McAfee VirusScan
Command-Line
Anti-Virus Software

User’s Guide

Version 4.14.0

COPYRIGHT

LICENSE AGREEMENT

NETWORK ASSOCIATES TRADEMARK ATTRIBUTIONS

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 50,000 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 much more than $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 a 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 disk 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 McAfee 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, always threatens 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 DOS used to load itself into memory. Once there, loaded alongside DOS itself, the virus 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. That way, 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 by providing 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

McAfee 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 500 viruses and variants appear each month, the data (.DAT) files that enable McAfee 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. McAfee has, however, assembled the world's largest and most experienced anti-virus research staff within its Anti-Virus Emergency Response Team (AVERT)* 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. No 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 AVERT website.

McAfee 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. McAfee backs them both with outstanding support, training and a worldwide network of research and development teams. Contact your McAfee representative, or visit the McAfee website, to find out how to enlist the power of Total Virus Defense on your side.

How to contact McAfee and Network Associates

Customer service

On December 1, 1997, McAfee Associates merged with Network General Corporation, Pretty Good Privacy, Inc., and Helix Software, Inc. to form Network Associates, Inc. The combined Company subsequently acquired Dr Solomon's Software, Trusted Information Systems, Magic Solutions, and CyberMedia, Inc.

A January 2000 company reorganization formed four independent business units, each concerned with a particular product line. These are:

- **Magic Solutions**. This division supplies the Total Service desk product line and related products
- **McAfee**. This division provides the Active Virus Defense product suite and related anti-virus software solutions to corporate and retail customers.

- **PGP Security**. This division provides award-winning encryption and security solutions, including the PGP data security and encryption product line, the Gauntlet firewall product line, the WebShield E-ppliance hardware line, and the CyberCop Scanner and Monitor product series.
- **Sniffer Technologies**. This division supplies the industry-leading Sniffer network monitoring, reporting, and analysis utility and related software.

Network Associates continues to market and support the product lines from each of the new independent business units. You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to the Network Associates Customer Service department at the following address:

Network Associates Customer Service
4099 McEwen, Suite 500
Dallas, Texas 75244
U.S.A.

The department's hours of operation are 8:00 a.m. to 8:00 p.m. Central time, Monday through Friday

Other contact information for McAfee corporate-licensed customers:

Phone:	(888) VIRUS NO or (888) 847- 8766
E-Mail:	services_corporate_division@nai.com
Web:	http://www.nai.com/asp_set/services/customer_support /customer_intro.asp

Other contact information for retail-licensed customers:

Phone:	(972) 308-9960
E-Mail:	cust_care@nai.com
Web:	http://www.mcafee.com/

Technical support

McAfee and Network Associates are famous for their dedication to customer satisfaction. The companies have continued this tradition by making their sites on the World Wide Web valuable resources for answers to technical support issues. McAfee encourages you to make this your first stop for answers to frequently asked questions, for updates to McAfee and Network Associates software, and for access to news and virus information.

World Wide Web	http://www.nai.com/asp_set/services/technical_support /tech_intro.asp

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

Internet	techsupport@mcafee.com
CompuServe	GO NAI
America Online	keyword MCAFEE

If the automated services do not have the answers you need, contact McAfee at one of the following numbers Monday through Friday between 8:00 A.M. and 8:00 P.M. Central time to find out about McAfee technical support plans.

For corporate-licensed customers:

Phone	(888) VIRUS NO or (888) 847-8766
Fax	(972) 619-7845

For retail-licensed customers:

Phone	(972) 855-7044
Fax	(972) 619-7845

This guide includes a summary of the PrimeSupport plans available to McAfee customers. To learn more about plan features and other details, see Appendix A, "Network Associates Support Services."

To provide the answers you need quickly and efficiently, the McAfee technical support staff needs some information about your computer and your software. Please include this information in your correspondence:

- 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

Download support

To get help with navigating or downloading files from the Network Associates or McAfee websites or FTP sites, call:

Corporate customers	(801) 492-2650
Retail customers	(801) 492-2600

Network Associates training

For information about scheduling on-site training for any McAfee or Network Associates product, call Network Associates Customer Service at: (972) 308-9960.

Comments and feedback

McAfee 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 McAfee anti-virus product documentation to: McAfee, 20460 NW Von Neumann Drive, Beaverton, OR 97006-6942, U.S.A. You can also send faxed comments to (503) 466-9671 or e-mail to tvd_documentation@nai.com.

Reporting new items for anti-virus data file updates

McAfee 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 McAfee 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 McAfee 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 the McAfee European or South Africa research office, 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_sa@nai.com
Use this address to send questions or virus samples to our South Africa offices

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 the McAfee Asia-Pacific research office, or the 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 Southeast 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
Belgique

BDC Heyzel Esplanade, boîte 43
1020 Bruxelles
Belgique
Phone: 0032-2 478.10.29
Fax: 0032-2 478.66.21

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

Room 913, Tower B
Full Link Plaza
No. 18 Chao Yang Men Wai Avenue
Beijing
People’s Republic of China 100020
Phone: 86-10-6538-3399
Fax: 86-10-6588-5601

Network Associates Denmark

Lautruphoej 1-3
2750 Ballerup
Danmark
Phone: 45 70 277 277
Fax: 45 44 209 910

NA Network Associates Oy

Mikonkatu 9, 5. krs.
00100 Helsinki
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 Hong Kong

14th Floor, Plaza 2000
2-4 Russell Way
Causeway Bay, Hong Kong
Phone: 852-2892-9500
Fax: 852-2832-9530

Network Associates Japan, Inc.

Shibuya Mark City West 20F
1-12-1 Dougenzaka, Shibuya-ku
Tokyo 150-0043, Japan
Phone: 81 3 5428 1100
Fax: 81 3 5428 1480

Network Associates
México

Andrés Bello No. 10, 4o. Piso
Col. Polanco
México D.F. C.P. 11560
Phone: 52 (5) 282-9180
Fax: 52 (5) 282-9183

Network Associates
Deutschland GmbH

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

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italy
Phone: 39 02 92 65 01
Fax: 39 02 92 14 16 44

Network Associates Latin America

1200 S. Pine Island Road, Suite 375
Plantation, Florida 33324
United States
Phone: (954) 577-4290
Fax: (954) 236-8031

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

Hawthorne House
St. Andrews Business Park
Meadowbrook Lane
Bryanston, Johannesburg
South Africa 2021
Phone: 27 11 700-8200
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 9141 88 500
Fax: 34 9155 61 404

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
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

Network Associates
International Ltd.

227 Bath Road
Slough, Berkshire
SL1 5PP
United Kingdom
Phone: 44 (0)1753 217 500
Fax: 44 (0)1753 217 520

Introduction 1

What are the command-line scanners?

The command-line scanners enable you to search for viruses in any drive, folder, or file in your computer "on demand" or, in other words, at any time. You can also set the scanners to examine your files whenever you open, save, copy, rename, or otherwise modify them or, in other words, "on access." The command-line scanners also feature options that can alert you when they detect a virus or take a variety of automatic actions.

These scanners, kept current with updated virus definition (.DAT) files from McAfee AVERT labs, can serve as an important part of your network security. McAfee strongly urges you to set up an anti-virus security policy for your network, incorporating as many protective measures as possible.

How do command-line scanners work?

To run an *on-access* scan session, type `vshield` at the command line, with any options you want for controlling how the session runs. For a complete list of options, see "On-Access Scanning" on page 59.

To run an *on-demand* scan operation, type `scan` at the command line, again with the options you want. For a complete list of options, see "On-Demand Scanning" on page 35.

Both scanners act as an interface to the powerful anti-virus scanning engine—the engine common to all McAfee and Dr Solomon's products.

The two Command-Line scanners consists of a set of programs for running targeted scan operations from the MS-DOS Prompt or Command Prompt windows, or from protected MS-DOS mode. The set includes:

- SCAN.EXE. This scanner runs only in 32-bit environments. This is the main command-line interface. When you run this file, it first checks its environment to see whether it can run by itself. If your computer is running in 16-bit or protected mode, SCAN.EXE transfers control to one of the other on-demand scanners—SCANPM.EXE or SCAN86.EXE.

  – SCANPM.EXE. This scanner runs in 16-bit and 32-bit environments. It provides you with a full set of scan options for 16-bit and 32-bit protected-mode DOS environments. It also includes support for extended memory and flexible memory allocations. SCAN.EXE transfers control to this scanner when its specialized capabilities can enable your scan operation to run more efficiently.

  - SCAN86.EXE. This scanner runs only in 16-bit environments. It includes a limited set of capabilities for 16-bit environments. SCAN.EXE transfers control to this scanner if your computer is running in 16-bit mode, but without special memory configurations.

- VSHIELD.EXE. This on-access scanner looks for viruses when you open, create, save, copy, rename or otherwise modify a file. You can also configure this scanner to start when you start your computer. To learn about on-access scanning, see page 59, Chapter 4, “On-Access Scanning.”

