured your AUTOEXEC.BAT file to load the VShield scanner at startup, you do not need to complete this step; the VShield scanner loads itself automatically as you restart your system.

9. Reboot your computer so that changes take place immediately.

New developments in updating the VirusScan software

Network Associates is now offering self-installing upgrades to the scanning engine as well as the virus data (.DAT) files which the engine uses in its virus handling tasks. Both these updating tasks are now efficiently handled by a single utility. See "How VirusScan works" on page 22 for details.

Preventing Virus Infection A

Keys to a secure system environment

The VirusScan software is a powerful tool for preventing, detecting, and recovering from virus infection. It is most effective, however, as the cornerstone of a comprehensive computing security program that includes a variety of safety measures such as regular backups, meaningful password protection, user training, and virus awareness.

To help minimize your chance of infection, incorporate these safeguards into your work routine:

- Install the VirusScan software on your system, follow the installation procedures described in Chapter 2, "Installing Your Scanning Software." If you are concerned that your computer may already be harboring infected data, take steps to clean your system before installing the product. See "If you suspect you have a virus ..." on page 65.
- Be prepared to recover from a system crash without compromising desktop security. Create a start-up disk containing the VirusScan software by following the instructions outlined in "Creating an emergency disk" on page 76. Make sure to write-protect this disk so that it cannot become infected.
- Make frequent backups of important files. Even with the VirusScan program's abilities to contain and clean most viruses, certain malicious viruses (as well as fire, theft, vandalism, or ordinary disk failure) can render infected files unrecoverable. Without recent backups, you cannot recover your data.
- Scan all floppy disks that you use. See page 57 for detailed instructions.
- Never start your computer from an unscanned disk.
- Always make sure your disk drives are empty before starting your computer.
- Always scan programs that are new to your computer. Before running the software for the first time, be sure to scan the directory containing the new program files.
- Validate your VirusScan program files as soon as you receive your software.

- Update your VirusScan data files regularly. These are the files with information on current viruses that the VirusScan scanners use for detection and cleaning.

Outlining a full security program is beyond the scope of this manual. However, by following the steps provided in this appendix and reading the information provided in the Preface, "Where do viruses come from?" on page viii, you can gain a clearer understanding of what viruses are, how they affect your system, and what you can do to prevent an infection.

Validating the VirusScan program files

When you download a file from any source other than the Network Associates bulletin board or other Network Associates service, it is important to verify that it is authentic, unaltered, and uninfected. To facilitate this, the VirusScan package includes a utility program called Validate that you can use to ensure that your version of the VirusScan software is authentic. When you receive a new version of this software, run Validate on all of its program files and .DAT files.

For detailed instructions, see "How to validate your copy of the VirusScan software" on page 32.

Creating an emergency disk

In case your system becomes infected, you should have a clean start-up (also called boot, or emergency) disk. This section describes how to create that emergency disk. Since any virus residing in your system could be transferred to your emergency disk and reinfect your system, your system *must* be virus-free to create it. If your computer is infected, go to another computer and scan it. If it is virus-free, create your boot disk at this alternate workstation.

This emergency disk is for scanning the boot sector and system files only; it is not intended for normal scanning.

IMPORTANT: Because Windows NT cannot boot from a floppy disk, this boot disk cannot be formatted from within a Windows NT environment.

To create a boot disk:

1. Exit from Windows or any applications to get the command prompt (`C:\>`).
2. Insert a blank, *unformatted* disk into the A: drive.

3. Format the disk by typing the following command at the command prompt:

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

   This overwrites any information already on the disk.

4. When the system prompts you for a volume label, enter an appropriate name for your start-up disk.

5. Locate HIMEM.SYS on your hard drive.

   - DOS users: by default, this can be found in the \DOS directory.
   - Windows users: by default, this file can be found in the \WINDOWS\COMMAND directory.

6. Copy HIMEM.SYS to your A: drive by typing the following at the command prompt:

   ```
   copy himem.sys a:\
   ```

7. Create a file called CONFIG.SYS.

   You can do this from within DOS, or by using Notepad or any other text editor of your choice.

❑ **NOTE:** A true text editor such as Edit (in MS-DOS), or Notepad, saves characters to a file without additional formatting. Most word processing programs, however, add additional information that can render a file unusable as a .txt file. If you use a program such as Word or Wordpad to create text files, *be certain to save them in .txt format.*

- To create CONFIG.SYS at the command prompt:

  a. Type:

     ```
     Edit
     ```

     The DOS editing program starts.

  b. Type the following lines:

     ```
     DEVICE=HIMEM.SYS
     DOS=HIGH
     ```

  c. Select **File, Save As ...** and enter the name CONFIG.SYS.

