



McAfee VirusScan

Administrator's Guide

Version 4.5

COPYRIGHT

Copyright © 1998-2000 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

* *ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, CNX, Compass 7, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, GroupShield, HelpDesk, Hunter, ISDN Tel/Scope, LM 1, LANGuru, Leading Help Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee, McAfee Associates, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetOctopus, NetRoom, NetScan, Net Shield, NetShield, NetStalker, Net Tools, Network Associates, Network General, Network Uptime!, NetXRay, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, Pop-Up, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey-International, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, Site Meter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, Switch PM, TeleSniffer, TIS, TMach, TMeg, Total Network Security, Total Network Visibility, Total Service Desk, Total Virus Defense, T-POD, Trusted Mach, Trusted Mail, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker WebWall, and ZAC 2000* are registered trademarks of Network Associates and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

LICENSE AGREEMENT

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENTATION DESCRIBES, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Table of Contents

Preface	vii
Anti-virus protection as information security	vii
Information security as a business necessity	x
Active Virus Defense security perimeters	xi
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. About VirusScan Software	 21
Introducing VirusScan anti-virus software	21
How does VirusScan software work?	23
What comes with VirusScan software?	25
What's new in this release?	29
 Chapter 2. Installing VirusScan Software	 33
Before you begin	33
System requirements	33
Installing VirusScan software on a local computer	34
Installation steps	34
Using the Emergency Disk Creation utility	47
Determining when you must restart your computer	53
Testing your installation	54
Modifying or removing your local VirusScan installation	55

Installing VirusScan software on other computers	57
Using Active Directory and Group Policies	57
Installing VirusScan software using command-line options	58
Using Management Edition software	65
Using ePolicy Orchestrator to deploy VirusScan software	66
Installing via System Management Server	67
Installing via Tivoli IT Director	67
Installing via ZENworks	68
Exporting VirusScan custom settings	68
Chapter 3. Removing Infections From Your System	71
If you suspect you have a virus... ..	71
Deciding when to scan for viruses	74
Recognizing when you don't have a virus	75
Understanding false detections	76
Responding to viruses or malicious software	77
Submitting a virus sample	88
Using the SendVirus utility to submit a file sample	88
Capturing boot sector, file-infesting, and macro viruses	91
Chapter 4. Using VirusScan Software	97
Using the VShield scanner	97
Using the VirusScan application	97
Scheduling scan tasks	98
Using specialized scanning tools	98
Chapter 5. Sending Alert Messages	99
Using the Alert Manager Client Configuration utility	99
VirusScan software as an Alert Manager Client	100
Configuring the Alert Manager Client utility	100
Chapter 6. Updating and Upgrading VirusScan Software	105
Developing an updating strategy	105
Update and upgrade methods	106
Understanding the AutoUpdate utility	108
Configuring the AutoUpdate Utility	109

Understanding the AutoUpgrade utility	118
Configuring the AutoUpgrade utility	119
Using the AutoUpgrade and SuperDAT utilities together	128
Deploying an EXTRA.DAT file	130
Appendix A. Using VirusScan Administrative Utilities	133
Understanding the VirusScan control panel	133
Opening the VirusScan control panel	133
Choosing VirusScan control panel options	134
Appendix B. Installed Files	137
What's in this appendix?	137
VShield scanner	137
Dependent and related files for the VirusScan application	143
Alert Manager	146
VirusScan control panel files	147
ScreenScan	148
VirusScan Emergency Disk files	150
Dependent and related files for the E-Mail Scan extension	152
Appendix C. Using VirusScan Command-line Options	155
Adding advanced VirusScan engine options	155
Running the VirusScan Command Line program	155
Running the on-demand scanner with command-line arguments	164
Appendix D. Using the SecureCast Service to Get New Data Files ..	171
Introducing the SecureCast service	171
Why should I update my data files?	172
Which data files does the SecureCast service deliver?	172
Installing the BackWeb client and SecureCast service	173
System requirements	173
Troubleshooting the Enterprise SecureCast service	183
Unsubscribing from the SecureCast service	183
Support resources	183
SecureCast service	183
BackWeb client	184

Appendix E. Network Associates Support Services185

- Adding value to your McAfee product185**
 - PrimeSupport options for corporate customers185**
 - Ordering a corporate PrimeSupport plan188**
- PrimeSupport options for home users190**
 - How to reach international home user support192**
 - Ordering a PrimeSupport plan for home users192**
- Network Associates consulting and training193**
 - Professional Services193**
 - Total Education Services194**

Appendix F. Understanding iDAT Technology195

- Understanding incremental .DAT files195**
- How does iDAT updating work?196**
 - What does McAfee post each week?197**
- Best practices198**
- Frequently asked questions199**

Index201

Preface

Anti-virus protection as information security

“The world changed [on March 26, 1999]—does anyone doubt that? The world is different. Melissa proved that ... and we are very fortunate ... the world could have gone very close to meltdown.”

—Padgett Peterson, *Chief Info Security Architect, Lockheed Martin Corporation, on the 1999 “Melissa” virus epidemic*

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

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

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

Information security as a business necessity

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

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

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

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

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

Active Virus Defense security perimeters

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

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

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

At the desktop: VirusScan software

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

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

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

- System memory, boot sectors, and master boot records. You can configure regularly scheduled scan operations that examine these favorite virus hideouts, or set up periodic operations whenever a threat seems likely.
- Microsoft Exchange mailboxes. VirusScan software includes a specialized E-Mail Scan extension that assumes your network user's Microsoft Exchange or Outlook identity to scan his or her mailbox directly—*before* viruses get downloaded to the local workstation. This can prevent some Melissa-style infections and avoid infections from the next generation of VBS/Bubbleboy descendants.
- Internet mail and file downloads. The VShield scanner includes two modules that specialize in intercepting SMTP and POP-3 e-mail messages, and that can examine files 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 contains infections, 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 get quickly outdated. If you have not updated the files that originally came with your software, you could risk infection from newly emerging viruses. McAfee has, however, assembled the world's largest and most experienced anti-virus research staff 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:

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

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

<http://www.mcafeeb2b.com/>

How to contact McAfee and Network Associates

Customer service

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

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

- **Magic Solutions.** This division supplies the Total Service desk product line and related products
- **McAfee.** This division provides the Active Virus Defense product suite and related anti-virus software solutions to corporate and retail customers.
- **PGP Security.** This division provides award-winning encryption and security solutions, including the PGP data security and encryption product line, the Gauntlet firewall product line, the WebShield E-ppliance hardware line, and the CyberCop Scanner and Monitor product series.
- **Sniffer Technologies.** This division supplies the industry-leading Sniffer network monitoring, reporting, and analysis utility and related software.

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

Network Associates Customer Service
4099 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>

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.

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

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

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

If the automated services do not have the answers you need, contact 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 E, “Network Associates 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

To report items to the McAfee European research office, use these e-mail addresses:

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

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

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

International contact information

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

Network Associates Australia

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

Network Associates Austria

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

Network Associates Belgique

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

Network Associates do Brasil

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

Network Associates Canada

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

Network Associates People's Republic of China

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

Network Associates Denmark

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

NA Network Associates Oy

Mikonkatu 9, 5. krs.
00100 Helsinki
Finland
Phone: 358 9 5270 70
Fax: 358 9 5270 7100

**Network Associates
France S.A.**

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

**Network Associates
Deutschland GmbH**

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

Network Associates Hong Kong

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

Network Associates Srl

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

Network Associates Japan, Inc.

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

Network Associates Latin America

1200 S. Pine Island Road, Suite 375
Plantation, Florida 33324
United States
Phone: (954) 452-1731
Fax: (954) 236-8031

**Network Associates
de Mexico**

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

**Network Associates
International B.V.**

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

**Network Associates
Portugal**

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

**Net Tools Network Associates
South Africa**

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

**Network Associates
South East Asia**

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

**Network Associates
Spain**

Orense 4, 4^a 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

Baeulerwissenstrasse 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 anti-virus software

Eighty percent of the Fortune 100—and more than 50 million users worldwide—choose VirusScan anti-virus software to protect their computers from the staggering range of viruses and other malicious agents that has emerged in the last decade to invade corporate networks and cause havoc for business users. They do so because VirusScan software offers the most comprehensive desktop anti-virus security solution available, with features that spot viruses, block hostile ActiveX and Java objects, identify dangerous websites, stop infectious e-mail messages—and even root out “zombie” agents that assist in large-scale denial-of-service attacks from across the Internet. They do so also because they recognize how much value McAfee anti-virus research and development brings to their fight to maintain network integrity and service levels, ensure data security, and reduce ownership costs.

With more than 50,000 viruses and malicious agents now in circulation, the stakes in this battle have risen considerably. Viruses and worms now have capabilities that can cost an enterprise real money, not just in terms of lost productivity and cleanup costs, but in direct bottom-line reductions in revenue, as more businesses move into e-commerce and online sales, and as virus attacks proliferate.

VirusScan software first honed its technological edge as one of a handful of pioneering utilities developed to combat the earliest virus epidemics of the personal computer age. It has developed considerably in the intervening years to keep pace with each new subterfuge that virus writers have unleashed. As one of the first Internet-aware anti-virus applications, it maintains its value today as an indispensable business utility for the new electronic economy. Now, with this release, VirusScan software adds a whole new level of manageability and integration with other McAfee anti-virus tools.

Architectural improvements mean that each VirusScan component meshes closely with the others, sharing data and resources for better application response and fewer demands on your system. Full support for McAfee ePolicy Orchestrator management software means that network administrators can handle the details of component and task configuration, leaving you free to concentrate on your own work. A new incremental updating technology, meanwhile, means speedier and less bandwidth-intensive virus definition and scan engine downloads—now the protection you need to deal with the blindingly quick distribution rates of new-generation viruses can arrive faster than ever before. To learn more about these features, see [“What’s new in this release?” on page 29](#).

The new release also adds multiplatform support for Windows 95, Windows 98, Windows NT Workstation v4.0, and Windows 2000 Professional, all in a single package with a single installer, but optimized to take advantage of the benefits each platform offers. Windows NT Workstation v4.0 and Windows 2000 Professional users, for example, can run VirusScan software with differing security levels that provide a range of enforcement options for system administrators. That way, corporate anti-virus policy implementation can vary from the relatively casual—where an administrator might lock down a few critical settings, for example—to the very strict, with predefined settings that users cannot change or disable at all.

At the same time, as the cornerstone product in the McAfee Active Virus Defense and Total Virus Defense security suites, VirusScan software retains the same core features that have made it the utility of choice for the corporate desktop. These include a virus detection rate second to none, powerful heuristic capabilities, Trojan horse program detection and removal, rapid-response updating with weekly virus definition (.DAT) file releases, daily beta .DAT releases, and EXTRA.DAT file support in crisis or outbreak situations. Because more than 300 new viruses or malicious software agents appear each month McAfee backs its software with a worldwide reach and 24-hour “follow the sun” coverage from its Anti-Virus Emergency Response Team (AVERT).

Even with the rise of viruses and worms that use e-mail to spread, that flood e-mail servers, or that infect groupware products and file servers directly, the individual desktop remains the single largest source of infections, and is often the most vulnerable point of entry. VirusScan software acts as a tireless desktop sentry, guarding your system against more venerable virus threats and against the latest threats that lurk on websites, often without the site owner’s knowledge, or spread via e-mail, whether solicited or not.

In this environment, taking precautions to protect yourself from malicious software is no longer a luxury, but a necessity. Consider the extent to which you rely on the data on your computer and the time, trouble and money it would take to replace that data if it became corrupted or unusable because of a virus infection. Corporate anti-virus cleanup costs, by some estimates, topped \$16 billion in 1999 alone. Balance the probability of infection—and your company’s share of the resulting costs—against the time and effort it takes to put a few common sense security measures in place, and you can quickly see the utility in protecting yourself.

Even if your own data is relatively unimportant to you, neglecting to guard against viruses might mean that your computer could play unwitting host to a virus that could spread to computers that your co-workers and colleagues use. Checking your hard disk periodically with VirusScan software significantly reduces your system’s vulnerability to infection and keeps you from losing time, money and data unnecessarily.

How does VirusScan software work?

VirusScan software combines the anti-virus industry's most capable scan engine with top-notch interface enhancements that give you complete access to that engine's power. The VirusScan graphical user interface unifies its specialized program components, but without sacrificing the flexibility you need to fit the software into your computing environment. The scan engine, meanwhile, combines the best features of technologies that McAfee and Dr Solomon researchers developed independently for more than a decade.

Fast, accurate virus detection

The foundation for that combination is the unique development environment that McAfee and Dr Solomon researchers constructed for the engine. That environment includes Virtran, a specialized programming language with a structure and "vocabulary" optimized for the particular requirements that virus detection and removal impose. Using specific library functions from this language, for instance, virus researchers can pinpoint those sections within a file, a boot sector, or a master boot record that viruses tend to infect, either because they can hide within them, or because they can hijack their execution routines. This way, the scanner avoids having to examine the entire file for virus code; it can instead sample the file at well defined points to look for virus code signatures that indicate an infection.

The development environment brings as much speed to .DAT file construction as it does to scan engine routines. The environment provides tools researchers can use to write "generic" definitions that identify entire virus families, and that can easily detect the tens or hundreds of variants that make up the bulk of new virus sightings. Continual refinements to this technique have moved most of the hand-tooled virus definitions that used to reside in .DAT file updates directly into the scan engine as bundles of generic routines. Researchers can even employ a Virtran architectural feature to plug in new engine "verbs" that, when combined with existing engine functions, can add functionality needed to deal with new infection techniques, new variants, or other problems that emerging viruses now pose.

This results in blazingly quick enhancements the engine's detection capabilities and removes the need for continuous updates that target virus variants.

Encrypted polymorphic virus detection

Along with generic virus variant detection, the scan engine now incorporates a generic decryption engine, a set of routines that enables VirusScan software to track viruses that try to conceal themselves by encrypting and mutating their code signatures. These "polymorphic" viruses are notoriously difficult to detect, since they change their code signature each time they replicate.

This meant that the simple pattern-matching method that earlier scan engine incarnations used to find many viruses simply no longer worked, since no constant sequence of bytes existed to detect. To respond to this threat, McAfee researchers developed the PolyScan Decryption Engine, which locates and analyzes the algorithm that these types of viruses use to encrypt and decrypt themselves. It then runs this code through its paces in an emulated virtual machine in order to understand how the viruses mutate themselves. Once it does so, the engine can spot the “undisguised” nature of these viruses, and thereby detect them reliably no matter how they try to hide themselves.

“Double heuristics” analysis

As a further engine enhancement, McAfee researchers have honed early heuristic scanning technologies—originally developed to detect the astonishing flood of macro virus variants that erupted after 1995—into a set of precision instruments. Heuristic scanning techniques rely on the engine’s experience with previous viruses to predict the likelihood that a suspicious file is an as-yet unidentified or unclassified new virus.

The scan engine now incorporates ViruLogic, a heuristic technique that can observe a program’s behavior and evaluate how closely it resembles either a macro virus *or* a file-infecting virus. ViruLogic looks for virus-like behaviors in program functions, such as covert file modifications, background calls or invocations of e-mail clients, and other methods that viruses can use to replicate themselves. When the number of these types of behaviors—or their inherent quality—reaches a predetermined threshold of tolerance, the engine fingers the program as a likely virus.

The engine also “triangulates” its evaluation by looking for program behavior that no virus would display—prompting for some types of user input, for example—in order to eliminate false positive detections. This double-heuristic combination of “positive” and “negative” techniques results in an unsurpassed detection rate with few, if any, costly misidentifications.

Wide-spectrum coverage

As malicious agents have evolved to take advantage of the instant communication and pervasive reach of the Internet, so VirusScan software has evolved to counter the threats they present. A computer “virus” once meant a specific type of agent—one designed to replicate on its own and cause a limited type of havoc on the unlucky recipient’s computer. In recent years, however, an astounding range of malicious agents has emerged to assault personal computer users from nearly every conceivable angle. Many of these agents—some of the fastest-spreading worms, for instance—use updated versions of vintage techniques to infect systems, but many others make full use of the new opportunities that web-based scripting and application hosting present.

Still others open “back doors” into desktop systems or create security holes in a way that closely resembles a deliberate attempt at network penetration, rather than the more random mayhem that most viruses tend to leave in their wakes.