What is heuristic analysis?

An anti-virus scanner uses two techniques to detect viruses: signatures and heuristic analysis. A *virus signature* is simply a binary pattern that is found in a virus-infected file. Using information in the .DAT files, the scanners search for those patterns. This approach cannot detect a new virus because its signature is not yet known, therefore another technique, known as *heuristic analysis* is employed.

Programs that carry a virus often have distinctive features. They might attempt unprompted modification of files, invoke mail clients or use other means of self-propagation. The scanner analyzes the program code to detect these kinds of computer instructions. The scanner also searches for “legitimate,” non-virus-like behavior, such as prompting the user before taking action, and thereby avoids raising false alarms.

In an attempt to avoid being detected, some viruses are encrypted. Eeach computer instruction is simply a binary number, but the computer does not use all the possible numbers. By searching for unexpected numbers inside a program file, the scanner can detect an encrypted virus.

By using these techniques, the scanners can detect both known viruses and many new viruses and variants.

What changed in this release?

- Heuristic scanning inside Visual Basic Scripts. The software can now detect unknown virus infections within Visual Basic Scripts. Some viruses can conceal Visual Basic Scripts within the body of an e-mail message. Some Windows and Internet Explorer configurations allow the embedded script to run when the e-mail message is opened in Microsoft Outlook.

- Reporting of Windows Word 98 and Windows 2000 password-protected documents. The software reports password-protected files as it scans them.

- Support for new unpacker formats, Windows executable compressors and encryptors. The software can now detect virus infections within files packed by NeoLite, PE-Crypt, PECompact, PE-PaCK, and .BJFnt.

- Support for new versions of unpacker formats. The software can now detect virus infections within files packed by new versions of UPX, ASPack, WWPack32, and Petite.

- Support for new RTF (Embedded) format of Object Packager. The software can now detect virus infections within embedded objects in RTF files created by Object Packager.

- Support for various MIME formats. The software can now detect virus infections within files containing 7-bit, 8-bit binary data or Quoted-Printable data in MIME format

- Support for Autodesk AutoCAD 2000. The software can now detect virus infections within Autodesk AutoCAD 2000 drawing format files - file extensions, .DWG, and .D?B

- Support for Corel Photo-Paint 9. The software can now detect virus infections within Corel Photo-Paint 9 files - file extension .CPT.

- More file types are scanned. The software now scans more of the types of files which are vulnerable to virus infection. This list is frequently updated. For a complete list, use the /EXTLIST option. Note that compressed files are only scanned if the appropriate scanning option is set.

- Display of file extensions. A new switch, /EXTLIST, displays a list of all the file extensions for vulnerable file types which are scanned for viruses.

- Improved renaming of infected files. Previously, files with a file extension of .V?? were not renamed. They are now renamed with a .VIR extension. Read this Guide for full details.

- Updated on-screen help for DOS command-line scanner. The on-screen help display lists the most common options. A full list of options is available in the User Guide.

- Reporting of 'Trojan horse' variants. Although the scanner already detects Trojan horse files, it now states whether it has detected an original file or a variant.

Installing Command-Line Software 2

Before you begin

To prevent the spread of viruses that might already be on your system before you install the anti-virus software:

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

- An IBM-compatible personal computer with an Intel 80386 processor, or an equivalent, running DOS version 5.0 or later. The SCAN86.EXE component requires a computer with only an Intel 8086 processor or equivalent.
- For best results, McAfee recommends at least 4MB of memory and 4MB of free hard drive space. The SCAN86.EXE component requires only 500KB of memory.

Installing VirusScan software

To learn how to use the installation batch file to copy Command-Line scanner files to your hard disk, see "Batch installation of VirusScan software" on page 26. To copy the program files directly to your hard disk, see "Manual installation of VirusScan software" on page 28.

NOTE: If you suspect your system is already infected, see "If you suspect you have a virus" on page 67 before you install the scanner software.

Batch installation of VirusScan software

The software includes an installation batch file, INSTALL.EXE, for copying all the files you need to your hard disk. This batch file will search your system for previous versions of this software. If you are installing the software for the first time, the batch file will create an installation directory, then complete the installation according to the options you choose.

To use the installation batch file to install the software:

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

   a. If you are installing from a compact disc, insert the compact disc that contains the files into your CD-ROM drive.

   b. If you are installing from diskettes:

      - Insert the first diskette into your A drive.

      - Change to the A drive.

   c. If you are installing from files you downloaded from the McAfee website, decompress the zipped files into a temporary directory on your hard drive.

   ❑ **NOTE:** McAfee recommends that you use the -d option to extract command-line files and preserve their directory structure. Type `cd` to change to the directory to which you extracted the program files.

2. Type `install.bat` at the command prompt to launch the setup batch file.

   The first dialog box appears.

3. Type `n` to continue.

4. If you are running the installation batch file from within Windows 3.1x, Windows 95, or Windows NT, the following message appears:

```
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?
```

   Type `y` to continue, or `n` to stop the installation.

5. The batch file then shows the default installation directory: C:\NETA\SCAN. To install the files to this directory, type `n` to continue.

   Otherwise, press BACKSPACE on your keyboard to erase the existing path, then type the full path to the directory you prefer to use in the space provided. When you finish, press TAB on your keyboard to move to the **Next** button, then press ENTER on your keyboard to continue.

6. If the directory you specify does not yet exist, you are prompted to create it. Type `y` to create the directory, or type `n` to choose a different directory. The batch file will tell you that it needs a valid path to continue.

   The batch file then checks your system for an existing installation of the software or any of its components.

   - If it does not find existing files, the batch file creates the installation directory you specified, then copies the the VirusScan program files to your hard disk.

   - If it finds existing files, the batch file prompts you to overwrite those files.

     – Type `n` to continue the installation and overwrite your existing files. If you are installing from diskettes, follow the prompts to insert the correct diskettes.

     – Type `b` to choose a different installation directory. Next, press BACKSPACE to erase the existing directory path in the space provided, then type the full pathname to the location you prefer.

     – Type `c` to quit the batch file completely.

7. When it finishes copying files, the batch file will ask you whether you want to start the VShield scanner when you start your computer. To do so, it must add an entry to your system's AUTOEXEC.BAT file. You can:

   - Type y to continue. The batch file adds these lines to your AUTOEXEC.BAT file:

     ```
     @REM This line loads VShield
     C:\NETA\SCAN\VSHIELD
     @REM End VShield

     @REM This line loads VShield after any Network
     @REM or Keyboard drivers
     C:\NETA\SCAN\VSHIELD /RECONNECT
     PATH=%PATH%;C:\NETA\SCAN
     ```

     This configures your system to start the VShield scanner when you start your computer.

- Type n to keep the batch file from modifying the AUTOEXEC.BAT file. The batch file will instead create a copy of the file, name the copy AUTOEXEC.NAI and leave it in the command-line program directory for your reference. You can copy the modifications to your own AUTOEXEC.BAT file in the future, or rename the AUTOEXEC.NAI file if you want to use it in the future.

8. The batch file next offers to have the scanner examine your system for viruses immediately. You can:

   - Type s to scan the master boot record, boot sectors, and system files on your hard disk, and your computer's memory.
   - Type f to scan files on all of your computer's local hard disks.
   - Type c to quit the batch file without running a scan operation.

Manual installation of VirusScan software

Follow the directions below if your copy of the software does not include INSTALL.BAT or the VShield scanner.

To learn how to use the installation batch file to copy the software to your hard disk, see "Batch installation of VirusScan software" on page 26.

To copy VirusScan Command-Line software to your hard disk:

1. Create a directory for the software on your hard disk.
2. Complete a, b, or c, depending on the source of your command-line program files:

   a. If you are installing from a compact disc, insert the compact disc containing the files into your CD-ROM drive, then copy the files from the CD-ROM to the directory you created earlier.

   b. If you are installing from diskettes:

      - Insert the first diskette into your A drive.
      - Change to the A drive, then copy the files from your diskette drive to the directory you created in Step 1.

c. If you are installing from files you downloaded from the McAfee website, decompress the zipped files into the directory you created on your hard disk.

> ❑ **NOTE:** McAfee recommends that you use the `-d` option to extract the files and preserve their directory structure.

3. Add the directory you created to the path statement in your AUTOEXEC.BAT file.
4. Make a clean start-up disk. See "Creating an emergency diskette" on page 71 for more information.

To run the scanner 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. Add a call to the scanner, with the options you want to include, to the first line of the batch file.
4. Add a call to the file LOGIN1.EXE to the second line of the batch file.

