VirusScan for UNIX

Administrator’s Guide

4.7
Table of Contents

Preface .................................................................................................................. vii
  Anti-virus protection as information security .................................................... vii
  Information security as a business necessity .................................................... vi
  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 ............................................................................... 23
    Other recommendations ................................................................................ 24
  Installation steps .............................................................................................. 24
  Troubleshooting ............................................................................................... 26
  Testing your installation ................................................................................... 26
  Removing the VirusScan for UNIX program ................................................ 27
Chapter 3. Using VirusScan for UNIX Software ........................................... 29
  Overview ........................................................................................................ 29
  Syntax ............................................................................................................. 29
  Performing on-demand scan operations ....................................................... 30
    Command line conventions .......................................................................... 30
    General hints and tips: ................................................................................. 31
  Preconfiguring scan operations ................................................................... 32
  Scheduling scan operations .......................................................................... 33
  What to do if VirusScan for UNIX software detects a virus ...................... 35
    Scenario No. 1 ............................................................................................. 35
    Scenario No. 2 ............................................................................................. 36
    Scenario No. 3 ............................................................................................. 36
  Exit codes ........................................................................................................ 36
  The VirusScan for UNIX program report features ..................................... 37
  Options tables ................................................................................................. 38
    Scanning options ........................................................................................ 38
    Response options ........................................................................................ 44
    General options .......................................................................................... 46

Appendix A. Preventing Virus Infection ......................................................... 47
  Keys to a secure system environment .......................................................... 47
  Detecting new and unidentified viruses ....................................................... 47
    Why would I need a new .DAT file? ............................................................ 48
  Updating your .DAT files ............................................................................. 48
    Sample update script .................................................................................. 49

Appendix B. McAfee Support Services .......................................................... 53
  PrimeSupport options for corporate customers ......................................... 53
    PrimeSupport KnowledgeCenter ............................................................... 53
    PrimeSupport Connect .............................................................................. 54
    PrimeSupport Priority ............................................................................... 54
    PrimeSupport Enterprise .......................................................................... 55
  Ordering Corporate PrimeSupport ............................................................... 56
  PrimeSupport options for retail customers ............................................... 58
  Ordering Retail PrimeSupport ..................................................................... 59
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee consulting and training</td>
<td>60</td>
</tr>
<tr>
<td>Professional consulting services</td>
<td>60</td>
</tr>
<tr>
<td>Jumpstart services</td>
<td>60</td>
</tr>
<tr>
<td>Network consulting</td>
<td>60</td>
</tr>
<tr>
<td>Total Education Services</td>
<td>61</td>
</tr>
</tbody>
</table>

## Index

| Index | 63   |
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.
Preface

- 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 200 to 300 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 that 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:


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.mcafee2b.com/

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 McEwan, Suite 500  
Dallas, Texas 75244  
U.S.A.

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

Other contact information for corporate-licensed customers:

Phone: (972) 308-9960  
Fax: (972) 619-7485 (24-hour, Group III fax)  
E-Mail: services_corporate_division@nai.com  
Web: [http://www.nai.com](http://www.nai.com)
Other contact information for retail-licensed customers:

Phone:  (972) 308-9960
Fax: (972) 619-7485 (24-hour, Group III fax)
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.


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 Network Associates 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 Network Associates technical support plans.

For corporate-licensed customers:

Phone (972) 308-9960
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, “McAfee Support Services.”
To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please 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, 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

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

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.

<table>
<thead>
<tr>
<th>Company</th>
<th>Address</th>
<th>Phone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Associates Australia</td>
<td>Level 1, 500 Pacific Highway  St. Leonards, NSW  Sydney, Australia 2065</td>
<td>61-2-8425-4200</td>
<td>61-2-9439-5166</td>
</tr>
<tr>
<td>Network Associates Austria</td>
<td>Pulvermuehlstrasse 17  Linz, Austria  Postal Code A-4040</td>
<td>43-732-757-244</td>
<td>43-732-757-244-20</td>
</tr>
<tr>
<td>Network Associates Belgique</td>
<td>BDC Heyzel Esplanade, boîte 43  1020 Bruxelles  Belgique</td>
<td>0032-2 478.10.29</td>
<td>0032-2 478.66.21</td>
</tr>
<tr>
<td>Network Associates Canada</td>
<td>139 Main Street, Suite 201  Unionville, Ontario  Canada L3R 2G6</td>
<td>(905) 479-4189</td>
<td>(905) 479-4540</td>
</tr>
<tr>
<td>Network Associates People’s Republic of China</td>
<td>New Century Office Tower, Room 1557  No. 6 Southern Road Capitol Gym  Beijing  People’s Republic of China 100044</td>
<td>8610-6849-2650</td>
<td>8610-6849-2069</td>
</tr>
<tr>
<td>Network Associates Denmark</td>
<td>Lautruphøj 1-3  2750 Ballerup  Danmark</td>
<td>45 70 277 277</td>
<td>45 44 209 910</td>
</tr>
<tr>
<td>NA Network Associates Oy</td>
<td>Mikonkatu 9, 5. krs.  00100 Helsinki  Finland</td>
<td>358 9 5270 70</td>
<td>358 9 5270 7100</td>
</tr>
</tbody>
</table>
Preface
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

Welcome

Thank you for purchasing VirusScan for UNIX—the McAfee virus detection and removal solution for UNIX-based systems.