The latest VirusScan software releases, as a consequence, do not simply wait for viruses to appear on your system, they scan proactively at the source or work to deflect hostile agents away from your system. The VShield scanner that comes with VirusScan software has three modules that concentrate on agents that arrive from the Internet, that spread via e-mail, or that lurk on Internet sites. It can look for particular Java and ActiveX objects that pose a threat, or block access to dangerous Internet sites. Meanwhile, an E-Mail Scan extension to Microsoft Exchange e-mail clients, such as Microsoft Outlook, can “x-ray” your mailbox on the server, looking for malicious agents before they arrive on your desktop.

VirusScan software even protects itself against attempts to use its own functionality against your computer. Some virus writers embed their viruses inside documents that, in turn, they embed in other files in an attempt to evade detection. Still others take this technique to an absurd extreme, constructing highly recursive—and very large—compressed archive files in an attempt to tie up the scanner as it digs through the file looking for infections. VirusScan software accurately scans the majority of popular compressed file and archive file formats, but it also includes logic that keeps it from getting trapped in an endless hunt for a virus chimera.

What comes with VirusScan software?

VirusScan software consists of several components that combine one or more related programs, each of which play a part in defending your computer against viruses and other malicious software. The components are:

- **The VirusScan application.** This component gives you unmatched control over your scanning operations. You can configure and start a scan operation at any time—a feature known as “on-demand” scanning—specify local and network disks as scan targets, tell the application how to respond to any infections it finds, and see reports on its actions. You can start with the VirusScan Classic window, a basic configuration mode, then move to the VirusScan Advanced mode for maximum flexibility. A related Windows shell extension lets you right-click any object on your system to scan it.
- **The VirusScan Console.** This component allows you to create, configure and run VirusScan tasks at times you specify. A “task” can include anything from running a scan operation on a set of disks at a specific time or interval, to running an update or upgrade operation. You can also enable or disable the VShield scanner from the Console window.

the Console comes with a preset list of tasks that ensures a minimal level of protection for your system—you can, for example, immediately scan and clean your C: drive or all disks on your computer.

- **The VShield scanner.** This component gives you continuous anti-virus protection from viruses that arrive on floppy disks, from your network, or from various sources on the Internet. The VShield scanner starts when you start your computer, and stays in memory until you shut down. A flexible set of property pages lets you tell the scanner which parts of your system to examine, what to look for, which parts to leave alone, and how to respond to any infected files it finds. In addition, the scanner can alert you when it finds a virus, and can generate reports that summarize each of its actions.

The VShield scanner comes with three other specialized modules that guard against hostile Java applets and ActiveX controls, that scan e-mail messages and attachments that you receive from the Internet via Lotus cc:Mail, Microsoft Mail or other mail clients that comply with Microsoft's Messaging Application Programming Interface (MAPI) standard, and that block access to dangerous Internet sites. Secure password protection for your configuration options prevents others from making unauthorized changes. The same convenient dialog box controls configuration options for all VShield modules.

- **The E-Mail Scan extension.** This component allows you to scan your Microsoft Exchange or Outlook mailbox, or public folders to which you have access, directly on the server. This invaluable “x-ray” peek into your mailbox means that VirusScan software can find potential infections before they make their way to your desktop, which can stop a Melissa-like virus in its tracks.
- **A cc:Mail scanner.** This component includes technology optimized for scanning Lotus cc:Mail mailboxes that do not use the MAPI standard. Install and use this component if your workgroup or network uses cc:Mail v7.x or earlier.
- **The Alert Manager Client configuration utility.** This component lets you choose a destination for Alert Manager “events” that VirusScan software generates when it detects a virus or takes other noteworthy actions. You can also specify a destination directory for older-style Centralized Alerting messages, or supplement either method with Desktop Management Interface (DMI) alerts sent via your DMI client software.
- **The ScreenScan utility.** This optional component scans your computer as your screen saver runs during idle periods.

- **The SendVirus utility.** This component gives you an easy and painless way to submit files that you believe are infected directly to McAfee anti-virus researchers. A simple wizard guides you as you choose files to submit, include contact details and, if you prefer, strip out any personal or confidential data from document files.
- **The Emergency Disk creation utility.** This essential utility helps you to create a floppy disk that you can use to boot your computer into a virus-free environment, then scan essential system areas to remove any viruses that could load at startup.
- **Command-line scanners.** This component consists of a set of full-featured scanners you can use to run targeted scan operations from the MS-DOS Prompt or Command Prompt windows, or from protected MS-DOS mode. The set includes:
 - SCAN.EXE, a scanner for 32-bit environments only. This is the primary command-line interface. When you run this file, it first checks its environment to see whether it can run by itself. If your computer is running in 16-bit or protected mode, it will transfer control to one of the other scanners.
 - SCANPM.EXE, a scanner for 16- and 32-bit environments. This scanner provides you with a full set of scanning options for 16- and 32-bit protected-mode DOS environments. It also includes support for extended memory and flexible memory allocations. SCAN.EXE will transfer control to this scanner when its specialized capabilities can enable your scan operation to run more efficiently.
 - SCAN86.EXE, a scanner for 16-bit environments only. This scanner includes a limited set of capabilities geared to 16-bit environments. SCAN.EXE will transfer control to this scanner if your computer is running in 16-bit mode, but without special memory configurations.
 - BOOTSCAN.EXE, a smaller, specialized scanner for use primarily with the Emergency Disk utility. This scanner ordinarily runs from a floppy disk you create to provide you with a virus-free boot environment.

When you run the Emergency Disk creation wizard, VirusScan software copies BOOTSCAN.EXE, and a specialized set of .DAT files to a single floppy disk. BOOTSCAN.EXE will not detect or clean macro viruses, but it will detect or clean other viruses that can jeopardize your VirusScan software installation or infect files at system startup. Once you identify and respond to those viruses, you can safely run VirusScan software to clean the rest of your system.

All of the command-line scanners allow you to initiate targeted scan operations from an MS-DOS Prompt or Command Prompt window, or from protected MS-DOS mode. Ordinarily, you'll use the VirusScan application's graphical user interface (GUI) to perform most scanning operations, but if you have trouble starting Windows or if the VirusScan GUI components will not run in your environment, you can use the command-line scanners as a backup.

- **Documentation.** VirusScan software documentation includes:
 - A printed *Getting Started Guide*, which introduces the product, provides installation instructions, outlines how to respond if you suspect your computer has a virus, and provides a brief product overview. The printed *Getting Started Guide* comes with the VirusScan software copies distributed on CD-ROM discs—you can also download it as VSC45WGS.PDF from Network Associates website or from other electronic services.
 - This user's guide saved on the VirusScan software CD-ROM or installed on your hard disk in Adobe Acrobat .PDF format. You can also download it as VSC45WUG.PDF from Network Associates website or from other electronic services. The *VirusScan User's Guide* describes in detail how to use VirusScan and includes other information useful as background or as advanced configuration options. Acrobat .PDF files are flexible online documents that contain hyperlinks, outlines and other aids for easy navigation and information retrieval.
 - An administrator's guide saved on the VirusScan software CD-ROM or installed on your hard disk in Adobe Acrobat .PDF format. You can also download it as VSC45WAG.PDF from Network Associates website or from other electronic services. The *VirusScan Administrator's Guide* describes in detail how to manage and configure VirusScan software from a local or remote desktop.
 - An online help file. This file gives you quick access to a full range of topics that describe VirusScan software. You can open this file either by choosing **Help Topics** from the **Help** menu in the VirusScan main window, or by clicking any of the **Help** buttons displayed in VirusScan dialog boxes.

The help file also includes extensive context-sensitive—or “What's This”—help. To see these help topics, right-click buttons, lists, icons, some text boxes, and other elements that you see within dialog boxes. You can also click the **?** symbol at the top-right corner in most dialog boxes, then click the element you want to see described to display the relevant topic. The dialog boxes with **Help** buttons open the help file to the specific topic that describes the entire dialog box.

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

What's new in this release?

This VirusScan release introduces a number of innovative new features to the product's core functionality, to its range of coverage, and to the details of its application architecture. A previous section, [“How does VirusScan software work?” on page 23](#), discusses many of these features. The single most significant change between previous VirusScan versions and this release, however, is the integration of two separate VirusScan versions optimized to run on separate Windows platforms into a single product that runs on both. This single product also takes full advantage of each platform's strengths.

The next sections discuss other changes that this VirusScan release introduces.

Installation and distribution features

McAfee anti-virus products, including VirusScan software, now use the Microsoft Windows Installer (MSI), which comes with all Windows 2000 Professional systems. This Setup utility offers a wealth of custom installation and configuration features that make VirusScan software rollout across large organizations much easier and more intuitive. To learn more about how to run custom Setup operations with MSI, see [Chapter 2, “Installing VirusScan Software”](#) in the *VirusScan Administrator's Guide*.





This VirusScan version also comes with complete support for the McAfee ePolicy Orchestrator software distribution tool. A specially packaged VirusScan version ships with the ePolicy Orchestrator software, ready for enterprise-wide distribution. You can distribute VirusScan software, configure it from the ePolicy Orchestrator console, update that configuration and any program or .DAT files at any time, and schedule scan operations, all for your entire network user base. To learn more about using ePolicy Orchestrator software for VirusScan distribution and configuration, consult the ePolicy Orchestrator *Administrator's Guide*.

This VirusScan version also includes package description information for other distribution tools, including Microsoft System Management Server and Tivoli Systems software management products.

Interface enhancements

This release moves the VirusScan interface for all supported platforms solidly into the territory VirusScan for Windows 95 and Windows 98 pioneered with its v4.0.1 release. This adds extensive VShield scanner configuration options for the Windows NT Workstation v4.0 and Windows 2000 Professional platforms, while reducing the complexity of some previous configuration options. Alert Manager server configuration, for example, moves entirely over to the NetShield product line—VirusScan software now acts strictly as a configurable client application.

This release also adds a new VirusScan control panel, which functions as a central point from which you can enable and disable all VirusScan components. This control panel also lets you set a ceiling for the number of items you can scan in or exclude from a single operation, and can set the VShield scanner and VirusScan control panel to run at startup. Other changes include:

- New VShield system tray icon states tell you more about which VShield modules are active. These states are:
 -  All VShield modules are active
 -  The System Scan module is active, but one or more of the other VShield modules is inactive
 -  The System Scan module is inactive, but one or more of the other VShield modules is active
 -  All VShield modules are inactive
- New interface settings for task configuration allow you to tell the VirusScan application how you want it to appear as your scheduled task runs and what you want it to do when it finishes. You can also set a password to protect individual task settings from changes, or to protect an entire task configuration at once.
- An updated randomization feature for scheduled tasks allows you to set a time for the task to run, then set a randomization “window.” The VirusScan Console then picks a random time within the window to actually start the task.
- System Scan module action options now include a new Prompt Type configuration option for Windows 95 and Windows 98 systems. This option lets you determine how the **Prompt for user action** alert appears.

Changes in product functionality

- A new Alert Manager Client configuration utility allows you to choose an Alert Manager server installed on your network as an alert message destination, or to select a network share as a destination for Centralized Alerting messages. You can also supplement either of these alert methods with Desktop Management Interface alert messages.
- The Alert Manager server supports Intel Pentium III processor serial numbers to identify individual machines for virus notification. For more information about Intel processor serial numbers, consult the Intel FAQ at <http://support.intel.com/support/processors/pentiumiii/psqa.htm>.

New update options for your VirusScan software

Even with the majority of the virus definitions it requires now incorporated directly into its engine in generic routines, VirusScan software still requires regular .DAT file updates to keep pace with the 200 to 300 new viruses that appear each month. To meet this need, McAfee has incorporated updating technology in VirusScan software from its earliest incarnations. With this release, that technology takes a quantum leap forward with incremental .DAT file updating.

Incremental .DAT files are small packages of virus definition files that collect data from a certain range of .DAT file releases. The latest versions of the AutoUpdate and AutoUpgrade utilities come with transparent support for the new updates, downloading and installing only those virus definitions you don't already have installed on your system. This means a substantial reduction in download and rollout time, along with similar reductions in network bandwidth demand.

Before you begin

During Setup, you can choose to install VirusScan software either on your local computer, or on other computers elsewhere on the network. The first option copies VirusScan program files to your computer's hard disk. The second option copies selected components to the target workstation.

McAfee distributes VirusScan software in two ways: as an archived file that you can download from the McAfee website or from other electronic services, and on CD-ROM disc. Once you have downloaded a VirusScan archive or placed your VirusScan installation disc in your CD-ROM drive, the installation steps are the same.

To install VirusScan software, you must have Administrator privileges for the workstation on which you plan to install the program. Review the items shown in ["System requirements"](#) to determine whether your target workstations can run VirusScan software.

System requirements


VirusScan software installs and runs on any IBM PC or PC-compatible computer equipped with:

- A processor equivalent to an Intel Pentium-class or compatible processor. McAfee recommends an Intel Pentium processor or Celeron running a minimum of 166MHz.
- A CD-ROM drive. Not required if you download the VirusScan software.
- At least 40MB of free hard disk space for a full installation. McAfee recommends 75MB.
- At least 16MB of free random-access memory (RAM). McAfee recommends 20MB.
- Microsoft Windows 95, Windows 98, Windows NT 4.0 with Service Pack 4 or later, or Windows 2000 Professional. McAfee recommends that you also have Microsoft Internet Explorer v4.0.1 or later installed, particularly if your system runs any Windows 95 version.

Installing VirusScan software on a local computer


Note which type of VirusScan software distribution you have, then follow the corresponding steps to prepare your files for installation.

- **If you downloaded your copy of VirusScan software** from the Network Associates website, from a server on your local network, or from another electronic service, make a new, temporary folder on your hard disk, then use WinZip, PKZIP, or a similar utility to extract the VirusScan installation files to that temporary folder. You can download the necessary utilities from most online services.

 **IMPORTANT:** If you suspect that your computer has a virus, download the VirusScan software installation files onto a computer that is *not* infected. Install the copy onto the uninfected computer, then use the Emergency Disk utility to make a disk that you can use to boot the infected computer and remove the virus. To learn more, see [“If you suspect you have a virus...” on page 63](#).

- **If your copy of VirusScan software came on a CD-ROM**, insert that disc into your computer’s CD-ROM drive.

If you inserted a CD-ROM, you should see a VirusScan welcome image appear automatically. To install VirusScan software immediately, click **Install**, then skip to [Step 5 on page 36](#) to continue with Setup. If the welcome image does not appear, or if you are installing VirusScan software from files you downloaded, start with [Step 2 on page 35](#).

 **IMPORTANT:** Because Setup installs some VirusScan files as services on Windows NT Workstation v4.0 and Windows 2000 Professional systems, you must log in to your system with Administrator rights to install this product. To run Setup on Windows 95 or Windows 98, you do not need to log in with any particular profile or rights.

Installation steps

McAfee recommends that you first quit all other applications you have running on your system before you start Setup. Doing so reduces the possibility that software conflicts will interfere with your installation.

To install VirusScan software, follow these steps:

1. If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, log on to your system as Administrator. You must have administrative rights to install VirusScan software on your system.

2. Choose **Run** from the **Start** menu in the Windows taskbar.

The Run dialog box will appear (Figure 2-1).

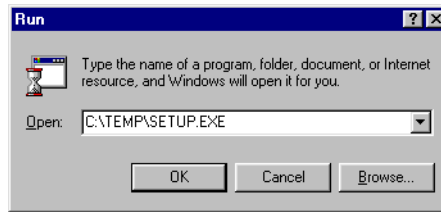


Figure 2-1. Run dialog box

3. Type `<X>:\SETUP.EXE` in the text box provided, then click **OK**.

Here, `<X>` represents the drive letter for your CD-ROM drive or the path to the folder that contains your extracted VirusScan files. To search for the correct files on your hard disk or CD-ROM, click **Browse**.

☐ **NOTE:** If your VirusScan software copy came on an Active Virus Defense or a Total Virus Defense CD-ROM, you must also specify which folder contains the VirusScan software.

Before it continues with the installation, Setup first asks you whether it should check to see whether you have previous VirusScan versions installed on your computer (Figure 2-2).

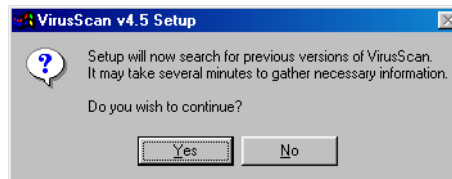


Figure 2-2. Previous versions dialog box

4. Click **Yes** to continue. If you click **No**, Setup quits immediately.

If you have a previous VirusScan version on your system, Setup will find it immediately. It will then remove the previous version, but will temporarily preserve the configuration options you set for that version if your system is running Windows 95 or Windows 98. A later step (see [Step 7 on page 37](#)) will allow you to transfer those options to the current VirusScan installation.