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

Validating your files

When you download or copy files from any outside source, this places your computer at risk of virus infection—even if the risk is small. Downloading anti-virus software is no exception. It is important to verify that the software is authentic, unaltered, and uninfected. Strict, extensive security measures 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 attracts the attention of virus-writers and Trojan horse writers, and some 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 McAfee or Network Associates website, bulletin board, or other approved electronic source such as AOL or CompuServe; and
- Validate the files that you download. (The software package includes a validation program, VALIDATE.EXE.)

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

To ensure that you have exactly the same files as the original 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 were generated from a cyclical redundancy check (CRC) when the software was packaged for delivery.

To validate your files:

1. Install the VirusScan software as described in "Installing VirusScan software" on page 25.
2. Click **Start** in the Windows taskbar, point to **Programs,** then choose **Command 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, the files are located in this path:

   C:\PROGRAM FILES\NETA\SCAN
4. Run VALIDATE.EXE by typing `VALIDATE *.*` at the command prompt.

   VALIDATE.EXE examines all of the files 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 verify individual files, follow the command, `validate` with the name of the file at the command prompt. You can also specify a range of files, using the DOS wildcards `?` and `*`.

5. McAfee 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 command 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 on your hard drive. You can then print that 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 prompt.

    To finish the validation, you need to compare your output from VALIDATE.EXE with the validation codes in your copy of the software. Complete the sequence below to generate the packing list.

To generate the packing list and complete your comparison:

1. To display the packing list, type `type packing.lst` at the command 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 command prompt to redirect the output from PACKING.LST to your printer.

    - Alternatively, you can direct the output to a file 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 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 must 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.

Testing your installation

After you install it, the VirusScan software is ready to scan your system for infected files. You can verify that it has installed correctly and that it can properly scan for viruses with a test. This was developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors, as a method for their customers to test any anti-virus software installation.

To test your installation:

1. Open a standard DOS or Windows text editor, then type the following character string as *one line, with no spaces or carriage returns*:

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

   NOTE: The line shown above should appear as *one line* in your text editor window, so be sure to maximize your text editor window and delete any carriage returns. Also, be sure to type the letter O, not the number 0, in the "X5O..." that begins the test message.

   If you are reading this manual on your computer, you can copy the line directly from the Acrobat PDF file and paste it into Notepad. You can also copy this text string directly from the "Testing your installation" section of the README.TXT file, which is in your VirusScan program directory. If you copy the line from either of these sources, be sure to delete any carriage returns or spaces.

2. Save the file with the name EICAR.COM. The file size will be 68 or 70 bytes.

3. Start your VirusScan software and allow it to scan the directory that contains EICAR.COM. When the VirusScan software examines this file, it will report "`Found the EICAR test file, not a virus.`"

> 🚨 **IMPORTANT:** This file is *not a virus*—it cannot spread or infect other files, or otherwise harm your system. Delete the file when you have finished testing your installation to avoid alarming other users. Please note that VirusScan products that operate through a graphical user interface do *not* return this same EICAR identification message.

Removing VirusScan software

To remove the VirusScan Command-Line software from your hard disk:

1. If you have the VShield scanner running on your computer, first remove it from memory by typing `VSHIELD /REMOVE` at the command prompt.

   If you see an error message that tells you that you cannot remove the VShield scanner from memory, use any text editor to open your AUTOEXEC.BAT file, then remove all lines that refer to the VShield scanner. Next, reboot your computer. The VShield scanner will not load into memory now.

   If you remove VirusScan files from your hard disk before you remove the VShield scanner from memory, you see an error message that will remain until you remove the VShield on-access scanner from memory or restart your computer.

2. Change to the VirusScan Command-Line program directory, then delete all VirusScan files from your hard disk.

On-Demand Scanning 3

What is on-demand scanning?

An on-demand scan operation is one that you initiate. You maintain full control over the scope of the scan operation, how the software will notify you or others if it finds a virus, and how you want it to handle any corrupted files.

If you also have VShield software installed, you can set that to run in the background to provide continuous on-access protection. To learn how to set options for the VShield on-access scanner, see Chapter 4, page 59.

When should you scan?

You should scan any file that is new to your system, especially any newly downloaded or installed files. Depending on how susceptible your system is to virus infection, you should scan as often as once a day.

The on-demand scanner operates with minimal use of system resources. The program also includes options for administrators that help to ensure that the scanner is being used most efficiently. For example, the scanner's FREQUENCY option sets a mandatory period between scans, to help minimize resources when the network is most busy. A full list of options begins on page 40.

What can you scan?

File types scanned by default

These file types as well as many other common file types are scanned by default: .BIN, .COM, .DLL, .DOC, .DOT, .EXE, .HTM, .INI, .OVL, .RTF, .SYS, .VBS, .VXD, .XLA, .XLS, and .XLT,

Archived and compressed files recognized by the scanners

You can scan compressed and archive file formats which include .ARC, .ARJ, .CAB, Diet, .GZIP, LZEXE, .LZH, PKLite, .RAR, .TAR, .TD0, .??_, and .ZIP files.

The scanner detects, cleans and reports any infections found in any compressed or archive file. If you have access to Windows, you can clean certain infections from compressed files using VirusScan for Windows software.

NOTES: You can use the switches /UNZIP and /NOCOMP to help configure how the scanner handles compressed files. These and other scan options are described in the tables from pages 43 to 46.

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

Understanding on-demand scan operations

The examples in the following sections describe how to run typical on-demand scan operations. In the example on page 38, you can learn how to save the details of scan operations that you find useful as scanning *profiles*. Profiles provide an efficient means to handle multiple or repetitive scans, and you can also use them as templates for new scan operations as your needs evolve.

NOTE: 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 want to examine. You can easily scan one file or folder at a time, but many scan options make targeting specific directories or drives easy. See page 43 for a list of these options.

To start a scan operation from the command line:

1. If you do not already have the VirusScan program directory listed in your path statement, change to the directory where you stored your VirusScan program files.
2. At the command prompt, type

   ```
   scan /adn
   ```

3. Press ENTER on your keyboard to start the scan operation.

   The scanner scans all network drives and displays its results on-screen.

Example 2: Creating a report

The scanner can report its results in a log file you create and name. In this example, the scanner create its report in a log file called WEEK40.TXT, which appears in your current working directory.

To create a report:

1. If you do not already have the VirusScan program directory listed in your path statement, change to the directory where you stored your VirusScan program files.

2. At the command prompt, type:

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

3. Press ENTER on your keyboard to start the scan operation.

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

Example 3: Saving the report to a file

To create a running report of the scanner's actions, use the /APPEND option to add any results of the scan operation to a file.

To add to a file:

1. If you do not already have the VirusScan program directory listed in your path statement, change to the directory where your VirusScan program files are stored.

2. At the command prompt, type:

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

3. Press ENTER on your keyboard to start the scan operation.

The scanner scans all network drives, and appends the results of the scan operation to an existing file called WEEK40.TXT.

Example 4: Creating a scanning profile

Instead of typing all of the options for a scan operation at the command line each time you want to run the task, you can save the options in a text file as a "scanning profile." You can then tell the scanner to load the options from that file.

To create a scanning profile:

1. Using any text editor, open a new file.
2. Add the command-line options to configure your scan task in the same way that you type them at the command line. Save the file to the VirusScan program directory as SAMPLE.TXT.
3. To start a scan operation with these options, type the following line at the command prompt:

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

Configuring a scan operation to run at system startup

To have your computer scan for viruses each time it starts, you can have the scanner start when you start your computer and load its command-line options from a scanning profile you created.

To configure a virus scan operation at system startup:

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

   ```
   edit autoexec.bat
   ```

   The DOS text editor starts.
3. Locate the first line that has a reference to either the VShield scanner or SCAN.EXE. Insert one space after the reference, then type:

   ```
   /load <filename>
   ```

   where <*filename*> is the name of the scanning profile you want to run at system startup. You can add a series of such files, each separated with a space, to load multiple scan profiles.
4. When you finish editing your AUTOEXEC.BAT file, save your changes, then quit your text editor.

5. Restart your computer to have the software run and load the command-line options you chose.

Creating a list of infected files

Although a summary report can be useful, you can also create a simple list that contains only the names of the infected files. You can create and control this list using the options, BADLIST, APPENDBAD, and CHECKLIST.