McAfee anti-virus researchers provide fast, responsive coverage for new viruses and other malicious software. New-generation VirusScan for UNIX scanning technology has the ability to 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 virus scanning engine update and virus definition .DAT file release.

McAfee worldwide virus research team develops weekly updates for the VirusScan for UNIX 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 world, however, is different. DOS computers have no security and are very susceptible to virus infections. Since DOS system viruses don’t affect UNIX systems, you might be asking: “Why should I be concerned?”

One reason for concern is that DOS- and Windows-based computers are a rapidly expanding presence on the Internet—and most of these computers use the Internet for file transfer. A UNIX server may still harbor DOS system viruses and, while not itself affected, 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 a variety of 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 for UNIX documentation includes:

- **Administrator’s Guide.** This Administrator’s Guide describes in detail how to use the VirusScan for UNIX software. It includes background information and advanced configuration options. You can get the *Administrator’s Guide* directly from the McAfee product CD-ROM or install it on your hard disk 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, lists any known behavior or other issues with the product release, and often describes new product features incorporated into product updates. You’ll find the README.TXT file at the root level of your McAfee product CD-ROM—you can open and print it 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 VirusScan for UNIX software. You’ll find the LICENSE.TXT file at the root level of your McAfee product CD-ROM. Read it carefully—by installing the VirusScan for UNIX software you agree to its terms.

- **RESELLER.TXT file.** This file contains a list of McAfee resellers and their addresses and telephone numbers.
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, and on a McAfee product CD-ROM disc. Once you have downloaded a VirusScan for UNIX archive or placed your product installation disc in your CD-ROM drive, the installation steps you follow are the same for each type of distribution.

Review the "Installation requirements" at the bottom of this page to verify that the VirusScan for UNIX software will run on your system, then follow the installation steps on page 24.

About the distributions

The VirusScan for UNIX program comes in six distribution versions, one for each supported operating system. If you install the VirusScan program from CD-ROM, you will find each version is in its own directory. Each distribution has its own installation script.

- 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

Installation requirements

To install and run VirusScan for UNIX 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 downloaded the VirusScan for UNIX software from the Network Associates web site, this is an optional item.

Other recommendations

• To install the VirusScan for UNIX 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 anti-virus .DAT file updates that Network Associates offers from its website, you should have an Internet connection, either through your local area network, or via a high-speed modem and an Internet service provider.

Installation steps

This example gives step by step instructions to install VirusScan for UNIX software on the Solaris distribution. To install other distributions, substitute the correct filename where the example specifies vsun407l.tar.Z.

To start the VirusScan for UNIX installation script, follow these steps:

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

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

2. Copy the file vsun407l.tar.Z to a directory on your system.

   NOTE: McAfee recommends that you do not copy this file to the directory in which you plan to install the VirusScan for UNIX program.

3. Type this line at the command prompt:

   zcat vsun407l.tar.Z | tar -xf -

   This decompresses the file to your hard disk.
4. Type this line at the command prompt to execute the installation script:
   ./install-uvscan [installation directory]

   Here [installation directory] is the target directory where you want to install VirusScan for UNIX 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 target installation directory that you specify does not exist, the installation script asks whether you want 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 a link to uvscan in the directory /usr/local/bin. Type \texttt{Y} to create the link or type \texttt{N} to skip this step.

   McAfee recommends that you include the link in your search path.

6. The installation script asks whether you want to place a link to the shared library path \texttt{libsunfv.so} in the directory /usr/local/lib. Type \texttt{Y} to create the link or type \texttt{N} to skip this step.

   McAfee recommends that you create this link or you will need to set these environment variables to contain the installation directory:
   
   \begin{itemize}
   \item LD\_LIBRARY\_PATH for the Solaris 2.x distribution or the SCO OpenServer Release 5 distribution; or
   \item SHLIB\_PATH for the HP-UX distribution; or
   \item LIBPATH for the AIX distribution.
   \end{itemize}

   \textbf{NOTE:} The VirusScan for UNIX program also looks in the /usr/lib or /lib directory or the current directory for the shared library. If you installed the VirusScan for UNIX distributions for Linux and FreeBSD the shared library does not exist.

7. The installation program copies the VirusScan for UNIX program files to your hard disk, then scans your default home directory.

   If the software discovers a virus, see “What to do if VirusScan for UNIX software detects a virus” on page 35 to learn about the actions you can take.

   If the installation fails, see “Troubleshooting” on page 26 to learn about possible errors and get suggested courses of action that you can take.
Troubleshooting

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

Table 2-1. Error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Cause or action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to create install_dir</td>
<td>Verify that you have permission to create install_dir</td>
</tr>
<tr>
<td>Cannot write to install_dir</td>
<td>Verify that you have permission to create install_dir</td>
</tr>
<tr>
<td>The install_dir exists, but is not a subdirectory</td>
<td>Choose another installation directory</td>
</tr>
<tr>
<td>&lt;file&gt; is missing</td>
<td>The file might not exist</td>
</tr>
<tr>
<td>&lt;file&gt; is not correct</td>
<td>The file did not install correctly</td>
</tr>
</tbody>
</table>

Testing your installation

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

To test your installation, follow these steps:

1. Open a standard 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 shown above should appear as one line in your text editor window.

