VirusScan for UNIX

Administrator’s Guide

4.14.0

Table of Contents

Preface vii

Anti-virus protection as information security vii

Information security as a business necessity x

Active Virus Defense security perimeters xi

At the desktop: VirusScan software xi

McAfee anti-virus research xiii

How to contact McAfee and Network Associates xiv

Customer service xiv

Technical support xv

Download support xvi

Network Associates training xvi

Comments and feedback xvi

Reporting new items for anti-virus data file updates xvii

International contact information xviii

Chapter 1. Introducing VirusScan for UNIX Software 21

Welcome 21

Why use VirusScan for UNIX software? 21

What comes with the VirusScan for UNIX software? 22

Chapter 2. Installing VirusScan for UNIX Software 23

Before you begin 23

About the distributions 23

Installation requirements 24

Other recommendations 24

Installing 24

Troubleshooting during installation 26

Testing your installation 26

Troubleshooting when scanning 27

Removing the program 29

Chapter 3. Using VirusScan for UNIX Software .31

Overview 31
Syntax 31
Performing on-demand scan operations 32
Command-line conventions 33
General hints and tips 33
Preconfiguring scan operations 34
Scheduling a virus scan operation 36
What to do if the scanner detects a virus 36
Handling an infected file that cannot be cleaned 38
Exit codes 39
Report features 40
Choosing the options 41
Scanning options 41
Response options 44
General options 45
Options in alphabetic order 46

Appendix A. Preventing Virus Infection 49

Creating a secure system environment 49
Detecting new and unidentified viruses 49
Why do I need a new .DAT file? 50
Updating your .DAT files 50
Sample update script 51

Appendix B. Network Associates Support Services 55

Adding value to your McAfee product 55
PrimeSupport options for corporate customers 55
The PrimeSupport KnowledgeCenter plan 55
The PrimeSupport Connect plan 56
The PrimeSupport Priority plan 57
The PrimeSupport Enterprise plan 57
Ordering a corporate PrimeSupport plan 58

PrimeSupport options for home users 60
How to reach international home user support .62
Ordering a PrimeSupport plan for home users .62
Network Associates consulting and training 63
Professional Services 63
Jumpstart Services 63
Network consulting 64
Total Education Services 64

Index 67

Preface

Anti-virus protection as information security

> "The world changed [on March 26, 1999]—does anyone doubt that? The world is different. Melissa proved that ... and we are very fortunate ... the world could have gone very close to meltdown."
>
> —*Padgett Peterson, Chief Info Security Architect, Lockheed Martin Corporation, on the 1999 "Melissa" virus epidemic*

By the end of the 1990s, many information technology professionals had begun to recognize that they could not easily separate how they needed to respond to new virus threats from how they already dealt with deliberate network security breaches. Dorothy Denning, co-editor of the 1998 computer security handbook *Internet Besieged: Countering Cyberspace Scofflaws*, explicitly grouped anti-virus security measures in with other network security measures, classifying them as a defense against malicious "injected code."

Denning justified her inclusive grouping based on her definition of information security as "the effective use of safeguards to protect the confidentiality, integrity, authenticity, availability, and non-repudiation of information and information processing systems." Virus payloads had always threatened or damaged data integrity, but by the time she wrote her survey article, newer viruses had already begun to mount sophisticated attacks that struck at the remaining underpinnings of information security. Denning's classification recognized that newer viruses no longer merely annoyed system administrators or posed a relatively low-grade threat; they had in fact graduated to become a serious hazard.

Though not targeted with as much precision as an unauthorized network intrusion, virus attacks had begun to take on the color of deliberate information warfare. Consider these examples, many of which introduced quickly-copied innovations to the virus writer's repertoire:

- W32/CIH.Spacefiller destroyed the flash BIOS in workstations it infected, effectively preventing them from booting. It also overwrote parts of the infected hard disk with garbage data.
- XM/Compat.A rewrote the data inside Microsoft Excel spreadsheet files. It used advanced polymorphic concealment techniques, which meant that with each infection it changed the signature bytes that indicated its presence and allowed anti-virus scanners to find it.

- W32/Ska, though technically a worm, replaced the infected computer's Winsock file so that it could attach itself to outgoing Simple Mail Transfer Protocol (SMTP) messages and postings to Usenet news groups. This strategy made it commonplace in many areas.
- Remote Explorer stole the security privileges of a Windows NT domain administrator and used them to install itself as a Windows NT Service. It also deposited copies of itself in the Windows NT driver directory and carried with it a supporting Dynamic Link Library (.DLL) file that allowed it to randomly encrypt data files. Because it appeared almost exclusively at one corporate site, security experts speculated that it was a deliberate, targeted attack on the unfortunate company's network integrity.
- Back Orifice, the product of a group calling itself the Cult of the Dead Cow, purported to give the owner of the client portion of the Back Orifice application complete remote access to any Windows 95 or Windows 98 workstation that runs the concealed companion server. That access—from anywhere on the Internet—allowed the client to capture keystrokes; open, copy, delete, or run files; transmit screen captures; and restart, crash, or shut down the infected computer. To add insult to injury, early Back Orifice releases on CD-ROM carried a W32/CIH.Spacefiller infection.

Throughout much of 1999, virus and worm attacks suddenly stepped up in intensity and in the public eye. Part of the reason for this, of course, is that many of the more notorious viruses and worms took full advantage of the Internet, beginning a long-predicted assault by flooding e-mail transmissions, websites, newsgroups and other available channels at an almost exponential rate of growth. They now bullied their way into network environments, spreading quickly and leaving a costly trail of havoc behind them.

W97M/Melissa, the "Melissa" virus, jolted most corporate information technology departments out of whatever remaining complacency they had held onto in the face of the newer virus strains. Melissa brought corporate e-mail servers down across the United States and elsewhere when it struck in March 1999. Melissa instructed e-mail client programs to send out infected e-mail messages to the first 50 entries in each target computer's address book. This transformed a simple macro virus infection with no real payload into an effective denial-of-service attack on mail servers.

Melissa's other principle innovation was its direct attempt to play on end-user psychology: it forged an e-mail message from a sender the recipient knew, and sent it with a subject line that urged that recipient to open both the message and the attached file. In this way, Melissa almost made the need for viral code to spread itself obsolete—end users themselves cooperated in its propagation, and their own computers blindly participated.