For example, the following command scans the directory DIR1 and all its subdirectories, and produces information on screen:

```
SCAN C:\DIR1\*.* /SUB
```

To produce a simple list of infected files, you can add the BADLIST option:

```
SCAN C:\DIR1\*.* /SUB /BADLIST BAD1.TXT
```

The contents of BAD1.TXT might look like this list:

```
C:\DIR1\Games\hotGame.exe ... Found the Acid.674 virus !!!

C:\DIR1\SCANTEST\virtest.com ... Found: EICAR test file NOT a virus.
```

You can add to the list of infected files by using the APPENDBAD option. For example, the following command scans the directory DIR2, and any infected files found here are added to the existing list:

```
SCAN C:\DIR2\*.* /SUB /BADLIST BAD1.TXT /APPENDBAD
```

Then, the contents of BAD1.TXT might look like this:

```
C:\DIR1\Games\hotGame.exe ... Found the Acid.674 virus !!!

C:\DIR1\SCANTEST\virtest.com ... Found: EICAR test file NOT a virus.

C:\DIR2\prices.doc ... Found: virus or variant W97M/Concept !!!

C:\DIR2\Costs\may2000.doc ... Found the W97M/Ethan virus !!!
```

Using the CHECKLIST option, you can refer to that list, and scan the same files again later:

```
SCAN /CHECKLIST BAD1.TXT
```

On-demand scanning options

The scanning options are organized into several functional groups:

- "General options" on page 40
- "Target options" on page 43
- "Response and notification options" on page 46
- "Report options" on page 49

The options are also listed alphabetically (with briefer descriptions) on page 51.

General options

The following table lists the general scanning options.

General Command-Line Option	Limitations	Description
/?	None.	Display a list of command-line options, each with a brief description. You can add a list of scanning options to a report file. To do this, type at the command prompt: `SCAN  /? /REPORT <filename>` The report is appended with the full set of options available for that scan task.
/ANALYZE	Extended memory is required.	Scan using heuristics for both program viruses and macro viruses. You may type /ANALYSE instead. Note: Use /MANALYZE for macro viruses only; use /PANALYZE for program viruses only.
/APPENDBAD	Use with BADLIST.	Append names of infected files to an existing file, as specified by BADLIST. See "Creating a list of infected files" on page 39 for details.
/BADLIST *<filename>*	None.	Create a list of infected files.
/BEEP	None.	Issue a tone when an infected file is found. By default, a tone is only issued when the whole scan operation ends.
/BPRESTORE	None.	Restore sectors from backup after a repair.

General Command-Line Option	Limitations	Description
/EXTLIST	None.	Display names of file extensions that are scanned by default.
/EXTRA *<filename>*	None.	Specify an extra driver.
/FREQUENCY *<hours>*	None.	Do not scan before the specified number of hours after the previous scan. In environments where the risk of virus infection is very low, this option prevents unnecessary scans. Remember, frequent scanning provides greater protection against viruses.
/HELP	None.	Display a list of command-line options, each with a brief description. See “/?” on page 40 for more details.
/HTML *<filename>*	None.	Display the results in HTML format.
!IVN	None.	Display the internal version number. Note: The prefix here is “!”, instead of “/”.
/LOAD *<filename>*	None.	Load scanning options from the named file, or “scanning profile.” You can call scanning profiles from any local directory. You can use this option to perform a scan operation you have already configured by loading custom settings already saved in an ASCII-formatted file.
/MANALYZE	Extended memory is required.	Set the heuristic scanning features to find new macro viruses. You may type /MANALYSE instead. Note*:* Use /PANALYZE for program viruses only; use /ANALYZE for program and macro viruses.
/NOEXPIRE	None.	Disable the “expiration date” message if the scanner’s data files are out of date. For more details, see “What are the .DAT files?” on page 75.
/PANALYZE	Extended memory is required.	Enable heuristics scanning for new program viruses. You may type /PANALYSE instead. Note*:* Use /MANALYZE for macro viruses only; use /ANALYZE for program and macro viruses.

General Command-Line Option	Limitations	Description
/SILENT	None.	Do not display any information on screen.
/TIMEOUT *<seconds>*	None.	Set the maximum time to spend scanning any one file.

Target options

The following table lists scanning options that define the type of object or area to be scanned.

□ **NOTE:** To configure an on-demand scan operation, you must specify a target location for the scan (such as C:\, A:\, /ADL, /ADN).

Target Command-Line Option	Limitations	Description
/AD	None.	Same as /ALLDRIVES.
/ADL	None.	Scan all local drives—including compressed and PC drives, but not diskette drives—in addition to any other drive specified on the command line.
/ADN	None.	Scan all network drives for viruses, in addition to any other drives specified on the command line.
/ALL	None.	Scan all files regardless of extension. Note: By default, only executable files are scanned. Using this option substantially increases the scanning time. Use it only if you find a virus or suspect you have one.
/ALLDRIVES	None.	Scan all drives. Scan all network drives and local drives, but not diskette drives. This is a combination of /ADN and /ADL.
/ALLOLE	None.	Treat all files as compound/OLE files regardless of file extension.
/BOOT	Not with /NODDA.	Scan boot sector and master boot record only. Do not use this option with /NODDA.
/CHECKLIST *<filename>*	None.	Scan the files listed in the specified file. See page 39 for more details.
/DOHSM	On Windows NT only.	Scan files that are offline. Note: These are files that NT's Hierarchical Storage Management has archived because they have not been accessed for some time.
/EXCLUDE *<filename>*	None.	Do not scan the files listed in the specified file. Use this option to exclude specific files from a scan operation. List the complete path to each file on its own line. You may use wildcards, * and ?.

Target Command-Line Option	Limitations	Description
/MANY	None.	Scan multiple diskettes consecutively in a single drive. The program prompts you for each disk. You can use this option to check several diskettes quickly. You cannot use this option if you run the scanner from a boot disk and you have only one diskette drive.
/MAXFILESIZE *<nn.n>*	None.	Scan only files that are not larger than the specified number of megabytes.
/MIME	None.	Scan inside UU-encoded/base-64 files.
/NOBACKUP	None.	Do not prompt for backup of sectors before attempting repair.
/NOBOOT	None.	Do not scan the boot sector.
/NOBREAK	None.	Disable CTRL-C and CTRL-BREAK during scan operations. Users can not halt scan operations in progress if this option is set.
/NOCOMP	Extended memory is required when decompressing files.	Do not check 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 scanner checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for viruses.
/NOD	None.	Do not repair *all* file types. Repair only the susceptible filetypes. (Use with /CLEAN.) By default, /CLEAN scans and tries to repair viruses in *all* file types. When you include this option, the repair is limited to the susceptible file types only, as recognized by their file extensions.
/NODDA	Do not use this option with /BOOT.	Do not access disk directly. This prevents the scanner from accessing the boot record. This feature allows the scanner to run under Windows NT. You might need to use this option on some device-driven drives.
/NODOC	None.	Do not scan Microsoft Office document files.

Target Command-Line Option	Limitations	Description
/NODECRYPT	None.	Do not decrypt Microsoft Office compound documents that are password-protected. By default, macros inside password-protected compound documents are scanned by employing “password cracking” techniques. If, for reasons of security, you do not require these techniques, use this option. Password cracking does not render the file readable.
/NOJOKES	None.	Do not report any jokes.
/NOMEM	None.	Do not scan memory for viruses. Use this option only when you are certain that your computer is virus-free.
/SECURE	None.	Scan inside all files (including compressed files) regardless of file extension, and use heuristic analysis. This is a combination of /ALL, /ANALYZE, and /UNZIP.
/SUB	None.	Scan subdirectories inside a directory. By default, when you specify a directory to scan rather than a drive, the scanner examines only the files it contains, not its subdirectories. Use this option to scan all subdirectories within the specified directories. This option is not necessary if you specify an entire drive as a target.
/UNZIP	Extended memory is required.	Scan inside compressed files.

Response and notification options

The following table lists the response and notification options after a virus has been detected.

Response and Notification Option	Limitations	Description

/ALERTPATH *<dir>*	This can only be used on networks where the servers are running the correct version of NetShield.	Designate a directory as a network path to a remote NetWare volume or Windows NT directory that is monitored by Centralized Alerting.
		The scanner 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.
/CONTACTFILE *<filename>*	None.	Display the contents of the specified file when a virus is found. This enables you to provide contact information and instructions to the user when a virus is encountered. McAfee recommends using /LOCK with this option. This option is especially useful for networks, because you can 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.

Response and Notification Option	Limitations	Description
/DAM	None.	Delete all macros in a file if an infected macro is found. If you suspect you have an infection in your file, you may choose to remove all macros from a data file to prevent any exposure to a virus. To pre-emptively delete all macros in a file, use this option with /FAM: `scan <filename> /fam /dam` If you use these two options together, all found macros are deleted, regardless of the presence of an infection.
/DEL	None.	Delete infected .COM and .EXE files permanently. This option does *not* delete infected Word documents or ZIP archives. If the scanner detects infected files within a ZIP archive, it does not delete the files within the archive, nor does it delete the archive itself. McAfee recommends that you use the /CLEAN switch to protect against viruses that infect file types other than .COM or .EXE.
/EVLOG	None.	Use NT Event Logging. Any detections are recorded in the Application Log of the Event Viewer.
/FAM	None.	Find all macros, not just macros suspected of being infected. The scanner treats any macro as a possible virus and reports that the file “contains one or more macros.” However, the macros are *not* removed. If you suspect you have an infection in a file, you can remove all macros from the file by using the /FAM and /DAM options together. For example: `scan <filename> /fam /dam`
/LOCK	None.	Halt and lock the system if a virus is found. This option is appropriate in vulnerable network environments, such as open-use computer labs. McAfee recommends you use this option with the /CONTACTFILE <filename> option to tell users what to do or whom to contact if the scanner locks their system.