2. Save the file with the name EICAR.COM. The file size will be 68 or 70 bytes.
3. Create an on-demand scan operation and specify it to scan the EICAR.COM file.

See “Performing on-demand scan operations” on page 30 to learn how to create an on-demand scan operation.

When the VirusScan for UNIX software 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. Delete the file when you have finished testing your installation to avoid alarming other users.

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

### Removing the VirusScan for UNIX program

The uninstallation script is installed at the same time as the VirusScan for UNIX program and enables you to remove the product quickly and easily. To remove the VirusScan for UNIX program from your system quickly, you can:

Run the uninstallation script uninstall-uvscan which you’ll find in the VirusScan for UNIX program directory, for example type the following command at the command line:

```
cd /usr/local/uvscan
./uninstall-uvscan
```

When the VirusScan for UNIX software has been removed, you must go back and delete the uninstallation script `uninstall-uvscan` from the program directory to remove the program completely from your system.

- Delete the individual VirusScan for UNIX program files from the command line using the `rm` command.

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

Administrators should take precautions to ensure that users cannot accidentally remove their VirusScan for UNIX software.

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

The VirusScan for UNIX program is a command-line driven software package designed to offer sophisticated virus scanning capability without sacrificing flexibility. In this chapter, you will learn how to use its powerful features and functions, and customize the program to meet your specific needs.

The following VirusScan for UNIX features offer optimum protection for you and your network:

- Powerful on-demand scanning options let you start a scan operation immediately or schedule automatic scan operations to suit your work flow.
- Advanced heuristic scanning technology detects previously unidentified or unclassified macro and program viruses.
- Virus definition file updates and program component upgrades ensure that the VirusScan for UNIX software has up-to-the-minute scanning technology to deal with viruses as they emerge from the field.

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 on page 30. A full description of each command appears in “Options tables” on page 38.

⚠️ NOTE: Some of the options in the syntax summary consists of 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.
Using VirusScan for UNIX Software

uvscan
[--allole] [--analyze,--analyse] [-c |--clean]
[--cleandocall] [--config file] [--dam] [--dat]
[-d |--data-directory directory] [--delete] [--exclude file]
[--ignore-compressed] [--ignore-links] [--load file]
[--manalyze,--manalyse,--macro-heuristics] [--maxfilesize X]
[-m |--move directory] [--noboot] [--nocomp] [--nodecrypt]
[--nodoc] [--noexpire] [--one-file-system]
[--panalyze,--panalyse] [-p|--atime-preserve] [--pcad] [-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 one or a combination of options to the basic commands.

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

The VirusScan for UNIX program includes three groups of options:

- **Scanning and targeting options.** These options govern how and where the VirusScan program looks for infected files.
- **Response options.** These options tell the VirusScan for UNIX program how to respond to any infected files it detects.
- **General options.** These options tell the VirusScan for UNIX program to report its scanning activities.

Each group of options appears in its own table with a full description of its function. See “Options tables” on page 38 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.

Type single consecutive switches as one switch for your convenience. For example, instead of:

   -c -r --one-file-system,

you can type:

   -cr --one-file-system

To start running the VirusScan for UNIX software, at the UNIX command prompts, type:

   uvscan

To have the VirusScan for UNIX software 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 simply add the name of the text file to the command line. See “Preconfiguring scan operations” on page 32 to learn how.

NOTE: By default, the VirusScan for UNIX software 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 “Options tables” on page 38 for details.

General hints and tips:

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

   uvscan --help

- To display a list of all the viruses that the VirusScan for UNIX software detects, type:

   uvscan --virus-list

- To display information about the version of the VirusScan for UNIX software, type:

   uvscan --version

To ensure that your VirusScan for UNIX software gives you 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 attendant 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. The scan task can specify targets for the VirusScan for UNIX program to examine and the actions it should take when it detects a virus.

To preconfigure a scan operation, follow these steps:

1. Choose the command options you want to use.
   
   See “Options tables” on page 38 for a description of available options.

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

3. Save your text in a file.

4. Start the VirusScan for UNIX program, then type either of these lines at the command prompt.

   \texttt{uvscan --load <file> OR uvscan --config <file>}

   Here <file> is the name of the text file you created.

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

   If the VirusScan for UNIX program detects no virus infection, it displays no output.

---

\textbf{NOTE:} To learn how to specify the options you want to use, see “Command line conventions” on page 30.
Using VirusScan for UNIX Software

Scheduling scan operations

The VirusScan for UNIX program can work with the UNIX cron scheduler to run automated scan operations. Cron stores regularly scheduled commands in crontab files.

Crontab files contain commands that execute automatically at the time you specify. The files consist of six fields. The first five fields are integers, each of which specifies a date or time for cron to execute.