After it removes any previous VirusScan versions you have on your system, Setup checks to see whether your computer already has version 1.1 of the Microsoft Windows Installer (MSI) utility running as part of your system software.

If your computer runs Windows 2000 Professional, the correct MSI version already exists on your system. If your computer runs an earlier Windows release, you might still have this MSI version on your system if you previously installed other software that uses MSI.

If you have the correct MSI version on your computer and do not have any previous VirusScan versions installed on your system, Setup will display its first wizard panel immediately. Skip to [Step 5](#) to continue.

If Setup does not find MSI v1.1 on your computer, it installs files that it needs to continue the installation, then prompts you to restart your computer. Click **Restart System**. If Setup removed a previous VirusScan version from your system, Setup will also ask you to restart your computer.

For a list of circumstances in which Setup or system upgrades require you to reboot your system, see [“Determining when you must restart your computer” on page 53](#).

When your computer restarts, Setup will continue from where it left off. The Setup welcome panel will appear ([Figure 2-3](#)).

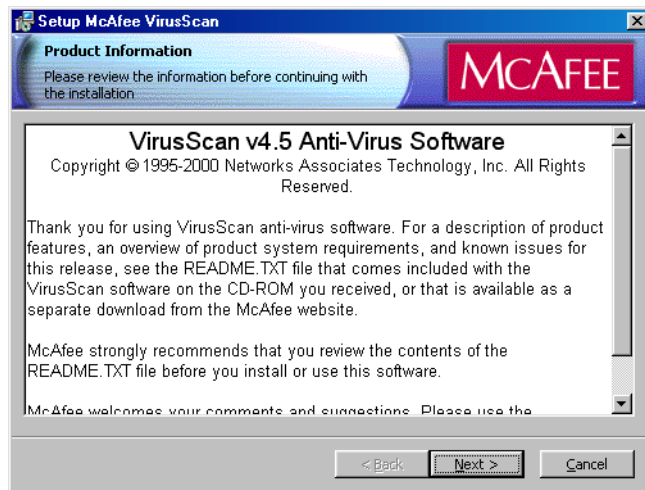


Figure 2-3. Setup welcome panel

5. This first panel tells you where to locate the README.TXT file, which describes product features, lists any known issues, and includes the latest available product information for this VirusScan version. When you have read the text, click **Next>** to continue.
6. The next wizard panel displays the VirusScan software end-user license agreement. Read this agreement carefully—if you install VirusScan software, you agree to abide by the terms of the license.

If you do not agree to the license terms, select **I do not agree to the terms of the License Agreement**, then click **Cancel**. Setup will quit immediately. Otherwise, click **I agree to the terms of the License Agreement**, then click **Next>** to continue.

Setup next checks to see whether incompatible software exists on your computer. If you have no other anti-virus software on your system, Setup then moves to the Security Type panel for Windows NT Workstation or Windows 2000 Professional systems. Otherwise, it will display the Setup Type panel (see [Figure 2-6 on page 39](#) or [Figure 2-7 on page 40](#)). Skip to [Step 9 on page 39](#) to continue.

If your computer runs Windows 95 or Windows 98, Setup also gives you the option to preserve the VShield configuration settings you chose for the earlier version ([Figure 2-4](#)).

-
- ❏ **NOTE:** If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, Setup will remove the previous VirusScan version in [Step 4 on page 35](#), but will *not* preserve any previous VShield scanner settings.
-



Figure 2-4. Previous Version Detected panel

7. Select **Preserve On Access Settings**, if the option is available, then click **Next>** to continue.

If Setup finds incompatible software, it will display a wizard panel that gives you the option to remove the conflicting software (see [Figure 2-5 on page 38](#)).

If you have no incompatible software on your system and your computer runs Windows 95 or Windows 98, skip to [Step 10 on page 40](#) to continue with the installation. If you have no incompatible software and your system runs Windows NT Workstation v4.0 or Windows 2000 Professional, skip to [Step 9 on page 39](#) to continue. Otherwise, continue with [Step 8](#).

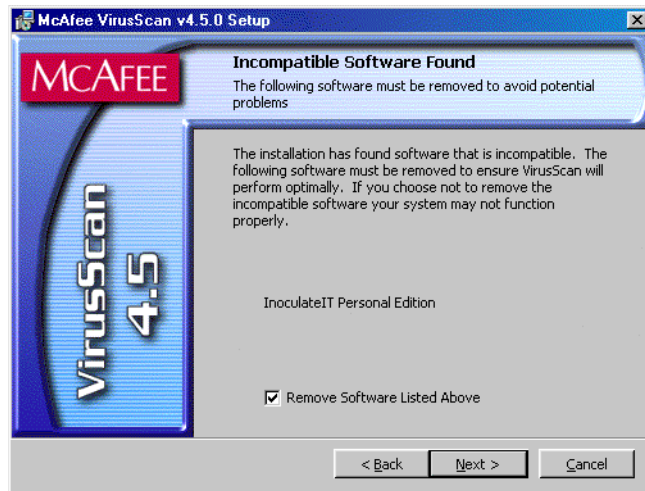



Figure 2-5. Incompatible software panel

8. Select the checkbox shown, then click **Next>**. Setup will start the uninstallation utility that the conflicting software normally uses, and allow it to remove the software. The uninstallation utility might tell you that you need to restart your computer to completely remove the other software. You do *not* need to do so to continue with your VirusScan installation—so long as the other software is not active, Setup can continue without conflicts.

 **NOTE:** McAfee strongly recommends that you remove incompatible software. Because most anti-virus software operates at a very low level within your system, two anti-virus programs that compete for access to the same files or that perform critical operations can make your system very unstable.

If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, Setup next asks you which security mode you want to use to run VirusScan software on your system (see [Figure 2-6 on page 39](#)).

The options in this panel govern whether others who use your computer can make changes to the configuration options you choose, can schedule and run tasks, or can enable and disable VirusScan components. VirusScan software includes extensive security measures to ensure that unauthorized users cannot make any changes to software configurations in Maximum Security mode. The Standard Security mode allows all users to have access to all configuration options.

Either option you choose here will install the same VirusScan version, with the same configuration options, and with the same scheduled tasks for all system users.



Figure 2-6. Security Type panel

9. Select the security mode you prefer. Your choices are:

- **Use Maximum Security.** Select this option to require users to have Administrator rights to your computer in order to change any configuration options, to enable or disable any VirusScan component, or to configure and run scheduled tasks.

Users who do not have administrative rights may still configure and run their own scan operations with the VirusScan application and save settings for those operations in a .VSC file, but they cannot change default VirusScan application settings. To learn more about how to configure and save VirusScan application settings, see [Chapter 5, “Using the VirusScan application,”](#) in the *User’s Guide*.

- **Use Standard Security.** Select this option to give any user who logs into your computer the ability to change any configuration option, enable or disable and VirusScan component, or schedule and run any task.

Setup next asks you to choose a Typical or a Custom setup for this computer (Figure 2-7).

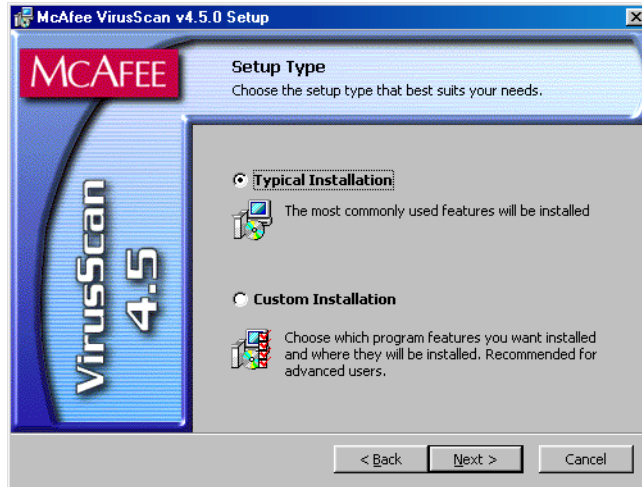


Figure 2-7. Setup Type panel

10. Choose the Setup Type you prefer. Your choices are:

- **Typical Installation.** This option installs a basic component set that includes:
 - the VirusScan application, and application extensions that allow you to right-click any object on your hard disk to start a scan operation
 - the VirusScan Console
 - the VShield System Scan module
 - the Alert Manager Client configuration utility
 - the Send Virus utility
 - the Emergency Disk utility
 - the VirusScan Command Line scanner software
- **Custom Installation.** This option starts with the same components as the Typical setup, but allows you to choose from among these additional items:
 - The VShield E-Mail Scan, Download Scan, and Internet Filter modules
 - The ScreenScan utility

To learn more about what each component does, see [“What comes with VirusScan software?” on page 29](#) of the *VirusScan User’s Guide*.

11. Choose the option you prefer, then click **Next>** to continue.

If you chose **Custom Setup**, you’ll see the panel shown in [Figure 2-8](#). Otherwise, skip to [Step 14 on page 42](#) to continue with your installation.

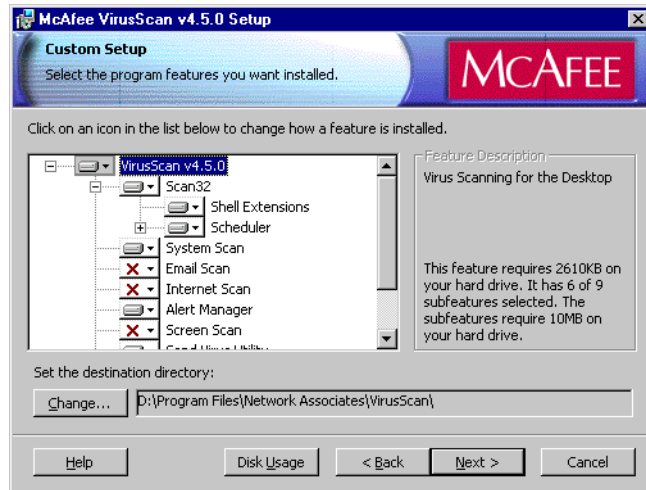








Figure 2-8. Custom Setup panel

12. Choose the VirusScan components you want to install. You can:

- Add a component to the installation. Click  beside a component name, then choose  **This feature will be installed on local hard drive** from the menu that appears. To add a component and any related modules within the component, choose  **This feature, and all subfeatures, will be installed on local hard drive** instead. You can choose this option only if a component has related modules.
- Remove a component from the installation. Click  beside a component name, then choose  **This feature will not be available** from the menu that appears.

 **NOTE:** The VirusScan Setup utility does not support the other options shown in this menu. You may not install VirusScan components to run from a network, and VirusScan software has no components that you can install on an as-needed basis.

You can also specify a different disk and destination directory for the installation. Click **Change**, then locate the drive or directory you want to use in the dialog box that appears. To see a summary of VirusScan disk usage requirements relative to your available hard disk space, click **Disk Usage**. The wizard will highlight disks that have insufficient space.

13. When you have chosen the components you want to install, click **Next>** to continue.

Setup will show you a wizard panel that confirms its readiness to begin installing files ([Figure 2-9](#)).

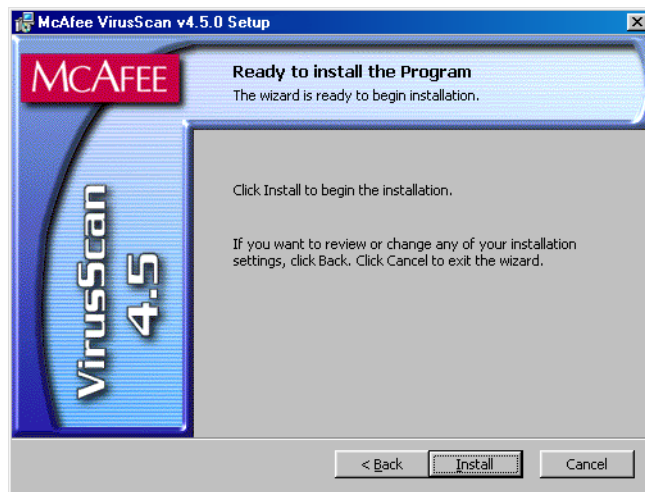


Figure 2-9. Ready to Install panel

14. Click **Install** to begin copying files to your hard drive. Otherwise, click **<Back** to change any of the Setup options you chose.

Setup first removes any incompatible software from your system. It then copies VirusScan program files to your hard disk. When it has finished, it displays a panel that asks if you want to configure the product you installed (see [Figure 2-10 on page 43](#)).

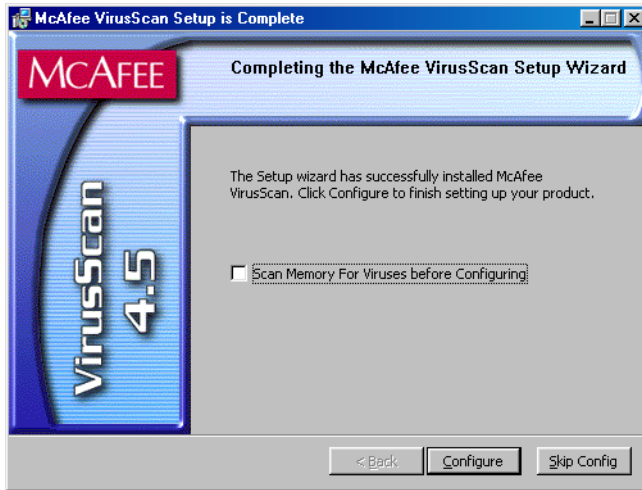



Figure 2-10. Completing Setup panel

15. At this point, you can:

- Finish your installation. Leave the **Scan Memory for Viruses before Configuring** checkbox clear, then click **Skip Config** to finish your installation. Setup will ask if you want to start the VShield scanner and the VirusScan Console immediately. To do so, select the **Start VirusScan** checkbox, then click **Finish**. Your VirusScan software is ready for use.

 **NOTE:** If you had a previous VirusScan version installed on your computer, you must restart your system once again in order to start the VShield scanner. Setup will prompt you to restart your system.

- Choose configuration options for your installation. You can choose to scan your system, create an emergency disk, or update your virus definition files before you start the VShield scanner and the VirusScan Console.

To do so, select the **Scan Memory for Viruses before Configuring** checkbox to have Setup start the VirusScan application briefly to check your system memory. Next, click **Configure**.

Setup will start the VirusScan application to examine your system memory for viruses before it continues. If it finds an infection, it will alert you and give you a chance to respond to the virus. To learn about your options, see [Chapter 3, “Removing Infections From Your System.”](#) If it finds nothing, the application will flash briefly as it scans your system, then Setup will display the first of two configuration panels (see [Figure 2-11 on page 44](#)).

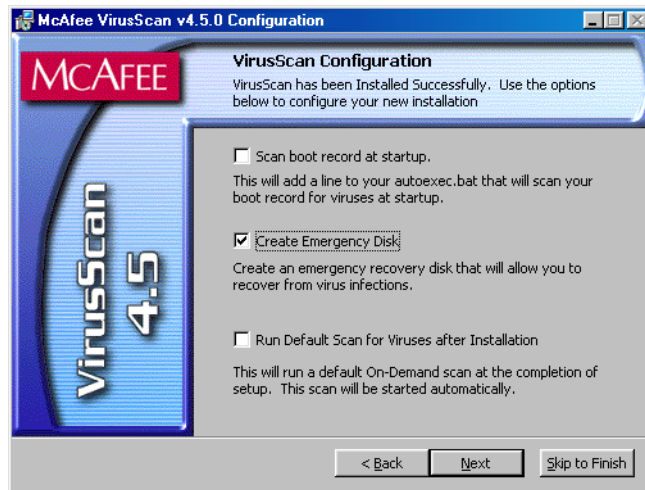


Figure 2-11. Configuration panel

16. If your computer runs Windows 95 or Windows 98, you can choose any of the configuration options shown here. These are:

- **Scan boot record at startup.** Select this checkbox to have Setup write these lines to your Windows AUTOEXEC.BAT file:

```
C : \PROGRA~1\NETWOR~1\MCAFEE~1\SCAN.EXE C : \
@IF ERRORLEVEL 1 PAUSE
```

This tells your system to start the VirusScan Command Line scanner when your system starts. The scanner, in turn, will pause if it detects a virus on your system so that you can shut down and use the VirusScan Emergency Disk to restart.

- **Create Emergency Disk.** This option is active by default. It tells Setup to depart from its normal sequence to start the Emergency Disk creation utility. The creation utility formats and copies a scanner and support files onto a bootable floppy disk you can use to start your system in a virus-free environment. You can use this disk to scan portions of your hard disk for viruses. After the utility creates the disk, it returns to the regular Setup sequence. Clear this checkbox to skip the Emergency Disk creation. You can start the utility at any time after installation.