Response and Notification Option	Limitations	Description
/MOVE *<dir>*	None.	Move all infected files found during a scan operation to the specified directory, preserving the drive letter and directory structure. Note*:* This option has no effect if the Master Boot Record or boot sector is infected, because these are not files.
/NOBEEP	None.	Do not issue a tone when the scan operation ends. By default, a tone is issued at the end of a scan operation.
/NORENAME	None.	Do not rename an infected file that cannot be repaired. For information about renaming, see page 69.
/PLAD	None.	Preserve the file’s Last Access Date after a repair. Some software (such as used for creating backups or archives) relies on a file’s Last Access Date to work correctly. If you set this option, the engine resets that date to its original value after repairing the file.

Report options

By default, the results of a scan operation appear on screen. The following table lists the options for displaying the results elsewhere. To capture a scanner report to a text file, use /REPORT with any additional switches as needed. For examples of using reporting options, see page 37.

Report Command-Line Option	Limitations	Description
/ALERTPATH *<dir>*	None.	Designate the directory *<dir>* as a network path monitored by Centralized Alerting. See page 46 for a full description.
/APPEND	None.	*A*ppend information to the specified report file instead of overwriting it. Use this option with /REPORT <filename>*.*
/PAUSE	Not with report options.	Enable a screen pause. When the screen is full of messages, the prompt "`Press any key to continue`" appears. Otherwise, by default, the screen fills and scrolls continuously without stopping. This allows the scanner to run without stopping on PCs with multiple drives or that have severe infections. McAfee recommends you do not use this option with the report options (REPORT, /RPTALL, /RPTCOR, and /RPTERR).

Report Command-Line Option	Limitations	Description
/REPORT *<filename>*	Not with /PAUSE.	Create a report of infected files and system errors, and save the data to the specified file in ASCII text file format. If that file already exists, /REPORT overwrites it. To avoid overwriting, use the /APPEND option with /REPORT. The scanner then adds report information to the end of the file, instead of overwriting it. You can also use /RPTALL, /RPTCOR and /RPTERR to add the names of 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. You may find it helpful to add a list of scanning options to the report files. To do this, type at the command prompt: `scan /help /report <filename>` The results of your scanning report are appended with the full set of options available for that scan task. McAfee recommends you do not use /PAUSE when using any report option.
/RPTALL	Specify with /REPORT.	Include the names of all scanned files in the report file.
/RPTCOR	Specify with /REPORT.	Include a list of corrupted files in the report file.
/RPTERR	Specify with /REPORT.	Include system errors in the report file. System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.
/VIRLIST	None.	Display the name of each virus that the scanner can detect. This option produces a long list, which is best viewed from a text file. To do this, type: `scan /virlist /report <filename.txt>` For full details about each virus, see the Virus Library on the website, http://vil.nai.com.

Alphabetic list of options

For convenience, the command-line options are repeated in this section with a brief description. For full descriptions, see the previous sections.

Command-line option	Description
/?	Display a list of command-line options, each with a brief description.
/AD	Same as /ALLDRIVES.
/ADL	Scan all local drives—including compressed and PC drives, but not diskette drives—in addition to any other drive specified on the command line.
/ADN	Scan all network drives for viruses, in addition to any other drives specified on the command line.
/ALERTPATH <dir>	Designate a directory as a network path to a remote NetWare volume or Windows NT directory that is monitored by Centralized Alerting.
/ALL	Scan all files regardless of extension.
/ALLDRIVES	Scan all drives. Scan all network drives and local drives, but not diskette drives.
/ALLOLE	Treat all files as compound/OLE files regardless of file extension.
/ANALYZE	Scan using heuristics for both program viruses and macro viruses.
/APPEND	Append information to the specified report file instead of overwriting it.
/APPENDBAD	Append names of infected files to an existing file, as specified by BADLIST.
/BADLIST <filename>	Create a list of infected files.
/BEEP	Issue a tone when an infected file is found.
/BOOT	Scan boot sector and master boot record only.
/BPRESTORE	Restore sectors from backup after a repair.
/CHECKLIST <filename>	Scan the files listed in the specified file.
/CLEAN	Clean viruses from all infected files and system areas.
/CONTACTFILE <filename>	Display the contents of the specified file when a virus is found.

Command-line option	Description
/DAM	Delete all macros in a file if an infected macro is found.
/DEL	Delete infected .COM and .EXE files permanently.
/DOHSM	Scan files that are offline.
/EVLOG	Use NT Event Logging.
/EXCLUDE <filename>	Do not scan the files listed in the specified file.
/EXTLIST	Display names of file extensions that are scanned by default.
/EXTRA <filename>	Specify an extra driver.
/FAM	Find all macros, not just macros suspected of being infected.
/FREQUENCY <hours>	Do not scan before the specified number of hours after the previous scan.
/HELP	Display a list of command-line options, each with a brief description.
/HTML <filename>	Display the results in HTML format.
!IVN	Display the internal version number.
/LOAD <filename>	Load scanning options from the named file, or “scanning profile.”
/LOCK	Halt and lock the system if a virus is found.
/MANALYZE	Set the heuristic scanning features to find new macro viruses.
/MANY	Scan multiple diskettes consecutively in a single drive.
/MAXFILESIZE <nn.n>	Scan only files that are not larger than the specified number of megabytes.
/MIME	Scan inside UU-encoded/base-64 files.
/MOVE <dir>	Move all infected files found during a scan operation to the specified directory, preserving the drive letter and directory structure.
/NOBACKUP	Do not prompt for backup of sectors before attempting repair.
/NOBEEP	Do not issue a tone when the scan operation ends.
/NOBOOT	Do not scan the boot sector.

Command-line option	Description
/NOBREAK	Disable CTRL-C and CTRL-BREAK during scan operations.
/NOCOMP	Do not check compressed executables created with the LZEXE or PkLite file-compression programs.
/NOD	Do not repair all file types. Repair only the susceptible filetypes. (Use with /CLEAN.)
/NODDA	Do not access disk directly. This prevents the scanner from accessing the boot record.
/NODECRYPT	Do not decrypt Microsoft Office compound documents that are password-protected.
/NODOC	Do not scan Microsoft Office document files.
/NOEXPIRE	Disable the “expiration date” message if the scanner’s data files are out of date.
/NOJOKES	Do not report any jokes.
/NOMEM	Do not scan memory for viruses.
/NORENAME	Do not rename an infected file that cannot be repaired.
/PANALYZE	Enable heuristics scanning for new program viruses.
/PAUSE	Enable a screen pause.
/PLAD	Preserve the file’s Last Access Date after a repair.
/REPORT <filename>	Create a report of infected files and system errors, and save the data to the specified file in ASCII text file format.
/RPTALL	Include the names of all scanned files in the report file.
/RPTCOR	Include a list of corrupted files in the report file.
/RPTERR	Include system errors in the report file.
/SECURE	Scan inside all files (including compressed files) regardless of file extension, and use heuristic analysis.
/SILENT	Do not display any information on screen.
/SUB	Scan subdirectories inside a directory.
/TIMEOUT <seconds>	Set the maximum time to spend scanning any one file.

Command-line option	Description
/UNZIP	Scan inside compressed files.
/VIRLIST	Display the name of each virus that the scanner can detect.

Scanning your diskettes

Why diskettes pose a threat

Many viruses invade computers when systems boot from an infected disk, or when users copy, run, or install programs or files that are infected. If you scan all new diskettes (floppy disks) *before first use* you can prevent new viruses entering any computer system.

You should always scan all diskettes you use. Do not assume that disks received from friends, co-workers, and others are virus-free.

Though it may be hard to believe, diskettes pose a threat even if they are not bootable. To help address this threat, McAfee recommends that you check that your disk drives are empty before you turn on your computer. Then your system will not pick up a boot-sector virus from an infected diskette that was inadvertantly left in a disk drive.

Preparing your system

The scanner needs to run from your hard drive in order to scan diskettes inserted into the diskette drive. This means that if you have the program running from diskettes, and you have only one diskette drive on your computer, you must install and run the scanner from your hard drive in order to scan diskettes in the diskette drive. (See Chapter 2, "Installing Command-Line Software," for installation instructions.)

Scanning a diskette

To scan a diskette:

1. Using the `cd` command, change to the directory where the scanner was installed.

2. Type:

   ```
   scan a: /many
   ```

3. Insert the first diskette 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 scanner detects a virus on this disk, it runs the command-line option you chose for dealing with the virus. See "Removing a virus found in a file" on page 69 for details on removing viruses.