A rash of Melissa variants and copycats appeared soon after. Some, such as W97M/Prilissa, included destructive payloads. Later the same year, a number of new viruses and worms either demonstrated novel or unexpected ways to get into networks and compromise information security, or actually perpetuated attacks. Examples included:

- W32/ExploreZip.worm and its variants, which used some of Melissa's techniques to spread, initially through e-mail. After it successfully infected a host machine, ExploreZip searched for unsecured network shares and quietly copied itself throughout a network. It carried a destructive payload that erased various Windows system files and Microsoft Office documents, replacing them with unrecoverable zero-byte-length files.
- W32/Pretty.worm, which did Melissa one better by sending itself to *every* entry in the infected computer's MAPI address book. It also connected to an Internet Relay Chat (IRC) server, joined a particular IRC channel, then opened a path to receive commands via the IRC connection. This potentially allowed those on the channel to siphon information from the infected computer, including the computer name and owner's name, his or her dial-up networking user name and password, and the path to the system root directory.
- W32/FunLove.4099, which infected ActiveX .OCX files, among others. This meant that it could lurk on web pages with ActiveX content, and infect systems with low or nonexistent browser security settings as they downloaded pages to their hard disks. If a Windows NT computer user had logged into a system with administrative rights, the infecting virus would patch two critical system files that gave *all* users on the network —*including* the virus—administrative rights to all files on the target computer. It spread further within the network by attaching itself to files with the extensions .SCR, .OCX, and .EXE.
- VBS/Bubbleboy, a proof-of-concept demonstration that showed that a virus could infect target computers directly from e-mail messages themselves, without needing to propagate through message attachments. It effectively circumvented desktop anti-virus protection altogether, at least initially. Its combination of HTML and VBScript exploited existing vulnerabilities in Internet-enabled mail systems; its author played upon the same end-user psychology that made Melissa successful.

The other remarkable development in the year was the degree to which virus writers copied, fused, and extended each others' techniques. This cross-pollination had always occurred previously, but the speed at which it took place and the increasing sophistication of the tools and techniques that became available during this period prepared very fertile ground for a nervously awaited bumper crop of intricate viruses.

Information security as a business necessity

Coincidentally or not, these darkly inventive new virus attacks and speedy propagation methods appeared as more businesses made the transition to Internet-based information systems and electronic commerce operations. The convenience and efficiency that the Internet brought to business saved money and increased profits. This probably also made these same businesses attractive targets for pranksters, the hacker underground, and those intent on striking at their favored targets.

Previously, the chief costs from a virus attack were the time and money it took to combat an infection and restore computer systems to working order. To those costs the new types of virus attacks now added the costs of lost productivity, network and server downtime, service denials for e-mail and other critical business tools, exposure—and perhaps widespread distribution—of confidential information, and other ills.

Ultimately, the qualifying differences between a hacker-directed security breach in a network and a security breach that results from a virus attack might become merely ones of intent and method, not results. Already new attacks have shaken the foundations of Net-enabled businesses, many of which require 24-hour availability for networks and e-mail, high data integrity, confidential customer lists, secure credit card data and purchase verification, reliable communications, and hundreds of other computer-aided transactional details. The costs from these virus attacks in the digital economy now cut directly into the bottom line.

Because they do, protecting that bottom line means implementing a total solution for information and network security—one that includes comprehensive anti-virus protection. It's not enough to rely only on desktop-based anti-virus protection, or on haphazard or ad hoc security measures. The best defense requires sealing all potential points by which viruses can enter or attack your network, from the firewall and gateway down to the individual workstation, and keeping the anti-virus sentries at those points updated and current.

Part of the solution is deploying the McAfee Active Virus Defense* software suite, which provides a comprehensive, multi-platform series of defensive perimeters for your network. You can also build on that security with the McAfee Active Security suite, which allows you to monitor your network against intrusions, watch actual network packet traffic, and encrypt e-mail and network transmissions. But even with anti-virus and security software installed, new and previously unidentified viruses will inevitably find their way into your network. That's where the other part of the equation comes in: a thorough, easy-to-follow anti-virus security policy and set of practices for your enterprise—in the last analysis, only that can help to stop a virus attack before it becomes a virus epidemic.

Active Virus Defense security perimeters

The McAfee Active Virus Defense product suite exists for one simple reason: there is no such thing as too much anti-virus protection for the modern, automated enterprise. Although at first glance it might seem needlessly redundant to protect all of your desktop computers, file and network servers, gateways, e-mail servers and firewalls, each of these network nodes serves a different function in your network, and has different duties. An anti-virus scanner designed to keep a production workstation virus-free, for example, can't intercept viruses that flood e-mail servers and effectively deny their services. Nor would you want to make a file server responsible for continuously scanning its client workstations—the cost in network bandwidth would be too high.

More to the point, each node's specialized functions mean that viruses infect them in different ways that, in turn, call for optimized anti-virus solutions. Viruses and other malicious code can enter your network from a variety of sources—floppy disks and CD-ROMs, e-mail attachments, downloaded files, and Internet sites, for example. These unpredictable points of entry mean that infecting agents can slip through the chinks in incomplete anti-virus armor.

Desktop workstations, for example, can spread viruses by any of a variety of means—via floppy disks, by downloading them from the Internet, by mapping server shares or other workstations' hard disks. E-mail servers, by contrast, rarely use floppy disks and tend not to use mapped drives; the Melissa virus showed, however, that they are quite vulnerable to e-mail–borne infections, even if they don't execute the virus code themselves.

At the desktop: VirusScan software

The McAfee Active Virus Defense product suite matches each point of vulnerability with a specialized, and optimized, anti-virus application. At the desktop level, the cornerstone of the suite is the VirusScan anti-virus product. VirusScan software protects some of your most vulnerable virus entry points with an interlocking set of scanners, utilities, and support files that allow it to cover:

- Local hard disks, floppy disks, CD-ROMs, and other removable media. The VShield scanner resides in memory, waiting for local file access of any sort. As soon as one of your network users opens, runs, copies, saves, renames, or sets attributes for any file on their system—even from mapped network drives—the VShield scanner examines it for infections.

  You can supplement this continuous protection with scan operations you configure and schedule for your own needs. Comprehensive security options let you protect individual options with a password, or run the entire application in secure mode to lock out all unauthorized access.

- System memory, boot sectors, and master boot records. You can configure regularly scheduled scan operations that examine these favorite virus hideouts, or set up periodic operations whenever a threat seems likely.
- Microsoft Exchange mailboxes. VirusScan software includes a specialized E-Mail Scan extension that assumes your network user's Microsoft Exchange or Outlook identity to scan his or her mailbox directly—*before* viruses get downloaded to the local workstation. This can prevent some Melissa-style infections and avoid infections from the next generation of VBS/Bubbleboy descendants.
- Internet mail and file downloads. The VShield scanner includes two modules that specialize in intercepting SMTP and POP-3 e-mail messages, and that can examine files that your network users download from Internet sites. The E-Mail Scan and Download Scan modules work together to scan the stream of file traffic that most workstations generate and receive daily.
- Hostile code. The Olympus scan engine at the heart of VirusScan software routinely looks for suspicious script code, macro code, known Trojan horse programs—even virus jokes or hoaxes. With the help of the VShield Internet Filter module, it also blocks hostile ActiveX and Java objects, many of which can lurk unnoticed on websites, waiting to deploy sophisticated virus-like payloads. The Internet Filter module can even block entire websites, preventing network users from visiting sites that pose a threat to network integrity.