The fields and their allowable range of values in the order they must appear in the crontab file are:

- Minute: 0-59
- Hour: 0-23
- Day of the month: 1-31
- Month: 1-12
- Day of the week: 0-6, with 0 = Sunday

Separate each field with spaces or tab stops. Use a comma to separate a list of elements within a field. For example, to set a scan operation to occur on the 1st, 15th and 28th day of any given month, type:

```
1, 15, 28
```

Specify a range within a field with a minus sign or dash (-). For example, to set a scan operation to occur every day Monday through Friday, type:

```
1-5
```

An asterisk (*) indicates all possible values.

The sixth field in a crontab file is the string of options that you want the shell to execute at the specified time.

NOTE: The following examples assume you have the uvscan executable available on your search path.

To set a scan operation to examine your target files or directories automatically, follow these steps:

1. In order to list all the cron entries and store them in a named text file that contains your crontab entries, on the command line, type:

   ```
crontab -l > <file>
   ```

   Here <file> is the name of the text file that lists your crontab entries.
2. To append a new entry to the named file and specify what type of scan operation you want to perform, type:

```
echo "<minute> <hour> <day> <month> <day of the week>
vuscan --options" >> <file>
```

where ‘minute | hour | day’ and so on indicates the time and date that you want to perform the scan operation, according to the guidelines given earlier in this section.

The double quotes must be typed as you see them in the example but do not type the angled brackets.

3. Then, to resubmit all the jobs to cron, type:

```
crontab <file>
```

Cron performs the scan operation automatically as instructed by the command line.

If a crontab file does not already exist, the message “can’t open your crontab file” appears. To set up a new crontab file, ignore step 1 above and create a text file, then continue with step 2.

For more detailed information on how to set up a crontab file, see the UNIX man page for crontab. To do so, type this line at the command prompt:

```
man crontab
```

---

To schedule a scan operation for a specific date and at a specific time, follow these steps:

1. Type this line at the command prompt:

```
crontab -1 > <file>
```

Here <file> is the name of the text file that lists your crontab entries.

2. Specify the type of scan operation you want to perform. To do so, type this line at the command prompt:

```
echo ’0 0 13 10 * uvscan --selected’ >> <file>
```

3. Then, to run the scan, type:

```
crontab <file>
```
What to do if VirusScan for UNIX software detects a virus

If the VirusScan for UNIX program discovers a virus, the scan operation returns exit code number 13. See “Exit codes” on page 36 for a full description of each code.

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

- `--clean`

  This option tells the VirusScan for UNIX software to try automatically to remove any viruses from infected files. McAfee recommends that you perform another scan operation after using this option to ensure that the program cannot detect any virus remnants in files it has cleaned.

- `--cleandocall`

  This option tells the VirusScan for UNIX program to remove all macros from any file that the program identified as being infected.

- `--move <directory>`

  The VirusScan for UNIX program moves any infected files it detects to a quarantine location that you specify. If the `-m <directory>` command is used with `-c`, the VirusScan 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.

- `--delete`

  The VirusScan for UNIX program deletes any infected files it finds.

Detailed descriptions of these options appear in the “Response options” table on page 44.

The following scenarios list some of the ways in which you can use these options to respond to a virus attack. They assume that the `uvscan` executable is available in your search path.

**Scenario No. 1**

To tell the VirusScan for UNIX program to scan and clean all files in the `/usr/dos` directory and all of its subdirectories, type:

```
uvscan -cr /usr/dos
```
The VirusScan for UNIX program scans /usr/dos and its subdirectories automatically, and cleans any infected files it encounters.

**Scenario No. 2**

To tell the VirusScan for UNIX program 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:

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

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

**Scenario No. 3**

To tell the VirusScan for UNIX program 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:

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

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

**Exit codes**

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

<table>
<thead>
<tr>
<th>Code number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The VirusScan for UNIX program found no viruses and returned no errors.</td>
</tr>
<tr>
<td>2</td>
<td>Driver integrity check failed.</td>
</tr>
<tr>
<td>6</td>
<td>A general problem occurred.</td>
</tr>
<tr>
<td>8</td>
<td>Could not find a driver.</td>
</tr>
<tr>
<td>13</td>
<td>One or more viruses or hostile objects were found.</td>
</tr>
</tbody>
</table>
The VirusScan for UNIX program report features

The VirusScan for UNIX program may take some time to complete a scan operation, particularly if it scans a lot of directories and files. It will, however, keep you informed of its progress and any viruses it finds together with the actions it took to respond to them.

The VirusScan for UNIX program displays this information on your screen provided that you add the --summary or --verbose options to the command line. To learn more about each option, see “Response options” on page 44.

A sample of the VirusScan for UNIX report information appears below where both the --summary and --verbose options have been used to perform a scan operation on files located in the /usr/data directory.

The --verbose option tells you which files the VirusScan program is examining. When the scan operation finishes, the --summary option identifies 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.