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

   e. Select **File, Exit** to close Edit and return to the command prompt.

- To create CONFIG.SYS using Notepad or any other text editor of your choice:

   a. Launch the editing program, and open a new file.

   b. Complete steps b.> through e.> above.

8. Change to the VirusScan program directory. By default, this is C:\NETA\SCAN.

9. Copy the command-line version of the VirusScan software to the disk by typing the following commands at the prompt:

```
copy bootscan.exe a:\
copy emscan.dat a:\scan.dat
copy emclean.dat a:\clean.dat
copy emnames.dat a:\names.dat
copy license.dat a:\
copy messages.dat a:\
```

   You have now copied, and renamed where necessary, all the files the VirusScan software needs to scan the boot sector of an infected computer.

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

11. You have now completed copying all necessary programs for rebooting your system onto this boot disk.

12. You may want to copy these additional useful command-line programs to a *second* disk:

NOTE: Do not attempt to copy these programs to the clean boot disk you are making. Conventional disks do not have enough storage space to accommodate both the VirusScan software and these programs.

- debug.*
- diskcopy.*
- fdisk.*

- format.*
- label.*
- mem.*
- sys.*
- xcopy.*

NOTE: If you use a disk compression utility or a password encryption utility, be sure to copy the drivers required to access your drives onto the clean boot disk. See the documentation for those utilities for more information about those drivers.

---

13. Label and write-protect these disks, then store them in a secure place. See “Write-protecting a disk” on page 80 for more information.

Write-protecting a disk

Floppy disks are convenient, portable devices for storage and retrieval of computer data. They are also a common vehicle viruses use to invade your computer's system.

One way to help avoid infection via floppy disk is to *write-protect* the disks you are using for read-only data. If your system becomes infected with a virus, the write-protection feature will keep these disks from becoming infected as well, preventing reinfection after your system is cleaned.

NOTE: You should scan and clean any disks before you write-protect them.

To write-protect 3.5" floppy disks:

1. Position the disk face down with the metal slide facing you.
2. Examine the small rectangular hole on the upper-left side. There should be a square, plastic tab that you can slide up and down across the hole.

   To write-protect the disk, slide the plastic tab upward toward the edge of the disk so that the hole is open. This stops you from accidentally changing data on the disk. It also prevents viruses from infecting the disk.

   NOTE: If there is no tab and the hole is open, the disk is permanently write-protected.

Network Associates Support Services

B

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

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

PrimeSupport Options for corporate customers

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

PrimeSupport KnowledgeCenter

PrimeSupport KnowledgeCenter gives you access to technical support assistance via a Network Associates online knowledge base, in addition to product upgrades via the Network Associates website. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport KnowledgeCenter as part of the package for either one or two years from your date of purchase, depending on the length of your subscription. If you purchased your Network Associates product with a one-year license, you can renew your PrimeSupport KnowledgeCenter plan for an annual fee.

To receive your KnowledgeCenter password or to register your PrimeSupport agreement with Network Associates, visit:

http://knowledge.nai.com/

Your completed form will go to the Network Associates Customer Care Center. You must complete this form before you connect to the PrimeSupport KnowledgeCenter or before you call Network Associates PrimeSupport.

PrimeSupport KnowledgeCenter features:

- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Connect

PrimeSupport Connect gives you telephone access to essential product assistance from experienced Network Associates technical support staff members.

PrimeSupport Connect features:

- Unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Connect 24-By-7*

PrimeSupport Connect 24-By-7 gives you round-the-clock telephone access to essential product assistance from experienced Network Associates technical support staff members. You can purchase PrimeSupport Connect 24-By-7 on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

PrimeSupport Connect 24-By-7 features:

- Unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- Priority call handling during business hours
- After-hours responses for urgent issues within one hour, including weekends and local holidays
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Enterprise*

PrimeSupport Enterprise gives you round-the-clock, 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 Enterprise representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Enterprise gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Enterprise on an annual basis when you purchase a Network Associates product either with a subscription license or a one-year license.