VirusScan software ties these powerful scanning capabilities together with a powerful set of alerting, updating, and management tools. These include:

- Alert Manager client configuration. VirusScan software includes a client configuration utility you can use to have it pass alert messages directly to Alert Manager servers on your network, to a Centralized Alerting share, or to a Desktop Management Interface administrative application. Other alert methods include local custom messages and beeps, detection alerts and response options, and e-mail alert messages.
- Next-generation AutoUpdate and AutoUpgrade utilities. AutoUpdate v4.5 features complete and transparent support for new incremental .DAT file updates, which save you time and network bandwidth by adding only virus definitions you don't already have installed on your system. The new AutoUpgrade version includes support for v1.2 of the McAfee SuperDAT utility, which you can use to update the Olympus scan engine and its support files.
- Integration with McAfee ePolicy Orchestrator management software. Centralized anti-virus management takes a quantum leap forward with this highly scalable management tool. VirusScan software ships with a plug-in library file that works with the ePolicy Orchestrator server to enforce enterprise-wide network security policies.

You can use ePolicy Orchestrator to configure, update, distribute and manage VirusScan installations at the group, workstation or user level. Schedule and run scan tasks, change configurations, update .DAT and engine files—all from a central console.

Taken together, the Active Virus Defense suite forms a tight series of anti-virus security perimeters around your network that protect you against both external and internal sources of infection. Those perimeters, correctly configured and implemented in conjunction with a clear enterprise-wide anti-virus security policy, do indeed offer useful redundancy, but their chief benefit lies in their ability to stop viruses as they *enter* your network, without your having to await a tardy or accidental discovery. Early detection controls virus outbreaks, saves on the costs of virus eradication, and in many cases can prevent a destructive virus payload from triggering.

McAfee anti-virus research

Even the best anti-virus software is only as good as its latest update. Because as many as 500 viruses and variants appear each month, the .DAT files that enable McAfee software to detect and remove viruses can become 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 in its Anti-Virus Emergency Response Team (AVERT)*. This premier anti-virus research organization has a worldwide reach and a "follow the sun" coverage policy, that ensures taht you get the files you need to combat new viruses as soon as—and often before—you need them. You can take advantage of many of the direct products of this research by visiting the AVERT research site on the Network Associates website:

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

Contact your McAfee representative, or visit the McAfee website, to find out how to enlist the power of the Active Virus Defense security solution on your side:

http://www.mcafeeb2b.com/

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 B, “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 Deutschland GmbH

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

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 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 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 Latin America

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

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 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

Introducing VirusScan for UNIX Software 1

Welcome

Thank you for purchasing VirusScan for UNIX—the McAfee solution for detecting and removing viruses on UNIX-based systems.

McAfee anti-virus researchers provide fast, responsive coverage for new viruses and other malicious software. New-generation VirusScan scanning technology can detect and remove more than 50,000 known boot, file, macro, multi-partite, stealth, encrypted, and polymorphic viruses.

A pre-eminent, worldwide staff backs each new update of the virus-scanning engine and release of virus definition .DAT files.

McAfee worldwide virus research team develops weekly updates for the VirusScan virus definition .DAT files, leaving you confident that your network is well protected from attack.

Why use VirusScan for UNIX software?

The UNIX operating system is a secure environment, relatively unaffected by computer viruses. The DOS and Windows environment, however, is different. DOS computers have no security and are very susceptible to virus infections. Because DOS system viruses don't affect UNIX systems, you might ask: "Why should I be concerned?"

One reason for concern is that DOS- and Windows-based computers are rapidly appearing on the Internet—and most of these computers use the Internet for file transfer. A UNIX server might still harbor DOS system viruses and, while not itself affected, can pass them on to numerous DOS- and Windows-based clients. Rather than trying to block viruses at each DOS- and Windows-based computer connected to a UNIX system, you can install the VirusScan for UNIX software and use it as an efficient centralized solution. In order to protect yourself and your users, it is more important than ever to maintain anti-virus security.

VirusScan for UNIX software provides the best available anti-virus security, but is only one important element of a comprehensive security program that includes safety measures such as regular backups, meaningful password protection, and training and awareness programs about virus issues.

What comes with the VirusScan for UNIX software?

The VirusScan documentation includes:

- **Administrator's Guide**. This Administrator's Guide describes how to use the software. It includes background information and advanced configuration options, and is in Adobe Acrobat PDF format. Acrobat PDF files are flexible online documents that contain hyperlinks, outlines, and other aids for easy navigation and information retrieval.
- **README.TXT file**. The README.TXT file contains last-minute additions or changes to the documentation. It lists any known behavior or other issues with the product release, and often describes new product features incorporated into product updates. You can open and print the README.TXT file from Microsoft Windows Notepad, or from nearly any word-processing software.
- **LICENSE.TXT file**. This file outlines the terms of your license to use the software. Read it carefully. By installing the software you agree to its terms.
- **RESELLER.TXT** file. This file contains a list of McAfee resellers and their addresses and telephone numbers.

Installing VirusScan for UNIX Software 2

Before you begin

McAfee distributes the VirusScan for UNIX software in two ways:

- As an archived file that you can download from the Network Associates website or from other electronic services.
- On a McAfee product CD-ROM.

After you have downloaded a file or placed your disk in your CD-ROM drive, the installation steps you follow are the same for each type of distribution version.

Review the "Installation requirements" to verify that the software will run on your system, then follow the installation steps on page 24.

About the distributions

VirusScan software comes in several distribution versions, one for each supported operating system.

- Solaris SPARC v2.5.1 or later
- HP-UX v10.20 or later
- AIX v4.2.1 or later
- Linux v2.x kernels on Intel-based systems
- SCO OpenServer release 5
- FreeBSD v3.2 on Intel-based systems

If you install VirusScan software from CD-ROM, you will find each version in its own directory. Each distribution has its own installation script.

Installation requirements

To install and run the software, you need:

- The correct version of the UNIX distribution that you require, installed and running correctly on the target machine. See "About the distributions" for information.
- 4MB of free hard disk space for a full installation.
- A CD-ROM drive if you are not downloading the software from a website.

Other recommendations

- To install the software and perform on-demand scan operations of your file system, McAfee recommends that you have root account permissions.
- To take full advantage of the regular updates to anti-virus .DAT files that Network Associates offers from its website, you need an Internet connection, either through your local area network, or via a high-speed modem and an Internet service provider.

Installing

This example shows how to install the software on the Solaris distribution. To install other distributions, substitute the correct filename (for example `vsun4110.tar.Z`) where the example specifies the distribution file.

To start the VirusScan installation script:

1. Download the appropriate VirusScan software distribution from the Network Associates website or insert the McAfee installation CD-ROM.

   If you are using the McAfee installation CD-ROM to obtain the software, you can mount the CD-ROM on to the filesystem.

2. Copy the distribution file to a directory on your system.

   NOTE: McAfee recommends that you do not copy this file to a separate directory from which you plan to install the program.

3. Type this line at the command prompt to decompress the file to your hard disk:

   `zcat` <*distribution file*> `| tar -xf -`

4. Type this line at the command prompt to execute the installation script:

   `./install-uvscan [installation directory]`

   Here, the `[installation directory]` is the directory where you want to install the software. Do not type the square brackets shown in the command example.

   If you do not specify an installation directory, the software is installed in `/usr/local/uvscan`.