$ 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)

<table>
<thead>
<tr>
<th>Description</th>
<th>Code number</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VirusScan for UNIX program self-check failed; it may be infected or damaged.</td>
<td>15</td>
</tr>
<tr>
<td>User quit using the --exit-on-error option. Code 102 is given when the scan operation encounters an unexpected condition; for example, if it can’t open a file or runs out of available memory. The program exits immediately and does not finish the scan operation. Code 102 occurs only if you specified the --exit-on-error option when you started the VirusScan for UNIX program. If you did not specify the --exit-on-error option, Exit Code 6 is returned.</td>
<td>102</td>
</tr>
</tbody>
</table>

Table 3-1. Exit code descriptions
Options tables

The following tables describe the options you can use to target your scan operations.

The descriptions use these conventions to identify the options or required variables:

- Short versions of each command line 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 30.

Scanning options

Scanning options describe how and where each scan operation will look for infected files. You may use a combination of these options to shape the scan operation to suit your needs. If the UVSCAN default column entry for that option is “on”, the option automatically runs without your needing to add it to the command line. You may override some of these default options with other options.

Table 3-2. Scanning options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td>--allele</td>
<td>This option checks every file that is scanned for containing OLE objects.</td>
<td>Off</td>
</tr>
<tr>
<td>--analyze, --analyse</td>
<td>This option tells uvscan to use heuristics to look for possible viruses in “clean” files. This step would occur after the software has checked for other viruses.</td>
<td>Off</td>
</tr>
<tr>
<td>--config &lt;file&gt;, --load &lt;file&gt;</td>
<td>This option causes uvscan to run the options specified in &lt;file&gt;. You may not nest configuration files within other configuration files.</td>
<td>Off</td>
</tr>
</tbody>
</table>
### Table 3-2. Scanning options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d &lt;directory&gt;</code>, <code>-dat &lt;directory&gt;</code>, <code>-data-directory &lt;directory&gt;</code></td>
<td>This option tells <code>uvscan</code> where to find <code>SCAN.DAT</code>, <code>NAMES.DAT</code>, and <code>CLEAN.DAT</code>.</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td>If the <code>-d</code> switch is not used in the command line, <code>uvscan</code> looks in the same directory from where it was executed. If <code>uvscan</code> cannot find these data files, the program issues exit code 6.</td>
<td></td>
</tr>
<tr>
<td><code>--exclude &lt;file&gt;</code></td>
<td>This option excludes the directories or files you specify within <code>&lt;file&gt;</code> from the scan operation.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--extensions &lt;EXT1,EXT2&gt;</code></td>
<td>This option directs <code>uvscan</code> to examine the files that have the extension that you specify. You can specify as many extensions as you wish, provided you separate each with a comma, but without a space. If you choose this option, it launches the <code>--s, --selected</code> option.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--fam</code></td>
<td>This option tells <code>uvscan</code> to locate all files that have macros. Use this option with caution if you use it in conjunction with the <code>--cleandocall, --dam</code> options.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--exclude &lt;file&gt;</code></td>
<td>This option excludes the directories or files you specify within <code>&lt;file&gt;</code> from the scan operation.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--exclude &lt;file&gt;</code></td>
<td>This option excludes the directories or files you specify within <code>&lt;file&gt;</code> from the scan operation.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--exit-on-error</code></td>
<td>This option tells <code>uvscan</code> to quit and display an error message if it encounters an error. The error message indicates the severity of the error. See page 36 for an explanation of exit codes.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--exit-on-error</code></td>
<td>This option tells <code>uvscan</code> to quit and display an error message if it encounters an error. The error message indicates the severity of the error. See page 36 for an explanation of exit codes.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--extensions &lt;EXT1,EXT2&gt;</code></td>
<td>This option directs <code>uvscan</code> to examine the files that have the extension that you specify. You can specify as many extensions as you wish, provided you separate each with a comma, but without a space. If you choose this option, it launches the <code>--s, --selected</code> option.</td>
<td>Off</td>
</tr>
<tr>
<td><code>--fam</code></td>
<td>This option tells <code>uvscan</code> to locate all files that have macros. Use this option with caution if you use it in conjunction with the <code>--cleandocall, --dam</code> options.</td>
<td>Off</td>
</tr>
</tbody>
</table>
Using VirusScan for UNIX Software