- **Run Default Scan for Viruses after Installation.** This option is active by default. The option tells Setup to finish the installation, then to run the VirusScan application immediately afterwards to scan your entire startup partition. The application will alert you if it finds any viruses on this partition, but otherwise will quit without any further notice. Clear this checkbox to skip this scan operation.

☐ **NOTE:** If you told Setup to remove any previous VirusScan versions from your system, it will run the scan operation *after* it restarts your computer. The VirusScan application will appear immediately after startup.

If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, you may not choose **Scan boot record at startup**, but you may choose either of the other options. Neither Windows NT Workstation nor Windows 2000 permit software to scan or make changes to hard disk boot sectors or master boot records. Also, these operating systems do not use an AUTOEXEC.BAT file for system startup.

17. When you have chosen the options you want, click **Next>** to continue.

If you selected the Create Emergency Disk option, the Emergency Disk creation wizard starts immediately. To learn how to use this utility, see [“Using the Emergency Disk Creation utility” on page 47](#).

After the utility creates an Emergency Disk, it will return to this point in the Setup sequence. To bypass the Emergency Disk utility once it starts, click **Cancel** when you see its first screen. Setup will display a second configuration panel you can use to update your virus definition files or to configure the AutoUpdate utility ([Figure 2-12](#)).

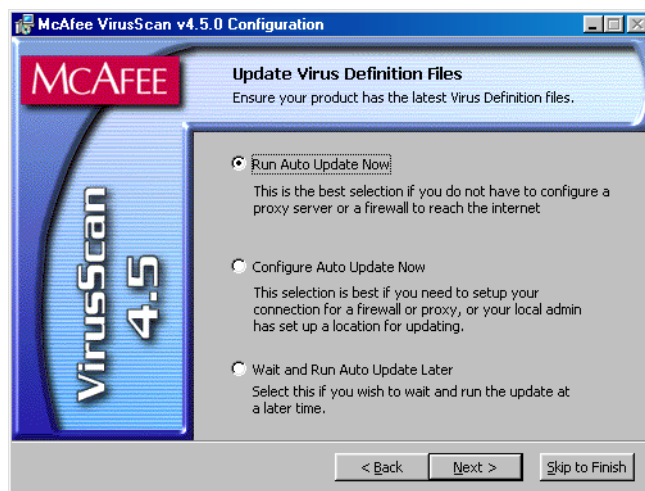


Figure 2-12. Update Virus Definition Files panel

18. Choose the update option you prefer. You can:

- **Run AutoUpdate Now.** This option uses default AutoUpdate configuration options to connect directly to the McAfee website and download the latest incremental .DAT file updates. Select this option if your company has not designated a location on your network as an update site, and if you do not need to configure proxy server or firewall settings. This ensures that any scan operation you run uses current files.
- **Configure AutoUpdate Now.** This option opens the Automatic Update dialog box, where you can add or configure an update site from which to download new files. Select this option if your company has designated a server for .DAT file updates somewhere on your network, or if you want to change some aspect of how your computer connects to the McAfee website—firewall or proxy server settings, for example.

To learn more about how to configure the AutoUpdate utility, see [“Configuring update options” on page 113](#).

- **Wait and Run AutoUpdate Later.** This option skips the update operation altogether. You can configure and schedule an AutoUpdate task to download new .DAT files at any later time. To learn how to schedule a task, see [Chapter 6, “Creating and Configuring Scheduled Tasks,”](#) in the *VirusScan User's Guide*.

19. When you have chosen the option you want, click **Next>**.

If you chose to run an AutoUpdate operation immediately, the utility will connect to the McAfee website to download new incremental .DAT files. After it finishes, the Setup sequence will resume.

If you chose to configure the AutoUpdate utility, the Automatic Update dialog box will appear. Choose your configuration options, then click **Update Now** to start an immediate update operation, or click **OK** to save the options you chose.

Setup next displays its final panel and asks if you want to start the VShield scanner and the VirusScan Console immediately (see [Figure 2-13 on page 47](#)).

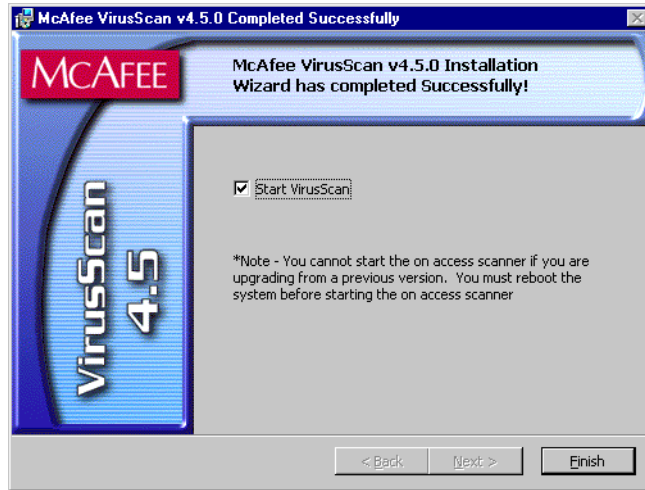


Figure 2-13. Successful Installation panel

20. To do so, select the **Start VirusScan** checkbox, then click **Finish**. The VirusScan software “splash screens” will appear, and the VShield scanner and VirusScan Console icons will appear in the Windows system tray. Your software is ready for use.

☐ **NOTE:** If you had a previous VirusScan version installed on your computer, you must restart your system in order to start the VShield scanner. Setup will prompt you to restart your system.

Using the Emergency Disk Creation utility

If you choose to create an Emergency Disk during installation, Setup will start the Emergency Disk wizard in the middle of the VirusScan software installation, then will return to the Setup sequence when it finishes. To learn how to create an Emergency Disk, begin with [Step 1 on page 49](#). You can also start the Emergency Disk wizard at any point after you install VirusScan software.

☐ **NOTE:** Network Associates strongly recommends that you create an Emergency Disk during installation, but that you do so after VirusScan software has scanned your system memory for viruses. If VirusScan software detects a virus on your system, do *not* create an Emergency Disk on the infected computer.

The Emergency Disk you create includes BOOTSCAN.EXE, a specialized, small-footprint command-line scanner that can scan your hard disk boot sectors and Master Boot Record (MBR). BOOTSCAN.EXE works with a specialized set of .DAT files that focus on ferreting out boot-sector viruses. If you have already installed VirusScan software with default Setup options, you can find these .DAT files in this location on your hard disk:

C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

The special .DAT files have these names:

- EMCLEAN.DAT
- EMNAMES.DAT
- EMSCAN.DAT

McAfee periodically updates these .DAT files to detect new boot-sector viruses. You can download new Emergency .DAT files from this location:

http://www.nai.com/asp_set/anti_virus/avert/tools.asp

☐ **NOTE:** McAfee recommends that you download new Emergency .DAT files directly to a newly formatted floppy disk in order to reduce the risk of infection.

Because the wizard renames the files and prepares them for use when it creates your floppy disk, you may not simply copy them directly to an Emergency Disk that you create yourself. Use the creation wizard to prepare your Emergency Disk.

To start the wizard, click **Start** in the Windows taskbar, point to **Programs**, then to **Network Associates**. Next, choose **Create Emergency Disk**. The Emergency Disk wizard welcome panel will appear (Figure 2-14).



Figure 2-14. Emergency Disk welcome panel

1. Click **Next>** to continue. The next wizard panel appears (Figure 2-15).



Figure 2-15. Second Emergency Disk panel

If your computer runs Windows NT Workstation or Windows 2000 Professional, the wizard tells you that it will format your Emergency Disk with the NAI-OS. You must use these operating system files to create your Emergency Disk, because Windows NT Workstation v4.0 and Windows 2000 Professional system files do not fit on a floppy disk.

If your computer runs Windows 95 or Windows 98, the wizard will offer to format your Emergency Disk either with the NAI-OS or with Windows startup files.

2. If the wizard offers you a choice, choose which operating system files you want to use, then click **Next>** to continue. Depending on which operating system you choose, the wizard displays a different panel next.

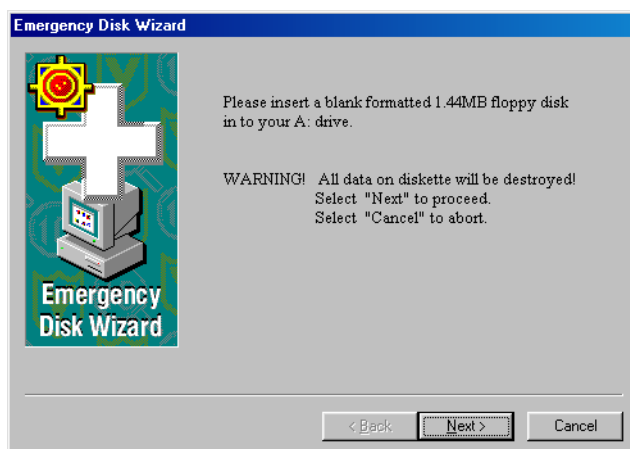


Figure 2-16. Emergency Disk informational panel

- If you chose to format your disk with the NAI-OS, the wizard displays an informational panel (see [Figure 2-16 on page 49](#)).

Follow these substeps to continue:

- a. Insert an unlocked and unformatted 1.44MB floppy disk into your floppy drive, then click **Next>**.

The Emergency Disk wizard will copy its files from a disk image stored in the VirusScan program directory. As it does so, it will display its progress in a wizard panel.

- b. Click **Finish** to quit the wizard when it has created your disk.

Next, remove the disk from your floppy drive, lock it, label it *McAfee Emergency Boot Disk* and store it in a safe place.

- If you chose to format your disk with Windows system files, the wizard displays a panel that lets you choose whether to format your floppy disk ([Figure 2-17](#)).



Figure 2-17. Third Emergency Disk panel

Your choices are:

- If you have a *virus-free*, formatted floppy disk that contains only DOS or Windows system files, insert it into your floppy drive. Next, select the **Don't Format** checkbox, then click **Next>** to continue.

This tells the Emergency Disk wizard to copy only the VirusScan software Command Line component the emergency .DAT files, and support files to the floppy disk. Skip to [Step 3 on page 51](#) to continue.

- If you do *not* have a virus-free floppy disk formatted with DOS or Windows system files, you must create one in order to use the Emergency Disk to start your computer. Follow these substeps:
 - a. Insert an unlocked and unformatted floppy disk into your floppy drive. McAfee recommends that you use a completely new disk that you have never previously formatted to prevent the possibility of virus infections on your Emergency Disk.
 - b. Verify that the **Don't format** checkbox is clear.
 - c. Click **Next>**.

The Windows disk format dialog box appears (Figure 2-18).

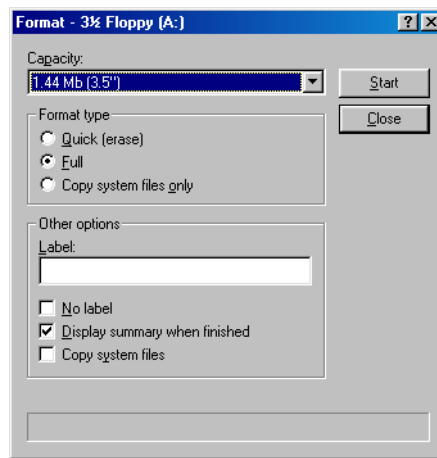


Figure 2-18. Windows Format dialog box

- d. Verify that the **Full** checkbox in the Format Type area and the **Copy system files** checkbox in the Other Options area are both selected. Next, click **Start**.
- Windows will format your floppy disk and copy the system files necessary to start your computer.
- e. Click **Close** when Windows has finished formatting your disk, then click **Close** again to return to the Emergency Disk panel.
3. Click **Next>** to continue. Setup will scan your newly formatted disk for viruses (see Figure 2-19 on page 52).

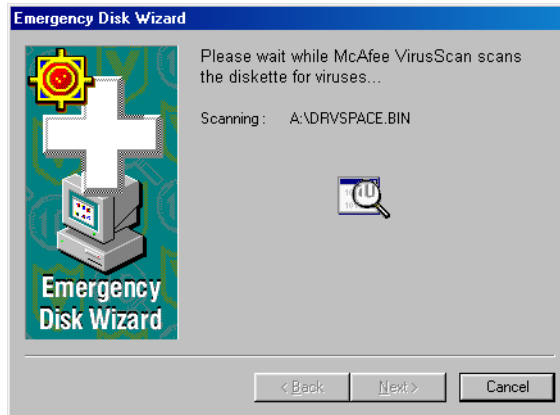


Figure 2-19. Scanning Emergency Disk for viruses

If VirusScan software does not detect any viruses during its scan operation, Setup will immediately copy BOOTSCAN.EXE and its support files to the floppy disk you created. If VirusScan software *does* detect a virus, quit Setup immediately. See [“If you suspect you have a virus...” on page 63](#) to learn what to do next.

4. When the wizard finishes copying the Emergency Disk files, it displays the final wizard panel (Figure 2-20).



Figure 2-20. Final Emergency Disk panel

5. Click **Finish** to quit the wizard. Next, remove the new Emergency Disk from your floppy drive, write-protect it, and store it in a safe place.

☐ **NOTE:** A locked or write-protected floppy disk shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the disk corners, then slide the tab until it locks in an open position.

Determining when you must restart your computer

In many circumstances, you can install and use this VirusScan release immediately, without needing to restart your computer. In some cases, however, the Microsoft Installer (MSI) will need to replace or initialize certain files, or previous McAfee product installations might require you to remove files in order for VirusScan software to run correctly. These requirements can also vary for each supported Windows platform.

In these cases, you will need to restart your system during the installation—usually to install MSI files—or after the installation itself.

To learn when you must restart your computer, see [Table 2-1](#).

Table 2-1. Circumstances that require you to restart your system

Circumstance	Windows 95 and Windows 98	Windows NT and Windows 2000
Installation on computer with no previous VirusScan version and no incompatible software	No restart required, unless you have Novell Client32 for NetWare installed, then restart required	Restart required
Installation on computer with previous VirusScan version	Restart required	Restart required
Installation on computer with incompatible software	No restart required, but Setup will ask if you wish to restart. You can safely click No .	No restart required, but Setup will ask if you wish to restart. You can safely click No .
Installation on a computer with Microsoft Installer (MSI) v1.0 NOTE: Microsoft Office 2000 installs this MSI version	Restart required after MSI files installed and before Setup can continue	Restart required after MSI files installed and before Setup can continue
Installation on a computer with Microsoft Installer v1.1	No restart required, except on Windows 98 Second Edition systems, or if some drivers or .DLL files used	No restart required
.DAT file update	No restart required	No restart required
Scan engine update via McAfee SuperDAT utility	No restart required	No restart required

Testing your installation

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

To test your installation, follow these steps:

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

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

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

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

2. Save the file with the name EICAR.COM. The file size will be 69 or 70 bytes.
3. Start your VirusScan software and allow it to scan the directory that contains EICAR.COM. When VirusScan software examines this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

-
- 🔥 **IMPORTANT:** This file is *not a virus*—it cannot spread or infect other files, or otherwise harm your system. Delete the file when you have finished testing your installation to avoid alarming other users.
-

Modifying or removing your local VirusScan installation

The Microsoft Windows Installer version that VirusScan software uses also includes a standard method to modify or remove a VirusScan installation from the local workstation.

To modify, or remove VirusScan software, follow these steps:

1. Click **Start** in the Windows taskbar, point to **Settings**, then choose **Control Panel**.
2. Locate and double-click the **Add/Remove Programs** control panel.
3. In the Add/Remove Programs Properties dialog box, choose **McAfee VirusScan v4.5.0** in the list, then click **Add/Remove**.

Setup will start and display the first Maintenance wizard panel ([Figure 2-21](#)).

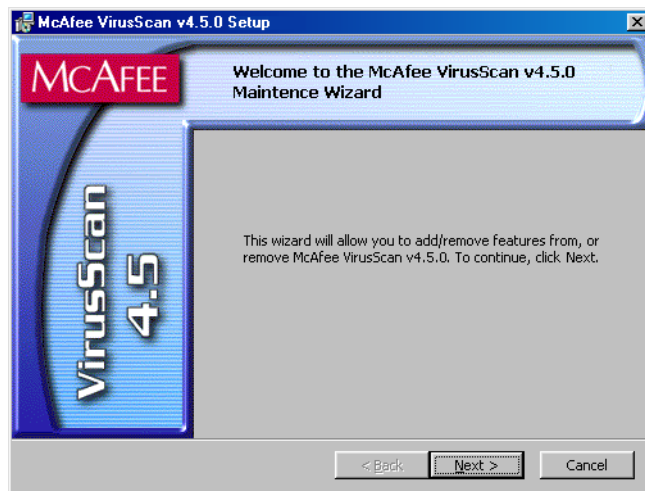


Figure 2-21. First maintenance panel

4. Click **Next>** to continue.

Setup displays the Program Maintenance wizard panel (see [Figure 2-22 on page 56](#)).