PrimeSupport Enterprise features:

- Unlimited, toll-free telephone access to an assigned technical support engineer on a 24-hour-per-day, seven-day-per-week basis, including on weekends and local holidays
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times from your support engineer, who will respond to pages within half an hour, to voice mail within one hour, and to e-mail within four hours

- Ability to designate at least five people in your organization as customer contacts
- The option to be a beta site for new Network Associates products
- Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes
- Unrestricted, 24-hour-per-day access to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

Ordering Corporate PrimeSupport*

To order PrimeSupport KnowledgeCenter, PrimeSupport Connect, PrimeSupport Connect 24-By-7, or PrimeSupport Enterprise for your Network Associates products:

- Contact your sales representative; or
- In North America, call Network Associates Support Services at (800) 988-5737 or (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.

Table B-1. Corporate PrimeSupport at a Glance

Feature	Knowledge Center	Connect	Connect 24-By-7	Enterprise
Technical support via website	Yes	Yes	Yes	Yes
Software updates	Yes	Yes	Yes	Yes
Technical support via telephone	—	Monday–Friday 8:00 am–8:00 pm Central Time	Monday–Friday 8:00 am–8:00 pm Central Time After-hours emergency response	24-hour-per-day access to your assigned support engineer (24 hours per day, 7 days per week)
Priority call handling	—	—	Yes	Yes
After hours support	—	—	Yes	Yes
Assigned support engineer	—	—	—	Yes
Proactive support contact	—	—	—	Yes
Designated customer contacts	—	—	—	At least 5
Committed response time	—	—	Within 1 hour for urgent issues	After hours pager: 30 minutes Voicemail: 1 hour E-mail: 4 hours

PrimeSupport Options for retail customers

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

- Free data (.DAT) file updates for the life of your product via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see the chapter or appendix about software updating in your anti-virus software *User's Guide* for details). You can also update your data files by using your web browser to visit:

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

- Free program (executable file) upgrades for one year via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service (see the chapter or appendix about software updating in your anti-virus software *User's Guide* for details). If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your web browser to visit:

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

- Free 24-hour-per-day, seven-days-per-week access to online or electronic support through the Network Associates voice and fax system, the Network Associates website, and through 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) 346-3414
  - Network Associates website: http://support.nai.com
  - CompuServe: GO NAI
  - America Online: keyword MCAFEE

- Free access to the PrimeSupport KnowledgeBase: online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes. Visit the KnowledgeBase at:

  http://knowledge.nai.com

- 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.

You can also take advantage of a variety of additional support options geared toward your needs. You can purchase these options either with your Network Associates product or after your complimentary 90-day support period expires:

- **Small Office/Home Office Annual Plan.** This plan gives you unlimited toll-free access to technical support during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.
- **Pay-Per-Minute Plan.** This plan gives you support only when you need it: 900-number access to technical support features priority call handling to minimize your hold time and the first two minutes of support free.
- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via Network Associates online or electronic services.
- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot access product upgrades online. This service is available for VirusScan and NetShield only.

Ordering Retail PrimeSupport*

To order the PrimeSupport Small Office / Home Office Annual Plan, Pay-Per-Minute Plan, Online Upgrades Plan, or Quarterly Disk / CD Plan for your Network Associates products:

- In North America, call Network Associates Customer Care at (972) 278-6100; or
- Visit the Network Associates website at:

http://www.nai.com/services/support/add_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 Global Professional 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.

Jumpstart Services

You can take advantage of a variety of Jumpstart Services to help you implement your new Network Associates product:

- **Basic and Advanced.** This service installs, configures, and optimizes your new Network Associates product, and gives basic operational product knowledge to your team.
- **Selfstart.** This service helps prepare you to perform your new product implementation on your own and, in some cases, installs the product.
- **Proposal Development.** This service evaluates processes and procedures as well as hardware and software requirements prior to a new product implementation, enabling a consultant to prepare your custom proposal.

Network Consulting

Network Associates consultants provide expertise in protocol analysis and a vendor-independent perspective that creates unbiased solutions for troubleshooting and optimizing your network. Also, their broad understanding of network management best practices and industry relationships speeds escalation of problems through vendor support.

You can order a custom consultation to help with planning, design, implementation, and ongoing management of your network. With it, you can assess the impact of rolling out new applications, network operating systems, or internetworking devices.

Contact Network Associates Consulting Services at 1-800-395-3151 to learn more about the options available, or visit the Network Associates website at:

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

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.

Contact your sales representative to learn more about these programs, or call Network Associates Total Education Services at 1-800-395-3151. You can also visit the Network Associates website at:

http://www.nai.com/services/education/

Reference C

VirusScan command-line options

The following table lists all of the VirusScan software options. When typing commands, remember that if you name a file that resides *outside* the directory where the VirusScan program is installed, you must include the full path to that file.