4. Remove the scanned diskette from the A drive.

5. Insert the next diskette and press `ENTER`.

Repeat Steps 4- 5 for all diskettes that need to be scanned.

Error levels

When you run the on-demand scanner in the DOS environment, a DOS error level is set. You can use the ERRORLEVEL in batch files to take actions based on the results of the scan operation. See your DOS operating-system documentation for more information.

The on-demand scanner 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	Can not find a data file.
10	A virus was found in memory.
12	Clean failed. The scanner tried to clean a file, and that clean failed for some reason and the file is still infected.
13	One or more viruses or hostile objects were found.
15	Self-check failed; it may be infected or damaged.
19	All clean. The scanner succeeded in cleaning all infected files.
20	Scanning was prevented because of the /FREQUENCY switch. See page 41.
102	The user quit via `ESC-X`, `^C` or `Exit` button. Note: This feature can be disabled with the /NOBREAK command-line option.

Handling error messages

You can often correct the message, *Invalid switch or incorrect usage* by checking the form of the command in the list in "Alphabetic list of options" on page 51.

Where an option has a parameter, insert only one space between them. For example, the following commands are intended to scan all directories on the C disk, and list any infected files in the file named BADLIST.TXT. The first two commands are valid, but the third command gives an error message because it has more than one space between the BADLIST option and its parameter, BADLIST.TXT.

```
SCAN C:\ /SUB /BADLIST BADLIST.TXT
SCAN C:\    /SUB     /BADLIST BADLIST.TXT


SCAN C:\ /SUB /BADLIST     BADLIST.TXT
```

On-Access Scanning 4

What is on-access scanning?

VShield is the on-access scanner. It automatically scans any file on your system when the file is opened, or any executable as it is launched. After you install the on-access scanner, it protects your computer immediately with a default set of options, and provides a strong defense against new viruses. You can further customize on-access scanning by using the options listed in the tables from pages 62.

You can also configure the on-access scanner to launch at system startup to ensure continuous on-access protection; see "Editing your AUTOEXEC.BAT file" on page 66 for instructions. The on-access scanner launches and runs silently in the background, and terminates 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. To perform on-access scanning in a Windows NT environment, McAfee recommends the graphical user interface version, VirusScan for Windows NT. See "How to contact McAfee and Network Associates" on page xiii for further details.

On-access scanning in the OS/2 environment

□ **NOTE:** For users needing on-access scanning protection in the OS/2 environment, McAfee recommends the VirusScan for OS/2 anti-virus software.

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

- The 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 tables in "Configuring the on-access scanner" on page 61, and in "On-access scanning options" on page 62, for details.

- The scanner detects only those viruses that can propagate in the OS/2-DOS environment.

Starting the on-access scanner

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

To check if the on-access scanner is active:

Follow either of these steps:

- Type `chkvshld` at the command prompt in the scanner's program directory. A message will tell you if the on-access scanner is running, and if so, which of its options are currently selected.
- Check your AUTOEXEC.BAT file for the VShield command line. (See "Editing your AUTOEXEC.BAT file" on page 66 for instructions.)

Disabling the on-access scanner

At times you may need to temporarily disable the on-access scanner—when updating the virus definition (.DAT) files, for example. (See page 76.) Remember, any files you download, or new data files that you open can not be properly scanned if this scanner is disabled.

To disable the on-access scanner temporarily:

1. If necessary, use the `cd` command to change to the directory where the scanner was installed.
2. Type `VSHIELD /REMOVE` at the command prompt. This unloads the on-access scanner from memory.
3. To enable on-access scanning again, complete either of the following steps, depending on how your system is configured:
   - Restart the on-access scanner by typing `VSHIELD` at the command prompt, followed by the scanning options that you want to use. (See pages 62 to 64 for the list of options.)
   - If you previously configured your AUTOEXEC.BAT file to load the on-access scanner at startup, reboot your computer to re-enable the scanner.

Optimizing the on-access scanner’s performance

The on-access 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.

However, if you have problems using on-access scanning, they might be caused by conflicts with other TSR programs in your system, or with other programs that monitor disk access. The on-access scanner minimizes the use of conventional memory by attempting to load into extended, expanded, upper memory, or a combination of these, before using conventional memory. If your computer has more than 640KB of memory, the on-access 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 (640KB to 1024KB, or UMB).

Configuring the on-access 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 do not have to worry about starting the scanner, or scheduling tasks for it.

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

To customize the on-access scanner:

1. Choose the on-access scanning options that are 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 see 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 66 to add these options to the VShield line in your AUTOEXEC.BAT file.

On-access scanning options

General options

Command-line option	Limitations	Description
/? or /HELP	None.	Display a list of 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 at the command prompt: `SCAN /? /REPORT <filename>` The results of your scanning report are appended with the full set of options available for that scan task.
/NOREMOVE	None.	Prevent the on-access scanner from being removed from memory with the /REMOVE switch.
/RECONNECT	None.	Restore the on-access scanner after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	None.	Unload the on-access scanner from memory.
/SAVE	None.	Save the command-line options to the VSHIELD.INI file.

Memory options

Command-line option	Limitations	Description
/MEMEXCL	Not available for Windows.	Exclude the memory address A0000:0000 (video memory) from scanning.
/NOEMS	None.	Prevent the on-access scanner using expanded memory (EMS).
/NOMEM	None.	Do not scan memory for viruses. This greatly reduces scan time. Use this option only when you are certain that your computer is virus-free.
/NOXMS	None.	Do not use extended memory (XMS).
/XMSDATA	None.	Load the virus definition files into XMS memory.

Target options

Command-line option	Limitations	Description
/ANYACCESS	Scans only diskette files for DOS sessions in OS/2.	Scan all access attempts. • The boot sector whenever a disk is either read or written to. • Executables. • Any newly created files.
/BOOTACCESS	Not available for DOS sessions in OS/2.	Scan a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/FILEACCESS	None.	Scan executable files on access as well as execution. Note: This scan does *not* check the boot sector.
/IGNORE *<drive(s)>*	None.	Do not check any files loaded from the specified drive(s).
/NODISK	None.	Do not scan boot sector while loading the on-access scanner.
/NOWARMBOOT	None.	Do not check the boot sector of the diskette in drive A for viruses during a warm boot (system reset or CTRL+ALT+DEL).

Notification options

Command-line option	Limitations	Description
/CONTACT *<message>*	None.	Display the specified message when a virus is detected. This message cannot exceed 255 characters. Note: Any character is valid in a contact message except a backslash (\). Place messages beginning with a slash (/) or a hyphen (-) inside quotation marks.
/CONTACTFILE *<filename>*	None.	Display the contents of a specified file when a virus is found. The file can provide contact information and instructions to the user. (McAfee recommends using /LOCK in conjunction with this option.) This option is useful in network environments, where a single central file can store the message text.
/LOCK	Not available in low-memory environments.	Halt and lock the computer system if a virus is found. This option is useful in vulnerable network environments, such as open-use computer labs. McAfee recommends using this option with the /CONTACTFILE option to tell users what to do or whom to contact if the scanner locks the system.

Alphabetic list of all options

Table 4-1. Alphabetic list of options

Command-line option	Description
/?	Display a list of command-line options, each with a brief description.
/ANYACCESS	Scan all access attempts.
/BOOTACCESS	Scan a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/CONTACT <message>	Display the specified message when a virus is detected.
/CONTACTFILE <filename>	Display the contents of a specified file when a virus is found.
/FILEACCESS	Scan executable files on access as well as execution.
/HELP	Display a list of command-line options, each with a brief description.
/IGNORE <drive(s)>	Do not check any files loaded from the specified drive(s).
/LOCK	Halt and lock the computer system if a virus is found.
/MEMEXCL	Exclude the memory address A0000:0000 (video memory) from scanning.
/NODISK	Do not scan boot sector while loading the on-access scanner.
/NOEMS	Prevent the on-access scanner using expanded memory (EMS).
/NOMEM	Do not scan memory for viruses.
/NOREMOVE	Prevent the on-access scanner from being removed from memory with the /REMOVE switch.
/NOWARMBOOT	Do not check the boot sector of the diskette in drive A for viruses during a warm boot (system reset or CTRL+ALT+DEL).
/NOXMS	Do not use extended memory (XMS).
/RECONNECT	Restore the on-access scanner after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	Unload the on-access scanner from memory.
/SAVE	Save the command-line options to the VSHIELD.INI file.
/XMSDATA	Load the virus definition files into XMS memory.

Editing your AUTOEXEC.BAT file

After you have selected the scanning options best suited to your computer environment (see "Configuring the on-access scanner" on page 61 for a list of options), you are ready to edit your AUTOEXEC.BAT file.