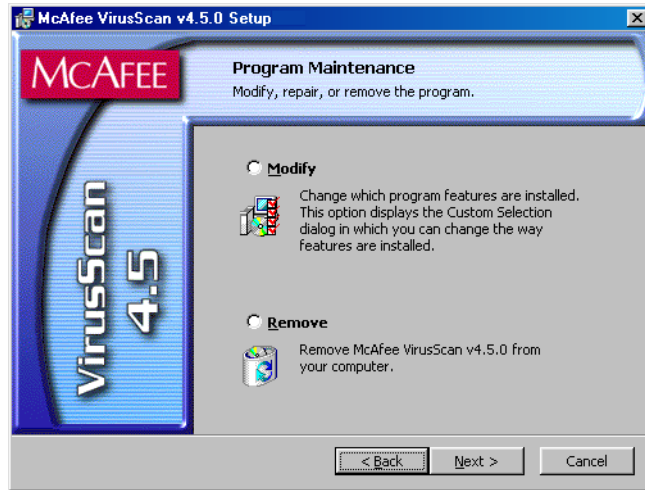



Figure 2-22. Program Maintenance panel

5. Choose whether to modify VirusScan components or to remove VirusScan software from your system completely. Your choices are:
 - **Modify.** Select this option to add or remove individual VirusScan components. Setup will display the Custom wizard panel (see [Figure 2-8 on page 41](#)). Start with [Step 12 on page 41](#) to choose the components you want to add or remove.

 **NOTE:** This panel differs from the one shown on [page 41](#): It will not allow you to change your VirusScan program directory, nor will it display disk usage statistics. To install VirusScan software in a different directory or on a different drive, you must first remove, then reinstall the software.

- **Remove.** Select this option to remove VirusScan software from your computer completely. Setup will ask you to confirm that you want to remove the software from your system (see [Figure 2-23 on page 57](#)).

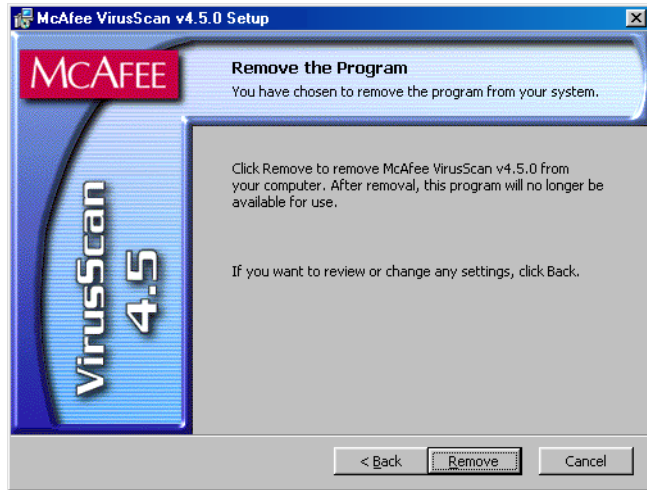


Figure 2-23. Remove the Program panel

6. Click **Remove**. Setup will display progress information as it deletes VirusScan software from your system. When it has finished, click **Finish** to close the wizard panel.

Installing VirusScan software on other computers

The next sections describe how to install VirusScan software over your network, to many workstations at once, and with various custom configurations. You can run Setup from a command prompt to choose many of these configuration options.

Using Active Directory and Group Policies

If you use Active Directory services in Windows 2000, you must distribute the software per machine, not per user. Set up the installation in the Microsoft Management Console; there you can choose the computers on which you want to install the VirusScan package. The installation takes place when you restart these computers.

-
- ❏ **NOTE:** The VirusScan package contains two versions of the Microsoft installer (MSI): one for Windows 95 and Windows 98, and one for Windows NT Workstation v4.0 and Windows 2000 Professional. You can remove these files from the package if your computers already have the installer. This makes the VirusScan file smaller and more manageable when you send it remotely.
-

Installing VirusScan software using command-line options

The VirusScan Setup utility runs as a Microsoft Installer (MSI) application, which allows a wide array of custom installation options. To shape the installation so that it runs the way you want it to, and so that you end up with exactly those product components you want, run Setup from the command line.

-
- ❏ **NOTE:** You can run Setup from the command line only to install VirusScan software to a local computer. To install the software over a network, you must use McAfee Management Edition or ePolicy Orchestrator software.
-

To do so, click **Start** in the Windows taskbar, then choose **Run**. Next, enter the command line you want to use in the Run dialog box, then click **OK**.

The Setup command-line syntax looks like this:

```
setup PROPERTY=VALUE [, VALUE] [/option] /i
```

This syntax does not require any particular order in its elements, except that you may not separate a property and its value, and you must terminate the line with the `/i` option so that Setup knows to look for a particular .MSI file it needs for installation. The syntax consists of:

- the name of the executable file: `setup.exe`.
- any options you choose to add, each preceded by a `/` character. Options are *not* case sensitive. The installation scenarios that appear later in this guide discuss some of the available options.
- any properties you want to use to shape how the installation runs.

Each property consists of a name, which must appear all in capitals, an `=` sign, and one or more values, each separated by commas. Most property values must appear in all capitals, too, but some—such as `True` and `False`, must appear in capitals and lower case. The Microsoft Installer permits a large variety of properties, all of which you can use to determine how your installation runs. To learn about those properties, see the Microsoft Installer documentation. To install VirusScan software, specifically, you can use these additional properties:

- `ADDLOCAL`. This property tells Setup to install particular components to the local computer.
- `INSTALLDIR`. This property specifies which installation directory you want to use. The value consists of the directory path you want to use.

- PRESERVESETTINGS. This property tells Setup whether it should retain the configuration options you used for previous VShield scanner installations. By default, its value is True.
- REBOOT. This property tells Setup whether it should restart your computer. You can either force the computer to restart, or prevent it from restarting.
- REMOVE. This property tells Setup to remove one or more program components. You can specify a particular component, or use the value ALL to remove all components. If you combine this property with the ADDLOCAL property, you can install all but one or two specific components.
- REMOVEINCOMPATIBLESOFTWARE. This property tells Setup to remove previous VirusScan versions or other anti-virus software that could conflict with this VirusScan version. By default, its value is True.
- STARTONACCESSSCANNER. This property tells Setup to start the VShield scanner after it finishes the installation. By default, its value is True.
- USEADMINONLYSECURITY. This property tells Setup which security mode you want this VirusScan copy to use when it runs. Possible values are 0, which runs the software with standard security, and 1, which runs the software with maximum security.

The following sections describe some common scenarios that use command-line options to run custom installations.

Silent installation

Use command-line options to set up VirusScan software on each network node with little or no interaction from end users. During a silent installation, Setup does not display any of its usual wizard panels or windows, or offer the end user any configuration options. Instead, you pre-configure these choices and run Setup in the background on each target workstation. If you want, you can install VirusScan software on any unattended workstation with or without the end user's knowledge, provided you have all the necessary administrative privileges.

`setup/q/i`

Use `/q` to run a silent installation. The `/i` should always appear last on the command line. It tells Setup to locate the .MSI file that controls the installation.

Other semi-silent installation methods are:

/qb	shows a small progress bar during installation, with a cancel button
/q+	shows a success/failure installation complete dialog box
/qb+	shows both the progress and completed dialog boxes
/qf	shows the full progress bar screen from the regular installation

Logging the installation

To record installation progress in a log file, add this option and parameter to the Setup command line:

```
/l*v "c:\temp\log.txt"
```

Here, `c:\temp\log.txt` can be any directory and any file name you want to use to create the log file. This option logs all installer activity, including all files copied, all registry keys added, and all .INI file changes.

Replace the `*` shown in the command-line example with one or more of these parameters to limit the type of data that the log file records:

i	status messages
w	non-fatal warnings
e	all error messages
a	action starts
r	action-specific records
u	user requests
c	initial user interface parameters
m	out-of-memory or fatal exit information
o	out-of-disk space messages
p	terminal properties
+	append to existing file
!	flush each line to the log

Installing to a custom directory

To install VirusScan software to a custom directory, add the `INSTALLDIR` property to the command line, then follow the property with a value for the directory you want to use. To install VirusScan software to `C:\My Anti-Virus Software`, for example, type this line at the command prompt:

```
setup INSTALLDIR= "c:\My Anti-Virus Software" /q/i
```

Use quotes only if the target directory name has spaces. You can add the `/q` switch run the installation silently, if you prefer. The `/i` switch is not optional—Setup needs it to locate the `.MSI` file that has current installation data.

Selecting specific features to install

When you run Setup from the command line to install specific program components, the utility installs those components according to a preexisting hierarchy. This means that if you choose to install only the VirusScan shell extensions, for example, Setup knows that you must have `SCAN32.EXE`, the VirusScan application, installed in order to use the extensions. It therefore will install both this file and any related files.

To specify the components you want to install, Setup requires you to add particular component names as command-line parameters. The component names you can specify from the command line are:

Component Name	Description
AlertManager	The Alert Manager Client configuration utility
CMD	The VirusScan Command Line scanners: <code>SCAN.EXE</code> , <code>SCANPM.EXE</code> , <code>SCAN86.EXE</code>
EdiskUtil	The Emergency Disk wizard and archived files
EmailScan	The VShield E-Mail Scan module and the E-Mail Scan extension
InternetScan	The VShield Download Scan and Internet Filter modules
SystemScan	The VShield System Scan module
Scan32	The VirusScan application, <code>SCAN32.EXE</code>
Scheduler	The VirusScan Console

Component Name	Description
McUpdate	The AutoUpdate and AutoUpgrade utilities
ShellExentions	Extensions that add right-click functionality that enables you to scan individual files
ScreenScan	The ScreenScan utility
SendVirus	An applet that allows you to send virus samples to AVERT Labs for analysis

To use these component names in a command line, specify the destination and the component name, exactly as it appears in the table.

For example, to add the VirusScan application to the local system, type this line at the command prompt:

```
setup.exe ADDLOCAL=Scan32/q/i
```

Use a comma to separate values in order to install more than one component. To add Scan32 and SystemScan together, for example, type this line at the command prompt:

```
setup.exe ADDLOCAL=SystemScan,Scan32/q/i
```

To do a complete installation, type this line at the command prompt:

```
setup.exe ADDLOCAL=ALL/q/i
```

To remove all VirusScan components, type this line at the command prompt:

```
setup.exe REMOVE=ALL/q/i
```

To install all components except for one—the SendVirus component, in this example—type this line at the command prompt:

```
setup.exe ADDLOCAL=ALL REMOVE=SendVirus/q/i
```

You can also choose different components for an installation that you do not run silently. If, for example, you leave off the /q option in any of the command line examples shown above the Custom Setup wizard panel (see [Figure 2-8 on page 41](#)) will show only the components you specify as those available for installation. If you use these same examples to specify a component set for installation, Setup will install only the components you specified during a Typical installation.

Setting reboot options

You can force or prevent the target computer from restarting during the installation. To do this, add the REBOOT property to the command line. REBOOT=F forces the restart, while REBOOT=R prevents the restart. If you must first install the Windows Installer service on a target computer, Setup will require you to restart whether you force or prevent a restart for other reasons. Setup will resume after MSI forces a restart. It will then use the options you set to determine whether to force or prevent a restart after the installation.

```
setup REBOOT=R /q /i
```

This example runs a silent installation and prevents a system restart.

Setting security type for Windows NT

If you install VirusScan software on Windows NT Workstation v4.0 or Windows 2000 Professional systems, you can choose to run the software with regular or maximum security. To set this value from the command line, run Setup with the USEADMINONLYSECURITY property and the value you want to use.

To run the software with standard security, give the property the value 0:

```
USEADMINONLYSECURITY=0
```

To run the software with maximum security, give the property the value 1:

```
USEADMINONLYSECURITY=1
```

To use the property from the command line, type a line similar to this:

```
setup USEADMINONLYSECURITY=1 /q /i
```

This runs a silent installation and sets the security level so that only a user with administrative rights can configure or stop the product.

Removing incompatible software

By default, Setup removes incompatible software during a silent installation. To prevent Setup from removing incompatible software, add the property REMOVEINCOMPATIBLESOFTWARE to the command line with the value False:

```
setup REMOVEINCOMPATIBLESOFTWARE=False
```

Scanning your system at startup

By default, Setup adds a line to the AUTOEXEC.BAT file for Windows 95 and Windows 98 systems that tells the VirusScan application to scan the master boot record (MBR) when your computer starts. To prevent Setup from doing so—during a silent installation, for example—add the property SCANATSTARTUP to the command line with the value False:

```
setup SCANATSTARTUP=False
```

Starting the VShield scanner

By default, Setup starts the VShield System Scan module if the installation does not require you to restart your computer—if you remove earlier VirusScan versions during installation, for example. To keep Setup from starting the VShield scanner, add the STARTONACCESSSCANNER property to the command line with the value False:

```
setup STARTONACCESSSCANNER=False
```

Preserving on access settings

By default, Setup preserves your VShield settings from previous VirusScan installations. To install the new VirusScan version without previous settings, add the PRESERVESETTINGS property to the command line with the value False:

```
setup PRESERVESETTINGS = False
```

Running Setup from a login script

To install VirusScan software at the time each of your target computers starts, you can add a Setup command line to your login script and include any logic you think necessary to ensure that the installation will run once—checking for the VirusScan default program directory, for example. The command line should include all of the options and properties you want to use to govern how Setup runs.


If you run the login script from a Windows 95 or Windows 98 workstation, you *must* add the option /LSCRIPT to the command line if the target computer has any previous VirusScan version installed, or if it might not have Microsoft Installer (MSI) v1.1 installed. Unlike other options, the /LSCRIPT option is case sensitive and must appear in the command line with all capitals.

Without the /LSCRIPT option, Setup will run and, if you do not have MSI v1.1 installed or if you have a previous VirusScan version on the target computer, will require the target computer to restart. Before it does so, however, it places a flag in the Windows RunOnce registry key.

Because Windows 95 and Windows 98 execute the login script at the same time they act on the contents of the RunOnce key, however, they will try to run another instance of Setup while, at the same time, they try to resume the previous Setup you started. MSI does not permit more than one instance of Setup to run at the same time.

Adding the /LSCRIPT option to the command line causes Setup to place a flag in the RunServicesOnce registry key, which Windows executes before it runs the login script. If your login script checks for the presence of the default VirusScan program directory before it runs Setup, therefore, Windows will not try to run Setup a second time.

In order to use a login script for this purpose, you must also copy or “push” the VirusScan installation package to a local directory on the target computer. You may *not* use a login script to install VirusScan software from elsewhere on your network. To install VirusScan software from a remote location on the network, use McAfee Management Edition or McAfee ePolicy Orchestrator management software.

 **NOTE:** If you plan to install VirusScan software to a Windows NT Workstation v4.0 or a Windows 2000 system via login scripts, you do not need to include the /LSCRIPT option in your command line.

Using Management Edition software

Management Edition distribution software allows you to distribute McAfee anti-virus software from a single console on your network. It installs, configures, upgrades, and removes anti-virus software for remote machines on a network. It installs anti-virus software to domains you create, and from repositories that you create. You control activities from the Management Edition Console, a drag-and-drop application that runs on Microsoft Windows NT.

Once the Management Edition components are installed in the master repository, you are ready to install anti-virus software into the Repository.

Follow these steps:

1. In the Management Console main menu, click **Tools**, then choose **Repository**.

The Repository dialog box displays the Products page. It contains the management components that are currently in the Repository.

2. Click **Install**.

3. Click **Product**.
4. Insert the VirusScan CD into your CD-ROM drive.

The Management Edition software copies VirusScan files into the Repository. Once it does so, the components you installed appear in the Repository list.

5. Click **Close** to complete the installation.

You can now use Management Edition software to install and configure VirusScan software, or add components to or remove them from an existing VirusScan installation. To learn how to do so, see the Management Edition *Administrator's Guide*.

To install all VirusScan components via Management Edition software, you must modify the Management Edition scripts that come with the VirusScan product package.