Table 3-2. Scanning options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-f <file>`, `--file <file>` | This option tells uvscan to scan the directories or files that you specify within `<file>`.
|                         | Save your list of target files as a text file and specify its path in the command line. |
| `--ignore-compressed`,  | This option tells uvscan to 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 time it takes to complete a scan, but also reduces file security. |
| `--nocomp`              | By default, VirusScan for UNIX software scans compressed files.              |
| `--ignore-links`        | This option tells uvscan not to resolve any symbolic links it finds and not to scan the link targets. |
| `--manalyze`, `--manalyse` | This option tells uvscan to use heuristic detection to identify potential macro viruses. This is a subset of `--analyze`, `--analyse`. |
| `--macro-heuristics`    | Off                                                                         |
| `--maxfilesize X`       | This option tells uvscan to examine only those files smaller than X size. Here, X is a file size measured in megabytes. |
| `--nocheck`             | Off                                                                         |
| `--noboot`              | This option tells uvscan to turn off boot sector scanning on startup.      |
### Table 3-2. Scanning options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td>--nodecrypt</td>
<td>This option tells uvscan not to decrypt encrypted files in order to scan them.</td>
<td>Off</td>
</tr>
<tr>
<td>--noexpire</td>
<td>This option tells uvscan not to warn you your .DAT files are out of date.</td>
<td>Off</td>
</tr>
<tr>
<td>--nodoc</td>
<td>This option tells uvscan not examine .DOC files.</td>
<td>Off</td>
</tr>
<tr>
<td>--one-file-system</td>
<td>This option allows you to scan an entire directory tree without scanning mounted file systems, if you use it in conjunction with the &quot;-r, --recursive, -sub&quot; option. Use this option to prevent uvscan from scanning mounted file systems.</td>
<td>Off. Normally, VirusScan for UNIX software treats a mount point as a subdirectory and scans that file system.</td>
</tr>
<tr>
<td>--panalyze, --panalyse</td>
<td>This option tells uvscan to use heuristic detection to identify potential program viruses. This is a subset of &quot;--analyze, --analyse.&quot;</td>
<td>Off</td>
</tr>
</tbody>
</table>
Table 3-2. Scanning options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-p, --atime-preserve,</td>
<td>This option tells uvscan to reset the time that the file was last accessed to what it was before the scan operation started. This enables you to correctly schedule file backups and their operations keyed to this value. If uvscan finds a virus in, or removes a virus from, a file or, if the person who starts the scan operation does not own the file, the program will not reset the access time.</td>
<td>Off</td>
</tr>
<tr>
<td>--plad</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-r, --recursive, -sub</td>
<td>This option tells uvscan to examine any target directories you specify and all its subdirectories.</td>
<td>Off</td>
</tr>
<tr>
<td>--secure</td>
<td>This option activates the --analyze and --unzip options and deactivates the --selected and --extensions options at the same time. Use this option to tell uvscan to examine all files.</td>
<td>Off</td>
</tr>
</tbody>
</table>
Using VirusScan for UNIX Software

Table 3-2. Scanning options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s, --selected</td>
<td>This option tells uvscan to look for viruses for any file that has execute permissions and all files that have any of these extensions: .EXE, .COM, .BAT, .SMM, .DOT, .BIN, .APP, .CMD, .OVL, .DLL, .DEV, .001, .002, .QLB, .XTP, .XLB, .SCR, .SYS, .MPP, .MPT, .MSG, .MSO, OBD, .OBT, .OLE, .POT, .RTF, .SHS, .SMM, .VXD, .386, .HT?, .INI, .VBS, .MD?, .BO?, .IM?, .MB?, .PP?, .OV?, .XL?, .DO?. VirusScan for UNIX software scans only those files susceptible to virus infection. Because VirusScan for UNIX software scans a smaller set of files, it can scan a target directory faster.</td>
<td>On</td>
</tr>
<tr>
<td>--unzip</td>
<td>This option tells uvscan to examine files saved in .zip, LHA, PKarc, ARJ, TAR and RAR formats.</td>
<td>Off</td>
</tr>
</tbody>
</table>
Response options

These options determine how your scan operation responds to a virus infection. You may use a combination of these options to shape the scan operation to suit your needs. None of the options in this table occur automatically; to activate each option, specify it as part of your command line instruction. You may override some of these default options with other options.

Table 3-3. Response options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c, --clean</td>
<td>This option tells uvscan to 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, run another scan operation afterwards to ensure that the program cannot detect any virus remnants in files it has cleaned.</td>
<td>Off</td>
</tr>
<tr>
<td>--cleandocall, --dam</td>
<td>This option has the scan operation delete all macros from a potentially infected file. Use this option with caution with the &quot;--fam&quot; option.</td>
<td>Off</td>
</tr>
</tbody>
</table>
Using VirusScan for UNIX Software

Table 3-3. Response options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td>--delete</td>
<td>This option tells uvscan to automatically delete any infected files that it finds.</td>
<td>Off</td>
</tr>
<tr>
<td>-m &lt;directory&gt;,</td>
<td>This option tells uvscan to move any infected files it finds to a quarantine location that you specify.</td>
<td>Off</td>
</tr>
<tr>
<td>--move &lt;directory&gt;</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the -m &lt;directory&gt; command is used with -c, the VirusScan 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.</td>
<td></td>
</tr>
</tbody>
</table>
General options

These options give you additional information that you can use as you run your scan operations or get further help. You may use a combination of these options to shape the scan operation to suit your needs. None of the options in this table occur automatically; to activate each option, specify it as part of your command line instruction. You may override some of these default options with other options.

Table 3-4. General options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>UVSCAN default</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>This option lists all of the uvscan options available, together with a short description.</td>
<td>Off</td>
</tr>
<tr>
<td>--summary</td>
<td>This option summarizes the results of your scan operation. The summary includes:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• How many files uvscan examined.</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td>• How many infected files uvscan found.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• How many viruses uvscan removed from infected files.</td>
<td></td>
</tr>
<tr>
<td>-v, --verbose</td>
<td>This option tells uvscan to display a progress summary as it conducts a scan operation.</td>
<td>Off</td>
</tr>
</tbody>
</table>
Preventing Virus Infection

Keys to 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 a comprehensive computing security program that includes a variety of safety measures, such as 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 for UNIX software and other McAfee anti-virus software.
- Include the uvscan command line and all appropriate options in a cron file.
- Make frequent backups of important files. Even if you have VirusScan for UNIX software available to prevent attacks from viruses, damage from fire, theft, or vandalism can render data unrecoverable without a recent backup.