To edit your AUTOEXEC.BAT file:

1. Change to the root directory by typing `cd c:\` at the command prompt.
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 /NOWARMBOOT).
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 command 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

Firstly, 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 rare viruses that carry a destructive payload usually produce their nasty effects in response to a trigger event. In most cases, unless you see evidence of a payload that has activated, you will have time to deal with the infection properly. However, this unwanted computer code can interfere with your computer’s normal operation, consume system resources and have other undesirable effects, so take them seriously and remove them when you encounter them.

Secondly, keep in mind that odd computer behavior, unexplained system crashes, or other unpredictable events might not be caused by a virus. If you believe you have a virus on your computer because of occurrences such as these, a virus scan operation might not produce the results you expect, but it helps eliminate one potential cause of your computer problems.

To clean your system:

If you have or suspect that you have a virus, and you haven’t yet installed the on-demand scanner, follow these steps.

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 diskette into the diskette drive. If you do not have a clean start-up disk, see “Creating an emergency diskette” on page 71.
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 diskette. Begin the installation procedure described in Chapter 2, “Installing Command-Line Software.”

   To find and eliminate the source of infection, scan your diskettes immediately after installation. For information, see “Scanning your diskettes” on page 55.

   If viruses were not removed:

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

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

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

   If the scanner finds a virus in a file and cannot remove it, you must delete the infected file and restore it from backups. If the virus was found in the Master Boot Record, refer to documents on the McAfee website about manually removing viruses.

If the scanner detects a virus

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

However, some viruses are designed to damage your files beyond repair. The scanner can move these irreparably damaged files, called “corrupted” files to a quarantine directory or delete them permanently to prevent further infection of your system.

If the scanner cannot repair an infected file, it renames the file to prevents its use. When a file is renamed, only the file extension (typically three letters) is changed. The following table shows the methods of renaming.

Table 5-1. Renaming infected files

Original	Renamed	Description
Not v*	v*	File extensions that do not start with *v* are renamed with v as the initial letter of the file extension. For example, *myfile.doc* becomes *myfile.voc*.
v*	vir	File extensions that start with *v* are renamed as *.vir*. For example, *.vbs* becomes *.vir*.
vir	v01	File extension, *.vir* is renamed as *.v01*.
v01	v02	File extensions, *.v01* and so on are renamed with the next number in sequence.
v99	v99	A file extension of v99 is not renamed.
<*blank*>	vir	Files with no extensions are renamed with *.vir*.

For file extensions with more than three letters, the name is usually not truncated. For example, notepad.class becomes notepad.vlass. However, an infected file called water.vapor becomes water.vir.

Removing a virus found in a file

If the scanner 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 scanner automatically moves the infected files to the specified quarantine directory.
- If you selected /CLEAN, the scanner attempts to repair the file.
- If you selected /DEL, the scanner deletes and permanently overwrites the infected file.
- If you selected /NORENAME, the scanner does not rename the infected file.

Running additional virus-cleaning tasks

Cleaning macro viruses from password-protected files

The scanner respects users' passwords and usually leaves them intact. For example, in password-protected Microsoft Excel 95 files, the scanner removes macro viruses without disturbing users' passwords.

However, macro viruses that infect Microsoft Word files sometimes plant their own passwords. Depending on the capabilities of the virus, the scanner takes one of the following actions when trying to clean a password-protected file:

- **If the macro virus cannot plant its own password:** The scanner notes the infection but does not remove the password.
- **If the macro virus can plant its own password:** The scanner cleans the file, removes the planted password, and removes the virus.

Cleaning Windows NT hard disks

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

1. Start the computer that has the NTFS file system partition from a virus-free DOS boot disk.
2. Run the scanner, using `SCAN /BOOT /CLEAN`. Be sure to run the scanner from a diskette that you know is free from viruses.

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

Creating an emergency diskette

In case your system becomes infected, you need a clean start-up (also called boot, or emergency) diskette. This section describes how to create that emergency diskette. Any virus in your system might be transferred to your emergency diskette and infect your system again, so 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 diskette at that computer.

This emergency diskette 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 diskette, you can format this boot diskette 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* diskette into the A drive.
3. Format the diskette by typing the following command at the command prompt:

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

   This overwrites any information already on the diskette.
4. When the system prompts you for a volume label, enter an appropriate name for your start-up diskette.
5. Locate HIMEM.SYS on your hard drive.
   - **DOS users:** By default, this is in the \DOS directory.
   - **Windows users:** By default, this file is 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.

   ❑ **IMPORTANT:** A true text editor such as Edit (in MS-DOS), or Notepad, saves characters to a file without additional formatting. However, most word-processing programs, 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:

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

     b. Complete steps b. through e. above.

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

9. Copy the command-line version of the scanner software to the disk by typing the following commands at the command 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 that the scanner needs to scan the boot sector of an infected computer.

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

11. You have now copied all necessary programs for rebooting your system onto this boot diskette.

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

❑ **NOTE:** Do not copy the following programs to the clean boot diskette you are making. Conventional diskettes do not have enough space to store both the scanner 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, copy the drivers required to access your drives onto the clean boot diskette. 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.

Using Virus Definition Files 6

What are the .DAT files?

Hundreds of new viruses are discovered each month. The virus definition (.DAT) files that came with your original copy of the anti-virus scanners might not be able to help the software detect a virus discovered months later.

The files named CLEAN.DAT, NAMES.DAT, and SCAN.DAT provide virus information to the anti-virus scanners. These are the virus definition files we are referring to in this Guide.

To have the best virus protection possible, you must regularly download and install updates to these three virus definition files that the anti-virus scanners use. McAfee continually updates these files. Weekly updates of .DAT files are available to licensed users at the McAfee website (www.nai.com) and other electronic services.

If 90 days have passed since you last updated the .DAT file, the scanner notifies you that an update is needed. (You can turn off this feature by using the /NOEXPIRE option. See page 41.) Please see “Updating .DAT files” on page 76 for instructions on updating the DATs.

NOTE: The command-line scanners use the same virus definition files as our other anti-virus products that might be installed in your network, so you can be sure that with current .DAT files in place, command-line scanners offer the same protection as other McAfee anti-virus software.

Updating .DAT files

The 4000 series of .DAT files are compatible with McAfee anti-virus products that use scan engine versions 4.0.xx only. The .DAT files included with this release of the software do *not* work with any VirusScan product that uses a 3.x or v2.x scan engine.

You may only download updated .DAT files as stated by the maintenance terms outlined in the README file that accompanies the software, and as detailed in the software license agreement.

To update .DAT files for the Command Line software:

1. Download the data file (for example, DAT-4090.ZIP) from any of these sources:

   - McAfee website, http://www.nai.com
   - McAfee ftp site, at ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
   - McAfee downloads are also available in the anti-virus area of AOL and CompuServe.

   🚨 **IMPORTANT:** When you are selecting the latest DATs, you will find references to self-installing .DAT files. You cannot use installable .DAT files with the 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 VShield already running on your system, you will need to unload it from memory by typing VSHIELD /REMOVE at the command prompt.
5. Locate the directories on your hard drive where Virus Scan 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 do not have the decompression software, you can download PKUNZIP (shareware) from any of the McAfee electronic sites.

7. You can unzip the files directly to the Virus Scan Command-Line program directory. Allow the updated files to overwrite the existing .DAT files.

   NOTE: If other Virus Scan products are loaded on your system, or if you chose custom installation options, some .DAT files might be 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 at the command prompt followed by the scanning options you want. (See pages 62 to 64 for a complete list of on-access options.)

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

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

Network Associates Support Services

A

Adding value to your McAfee product

Choosing McAfee anti-virus, Sniffer Technologies network management, and PGP security software helps to ensure that the critical 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 are a home user, you can choose a plan geared toward your needs from the Home User PrimeSupport program.

PrimeSupport options for corporate customers

The Corporate PrimeSupport program offers these four support plans:

- PrimeSupport KnowledgeCenter plan
- PrimeSupport Connect plan
- PrimeSupport Priority plan
- PrimeSupport Enterprise plan

Each plan has a range of features that provide you with cost-effective and timely support geared to meet your needs. The following sections describe each plan in detail.

The PrimeSupport KnowledgeCenter plan

The PrimeSupport KnowledgeCenter plan gives you access to an extensive array of technical support information via a Network Associates online knowledge base, and download access to product upgrades from the Network Associates website. If you purchased your Network Associates product with a subscription license, you receive the PrimeSupport KnowledgeCenter plan as part of the package, for the length of your subscription term.

If you purchased a perpetual license for your Network Associates product, you can purchase a PrimeSupport KnowledgeCenter plan for an annual fee.

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

http://www.nai.com/asp_set/support/introduction/default.asp

Your completed form will go to the Network Associates Customer Service Center. You must submit this form before you connect to the PrimeSupport KnowledgeCenter site.