   If the installation directory does not exist, the installation script prompts you to create it. If you do not create the installation directory, the installation cannot continue.

5. The installation script asks whether you want to place links to the executable, the shared library and the man page. Type **`Y`** to create each link, or **`N`** to skip the step.

   McAfee recommends that you create these links, or you will need to set one of these environment variables to contain the installation directory:

Variable	Distribution
LD_LIBRARY_PATH	Solaris
	SCO OpenServer Release 5
	Linux
	FreeBSD
SHLIB_PATH	HP-UX
LIBPATH	AIX

NOTE: The program also looks in the /usr/lib or /lib directory or the current directory for the shared library.

6. The installation program copies the program files to your hard disk, then scans your home directory.

   If the software discovers a virus, see “What to do if the scanner detects a virus” on page 36 to learn about the actions you can take.

   If the installation fails, see “Troubleshooting during installation” on page 26 to learn about possible errors and suggested courses of action.

Troubleshooting during installation

The following table lists the most common error messages returned if the installation fails. The table also suggests a likely reason for the error and recommends any solutions.

Table 2-1. Error messages

Error	Cause or action
Failed to create install_dir	Verify that you have permission to create the installation directory.
Cannot write to install_dir	Verify that you have permission to create installation directory.
The install_dir exists, but is not a subdirectory	Choose another installation directory.
<file> is missing	The file might not exist.
<file> is not correct	The file did not install correctly.

Testing your installation

After it is installed, the program is ready to scan your system for infected files. You can run a test to determine that the program is installed correctly and can scan properly for viruses. The test was developed by EICAR, a coalition of anti-virus vendors headquartered in Europe, as a method for testing any anti-virus software installation.

To test your installation:

1. Open a standard text editor, then type the following line:

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

   NOTE: The line must appear as *one line* in the window of your text editor.

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

3. Type the following command to scan the EICAR.COM file:

   ```
   uvscan -v eicar.com
   ```

When the program examines this file, it reports finding the EICAR test file, but you will not be able to clean or repair it.

IMPORTANT: The EICAR test file *does not contain a virus*—it cannot spread or infect other files, or otherwise harm your system.

4. When you have finished testing your installation, delete the test file to avoid alarming other users.

   If the software appears not to be working correctly, check that you have Read permissions on the test file.

Troubleshooting when scanning

VirusScan might produce an error message such as: `Cannot find shared object`. The table explains the system-specific reason.

Table 2-2. Error messages

Platform	Cause of error
AIX	The wrong version of the -xlC.rte is installed. VirusScan software will not run on versions before 4.0
Free BSD (Berkeley)	No problems are expected on this platform.
HP-UX	The aCC run-time patch is not installed.
Linux	LIBC6 is supported, but LIBC5 is not.
SCO	No problems are expected on this platform.
Solaris	No problems are expected on this platform.

Table 2-3. Program messages

Program message	Remedy
Unable to find shared library	Set the appropriate environment variable: AIX: LIBPATH HP-UX: SHLIB_PATH SCO OpenServer:LD_LIBRARY_PATH Solaris: LD_LIBRARY_PATH FreeBSD: LD_LIBRARY_PATH Linux: LD_LIBRARY_PATH
Cannot execute: pemission denied	Incorrect file permissions can prevent the scanner running correctly. All executables (including the shared libraries) must have Read and Execute permissions (`r_x`), but McAfee recommends `rwxr_xr_x` All .DAT files must have read permissions.
Missing or invalid .DAT files	Re-install the .DAT files.
The program has been altered; please replace with a good copy	The program could be infected. Re-install from the original media.

Removing the program

A script is installed at the same time as the VirusScan software, which enables you to remove the product quickly and easily.

To remove VirusScan software from your system:

1. Run the script `uninstall-uvscan` which is in the VirusScan program directory. For example, type the following command at the command prompt:

   ```
   /usr/local/uvscan/uninstall-uvscan
   ```

2. When the VirusScan software has been removed, delete the script `uninstall-uvscan` from the program directory to remove the program completely from your system.

If you created your own links to the VirusScan program and a shared library path when you installed the VirusScan software, you will need to remove those links yourself.

As the administrator, ensure that your users cannot accidentally remove their VirusScan software.

Removing VirusScan software leaves your computer unprotected against virus attack. Remove the product only when you are sure that you can upgrade quickly to a new version.

Using VirusScan for UNIX Software

3

Overview

VirusScan for UNIX is a command-line driven program that provides sophisticated virus scanning. In this chapter, you will learn how to use its powerful features and customize the program to meet your needs.

The following features offer optimum protection for your machine and network:

- Powerful on-demand scanning options let you start a scan operation immediately or schedule automatic scan operations.
- Advanced heuristic scanning detects previously unknown macro and program viruses.
- Updates to virus-definition files and upgrades to program components ensure that the program has up-to-the-minute scanning technology to deal with viruses as they emerge.

Later sections in this Administrator's Guide describe each of these features in detail.

Syntax

A summary of the command line and its associated options appears next. For a full description of each command, see "Choosing the options" on page 41.

NOTE: Some of the options in the syntax summary have a verbose form and an abbreviated form. The abbreviated form appears first, and the verbose form appears after the | symbol. You can use either form to add an option to the command line.

```
uvscan
[--allole] [--analyze,--analyse]
[-c |--clean] [--cleandocall] [--config file]
[--dam] [--dat] [-d |--data-directory directory] [--delete]
[--exclude file] [-e |--exit-on-error]
[--extensions EXT1,[EXT2]] [--extra file]
[--fam] [-f |--file file]
```

```
[--floppya], [--floppyb]
[-h |--help] [--ignore-compressed]
[--ignore-links] [--load file]
[--manalyze,--manalyse,--macro-heuristics]
[--maxfilesize X] [-m |--move directory]
[--noboot] [--nocomp] [--nodecrypt] [--nodoc] [--noexpire]
[--norename][--one-file-system]
[--panalyze,--panalyse][-p,--atime-preserve,--plad]
[-r |--recursive,--sub]
[--secure] [-s|--selected] [--summary]
[--unzip] [-v|--verbose] [--version] [--virus-list]
[-] {file / directory}
```

NOTE: Do not type the square brackets [ ] or the | symbol when you type your options in the command line.

Performing on-demand scan operations

You can scan any file or directory on your file system from the command line by adding options to the basic command.

NOTE: Only the Intel-based FreeBSD, SCO-UNIX and Linux distributions of the VirusScan program can scan for boot-sector viruses.

There are three groups of options:

- **Scanning options**. These determine how and where the scanner looks for infected files.
- **Response options**. These determine how the scanner responds to any infected files.
- **General options.** These determine how the scanner reports its scanning activities.

Each group of options appears in its own table with a full description of its function. See “Choosing the options” on page 41 for details.