Follow these steps:

1. Use WinZip, PKZip or a similar utility to extract the files VSC_9X.INI and VSC_NT.INI from the VirusScan package.
2. Locate this line in each file:

```
REGSETVAL LOCAL !VS_EXEC_KEY! "ExecCmdLine" SZ  
"!I_CMD_LINE!"
```

Change the macro reference I_CMD_LINE so that it reads I_CMD_LINE_ALL. When you have finished, the entire line in both the VSC_9X.INI and the VSC_NT.INI files should read:

```
REGSETVAL LOCAL !VS_EXEC_KEY! "ExecCmdLine" SZ  
"!I_CMD_LINE_ALL!"
```

3. Save both files, then return them to the VirusScan product package, overwriting the existing files in that package.
4. Deploy your modified VirusScan package via Management Edition software.

Using ePolicy Orchestrator to deploy VirusScan software

ePolicy Orchestrator management software provides a single point of control for all of your McAfee anti-virus products. It is a scalable anti-virus management tool that provides centralized policy management and enforcement, software distribution, and extensive reporting features.

With the ePolicy Orchestrator server, console, and agent you can manage a single database and software repository from any location on your company's network. Once you have installed the ePolicy Orchestrator server and console, and have loaded VirusScan software is loaded into the repository, you can use the console to push the agent onto the client machines. Through the agent, you gather data on the virus protection currently residing on the client machines. The server then responds by sending appropriate installation software. The agent installs the software using the instructions you set up during configuration.

Follow these steps:

1. In the ePolicy Orchestrator Console's main menu, place your cursor on **Software** in the console tree.
2. Click the **Action** menu, and then click **Install**.

The Select a Software Package dialog box displays your network. Locate the VirusScan software package that you want to place in the repository.

3. Click **VirusScan**.
4. Click **Open**.

VirusScan software is loaded in your repository. For more information, see the *ePolicy Orchestrator Administrator's Guide*.

Installing via System Management Server

VirusScan software is Microsoft BackOffice compliant and comes with a prewritten package definition file (.PDF) for use with System Management Server (SMS). You can use SMS to install the software on multiple workstations across your network. To learn how to use SMS to deploy the VirusScan installation package, consult your Microsoft SMS documentation.

Installing via Tivoli IT Director

You can create a distributable custom installation package using the Tivoli IT Director management console's Software Distribution feature.

Follow these steps:

1. Open the **Tivoli IT Director Management Console**.
2. Choose **Open** from the **Software Distribution** option, then choose **Custom Package**. The Create Custom Package configuration pages appear.

3. Click the General tab, then follow these substeps:
 - a. Enter a name for the package that you are about to create.
 - b. Select **Stream package directly to managed system**.
 - c. Enter a value of 32 in the **Required Memory** text box.
 - d. Enter a value of 30 in the **Disk Space** text box.
4. To enable Tivoli to distribute VirusScan software to Windows 95 and Windows 98 systems, select the **Windows 9x** tab. Enter the appropriate information in the panel.
5. To enable Tivoli to distribute VirusScan software to Windows NT systems, select the Windows NT tab. Enter the appropriate information in the panel.

For more information, consult your Tivoli documentation.

Installing via ZENworks

ZENworks allows network administrators to deploy VirusScan software to users' workstations. To learn how to use ZENworks to deploy the VirusScan installation package, consult your Novell ZENworks documentation.

Exporting VirusScan custom settings

McAfee provides a small utility that you can use to put a VirusScan installation package together with all of the configuration settings you want to use for each target computer. McAfee releases this utility, the Custom Installation Creator, apart from the VirusScan product package. In order to use it to create the package, you must import the configuration settings you want from an .INI file. This means that you must first install the VirusScan software on your computer, choose the settings you want to use, then export those settings to an .INI file.

The VirusScan program package contains another utility, MSI_INST.EXE, that allows you to import and export VirusScan configuration settings. You can use this utility to prepare an .INI for use with the Custom Installation Creator, or you can use it to import settings directly from an existing .INI file.

The MSI_INST.EXE utility runs from the command line with this syntax:

```
msi_inst.exe /option [value]
```

[Table 2-1 on page 53](#) lists the options you can use with the utility. To learn how to use the .INI file you create with MSI_INST.EXE to customize your installation, see the documentation for the Custom Installation Creator.

Table 2-1. MSI_INST.EXE command-line switches

Option	Purpose	Usage
IMPORT	Import settings into a VirusScan installation from an .INI file you designate	/IMPORT<path and filename>
EXPORT	Export settings from a VirusScan installation to an .INI file you designate	/EXPORT<path and filename>
EXOPTIONS	Export certain settings from VirusScan. Use this option in conjunction with the /EXPORT option. If you do not specify which components to export, MSI_INST.EXE will export all settings. You can export these VirusScan settings:	/EXOPTIONS <decimal value>

Export nothing [generally unused]	0x00000000h
-----------------------------------	-------------

Export System Scan	0x00000001h
--------------------	-------------

Export E-Mail Scan	0x00000002h
--------------------	-------------

Export Internet Scan	0x00000004h
----------------------	-------------

Export AvConsol.exe settings	0x00000008h
------------------------------	-------------

Export Scheduled Tasks	0x00000010h
------------------------	-------------

Export Default On-Demand Scan	0x00000020h
-------------------------------	-------------

Export All (default)	0x00000800h
----------------------	-------------

The settings specifiers appear here in hexadecimal format. To determine a value to use with the /EXOPTIONS option, combine each of the settings you want to use together with a logical OR operation, then pass the resulting value as a decimal.

Example: Suppose you want to export System Scan, AvConsol, and Scheduled Tasks settings only. Combine the hexadecimal values for these settings together in a logical OR operation:

$0x00000001h \mid 0x00000008h \mid 0x00000010h = 0x00000019h$

Next, take the resulting value and change the hexadecimal number to a decimal number:

$0x00000019h = 25$

Add the decimal value to the command line:

`msi_inst.exe /EXOPTIONS 25`

Table 2-1. MSI_INST.EXE command-line switches

Option	Purpose	Usage
RESTART	Start VirusScan after the MSI_INST.EXE utility finishes importing or exporting settings.	/RESTART
PRESERVE	Preserve existing paths. This tells MSI_INST.EXE to set a switch in the resulting .INI file that will adjust paths when the Custom Installation Creator or another VirusScan installation imports a new .INI file. This will update any paths that point to executables and log files to reflect the current installation. You may use this option only with the /EXPORT option; it will not work with the /IMPORT option.	/PRESERVE
PREVIOUS	Preserves the settings from previous VShield scanner settings. This option tells MSI_INST.EXE to read settings from a previous .INI file and set new installation settings appropriately. NOTE: You may use this option only to preserve VirusScan v4.0.2 and v4.0.3 settings.	/PREVIOUS <path and filename>
PREVIOUS_EXCLUDE	Preserves the exclusion settings from previous VShield scanner installations. This option tells MSI_INST.EXE to read the exclusion settings from a previous .INI file and set new installation appropriately. You must use this option with the /PREVIOUS option. NOTE: You may use this option only to preserve VirusScan v4.0.2 and v4.0.3 settings.	/PREVIOUS_EXCLUDE <path and filename>

Removing Infections From Your System

3

If you suspect you have a virus...

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

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

The safest course of action you can take is to install VirusScan software, then scan your system immediately and thoroughly.

When you install VirusScan software, Setup starts the VirusScan application to examine your computer's memory and your hard disk boot sectors in order to verify that it can safely copy its files to your hard disk without risking their infection. If the application does not detect any infections, continue with the installation, then scan your system thoroughly as soon as you restart your computer. File-infector viruses that don't load into your computer's memory or hide in your hard disk boot blocks might still be lurking somewhere on your system. See [Chapter 2, "Installing VirusScan Software,"](#) to learn about virus scanning during setup. See [Chapter 4, "Using VirusScan Software,"](#) to learn how to scan your system.

If the VirusScan application detects a virus during Setup, you'll need to remove it from your system before you install the program. To learn how to do so, follow the steps that begin on [page 72](#).



IMPORTANT: To ensure maximum security, you should also follow these same steps if a VirusScan component detects a virus in your computer's memory at some point after installation.

If VirusScan software found an infection during installation, follow these steps carefully:

1. Quit Setup immediately, then shut down your computer.

Be sure to turn the power to your system off completely. Do *not* press CTRL+ALT+DEL or reset your computer to restart your system—some viruses can remain intact during this type of “warm” reboot.

2. If you created a VirusScan Emergency Disk during installation, or if your VirusScan copy came with one, lock the disk, then insert it into your floppy drive.

☐ **NOTE:** If your VirusScan software copy did not come with an Emergency Disk, or if you could not create an Emergency Disk during Setup, you must create a disk on an *uninfected* computer. Locate a computer that you know is virus-free, then follow the steps outlined in [“Using the Emergency Disk Creation utility” on page 47](#).

3. Wait at least 15 seconds, then start your computer again.

☐ **NOTE:** If you have your computer's BIOS configured to look for its boot code first on your C: drive, you should change your BIOS settings so that your computer looks first on your A: or B: drive. Consult your hardware documentation to learn how to configure your BIOS settings.

After it starts your computer, the Emergency Disk runs a batch file that leads you through an emergency scan operation. The batch file first asks you whether you cycled the power on your computer.

4. Type y to continue, then skip to [Step 7](#). If you did not, type n, then turn your computer completely off and begin again.

The batch file next tells you that it will start a scan operation.

5. Read the notice shown on your screen, then press any key on your keyboard to continue.

The Emergency Disk will load the files it needs to conduct the scan operation into memory. If you have extended memory on your computer, it will load its database files into that memory for faster execution.

BOOTSCAN.EXE, the command-line scanner that comes with the Emergency Disk, will make four scanning passes to examine your hard disk boot sectors, your Master Boot Record (MBR), your system directories, program files, and other likely points of infection on all of your local computer's hard disks.

-
- ❏ **NOTE:** McAfee strongly recommends that you do not interrupt the BOOTSCAN.EXE scanner as it runs its scan operation. The Emergency Disk will not detect macro viruses, script viruses, or Trojan horse programs, but it will detect common file-infecting and boot-sector viruses.
-

If BOOTSCAN.EXE finds a virus, it will try to clean the infected file. If it fails, it will deny access to the file and continue the scan operation. After it finishes all of its scanning passes, it shows a summary report the actions it took for each hard disk on the screen. The report tells you:

- How many files the scanner examined
- How many files of that number are clean, or uninfected
- How many files contain potential infections
- How many files of that number the scanner cleaned
- How many boot sector and MBR files the scanner examined
- How many boot sector and MBR files contain potential infections

If the scanner detects a virus, it beeps and reports the name and location of the virus on the screen.

6. When the scanner finishes examining your hard disk, remove the Emergency Disk from your floppy drive, then shut your computer off again.
7. When BOOTSCAN.EXE finishes examining your system, you can either:
 - **Return to working with your computer.** If BOOTSCAN.EXE did not find a virus, or if it cleaned any infected files it did find, remove the Emergency Disk from your floppy drive, then restart your computer normally. If you had planned to install VirusScan software on your computer but stopped when Setup found an infection, you can now continue with your installation.
 - **Try to clean or delete infected files yourself.** If BOOTSCAN.EXE found a virus that it could not remove, it will identify the infected files and tell you that it could not clean them, or that it does not have a current remover for the infecting virus.

As your next step, locate and delete the infected file or files. You will need to restore any files that you delete from backup files. Be sure to check your backup files for infections also. Be sure also to use the VirusScan application at your earliest opportunity to scan your system completely in order to ensure that your system is virus-free.

Deciding when to scan for viruses

Maintaining a secure computing environment means scanning for viruses regularly. Depending on the degree to which you swap floppy disks with other users, share files over your local area network, or interact with other computers via the Internet, scanning “regularly” could mean scanning as little as once a month, or as often as several times a day. Other good habits to cultivate include scanning right before you back up your data, scanning before you install new or upgraded software—particularly software you download from other computers—and scanning when you start or shut down your computer each day. Use the VShield scanner to examine your computer’s memory and maintain a constant level of vigilance between scan operations. Under most circumstances this should protect your system’s integrity.

If you connect to the Internet frequently or download files often, you might want to supplement regular scan operations with tasks based on certain events. Use the VirusScan Console to schedule a set of scan tasks to monitor your system at likely points of virus entry, such as

- whenever you insert a floppy disk into your computer’s floppy drive
- whenever you start an application or open a file
- whenever you connect to or map a network drive to your system

Even the most diligent scan operation can miss new viruses, however, if your virus definition (.DAT) files are not up to date. Your VirusScan software purchase entitles you to free virus updates for the life of your product, so you can update frequently to keep current. The VirusScan Console includes AutoUpdate and AutoUpgrade tasks you can use to update your .DAT files and the VirusScan engine. To learn how to update your software, see [Chapter 6, “Updating and Upgrading VirusScan Software.”](#)

Recognizing when you don't have a virus

Personal computers have evolved, in their short life span, into highly complex machines that run ever-more-complicated software. Even the most farsighted of the early PC advocates could never have imagined the tasks for which workers, scientists and others have harnessed the modern PC's speed, flexibility and power. But that power comes with a price: hardware and software conflicts abound, applications and operating systems crash, and hundreds of other problems can crop up in unlikely places. In some cases, these failures can resemble the sorts of effects that you see when you have a virus infection with a destructive payload. Other computer failures seem to defy explanation or diagnosis, so frustrated users blame virus infections, perhaps as a last resort.

Because viruses do leave traces, however, you can usually eliminate a virus infection as a possible cause for computer failure relatively quickly and easily. Running a full VirusScan scan operation will uncover all of the known virus variants that can infect your computer, and quite a few of those that have no known name or defined behavior. Although that doesn't give you much help when your problem really results from an interrupt conflict, it does allow you to eliminate one possible cause. With that knowledge, you can then go on to troubleshoot your system with a full-featured system diagnosis utility.

More serious is the confusion that results from virus-like programs, virus hoaxes, and real security breaches. Anti-virus software simply cannot detect or respond to such destructive agents as Trojan horse programs that have never appeared previously, or the perception that a virus exists where none in fact does.

The best way to determine whether your computer failure resulted from a virus attack is to run a complete scan operation, then pay attention to the results. If the VirusScan application does not report a virus infection, the chances that your problem results from one are slight—look to other causes for the symptoms you see. Furthermore, in the very rare event that the VirusScan application does miss a macro virus or another virus type that has in fact infected your system, the chances are relatively small that serious failures will follow in its wake. You can, however, rely on McAfee researchers to identify and isolate the virus, then to update VirusScan software immediately so that you can detect and, if possible, remove the virus when you next encounter it. To learn how you can help the virus researchers help you, see [“Reporting new items for anti-virus data file updates” on page xvii](#).

Understanding false detections

A false detection occurs when VirusScan software sends a virus alert message or makes a log file entry that identifies a virus where none actually exists. You are more likely to see false detections if you have anti-virus software from more than one vendor installed on your computer, because some anti-virus software stores the code signatures it uses for detection unprotected in memory.

The safest course to take when you see an alert message or log entry is to treat it as a genuine virus threat, and to take the appropriate steps to remove the virus from your system. If, however, you believe that a VirusScan component has generated a false detection—it has, for example, flagged as infected a file that you have used safely for years—verify that you are not seeing one of these situations before you call Network Associates technical support:

- **You have more than one anti-virus program running.** If so, VirusScan components might detect unprotected code signatures that another program uses and report them as viruses. To avoid this problem, configure your computer to run only one anti-virus program, then shut the computer down and turn off the power. Wait a few seconds before you start the computer again so that the system can clear the other program's code signature strings from memory.
- **You have a BIOS chip with anti-virus features.** Some BIOS chips provide anti-virus features that can trigger false detections when VirusScan software runs. Consult the user's guide for your computer to learn about how its anti-virus features work and how to disable them if necessary.
- **You have an older Hewlett-Packard or Zenith PC.** Some older models from these manufacturers modify the boot sectors on their hard disks each time they start up. VirusScan components might detect these modifications as viruses, when they are not. Consult the user's guide for your computer to learn whether it uses self-modifying boot code. To solve the problem, use the VirusScan Command Line scanner to add validation information to the startup files themselves. This method does not save information about the boot sector or the master boot record.
- **You have copy-protected software.** Depending on the type of copy protection used, VirusScan components might detect a virus in the boot sector or the master boot record on some floppy disks or other media.

If none of these situations apply, contact Network Associates technical support or send e-mail to virus_research@nai.com with a detailed explanation of the problem you encountered.

Responding to viruses or malicious software

Because VirusScan software consists of several component programs, any one of which could be active at one time, your possible responses to a virus infection or to other malicious software will depend upon which program detected the harmful object, how you have that program configured to respond, and other circumstances. The following sections give an overview of the default responses available with each program component. To learn about other possible responses, see the chapter that discusses each component in detail.