Detecting new and unidentified viruses

The best way for you to deal with new or unidentified viruses that might affect your system is to frequently update your VirusScan for UNIX virus signature (.DAT) files.

To offer the best virus protection possible, McAfee continually updates the .DAT files that VirusScan for UNIX software uses to detect viruses. For maximum protection, you should update these files on a regular basis.

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 their backward compatibility with previous versions’ executable files. 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 would I need a new .DAT file?

More than 200 new viruses appear each month. Often, older .DAT files cannot assist the VirusScan for UNIX software in detecting these new variations. For example, the .DAT files that came with your original copy of VirusScan for UNIX may not detect a virus that was discovered after you bought the product.

If you suspect you may 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:

  
  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 data files.

Next, follow these steps to unpack the update and 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.
VirusScan for UNIX 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) }'`
```
Preventing Virus Infection

# 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, # don't 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
fi

# Delete the directory that you created.

cd /

rm -fr /tmp/dat-updates
Choosing McAfee anti-virus and security software helps to ensure that the critical information technology you rely on functions smoothly and effectively. Taking advantage of a McAfee 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 McAfee 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.

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

PrimeSupport options for corporate customers

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

PrimeSupport KnowledgeCenter

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

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

http://knowledge.nai.com/

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

PrimeSupport KnowledgeCenter features:
• Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user’s guides, FAQs, and release notes

• Unrestricted, 24-hour-per-day access to technical support information via the McAfee website

• Updates to data files and product upgrades via the McAfee website

**PrimeSupport Connect**

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

PrimeSupport Connect features:

• Unlimited toll-free telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central time

• Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user’s guides, FAQs, and release notes

• Unrestricted, 24-hour-per-day access to technical support information via the McAfee website

• Updates to data files and product upgrades via the McAfee website

**PrimeSupport Priority**

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

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

PrimeSupport Enterprise

PrimeSupport Enterprise gives you round-the-clock, personalized, proactive support from an assigned technical support engineer. You’ll enjoy a relationship with a support professional who is familiar with your McAfee 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 McAfee products. By calling in advance, your PrimeSupport Enterprise representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Enterprise gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Enterprise on an annual basis when you purchase a McAfee product either with a subscription license or a one-year license.

PrimeSupport Enterprise features:

- Unlimited, toll-free telephone access to an assigned technical support engineer on a 24-hour-per-day, seven-day-per-week basis, including on weekends and local holidays
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times from your support engineer, who will respond to pages within half an hour, to voice mail within one hour, and to e-mail within four hours
- Ability to designate at least five people in your organization as customer contacts
- The option to be a beta site for new McAfee products
Online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user’s guides, FAQs, and release notes

- Unrestricted, 24-hour-per-day access to technical support information via the McAfee website
- Updates to data files and product upgrades via the McAfee website

**Ordering Corporate PrimeSupport**

To order PrimeSupport KnowledgeCenter, PrimeSupport Connect, PrimeSupport Priority, or PrimeSupport Enterprise for your McAfee products:

- Contact your sales representative; or
- In North America, call Network Associates Support Services at (800) 988-5737 or (650) 473-2000 from 6:00 a.m. to 5:00 p.m. Pacific time, Monday through Friday.

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

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

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

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


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


- Free 24-hour-per-day, seven-days-per-week access to online or electronic support through the McAfee voice and fax system, the McAfee website, and through such other electronic services as America Online and CompuServe.

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

- Automated voice and fax system: (408) 346-3414
- McAfee website: http://support.nai.com
- CompuServe: GO NAI
- America Online: keyword MCAFEE

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

  http://knowledge.nai.com/

- Ninety days of complimentary technical support from a McAfee support technician during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central time.
You can also take advantage of a variety of additional support options geared toward your needs. You can purchase these options either with your McAfee product or after your complimentary 90-day support period expires:

- **Small Office/Home Office Annual Plan.** This plan gives you unlimited toll-free access to technical support during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central time.

- **Pay-Per-Minute Plan.** This plan gives you support only when you need it: 900-number access to technical support features priority call handling to minimize your hold time and the first two minutes of support free.

- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via McAfee online or electronic services.

- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot access product upgrades online. This service is available for VirusScan and NetShield only.

**Ordering Retail PrimeSupport**

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

- In North America, call McAfee Customer Service at (972) 278-6100; or
- Visit the McAfee website at:

  http://www.nai.com/asp_set/services/prime_support/intro.asp
McAfee consulting and training

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

Professional consulting services

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

Jumpstart services

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

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

Network consulting

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

You can order a custom consultation to help with planning, design, implementation, and ongoing management of your network. With it, you can assess the impact of rolling out new applications, network operating systems, or internetworking devices.
Contact Network Associates Consulting Services at 1-800-395-3151 to learn more about the options available, or visit the Network Associates website at:

http://www.nai.com/asp_set/services/professional_services/professional_intro.asp

Total Education Services

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

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

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

http://www.nai.com/asp_set/services/educational_services/education_intro.asp
Symbols
.DAT file updates, 47

A
America Online, technical support via, xv, 58
anti-virus software, reporting new viruses not detected by to McAfee, xvii
automatic scan operations, 33

C
cleaning infected files, 44
command line, typing options, 30
command syntax, variables, 38
compressed files, ignoring during scans, 40
CompuServe, technical support via, xv, 58
configuration file, option for loading saved, 38
consulting services, 60
conventions, typing options, 30
Cron, 33
crontab files, using to scan automatically, 33
Customer Care, contacting, xiv

D
.DAT file updates, reporting new items for, xvii
.DAT files, option for not showing expiration notice, 41
.DAT file updates, 48
distributions, versions of VirusScan for UNIX software, 23
documentation, 22

e
educational services, description of, 61
electronic services, contacting for technical support, 58
e-mail, addresses for reporting new viruses to McAfee, xvii
error messages, 26
exit codes, 36
exit on error, setting for scan operations, 39

H
help, UNIX man page on crontab files, 34
heuristics, options, 38, 40 to 41, 44

I
infected files, cleaning, 44
installation requirements, 23
installing VirusScan for UNIX software, 23

L
last access date of files, preserving, 42
library paths, 25
links, creating to uvscan and shared library, 25

M
macros, 44
McAfee contacting
via America Online, xv
via CompuServe, xv
within the United States, xv
Microsoft Word files, options for not including in scan operations, 41

N
Network Associates
consulting services from, 60
contacting
Customer Service, xiv
outside the United States, xviii
educational services, 61
support services, 53
training, xvi, 60
website address for software updates and upgrades, 58
new viruses, reporting to McAfee, xvii
no decrypt, 41

O
on demand scanning, 30
option for deleting from files, 44

P
performing a scan operation, 30
permissions, 24
preventing virus infection, 47
PrimeSupport
 corporate
 at a glance, 57
 Connect, 54
 Enterprise, 55
 KnowledgeCenter, 53
 ordering, 56
 Priority, 54
Professional Consulting Services, description of, 60

Q
quarantine, option for moving infected files to, 45

R
removing VirusScan for UNIX software
using the uninstallation script, 27
removing VirusScan for UNIX software by hand, 27
reporting viruses not detected to McAfee, xvii
root account, 24

S
scan operation results, displaying, 46
scheduling a scan operation, 33
shared library path
 creating links to, 25
 removing, 27
software updates and upgrades, website address for obtaining, 58
standard input, using to set scan targets, 40
summary of scan operation results, displaying, 46
support
corporate PrimeSupport
 at a glance, 57
 Connect, 54
 Enterprise, 55
 KnowledgeCenter, 53
 ordering, 56
 Priority, 54
hours of availability, 58
retail PrimeSupport, 58 to 59
via electronic services, 58
syntax
  summary of options, 29
  using variables in, 38

T
technical support
  corporate PrimeSupport
    at a glance, 57
    Connect, 54
    Enterprise, 55
    KnowledgeCenter, 53
  ordering, 56
  Priority, 54
  e-mail address for, xv
  hours of availability, 58
  information needed from user, xvi
  online, xv
  phone numbers for, xv
  via electronic services, 58
Total Education Services, description of, 60
Total Service Solutions, contacting, 60
training for anti-virus products, 60
training for Network Associates products, xvi
  scheduling, xvi
troubleshooting installation, 26

U
updates, 29
  updating VirusScan for UNIX software, methods, 48
  using a file to supply scan targets, 40

V
variables, use of in command line, 38
  verbose scan reports, setting, 46
viruses
  cleaning out of infected files, 44
  reporting new strains to McAfee, xvii
VirusScan for UNIX software
  components, 22
  documentation, 22
  installing, 23
  introducing, 21
  options
    --allole, 38
    -analyze, 38
    -c, --clean, 44
    --cleandocall, --dam, 44
    --config, 38
    --data-directory, 39
    --delete, 45
    -e, --exit on error, 39
    --exclude, 39
    --extensions, 39
    -f, --file, 40
    --fam, 39
    -h, --help, 46
    --ignore-compressed, --nocomp, 40
    --ignore-links, 40
    --load, 38
    -m, --move DIR, 45
    --manalyze, 40
    --maxfilesize X, 40
    --nobot, 40
    --nocomp, --ignore-compressed, 40
    --nodecrypt, 41
    --nodoc, 41
    --noexpire, 41
    --one-file-system, 41
-p, --atime-preserve, --plad, 42
--panalyze, 41
--recursive, -sub, 42
--s, --selected, 43
--secure, 42
--summary, 46
--unzip, 43
-v, --verbose, 46
overview of features, 21
system requirements, 23
updating methods, 48

W
website, Network Associates technical support via, 58
why use VirusScan for UNIX software?, 21

Z
zipped files, ignoring during scans, 40