Command-Line Option	Limitations	Description
All the options listed below can be used to configure both on-demand and on-access scans, unless otherwise noted.		
/? 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 the VirusScan program creates. To do this, type scan /? /REPORT <*filename*> at the command prompt. The results of your scanning report are appended with the full set of options available for that scan task.
/ADL	On-demand scanning option only.	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	On-demand scanning option only.	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	Limitations	Description
/ALERTPATH *<dir>*	On-demand scanning option only. Can only be used on networks whose servers are running the correct version of the NetShield software.	Designates the directory *<dir>* as a network path to a remote NetWare volume or Windows 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, through its Centralized Alerting feature, broadcasts or compiles 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. The directory must contain the NetShield-supplied CENTALRT.TXT file. Add these variables to your AUTOEXEC.BAT file to ensure that the .ALR file that the VirusScan software sends identifies the infected system and its user: Set COMPUTERNAME=<name of computer> Set USERNAME=<user name>
/ALL	On-demand scanning option only.	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, the VirusScan software only scans file types which are most susceptible to viruses: .BIN, .COM, .DLL, .DOC, .DOT, .EXE, .INI, .HTM, HTML, .OVL, .RTF, .SYS, .XLA, .XLS, .XLT, .VBS and .VXD, as well as the compressed file formats RAR, TAR, and GZIP. (See page 28 for details on how the VirusScan program handles compressed files.)
/ANALYZE	On-demand scanning option only. Extended memory required.	Sets the software to scan using its full heuristics, both program and macro. Note: /MANALYZE targets macro viruses only; /PANALYZE targets program viruses only.

Command-Line Option	Limitations	Description
/ANYACCESS	On-access scanning option only.	Scans: * the boot sector whenever a disk is either read or written to * executables * any newly created files.
/APPEND	On-demand scanning option only.	Used with /REPORT *<filename>* to append report message text to the specified report file instead of overwriting it.
/BOOT	On-demand scanning option only.	Scan boot sector and master boot record only.
/BOOTACCESS	On-access scanning option only.	Scans a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/CLEAN	On-demand scanning option only.	Clean viruses from all infected files and system areas.
/CLEANDOCALL	On-demand scanning option only.	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents if a single infection is found. Note: This option deletes all macros, including macros not infected by a virus.
/CONTACT <message>	On-access scanning option only.	Displays specified message when a virus is detected. This message cannot exceed 255 characters.
/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. (Network Associates recommends using /LOCK in tandem with this option.) This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. Note: Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.

Command-Line Option	Limitations	Description
/DAM	On-demand scanning option only.	A repair switch: deletes all macros in the event an infected macro is found. If no infected macro is found, no deletions will be made. If you have a suspect an infection in your file, you may choose to strip all macros from a data file in order to minimize any possible exposure to a virus. In order to pre-emptively delete all macros in a file, use this option with /FAM: scan <filename> /fam /dam With these two options used in tandem, all found macros will be deleted, regardless of the presence of an infection.
/DEL	On-demand scanning option only.	Deletes infected files permanently.
/EXCLUDE *<filename>*	On-demand scanning option only.	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 ?
/FAM	On-demand scanning option only.	Find all macros: not just macros suspected of being infected. It causes any macro found to be treated as a possible virus detection. No deletion of the found macros is made unless used in conjunction with the /DAM option. If you have a suspect an infection in your file, you may choose to strip all macros from a data file in order to minimize any possible exposure to a virus. In order to pre-emptively delete all macros in a file, use this option with /FAM: scan <filename> /fam /dam With these two options used in tandem, all found macros will be deleted, regardless of the presence of an infection.
/FILEACCESS	On-access scanning option only.	Scans executable files on access as well as execution. Note: This scan will not check the boot sector.
/FREQUENCY <n >	On-demand scanning option only.	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.

Command-Line Option	Limitations	Description
/HELP or /?	None.	Displays a list of scanning options, each with a brief description. You may find it helpful to add a list of scanning options to the report files the VirusScan program creates. To do this, type scan /? /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.
/IGNORE *<drive(s)>*	On-access scanning option only.	Does not check any files loaded from the specified drive(s).
/LOAD *<filename>*	On-demand scanning option only.	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.
/LOCK	Not available in low-memory environments	With this /LOCK option enabled, the software halts and locks your system if it finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. Network Associates recommends using /LOCK with the /CONTACTFILE <filename> option to tell users what to do or whom to contact if the VirusScan software locks the system.
/MANALYZE	On-demand scanning option only. Extended memory required.	Enables heuristic scanning target macro viruses. Note: /PANALYZE targets program viruses only; /ANALYZE targets both program and macro viruses.
/MANY	On-demand scanning option only.	Scans multiple disks consecutively in a single drive. The program prompts you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run the VirusScan software from a boot disk and you have only one floppy drives.
/MAXFILESIZE <xxx.x>x	On-demand scanning option only.	Scan only files no larger than <xxx.x> megabytes.