Responding when the VShield scanner detects malicious software

The VShield scanner consists of four related modules that provide you with continuous background protection against viruses, harmful Java and ActiveX objects, and dangerous websites. A fifth module controls security settings for the other four. You can configure and activate each module separately, or use them together to provide maximum protection. See [Chapter 4, “Using VirusScan Software,”](#) to learn how to configure each module. Because each module detects different objects or scans different virus entry points, each has a different set of default responses.

Responding when the System Scan module detects a virus

How this module reacts when it finds a virus depends on which operating system your computer runs and, on Windows 95 and Windows 98 systems, on which prompt option you chose in the module’s Action page.

By default on Windows 95 and Windows 98 systems, this module looks for viruses each time you run, copy, create, or rename any file on your system, or whenever you read from a floppy disk. On Windows NT Workstation v4.0 and Windows 2000 Professional systems, the System Scan module looks for viruses whenever your system or another computer reads files from or writes files to your hard disk or a floppy disk.

Because it scans files this way, the System Scan module can serve as a backup in case any of the other VShield modules does not detect a virus when it first enters your system. In its initial configuration, the module will deny access to any infected file it finds, whichever Windows version your computer runs. It will also display an alert message that asks you what you want to do about the virus (see [Figure 3-11 on page 87](#)). The response options you see in this dialog box come from default choices or choices you make in the System Scan module’s Action page.

As this dialog box awaits your response, your computer will continue to process any other tasks it is running in the background.

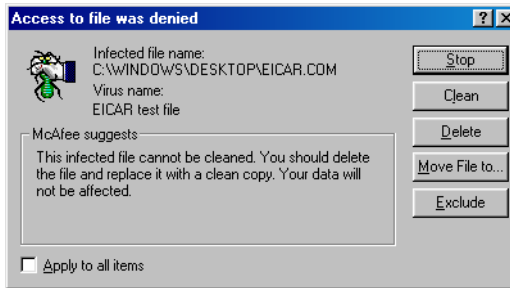


Figure 3-1. Initial System Scan response options

If your computer runs Windows 95 or Windows 98, you can choose to display a different virus alert message. If you select **BIOS** in the Prompt Type area in the System Scan module Action page, you'll see instead a full-screen warning that offers you response options (Figure 3-2).

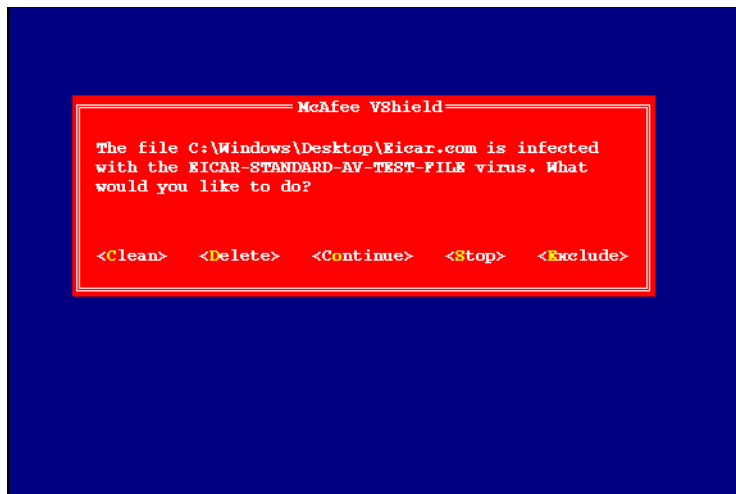



Figure 3-2. Full-screen Warning - System Scan response options

This alert message brings your system to a complete halt as it awaits your response. No other programs or system operations run on your system until you choose one of the response options shown.

The BIOS prompt type also allows you to substitute a **Continue** option for the **Move File** option. To do so, select the **Continue access** checkbox in the module's Action page.

-
-  **NOTE:** The Continue access checkbox is unavailable if your computer runs Windows NT Workstation v4.0 or Windows 2000, or if you choose the **GUI** prompt type on Windows 95 and Windows 98 systems.
-

To take one of the actions shown in an alert message, click a button in the Access to File Was Denied dialog box, or type the letter highlighted in yellow when you see the full-screen warning. If you want the same response to apply to all infected files that the System Scan module finds during this scan operation, select the **Apply to all items** checkbox in the dialog box. This option is not available in the full-screen alert message.

Your response options are:

- **Clean the file.** Click **Clean** in the dialog box, or type C when you see the full-screen warning, to tell the System Scan module to try to remove the virus code from the infected file. If the module succeeds, it will restore the file to its original state and record its success in its log file.

If the module cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will note this result in its log file, but will take no other action. In most cases, you should delete such files and restore them from backups.

- **Delete the file.** Click **Delete** in the dialog box, or type D when you see the full-screen warning, to tell the System Scan module to delete the infected file immediately. By default, the module notes the name of the infected file in its log file so that you have a record of which files it flagged as infected. You can then restore deleted files from backup copies.
- **Move the file to a different location.** Click **Move File to** in the dialog box. This opens a browse window you can use to locate your quarantine folder or another folder you want to use to isolate infected files. Once you select a folder, the System Scan module moves the infected file to it immediately. This option does not appear in the full-screen warning.
- **Continue working.** Type O when you see the full-screen warning to tell the System Scan module to let you continue working with the file and not take any other action. Normally, you would use this option to bypass files that you know do not have viruses. If you have its reporting option enabled, the module will note each incident in its log file. This option is not available in the Access to File Was Denied dialog box.
- **Stop the scan operation.** Click **Stop** in the dialog box, or type S when you see the full-screen warning, to tell the System Scan module to deny any access to the file but not to take any other action. Denying access to the file prevents anyone from opening, saving, copying or renaming it. To continue, you must click **OK**. If you have its reporting option enabled, the module will note each incident in its log file.
- **Exclude the file from scan operations.** Click **Exclude** in the dialog box, or type E when you see the full-screen warning, to tell the System Scan module to exclude this file from future scan operations. Normally, you would use this option to bypass files that you know do not have viruses.

Responding when the E-mail Scan module detects a virus

This module looks for viruses in e-mail messages you receive via corporate e-mail systems such as cc:Mail and Microsoft Exchange. In its initial configuration, the module will prompt you to choose a response from among five options whenever it detects a virus (Figure 3-3).

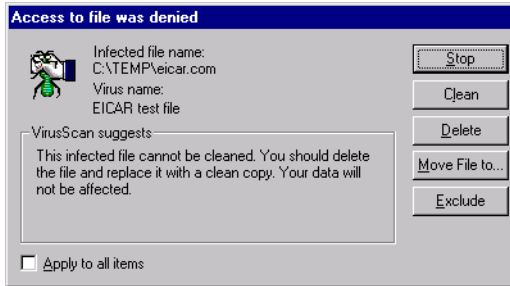


Figure 3-3. E-mail Scan module response options

Click the button that corresponds to the response you want. Your choices are:

- **Stop.** Click this button to stop the scan operation immediately. The E-Mail Scan module will record each detection in its log file, but it will take no other action to respond to the virus.
- **Clean.** Click this button to have the E-Mail Scan module software try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses. In the example shown in Figure 3-3, the module failed to clean the EICAR test file—a mock “virus” written specifically to test whether your anti-virus software installed correctly. Here, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.
- **Delete.** Click this button to delete the file from your system immediately. By default, the E-Mail Scan module will record the name of the infected file in its log so that you can restore the file from a backup copy.
- **Move file to.** Click this button to open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Exclude.** Click this button to prevent the E-Mail Scan module from flagging this file as a virus in future scan operations. If you copy this file to your hard disk, this also prevents the System Scan module from detecting the file as a virus.

When you choose your action, the E-Mail Scan module will implement it immediately and add a notice to the top of the e-mail message that contained the infected attachment. The notice gives the file name of the infected attachment, identifies the name of the infecting virus, and describes the action that the module took in response.

To apply the response you chose to all infected files that the E-Mail Scan module finds during this scan operation, select the **Apply to all items** checkbox in the dialog box.

Responding when the Download Scan module detects a virus

This module looks for viruses in e-mail messages and other files you receive over the Internet via a web browser or such e-mail client programs as Eudora Light, Netscape Mail, Outlook Express, and others. It will *not* detect files you download with FTP client applications, terminal applications, or through similar channels. In its initial configuration, the module will prompt you to choose a response from among three options whenever it detects a virus (Figure 3-4). A fourth option provides you with additional information.

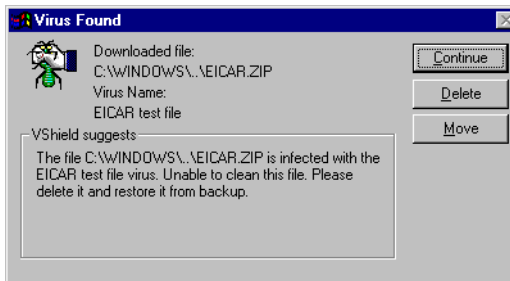


Figure 3-4. Download Scan response options

Click the button that corresponds to the response you want. Your choices are:

- **Continue.** Click this to tell the Download Scan module to take no action and to resume scanning. The module will continue until it finds another virus on your system or until it finishes the scan operation. Normally, you would use this option to bypass files that you know do not have viruses, or if you plan to leave your computer unattended as you download e-mail or other files. The module will note each incident in its log file.
- **Delete.** Click this to tell the Download Scan module to delete the infected file or e-mail attachment you received. By default, the module notes the name of the infected file in its log file.
- **Move.** Click this to tell the Download Scan module to move the infected file to the quarantine directory you chose in the module's Action property page.

When you choose your action, the Download Scan module will implement it immediately and add a notice to the top of the e-mail message that contained the infected attachment. The notice gives the file name of the infected attachment, identifies the name of the infecting virus, and describes the action that the module took in response.

Responding when Internet Filter detects a virus

This module looks for hostile Java classes or ActiveX controls whenever you visit a website or download files from the Internet. You can also use the module to block your browser from connecting to dangerous Internet sites. In its initial configuration, the module will ask you whenever it encounters a potentially harmful object whether you want to **Deny** the object access to your system or you want to **Continue** and allow the object access. It will offer you the same choice when you try to connect to a potentially dangerous website (Figure 3-5).



Figure 3-5. Internet Filter response options

Responding when the VirusScan application detects a virus

When you first run a scan operation with the VirusScan application, it will look at all files on your C: drive that are susceptible to virus infection. This provides you with a basic level of protection that you can extend by configuring VirusScan software to suit your own needs.

With this initial configuration, the program will prompt you for a response when it finds a virus (Figure 3-6).

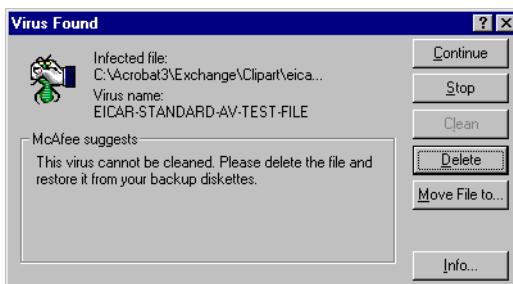


Figure 3-6. VirusScan response options

To respond to the infection, click one of the buttons shown. You can tell the VirusScan application to:

- **Continue.** Click this button to proceed with the scan operation and have the application list each infected file in the lower portion of its main window (Figure 3-7), record each detection in its log file, but take no other action to respond to the virus. Once the application finishes examining your system, you can right-click each file listed in the main window, then choose an individual response from the shortcut menu that appears.

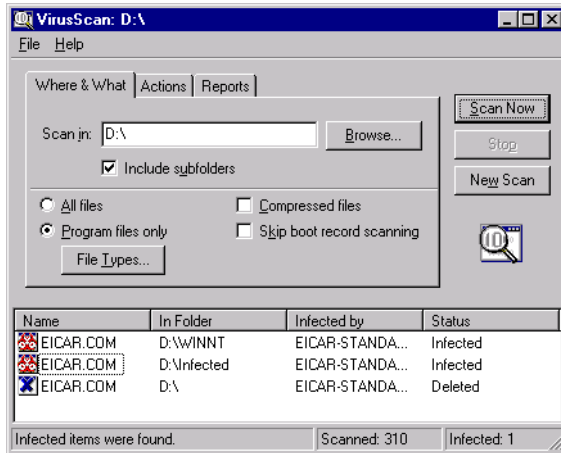


Figure 3-7. VirusScan main window

- **Stop.** Click this button to stop the scan operation immediately. The VirusScan application will list the infected files it has already found in the lower portion of its main window (Figure 3-7) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.
- **Clean.** Click this button to have the VirusScan application try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses.

In the example shown in Figure 3-6 on page 82, the application failed to clean the EICAR Test Virus—a mock “virus” written specifically to test whether your anti-virus software installed correctly. Here, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.

- **Delete.** Click this button to delete the file from your system immediately. By default, the VirusScan application will record the name of the infected file in its log so that you can restore the file from a backup copy.

- **Move file to.** Click this to open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not take any action against the virus that the application detected. See “Viewing virus information” on page 86 for more details.

Responding when the E-Mail Scan extension detects a virus

The E-Mail Scan extension included with VirusScan software lets you scan incoming Microsoft Exchange or Microsoft Outlook e-mail messages for viruses at your initiative. You can start it from within either e-mail client and use it to supplement the continuous e-mail background scanning you get with the VShield E-Mail Scan module. The E-Mail Scan module also offers the ability to clean infected file attachments or stop the scan operation, a capability that complements the continuous monitoring that the E-Mail Scan module provides. In its initial configuration, E-Mail Scan extension will prompt you for a response when it finds a virus (Figure 3-8).

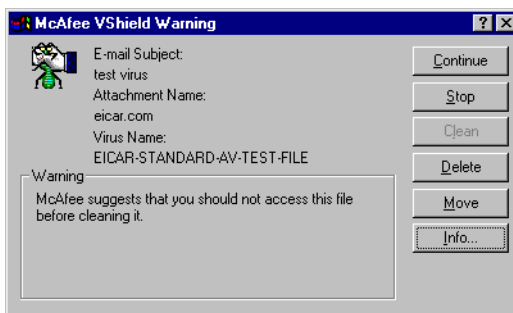


Figure 3-8. E-Mail Scan response options

To respond to the infection, click one of the buttons shown. You can tell the E-Mail Scan extension to:

- **Continue.** Click this button to have the E-Mail Scan extension proceed with its scan operation, list each infected file it finds in the lower portion of its main window (Figure 3-9), and record each detection in its log file, but it will take no other action to respond to the virus. The extension will continue until it finds another virus on your system or until it finishes the scan operation. Once it has finished examining your system, you can right-click each file listed in the main window, then choose an individual response from the shortcut menu that appears.

- **Stop.** Click this button to stop the scan operation immediately. The E-Mail Scan extension will list the infected files it has already found in the lower portion of its main window (Figure 3-9) and record each detection in its log file, but it will take no other action to respond to the virus. Right-click each infected file listed in the main window, then choose an individual response from the shortcut menu that appears.

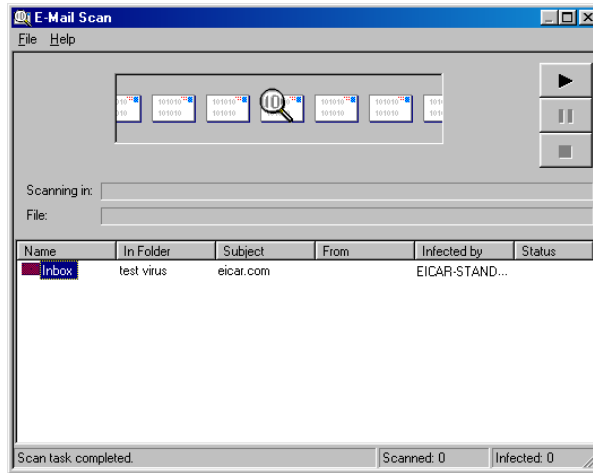


Figure 3-9. E-Mail Scan extension window

- **Clean.** Click this button to remove the virus code from the infected file. If the E-Mail Scan extension cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses. In the example shown in Figure 3-8, **Clean** is not an available response option. In most cases, you should delete such files and restore them from backups.
- **Delete.** Click this button to delete the file from your system. By default, the E-Mail Scan extension will record the name of the infected file in its log so that you can restore the file from a backup copy.
- **Move.** Click this button to open a dialog box that you can use to locate your quarantine folder, or another suitable folder. Once you have located the correct folder, click **OK** to transfer the file to that location.
- **Info.** Click this to connect to the Network Associates Virus Information Library. This choice does not cause the E-Mail Scan extension to take any action against the virus it detected. See “Viewing virus information” for more details.