Command-line conventions

Use these conventions to add options to the command line:

- Type each option in lower case and separate each with spaces.
- Do not use any option more than once on the command line.
- Follow the syntax correctly. The UNIX operating system is case-sensitive.
- For your convenience, you can type single consecutive switches as one switch. For example:

  ```
  -c -r --one-file-system
  ```

  You can type this instead:

  ```
  -cr --one-file-system
  ```

- To start running the program, at the UNIX command prompt, type:

  ```
  uvscan
  ```

  To have the program examine a specific file or list of files, add the target directories or files to the command line after `uvscan`. You can also create a text file that lists your target files, then add the name of the text file to the command line. See "Preconfiguring scan operations" on page 34.

NOTE: By default, the VirusScan program examines all files, no matter what their extensions. You can limit your scan operation by adding only those extensions you want to examine to the command line after the `--extensions` option, or you may exclude certain files from scan operations with the `--exclude` option. See "Choosing the options" on page 41 for details.

General hints and tips

- To display a list of all the options, each with a short description of their features, type:

  ```
  uvscan --help
  ```

- To display a list of all the viruses that the program detects, type:

  ```
  uvscan --virus-list
  ```

- To display information about the version of the program, type:

  ```
  uvscan --version
  ```

To ensure maximum protection from virus attack, you must regularly update your .DAT files. See Appendix A, "Preventing Virus Infection," for details.

Preconfiguring scan operations

Instead of running each scan operation with all its options directly from the command line, you can configure a scan operation with the options you choose, then save it in a text file as a scan task.

That way, you can run complete scan operations with ease, and at any time. Your scan task specifies the actions to take when a virus is detected.

To preconfigure a scan operation:

1. Choose the command options you want to use.

   See “Choosing the options” on page 41 for a description of available options.

2. Type the command options into a text editor just as you might on the command line.

3. Save your text in a file.

4. Type either of these lines at the command prompt.

   ```
   uvscan --load <file> <target>
   ```

   or

   ```
   uvscan --config <file> <target>
   ```

   Here, *<file>* is the name of the text file you created, and *<target>* is the file or directory you want to scan.

5. Press the **RETURN** or **ENTER** key on your keyboard to run the scan operation.

   If the scanner detects no virus infection, it displays no output.

   NOTE: To learn how to specify the options you want to use, see “Command-line conventions” on page 33.

Example 1

To scan files in the /usr/dos directory according to details given in the file, `/usr/local/config1`, type:

```
uvscan --load /usr/local/config1 /usr/dos
```

The contents of the task file, `/usr/local/config1` are:

```
-m /usr/local/viruses --ignore-compressed --maxfilesize 4
```

They instruct the scan to move any infected files to /usr/local/viruses, to ignore any compressed files in the target directory, and to examine only files smaller than 4 MB.

As an alternative, the contents of the task file can be arranged as single lines:

```
-m /usr/local/viruses
--ignore-compressed
--maxfilesize 4
```

Example 2

To scan only files smaller than 4 Mb and to ignore any compressed files in three separate directories, type:

```
uvscan --load /usr/local/config1 --file /usr/local/biglist
```

The contents of the task file, `/usr/local/config1,` are:

```
--ignore-compressed
--maxfilesize 4
```

The contents of the other file, `/usr/local/biglist,` are:

```
/usr/local/bin
/temp
/etc
```

Scheduling a virus scan operation

You can run the scanner using the UNIX `cron` scheduler to run automated scan operations. Cron stores the scheduling commands in its `crontab` files. For further information about `cron` and `crontab`, refer to your UNIX documentation or view the help text, using `man cron` and `man crontab`.

Examples

To schedule a scan operation to run at 18:30 every weekday, add this line to your crontab file:

```
30 18 * * 1-5 /usr/local/bin/uvscan
```

To schedule a scan operation to run and produce a summary at 11:50 p.m. every Sunday, add this line to your `crontab` file:

```
50 23 * * 0 /usr/local/bin/uvscan --summary
```

To schedule a scan operation to run on the `uz` directory at 10:15 a.m. every Saturday in accordance with options specified in a configuration file `conf1`, add this line to your `crontab` file:

```
15 10 * * 6 /usr/local/bin/uvscan --load /usr/local/conf1 /uz
```

To schedule a scan operation to run at 8:45 a.m. every Monday on the files specified in the file `biglist`, add this line to your crontab file:

```
45 8 * * 1 /usr/local/bin/uvscan --f /usr/local/biglist
```

What to do if the scanner detects a virus

If the scanner discovers a virus while scanning, it returns exit code number 13. See “Exit codes” on page 39 for a full description of each code.

To clean infected files or directories, or move them to a quarantine location on your network, you can configure your scan operations using one or more of these options:

- -c or --clean

  The scanner tries to automatically remove any viruses from infected files. McAfee recommends that you perform another scan operation after using this option to ensure that there are no more viruses in files that the scanner has cleaned.

- --cleandocall

  The scanner removes all macros from any file that the program identified as being infected.

- -m <*directory*> or --move <*directory*>

  The scanner moves any infected files it detects to a quarantine location that you specify. If you use the -m <*directory*> command with -c, the scanner copies the infected files to a quarantine location and attempts to clean the original. If the scanner can not clean the original, the file is deleted.

- --delete

  The scanner deletes any infected files it finds.

These options are described in detail in the "Response options" table on page 44.

The following examples show how you can use these options to respond to a virus attack. The examples assume that the scanner is available in your search path.

Example 1

To scan and clean all files in the /usr/dos directory and all of its subdirectories, type:

```
uvscan -cr /usr/dos
```

The VirusScan program (uvscan.exe) scans /usr/dos and its subdirectories automatically, and cleans any infected files it encounters.

Example 2

To scan and clean all files in the /usr/dos directory and its subdirectories, but to ignore any other file systems that are mounted, type:

```
uvscan -cr --one-file-system /usr/dos
```

The VirusScan program scans without moving across file systems, and cleans any infected files it detects.

Example 3

To scan all files, except compressed files, in the /usr/dos directory and its subdirectories and to move any infected files to /usr/local/viruses, type:

```
uvscan -m /usr/local/viruses -r --ignore-compressed /usr/dos
```

The VirusScan program scans the /usr/dos directory and its subdirectories automatically. It ignores any compressed files. It moves any infected files to /usr/local/viruses.

Example 4

To scan a file with a name prefixed with “-”., type:

```
uvscan -c -v - -myfile
```

The VirusScan program scans the named file. It cleans any detected viruses and issues a progress message. This format avoids confusion between the names of the options and the name of the target. Without the “-” option, the uvscan command appears to have three options and no target:

```
uvscan -c -v -myfile
```

Handling an infected file that cannot be cleaned

If the scanner cannot clean 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 method of renaming.

Table 3-1. 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 extensions *.vir* are 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 changed.
<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.

Exit codes

The VirusScan program returns an code when it exits. These codes identify any viruses or problems that were found during a scan operation.