Command-Line Option	Limitations	Description
/MOVE <dir>	On-demand scanning option only.	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	On-demand scanning option only.	Disables the tone that sounds whenever the scanners find a virus.
/NOBREAK	On-demand scanning option only.	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress with /NOBREAK in use.
/NOCOMP	On-demand scanning option only. 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	On-demand scanning option only.	No direct disk access. This prevents the scanners from accessing the boot record. This feature has been added to allow the scanners to run under Windows NT. You might need to use this option on some device-driven drives. Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.
/NODISK	On-access scanning option only.	Does not scan boot sector while loading the VShield scanner.
/NODOC	On-demand scanning option only.	Does not scan Microsoft Office files.
/NOEMS	On-access scanning option only.	Keeps the VShield scanner from using expanded memory (EMS).

Command-Line Option	Limitations	Description
/NOEXPIRE	On-demand scanning option only.	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMEM	None.	Does not scan memory for viruses. This greatly reduces scan time. Use /NOMEM only when you are absolutely certain that your computer is virus-free.
/NOREMOVE	On-access scanning option only.	Prevents the VShield scanner from being removed from memory with the /REMOVE switch.
/NOWARMBOOT	On-access scanning option only.	Does not check the disk boot sector of the floppy disk in the A: drive for viruses during warm boot (system reset or CTRL+ALT+DEL).
/NOXMS	On-access scanning option only.	Does not use extended memory (XMS).
/PANALYZE	On-demand scanning option only. Extended memory required.	Enables heuristic scanning for program viruses. Note: /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.
/PAUSE	On-demand scanning option only.	Enables screen pause. The “Press any key to continue” prompt appears when the program fills a screen with messages. Otherwise, by default, the program fills and scrolls a screen continuously without stopping, which allows it to run on PCs with multiple drives or that have severe infections without needing your input. Network Associates recommends omitting /PAUSE when using the report options (/REPORT, /RPTALL, /RPTCOR, and /RPTERR).
/RECONNECT	On-access scanning option only.	Restores the VShield scanner after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	On-access scanning option only.	Unloads the VShield scanner from memory.

Command-Line Option	Limitations	Description
/REPORT *<filename>*	On-demand scanning option only.	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 overwrites it. To avoid overwriting, use the /APPEND option with /REPORT: the software 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, modified files, and system errors to the report. You may find it helpful to add a list of scanning options to the report files the VirusScan program creates. To do this, type /? /report *<filename>* at the command prompt. The results of your scanning report are appended with 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. Network Associates recommends omitting /PAUSE when using any report option.
/RPTALL	On-demand scanning option only.	Includes the names of all scanned files in the /REPORT file. You can use /RPTCOR with /RPTERR on the same command line. Network Associates recommends omitting /PAUSE when using any report option.
/RPTCOR	On-demand scanning option only.	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 the VirusScan scanners find 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). Network Associates recommends omitting /PAUSE when using any report option.

Command-Line Option	Limitations	Description
/RPTERR	On-demand scanning option only.	Include errors in /REPORT file. When used with /REPORT, this option adds a list of system errors to the report file. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. 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. Network Associates recommends omitting /PAUSE when using any report option.
/SAVE	On-access scanning option only.	Saves the command-line options to the VSHIELD.INI file.
/SUB	On-demand scanning option only.	Scans subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, the VirusScan scanners 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 specify an entire drive as a target.
/UNZIP	On-demand scanning option only. Extended memory required.	Scan inside compressed files.
/VIRLIST	On-demand scanning option only.	Displays the name of each virus that the VirusScan software can detect. This file is over 250 pages long. This is too large for the MS-DOS “Edit” program to open; Network Associates recommends using Windows Notepad or another text editor to open the virus list.
/XMSDATA	On-access scanning option only.	Loads the VShield data files into XMS memory.

VirusScan error levels

When you run the VirusScan program in the DOS environment, a DOS error level is set. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan.

NOTE: See your DOS operating system documentation for more information.

The VirusScan program 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.

Index