With the PrimeSupport KnowledgeCenter plan, you get:

- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates website
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Online data file updates and product upgrades

The PrimeSupport Connect plan

The PrimeSupport Connect plan gives you telephone access to essential product assistance from experienced technical support staff members. With this plan, you get:

- In North America, unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- In Europe, the Middle East, and Africa, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 6:00 p.m. local time
- In the Asia-Pacific region, unlimited toll-free, telephone access to technical support, Monday through Friday, from 8:00 a.m. to 6:00 p.m. AEST
- In Latin America, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Central Time
- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates website
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Data file updates and product upgrades via the Network Associates website

The PrimeSupport Priority plan

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

The PrimeSupport Priority plan has these features:

- In North America, unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- In Europe, the Middle East, and Africa, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 6:00 p.m. local time
- In the Asia-Pacific region, unlimited toll-free, telephone access to technical support, Monday through Friday, from 8:00 a.m. to 6:00 p.m. AEST
- In Latin America, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Central Time
- Priority access to technical support staff members during regular business hours
- Responses within one hour for urgent issues that happen outside regular business hours, including those that happen during weekends and local holidays
- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates website
- Electronic incident and query submission
- Technical documents, including user’s guides, FAQ lists, and release notes
- Data file updates and product upgrades via the Network Associates website

The PrimeSupport Enterprise plan

The PrimeSupport Enterprise plan 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, the PrimeSupport Enterprise plan gives you a committed response time that assures you that help is on the way. You may purchase the PrimeSupport Enterprise plan on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

With the PrimeSupport Enterprise plan, you get:

- Unlimited, toll-free telephone access to an assigned technical support engineer on a 24-hour-per-day, seven-day-per-week basis, including during weekends and local holidays.

  NOTE: The availability of toll-free telephone support varies by region and is not available in some parts of Europe, the Middle East, Africa, and Latin America.

- Proactive support contacts from your assigned support engineer via telephone or e-mail, at intervals 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
- Assignable customer contacts, which allow you to designate five people in your organization who your support engineer can contact in your absence
- Optional beta site status, which gives you access to the absolute latest Network Associates products and technology
- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates website
- Electronic incident and query submission
- Technical documents, including user’s guides, FAQ lists, and release notes
- Online data file updates and product upgrades

Ordering a corporate PrimeSupport plan

To order any PrimeSupport plan, contact your sales representative, or

- In North America, call McAfee Customer Service at (888) VIRUS NO or (888) 847-8766, Monday through Friday from 8:00 a.m. to 7:00 p.m. Central Time. Press 3 on your telephone keypad for sales assistance.
- In Europe, the Middle East, and Africa, contact your local Network Associates office. Contact information appears near the front of this guide.

Table A-1. Corporate PrimeSupport Plans at a Glance

Plan Feature	Knowledge Center	Connect	Priority	Enterprise
Technical support via website	Yes	Yes	Yes	Yes
Software updates	Yes	Yes	Yes	Yes
Technical support via telephone	—	Monday–Friday North America: 8 a.m.–8 p.m. CT Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 a.m.-6 p.m. AEST Latin America: 9 a.m.-5 p.m. CT	Monday–Friday, after hours emergency access North America: 8 a.m.–8 p.m. CT Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 a.m.-6 p.m. AEST Latin America: 9 a.m.-5 p.m. CT	Monday–Friday, after hours emergency access North America: 8 a.m.–8 p.m. CT Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 am-6 p.m. AEST Latin America: 9 a.m.-5 p.m. CT
Priority call handling	—	—	Yes	Yes
After-hours support	—	—	Yes	Yes
Assigned support engineer	—	—	—	Yes
Proactive support	—	—	—	Yes
Designated contacts	—	—	—	At least 5
Response charter	E-mail within one business day	Calls answered in 3 minutes, response in one business day	Within 1 hour for urgent issues after business hours	After hours pager: 30 minutes Voicemail: 1 hour E-mail: 4 hours

The PrimeSupport options described in the rest of this chapter are available only in North America. To find out more about PrimeSupport, Training and Consultancy options available outside North America, contact your regional sales office. Contact information appears near the front of this guide.

PrimeSupport options for home users

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

- For anti-virus software products, free data file updates for the life of your product via the Network Associates website, your product's automatic update feature, or the SecureCast service. You can also update your data files by using your web browser to visit:

  http://www.nai.com/asp_set/download/dats/find.asp

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

  http://www.nai.com/asp_set/download/upgrade/login.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

  – Call the automated voice and fax system at (408) 346-3414

  – Visit the Network Associates website at http://support.nai.com

  – Visit the Network Associates CompuServe forum at GO NAI

  – Visit Network Associates on 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://www.nai.com/asp_set/support/technical/intro.asp

- Thirty days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 9:00 a.m. to 5:30 p.m. Central Time. Your thirty-day support period starts from the date of your first support phone call for all Network Associates products. To contact technical support, call

  (972) 855-7044

If you need additional support, Network Associates offers a variety of other support plans that you can purchase either with your Network Associates product or after your complimentary 30-day support period expires. These include:

❒ **NOTE:** The support plans described here are available only in North America—contact your regional sales representative to learn about local support options.

- **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 9:00 a.m. to 5:00 p.m. Central Time.
- **Pay-Per-Incident Plan.** This plan gives you support on a per-incident basis during business hours, Monday through Friday from 7:00 a.m. to 6:00 p.m. Pacific Time. You call a toll-free number, use a credit card to take care of the transaction, and get transferred to the technical support team within minutes. Your cost will be $35 per incident.

All McAfee products	(800) 950-1165

- **Pay-Per-Minute Plan.** This plan gives you support only when you need it. You get 900-number access to technical support staff members on a priority basis to minimize your hold time. Your first two minutes are free.

All products except PGP encryption software	(900) 225-5624

- **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 obtain product upgrades online. This service is available for McAfee VirusScan and NetShield software only.

How to reach international home user support

The following table lists telephone numbers for technical support in several international locations. The specific costs, availability of service, office hours and plan details might vary from location to location. Consult your sales representative or a regional Network Associates office for details.

Country or Region	Phone Number*	Bulletin Board System
Germany	+49 (0)69 21901 300	+49 89 894 28 999
France	+33 (0)1 4993 9002	+33 (0)1 4522 7601
United Kingdom	+44 (0)171 5126099	+44 1344-306890
Italy	+31 (0)55 538 4228	+31 (0)20 586 6128
Netherlands	+31 (0)55 538 4228	+31 (0)20 586 6128
Europe	+31 (0)55 538 4228	+31 (0)20 688 5521
Latin America	+55-11-3794-0125	+55-11-5506-9100

* long distance charges might apply

Ordering a PrimeSupport plan for home users

To order the PrimeSupport Small Office/Home Office Annual Plan, Pay-Per-Incident 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 Service at (972) 855-7044
- In international locations, contact the Network Associates retail technical support center closest to your location for more information. Some support options may not be available in some locations.

Network Associates consulting and training

The Network Associates Total Service Solutions program provides you with expert consulting and comprehensive education that can help you maximize the security and performance of your network investments. The Total Service Solutions program includes the Network Associates Professional Consulting arm and the Total Education Services program.

Professional Services

Network Associates Professional Services is ready to assist you during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert's independent perspective that you can use as a supplemental resource 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

For focused help with specific problem resolution or software implementation issues, Network Associates offers a Jumpstart Service that gives you the tools you need to manage your environment. This service can include these elements:

- **Installation and optimization.** This service brings a Network Associates consultant onsite to install, configure, and optimize your new Network Associates product and give basic operational product knowledge to your team.
- **Selfstart knowledge.** This service brings a Network Associates consultant onsite to help prepare you to perform your new product implementation on your own and, in some cases, to install the product.
- **Proposal Development.** This service helps you to evaluate which processes, procedures, hardware and software you need before you roll out or upgrade Network Associates products, after which a Network Associates consultant prepares a custom proposal for your environment.

Network consulting

Network Associates consultants provide expertise in protocol analysis and offer a vendor-independent perspective to recommend unbiased solutions for troubleshooting and optimizing your network. Consultants can also bring their broad understanding of network management best practices and industry relationships to speed problem escalation and resolution through vendor support.

You can order a custom consultation to help you plan, design, implement, and manage your network, which can enable you to assess the impact of rolling out new applications, network operating systems, or internetworking devices.

To learn more about the options available:

- Contact your regional sales representative.
- In North America, call McAfee Customer Service at (888) VIRUS NO or (888) 847-8766, Monday through Friday from 8:00 a.m. to 7:00 p.m. Central Time.
- Visit the Network Associates website at:

  http://www.nai.com/asp_set/services/introduction/default.asp

Total Education Services

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

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

- Contact your regional sales representative.
- Call Network Associates Total Education Services at (800) 395-3151 Ext. 2670 (for private course scheduling) or (888) 624-8724 (for public course scheduling).
- Visit the Network Associates website at:

http://www.nai.com/asp_set/services/educational_services/education_intro.asp

Index