Table 3-2. Exit codes

Code number	Description
0	The scanner found no viruses and returned no errors.
2	Driver integrity check failed.
6	A general problem occurred.
8	Could not find a driver.
12	The scanner tried to clean a file, and that attempt failed for some reason, and the file is still infected.
13	The scanner found one or more viruses or hostile objects (such as a Trojan horse, joke, or a test file).
15	The scanner's self-check failed; it may be infected or damaged.
19	The scanner succeeded in cleaning all infected files.
102	The user quit using the --exit-on-error option. This code appears when the scan operation encounters an unexpected condition; for example, if it cannot open a file or runs out of available memory. The program exits immediately and does not finish the scan operation. This code occurs only if you specified the --exit-on-error option when you started the program. If you did not specify the --exit-on-error option, the scanner returns exit code 6.

Report features

The program may take some time to complete a scan operation, particularly over many directories and files. However, the scanner can keep you informed of its progress, any viruses it finds, and its response to them.

The program displays this information on your screen if you add the --summary or --verbose options to the command line. To learn more about each option, see "Response options" on page 44.

The --verbose option tells you which files the program is examining.

When the scan operation finishes, the --summary option identifies the following:

- How many files the program scanned,
- How many files it cleaned,
- How many files it did not scan, and
- How many infected files it found.

Example

In the report information below, both the --summary and --verbose options have been used when scanning files in the /usr/data directory.

```
$ uvscan --summary  -v /usr/data
Scanning /usr/data/*
Scanning file /usr/data/command.com
Scanning file /usr/data/grep.com
Summary report on /usr/data/*
File(s)
        Total files: ..........       2
        Clean: ................       2
        Not scanned: ..........       0
        Possibly Infected: .....      0
```

Choosing the options

The following tables describe the options you can use to target your scan operation. The descriptions use these conventions to identify the options or required variables:

- Short versions of each command option appear after a single dash (-).
- Long versions of each command option, if any, appear after two dashes (--).
- Variables, such as filenames or paths, appear in italics within brackets < >.

To learn how to add these options to the command line, see "Command-line conventions" on page 33.

Scanning options

Scanning options describe how and where each scan operation will look for infected files. You can use a combination of these options to customize the scan operation to suit your needs. Most options are off by default. If the option is normally on, the option runs automatically; you do not need to add it to the command line. You can override some of these default options with other options.

Table 3-3. Scanning options

Option	Description
--allole	Check every file for OLE objects.
--analyze, --analyse	Use heuristics to find possible viruses in "clean" files. This step occurs after the program has checked for other viruses.
--config *<file>*, --load *<file>*	Run the options specified in *<file>*. You may not nest configuration files within other configuration files.
-d *<directory>*, --dat *<directory>* --data-directory *<directory>*	Specify where to find SCAN.DAT, NAMES.DAT, and CLEAN.DAT. If the -d switch is not used in the command line, the program looks in the same directory from where it was executed. If it cannot find these data files, the program issues exit code 6.
--exclude *<file>*	Exclude the directories or files from the scan operation as specified in *<file>*.

Table 3-3. Scanning options (Continued)

Option	Description
-e, --exit-on-error	Quit and display an error message if an error is found. The error message indicates the severity of the error. See page 39 for an explanation of exit codes.
--extensions *<EXT1[,EXT2,...]>*	Examine files that have the specified extension. You can specify as many extensions as you want. Separate each with a comma, but without a space. If you choose this option, it launches the "-s, --selected" option.
--extra *<file>*	Specify where to find EXTRA.DAT. If this switch is not used in the command line, the program looks in the same directory from where it was executed. If it cannot find this file, the program issues exit code 6.
--fam	Locate all files that have macros. Use this option with caution if you use it with the "--cleandocall" or "--dam" options.
-f *<file>*, --file *<file>*	Scan the directories or files as specified in *<file>*.
--floppya, --floppyb	Scan the boot sector of the floppy disk in drive A or B. This option is for Intel-based UNIX systems only, namely FreeBSD, SCO-UNIX and Linux.
--ignore-compressed, --nocomp	Ignore compressed files. By default, the program scans files saved in these compression formats: ICE, LZEXE, PKLITE, Cryptcom, COM2EXE, Diet, Teledisk, Microsoft Expand and GZIP. This option reduces the scanning time but also reduces file security. By default, the program scans compressed files.
--ignore-links	Do not resolve any symbolic links and do not scan the link targets.
--load *<file>*	See --config option.
--manalyze, --manalyse --macro-heuristics	Use heuristic detection to identify potential macro viruses. This is a subset of "--analyze, --analyse".
--maxfilesize *X*	Examine only those files smaller than *X* size. Here, *X* is a file size measured in megabytes.

Table 3-3. Scanning options (Continued)

Option	Description
--noboot	Do not scan the boot-sector on startup.
--nodecrypt	Do not decrypt encrypted files in order to scan them.
--noexpire	Do not issue a warning if the .DAT files are out of date.
--nodoc	Do not scan Microsoft Office document files.
--norename	Do not rename an infected file that cannot be repaired. See “Handling an infected file that cannot be cleaned” on page 38 for details about renaming.
--one-file-system	Scan an entire directory tree without scanning mounted file systems, if you use this option in conjunction with the “-r, --recursive, --sub” option. Normally, the program treats a mount point as a subdirectory and scans that file system. This option prevents the scan operation from running in subdirectories that are on a different file system to the original directory.
--panalyze, --panalyse	Use heuristic detection to identify potential program viruses. This is a subset of “--analyze, --analyse”.
-p, --atime-preserve, --plad	Reset the time that the file was last accessed to what it was before the scan operation. This enables backup software (which relies on this date) to run correctly. The scanner will not reset the access time if the file contained a virus or if the person who starts the scan operation does not own the file.
-r, --recursive, --sub	Examine any specified target directory and all its subdirectories.
--secure	Examine all files. This option activates the --analyze and --unzip options and deactivates the --selected and --extensions options at the same time.

Table 3-3. Scanning options (Continued)

Option	Description
-s, --selected	Look for viruses in any file that has execute permissions, and all files that are susceptible to virus infection. By default, this option is off. Over 80 file types are scanned including .EXE, .COM, .BAT, .DOT, .DOC, .BIN, and .VBS. By scanning only files which are susceptible to virus infection, the program can scan a directory faster.
--unzip	Examine files saved in ZIP, LHA, PKarc, ARJ, TAR and RAR formats.

Response options

These options determine how your scan operation responds to a virus infection. You can use a combination of these options to customize the scan operation. None of the options in this table occurs automatically. To activate each option, specify it in your command line. You may override some of these default options with other options.

Table 3-4. Response options

Option	Description
-c, --clean	Try automatically to remove any viruses from infected files. If the program cannot clean the file, it displays a warning message. If you use this option, repeat the scan operation to ensure there are no more infections.
--cleandocall --dam	Delete all macros from a potentially infected file. Use these options with caution when you also use the "--fam" option.
--delete	Automatically delete any infected files that are found.
-m *<directory>*, --move *<directory>*	Move any infected files to a quarantine location as specified. When the program moves an infected file, it replicates the full directory path for the infected file inside the quarantine directory so you can determine the infected file's original location. If you use the -m *<directory>* command with -c, the program copies the infected files to a quarantine location and attempts to clean the original. If it can't clean the original, the file is deleted.

General options

These options provide help or give you additional information about the scan operation. You may use a combination of these options to customize the scan operation. None of the options in this table occur automatically. To activate each option, specify it as part of your command line. You may override some of these default options with other options.

Table 3-5. General options

Option	Description
-	Denotes the end of the options and the start of the target to be scanned. This is optional. This feature is particularly useful with file names that are prefixed with "-", because it avoids confusion between the options and the target.
--extlist	Display a list of all file extensions which are susceptible to virus infection; that is, those that are scanned when -s or --selected is set.
-h, --help	List the most commonly used options, with a short description. For a full description, use `man uvscan`.
--summary	Produce a summary of the scan operation. This includes the following: • How many files the scanner examined. • How many infected files the scanner found. • How many viruses the scanner removed from infected files.
-v, --verbose	Display a progress summary during the scan operation.
--version	Display the program's version number.
--virus-list	Display a list of all the viruses that the program can detect.

Options in alphabetic order

For convenience, the options are repeated in this section in alphabetic order.

Table 3-6. Options in alphabetic order

Option	Description
-	Denotes the end of the options and the start of the target to be scanned. This is optional.
--allole	Check every file for OLE objects.
--analyze, --analyse	Use heuristics to find possible viruses in “clean” files.
--atime-preserve	Reset the time that the file was last accessed to what it was before the scan operation.
-c, --clean	Try automatically to remove any viruses from infected files.
--cleandocall	Delete all macros from a potentially infected file.
--config <*file*>	Run the options specified in <file>.
-d <directory>, --dat <directory> --data-directory <directory>	Specify where to find SCAN.DAT, NAMES.DAT, and CLEAN.DAT.
--dam	See --cleandocall.
--delete	Automatically delete any infected files that are found.
-e, --exit-on-error	Quit and display an error message if an error is found.
--exclude <file>	Exclude the directories or files from the scan operation as specified in <file>.
--extensions <EXT1[,EXT2,...]>	Examine files that have the specified extension.
--extlist	Display a list of all file extensions which are susceptible to virus infection; that is, those that are scanned when -s or --selected is set.
--extra <file>	Specify where to find EXTRA.DAT.
-f <*file*>, --file <*file*>	Scan the directories or files as specified in <file>.
--fam	Locate all files that have macros.
--floppya, --floppyb	Scan the boot sector of the floppy disk in drive A or B.
-h, --help	List the most commonly used options, with a short description. For a full description, use man uvscan.

Table 3-6. Options in alphabetic order (Continued)

Option	Description
--ignore-compressed	Ignore compressed files.
--ignore-links	Do not resolve any symbolic links and do not scan the link targets.
--load <file>	See --config option.
-m <directory>	Move any infected files to a quarantine location as specified.
--macro-heuristics, --manalyze, --manalyse	Use heuristic detection to identify potential macro viruses.
--maxfilesize X	Examine only those files smaller than X size.
--move <directory>	See -m <directory>.
--noboot	Do not scan the boot-sector on startup.
--nocomp	See --ignore-compressed.
--nodecrypt	Do not decrypt encrypted files in order to scan them.
--nodoc	Do not scan Microsoft Office document files.
--noexpire	Do not issue a warning if the .DAT files are out of date.
--norename	Do not rename an infected file that cannot be repaired.
--one-file-system	Scan an entire directory tree without scanning mounted file systems, if you use this option in conjunction with the “-r, --recursive, --sub” option.
-p, --plad	See --atime-preserve.
--panalyze, --panalyse	Use heuristic detection to identify potential program viruses.
-r, --recursive	Examine any specified target directory and all its subdirectories.
-s, --selected	Look for viruses in any file that has execute permissions, and all files that are susceptible to virus infection. By default, this option is off.
--secure	Examine all files.
--sub	See -r, --recursive.
--summary	Produce a summary of the scan operation.
--unzip	Examine files saved in ZIP, LHA, PKarc, ARJ, TAR and RAR formats.

Table 3-6. Options in alphabetic order (Continued)

Option	Description
-v, --verbose	Display a progress summary during the scan operation.
--version	Display the program’s version number.
--virus-list	Display a list of all the viruses that the program can detect.

Preventing Virus Infection A

Creating a secure system environment

VirusScan for UNIX anti-virus software is an effective tool for preventing virus infections, but it is most effective when used in conjunction with regular backups, meaningful password protection, user training, and awareness of virus threats.

To create a secure system environment and minimize your chance of infection, McAfee recommends that you:

- Install VirusScan software and other McAfee anti-virus software.
- Include a uvscan command in a `cron` file.
- Make frequent backups of important files. Even if you have VirusScan software to prevent attacks from viruses, damage from fire, theft, or vandalism can render data unrecoverable without a recent backup.

Detecting new and unidentified viruses

To offer the best virus protection possible, McAfee continually updates the virus definition (.DAT) files that the VirusScan software uses to detect viruses. For maximum protection, you should regularly update these files.

NOTE: The term "update" refers only to the .DAT files; the term "upgrade" refers to product version revisions, executables, and definition files. McAfee offers free online .DAT file updates for the life of your product, but cannot guarantee they will be compatible with previous versions. By upgrading your software to the latest product version and updating regularly to the latest .DAT files, you ensure complete virus protection for the term of your software subscription or maintenance plan.

Why do I need a new .DAT file?

More than 500 new viruses appear each month. Often, older .DAT files cannot assist the VirusScan software in detecting these new variations. For example, the .DAT files with your original copy of VirusScan might not detect a virus that was discovered after you bought the product.

If you suspect you have found a new virus, see “Reporting new items for anti-virus data file updates” on page xvii for instructions on contacting Network Associates.

Updating your .DAT files

Download the new files from either of these sources:

- **The Network Associates FTP server.** Open a connection to ftp.nai.com.

  Use `anonymous` as your user name and your e-mail address as your password to gain access. Look for VirusScan .DAT files in the directory pub/antivirus/datfiles/4.x.

- **The Network Associates Web Site.** Start your browser, then go to http://www.nai.com/download to download the latest .DAT files.

To use the new .DAT files:

1. Create a download directory.
2. Change to the download directory and download the new .DAT file from the source you have chosen.

   The number given to the .DAT file will change on a regular basis. A higher number indicates a later version of the .DAT file.
3. To unpack the .DAT file, type:

   ```
   tar -xf <file>
   ```

   Here, `file` is the name of the file you downloaded.
4. Type this line at the command prompt to move the .DAT files to the directory where your software is installed:

   ```
   mv *.dat /usr/local/uvscan
   ```

   Your system overwrites the old .DAT files with the new files.

   IMPORTANT: Name the file using lower case.

Your software will now use the new .DAT files to scan for viruses.

Sample update script

The following example shows an update script that gets new .DAT files from the Network Associates FTP site:

This entry must appear in the .netrc file for this script to work:

```
machine ftp.nai.com
login anonymous
password <e-mail address>
macdef init
cd pub/antivirus/datfiles/4.x
bin
prompt
mget dat-*.tar
close
bye
```

where *<e-mail address>* is the address of the user who is logging in to the FTP server

```
#!/bin/sh

# Assume uvscan is installed in the same directory
# as this script.
install_directory=`dirname $0`

# Create a download directory
mkdir /tmp/dat-updates
cd /tmp/dat-updates

# Get the version of the currently installed .DATs
# from the info given by the --version switch
current_version=`
    $install_directory/uvscan --version |
    grep "Virus data file" |
    awk '{ print substr($4,2,4) }'`

# Get the new .DATs.
```

```
# The entry in your .netrc file should take care
# of the downloading.
ftp ftp.nai.com

# Get the version of the new .DATs from the filename.
new_version=`echo dat-*.tar | awk '{ print substr($1,5,4) }'`

# If they are the same age or older than the current ones,
# do not install them
if [ "$current_version" -ge "$new_version" ]
then
    echo "No new .DATs available at this time"
    echo "Currently installed version:  $current_version"
    echo "Version on FTP site:          $new_version"
else
    tar -xf dat-*.tar

    # Move them to the install directory, making sure
    # the filename is lower case.
    for file in `tar -tf dat-*.tar`
    do
        newfile=`echo $file | tr [A-Z] [a-z]`
        mv ./$file "$install_directory/$newfile"
    done

    # Get the current version again and make sure
    # the new .DATs installed correctly.
    current_version=`
        $install_directory/uvscan --version |
        grep "Virus data file" |
        awk '{ print substr($4,2,4) }'`

    if [ ! "$current_version" -eq "$new_version" ]
    then
        echo "DAT file updates did not work correctly."
        echo "Please try manually."
    fi
```

```
fi
# Delete the directory that you created.
cd /
rm -fr /tmp/dat-updates
```

Network Associates Support Services

B

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 B-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

A

America Online

technical support via, xv

America Online, technical support via, 60

anti-virus software

reporting new viruses not detected by to McAfee, xvii

automatic scan operation, 36

B

boot-sector viruses, 32

C

cleaning infected files, 44

command line

typing options, 33

command syntax

variables, 41

compressed files, ignoring during scan operations, 42

CompuServe, technical support via, xv, 60

configuration file, option for loading saved, 41

consulting services, 63

conventions,typing options, 33

cron, UNIX command, 36

crontab files, using to scan automatically, 36

Customer Care

contacting, xiv

D

.DAT file updates, 49

reporting new items for, xvii

.DAT files, 50

option for not showing expiration notice, 42

diskette scanning, 42

distributions, versions of VirusScan software, 23

documentation, 22

E

educational services, description of, 64

electronic services, contacting for technical support, 60

e-mail

addresses for reporting new viruses to McAfee, xvii

error messages, 26

exit codes, 39

exit-on-error, setting for scan operations, 42

F

files , list of types scanned, 45

floppy disk, see diskette

H

help scanning options, 45

heuristics

options, 41 to 44

I

infected files
- cannot be cleaned, 38
- cleaning, 44
- renaming, 38

installation requirements, 24
installing VirusScan software, 24

L

last access date of files, preserving, 43
LIBC5 on Linux, 27
LIBC6 on Linux, 27
library paths, 25
links, creating to uvscan and shared library, 25
Linux, LIBC5 and LIBC6, 27

M

macros, 44
McAfee
- contacting
  - via America Online, xv
  - via CompuServe, xv
  - within the United States, xv

Microsoft Word files, do not scan, 42

N

Network Associates
- consulting services from, 63
- contacting
  - Customer Service, xiv
  - outside the United States, xviii
- educational services, 64
- support services, 55
- training, xvi, 63
- website address for software updates and upgrades, 60

new viruses, reporting to McAfee, xvii
no decrypt, 42

O

on-demand scanning, 32
option for deleting from files, 44

P

performing a scan operation, 32
permissions, 24
preventing virus infection, 49
PrimeSupport
- corporate
  - at a glance, 59
  - KnowledgeCenter, 55
  - ordering, 58
  - PrimeSupport Connect, 56
  - PrimeSupport Connect 24-By-7, 57
  - PrimeSupport Enterprise, 57
- for home users
  - Online Upgrades plan, 61
  - ordering, 62
  - Pay-Per-Minute plan, 61
  - Quarterly Disk/CD plan, 61
  - Small Office/Home Office Annual Plan, 61

Professional Consulting Services
- description of, 63

Q

quarantine, moving infected files to, 44

R

removing VirusScan software
- by hand, 29
- using the uninstallation script, 29

report, 40

reporting viruses not detected to McAfee, xvii

root account, 24

S

scan operation results, displaying, 45

scan targets, using a file to supply, 42

scan task, 34

scanning
- boot sector of diskette, 42
- diskette, 42

scheduling a scan operation, 36

shared library path
- removing, 29

software updates and upgrades, website address for obtaining, 60

standard input, using to set scan targets, 42

summary of scan operation results, displaying, 45

support
- corporate
  - at a glance, 59
  - KnowledgeCenter, 55
  - ordering, 58
  - PrimeSupport Connect, 56
  - PrimeSupport Connect 24-By-7, 57
  - PrimeSupport Enterprise, 57
- for home users, 60
  - Online Upgrades plan, 61
  - Pay-Per-Minute plan, 61
  - PrimeSupport
    - ordering, 62
    - Small Office/Home Office Annual Plan, 61
  - Quarterly Disk/CD plan, 61
- hours of availability, 60
- via electronic services, 60

syntax
- summary of options, 31
- using variables in, 41

T

technical support
- corporate
  - at a glance, 59
  - KnowledgeCenter, 55
  - ordering, 58
  - PrimeSupport Connect, 56
  - PrimeSupport Connect 24-By-7, 57
  - PrimeSupport Enterprise, 57
- e-mail address for, xv
- for home users
  - PrimeSupport
    - Online Upgrades plan, 61
    - Pay-Per-Minute plan, 61
    - Quarterly Disk/CD plan, 61
    - Small Office/Home Office Annual Plan, 61
- hours of availability, 60
- information needed from user, xvi

online, xv
phone numbers for, xv
PrimeSupport
for home users
ordering, 62
via electronic services, 60
Total Education Services
description of, 63
Total Service Solutions
contacting, 63
training for Network Associates products, xvi, 63
scheduling, xvi
troubleshooting installation, 26

U

updates, 31
updates and upgrades, website address for obtaining, 60
uvscan.exe (VirusScan executable), 37

V

variables, using in command line, 41
verbose scan reports, setting, 45
.vir, 38
viruses
cleaning infected files, 44
reporting new strains to McAfee, xvii
VirusScan software
cleaning options, 36
components, 22
configuration options, 34
documentation, 22
general options, 45
help, 33
installing, 24
introducing, 21
list of viruses, 33
options
-, 45
delete infected file, 37
examples, 34 to 35, 37 to 38
--exit-on-error, 39
move or quarantine, 37
options in alphabetic order, 46
overview of features, 21
report options, 40
response options, 44
scanning options, 41
scheduling, 36
system requirements, 24
uvscan.exe executable, 37
version number, 33

W

website, Network Associates technical support via, 60
why use VirusScan for UNIX software?, 21

Z

zipped files, ignoring during scan operations, 42