Viewing virus information

Clicking **Info** in any of the virus response dialog boxes will connect you to the Network Associates online Virus Information Library, provided you have an Internet connection and web browsing software available on your computer (Figure 3-10).

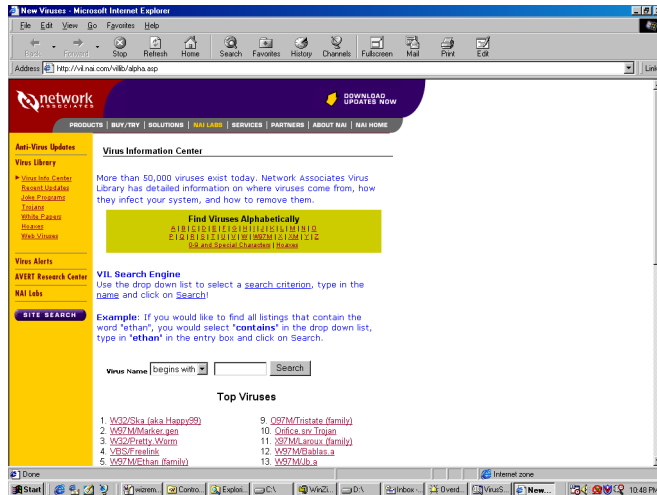


Figure 3-10. Network Associates Virus Information Library page

The Virus Information Library has a collection of documents that give you a detailed overview of each virus that VirusScan software can detect or clean, along with information about how the virus infects and alters files, and the sorts of payloads it deploys. The site lists the most prevalent or riskiest viruses, provides a search engine you can use to search for particular virus descriptions alphabetically or by virus name, displays prevalence tables, technical documents, and white papers, and gives you access to technical data you can use to remove viruses from your system.

To connect directly to the library, visit the site at:

<http://vil.nai.com/villib/alpha.asp>

You can also connect directly to the Library from the VirusScan Console—choose **Virus List** from the **View** menu in the Console window. To learn more about the Console, see [Chapter 6, “Creating and Configuring Scheduled Tasks”](#) in the *VirusScan User’s Guide*.

The Library is part of the McAfee AVERT website, which you can visit at:

http://www.nai.com/asp_set/anti_virus/avert/intro.asp

The AVERT website has a wealth of virus-related data and software.

Examples include:

- Current information and risk assessments on emerging and active virus threats
- Software tools you can use to extend or supplement your McAfee anti-virus software
- Contact addresses and other information for submitting questions, virus samples, and other data
- Virus definition updates-this includes daily beta .DAT file updates, EXTRA.DAT files, updated Emergency .DAT files, current scan engine versions, regular weekly .DAT and SuperDAT updates, and new incremental virus definition files (.UPD)
- Beta and “first look” software

Viewing file information

If you right-click a file listed either in the VirusScan main window or the E-Mail Scan window (see [Figure 3-9 on page 85](#)), then choose **File Info** from the shortcut menu that appears, VirusScan software will open an Infected Item Information dialog box that names the file, lists its type and size in bytes, gives its creation and modification dates, and describes its attributes ([Figure 3-11](#)).

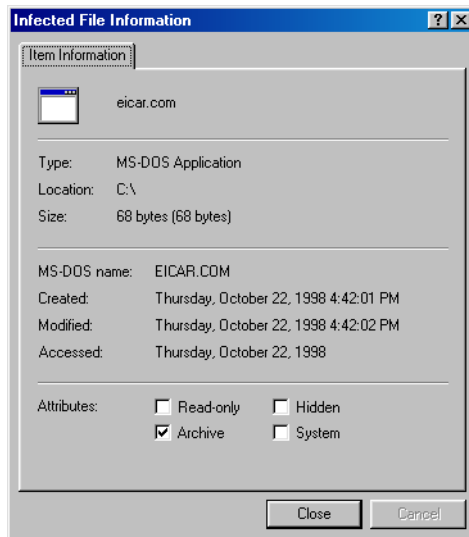


Figure 3-11. Infected File Information property page

Submitting a virus sample

If you have a suspicious file that you believe contains a virus, or experience a system condition that might result from an infection—but VirusScan software has not detected a virus—McAfee recommends that you send a sample to its anti-virus research team for analysis. When you do so, be sure to start your system in the apparently infected state—don't start your system from a clean floppy disk.

Several methods exist for capturing virus samples and submitting them. The next sections discuss methods suited to particular conditions.

Using the SendVirus utility to submit a file sample

Because the majority of later-generation viruses tend to infect document and executable files, VirusScan software comes with SENDVIR.EXE, a utility that makes it easy to submit an infected file sample to McAfee researchers for analysis.

To submit a sample file, follow these steps:

1. If you must connect to your network or Internet Service Provider (ISP) to send e-mail, do so first. If you are continuously connected to your network or ISP, skip this step and go to [Step 2](#).
2. Locate the file SENDVIR.EXE in your VirusScan program directory. If you installed your VirusScan software with default Setup options, you'll find the file here:

C:\Program Files\Network Associates\VirusScan

3. Double-click the file to display the first AVERT Labs Response Center wizard panel ([Figure 3-12](#)).



Figure 3-12. First SENDVIR.EXE panel

4. Read the welcome message, then click **Next>** to continue.

The Contact Information wizard panel appears.

Figure 3-13. Your Contact Information panel

5. If you want AVERT researchers to contact you about your submission, enter your name, e-mail address, and any message you would like to send along with your submission in the text boxes provided, then click **Next>** to continue.

☐ **NOTE:** You may submit samples anonymously, if you prefer—simply leave the text boxes in this panel blank. You are under no obligation to supply any information at all here.

The Choose Files to Submit panel appears (Figure 3-14).

Figure 3-14. Choose Files to Submit panel

6. Click **Add** to open a dialog box you can use to locate the files you believe are infected.

Choose as many files as you want to submit for analysis. To remove any of the files shown in the submission list, select it, then click **Remove**. When you have chosen all of the files you want to submit, click **Next>** to continue.

The Choose Upload Options panel appears (Figure 3-15).

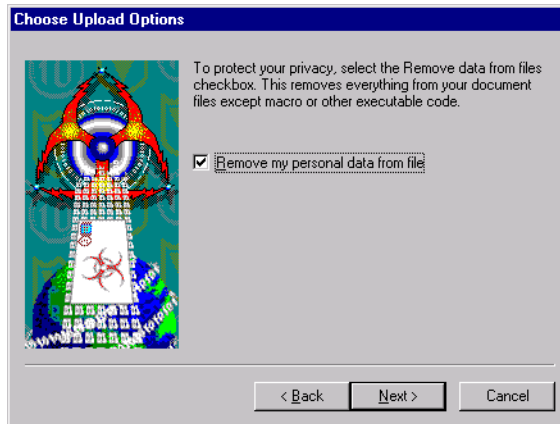


Figure 3-15. Choose Upload options panel

If the file you want to submit is a Microsoft Office document or another file that contains information you want to keep confidential, select the **Remove my personal data from file** checkbox, then click **Next>** to continue. This tells the SENDVIR.EXE utility to strip everything out of the file except macros or executable code.

The Choose E-Mail Service panel appears (Figure 3-16).

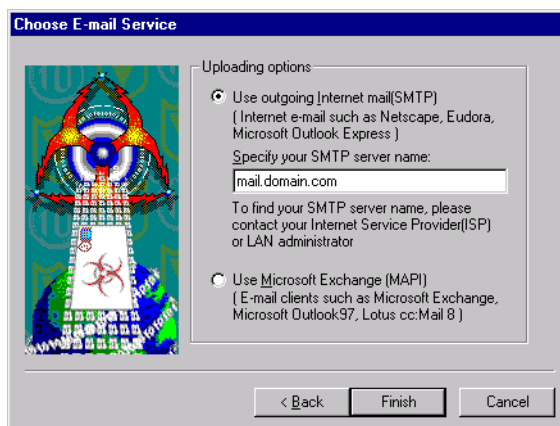


Figure 3-16. Choose E-mail Service panel

7. Select the type of e-mail client application you have installed on your computer. Your choices are:
 - **Use outgoing Internet mail.** Click this button to send your sample via a Simple Mail Transfer Protocol e-mail client, such as Eudora, NetScape Mail, or Microsoft Outlook Express. Next, enter the name of your outgoing mail server in the text box provided-mail.domain.com, for example.
 - **Use Microsoft Exchange.** Click this button to send your sample via your corporate e-mail system. To use this option, your e-mail system must support the Messaging Application Programming Interface (MAPI) standard. Examples of such systems include Microsoft Exchange, Microsoft Outlook, and Lotus cc:Mail v8.0 and later.
8. Click **Finish** to send your sample.

☐ **NOTE:** Although McAfee researchers appreciate your submission, their receipt of your message does not obligate them to take any action, provide any remedy, or respond in any way to you.

SENDVIR.EXE will use the e-mail client you specified to send your sample. You must have connected to your network or ISP in order for this process to succeed.

Capturing boot sector, file-infesting, and macro viruses

If you suspect you have a virus infection, you can collect a sample of the virus, then either create a floppy disk image to send via e-mail, or mail the floppy disk itself to McAfee anti-virus researchers. The researchers would also benefit from having samples of your current system files on a separate floppy disk.

Capturing boot-sector infections

Boot-sector viruses frequently hide in areas of your hard disk or floppy disks that you ordinarily cannot see or read. You can, however, capture a sample of a boot-sector virus by deliberately infecting a floppy disk with it.

To do so, follow these steps:

1. Insert a new, unformatted floppy disk into your floppy drive.
2. Click **Start** in the Windows taskbar, point to **Programs**, then choose **MS-DOS Prompt** if your computer runs Windows 95 or Windows 98, or **Command Prompt** if your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional.

3. Type this line at the command prompt:

```
format a: /s
```

If your system hangs as it tries to format the disk, remove the disk from your floppy drive. Next, label the disk “Damaged during infected format as boot disk,” then set it aside.

4. Insert a new, formatted floppy disk into your floppy drive.
5. Copy your current system files to that disk. For most DOS versions, those files will include:
 - IO.SYS
 - MSDOS.SYS
 - COMMAND.COM

For Windows systems, copy these files to the same preformatted disk:

- GDI.EXE
- KRNL286.EXE or KRNL386.EXE
- PROGMAN.EXE

6. Label the diskette “Contains infected files,” then set it aside.

Capturing file-infesting or macro viruses

If you suspect you have a file-infesting virus or a macro virus that has infected any of your Microsoft Word, Excel, or PowerPoint files, send these files to McAfee anti-virus researchers, either with the SENDVIR.EXE utility, via e-mail as floppy disk images, or through the mail on floppy disk:

- If you suspect that a virus has infected executable files on your system, copy COMMAND.COM to a formatted floppy disk, then change its file extension to a non-executable extension.
- If you suspected that a macro virus has infected your Microsoft Word files, copy NORMAL.DOT and all files from the Microsoft Office **Startup** folder to the floppy disk. You’ll find the Microsoft Office startup files here, if you installed Office to its default location:

C:\Program Files\Microsoft Office\Office\Startup

- If you suspect that a macro virus has infected your Microsoft Excel files, copy all files from C:\Program Files\Microsoft Office\Office\XLSTART to the disk. Include all files you have installed in alternative startup file locations.

- If you suspect that a macro virus has infected your PowerPoint files, copy the file BLANKPRESENTATION.POT from C:\Program Files\Microsoft Office\Templates to the disk.

Making disk images

To send the files now stored on any floppy disks you created, you can use a McAfee AVERT Labs tool called RWFLOPPY.EXE to make a floppy disk image that encapsulates the infection. The RWFLOPPY.EXE tool does not come with your VirusScan software, but you can download it from this location:

http://www.nai.com/asp_set/anti_virus/avert/tools.asp

The AVERT site stores the tool as a compressed .ZIP file. Download the file to your computer, then extract it to a temporary folder on your hard disk. The .ZIP package contains a brief text file that explains the syntax for using the RWFLOPPY.EXE utility.

NOTE: If you suspect you have a boot virus, you must use RWFLOPPY to send your samples electronically; otherwise, you must send your samples physically on a diskette. If you send them electronically without using RWFLOPPY, the samples will be incomplete or unusable, as boot viruses often hide beyond the last sectors of a diskette, and other diskette image creation programs cannot obtain this data.

Once you create images of the disks you want to send, you can send them as file attachments in an e-mail message to McAfee anti-virus researchers.

Preparing file archives to send

Try to fit as many of file samples as you can on a single floppy disk. To do so, compress the samples that you captured on disk to a single .ZIP file with password protection. Here's a suggested procedure that uses the WinZip utility:

1. Start WinZip.
2. Press **CTRL+N** to create a new archive.
The New Archive dialog box appears.
3. Enter a name for the new archive, then click **OK**.
4. Press **CTRL+A** to add files to the new archive.
The Add dialog box appears.
5. Click **Password** to display the Password dialog box.

6. Type **INFECTED** in the Password text box, then click **OK**.
7. When prompted, retype your password to verify its accuracy, then click **OK**.

The Add With Password dialog box appears.

8. Select your sample files, then click **OK**.

WinZip applies the password you entered to all files that you add to or extract from your archive. Password-protected files appear in the archive list with a plus sign (+) after their names.

☐ **NOTE:** If you do not protect your samples with the password **INFECTED**, McAfee anti-virus scanners may detect and clean samples before they reach our researchers.

9. Attach the .ZIP file that you created to an e-mail message.

Sending samples via e-mail

Once you've made disk images or created a file archive for your samples, send them to McAfee researchers at one of these e-mail addresses:

In the United States	virus_research@nai.com
In the United Kingdom	vsample@nai.com
In Germany	virus_research_de@nai.com
In Japan	virus_research_japan@nai.com
In Australia	virus_research_apac@nai.com
In the Netherlands	virus_research_europe@nai.com

In your message, include this information:

- Which symptoms cause you to suspect that your machine is infected
- Which product and version number detected the virus, if any did, and what the results were
- Your VirusScan and .DAT file version numbers
- Details about your system that might help to reproduce the environment in which you detected the virus
- Your name, company name, phone number, and e-mail address, if possible
- A list of all items contained in the package you are sending

Mailing infected floppy disks

You can also mail the actual disks you created directly to McAfee anti-virus researchers. McAfee recommends that you create a text file or write a message to accompany the disks that includes the same information you would submit with an electronic disk image. Send your sample to only one research lab address so that you can receive the fastest possible response to your issue. Use these mailing addresses:

In the United States:

Network Associates, Inc.
Virus Research
20460 NW Von Neumann Drive
Beaverton, OR 97006

In the United Kingdom:

Network Associates, Inc.
Virus Research
Gatehouse Way
Aylesbury, Bucks HP19 3XU
UK

In Germany:

Network Associates, Inc.
Virus Research
Luisenweg 40
20537 Hamburg
Germany

In Japan:

Network Associates, Inc.
Virus Research
9F Toranomori Mori-bldg. 33
3-8-21 Toranomori, Minato-Ku
Tokyo
Japan 105-0001

In Australia:

Network Associates, Inc.
Virus Research
500 Pacific Highway, Level 1
St. Leonards, NSW
Sydney
Australia 2065

In Europe:

Network Associates, Inc.
Virus Research
Gatwickstraat 25
1043 GL Amsterdam
Netherlands

☐ **NOTE:** McAfee AVERT Labs does keep all submitted samples, but once you submit a sample, AVERT cannot return it to you. AVERT does not accept or process Iomega Ditto or Jazz cartridges, Iomega Zip disks, or other types of removable media.

Using the VShield scanner

The VShield scanner protects your system in the background, as you work with your files, in order to prevent infection from viruses that arrive via floppy disks, from your network, embedded in file attachments that come with e-mail messages, or from your computer's memory. The scanner starts when you start your computer, and stays in memory until you shut down. The VShield scanner also includes technology that guards against hostile Java applets and ActiveX controls, and that keeps your computer from connecting to dangerous Internet sites. Secure password protection for your configuration options prevents others from making unauthorized changes.

-
- ❑ **NOTE:** In order for some VShield scanner features to become active, you must do a custom installation of these modules: Download Scan and Internet Filter.
-

To learn how to configure VShield properties and how to start and stop the VShield scanner, see [Chapter 4, "Using the VShield Scanner,"](#) in the *VirusScan User's Guide*.

Using the VirusScan application

The VirusScan name applies both to the entire set of desktop anti-virus program components described in the *User's Guide*, and to a particular component of that set: SCAN32.EXE, or the VirusScan application, which allows you to run "on-demand" scan operations. "On demand" means that you as a user control when VirusScan software starts and ends a scan operation, which targets it examines, what it does when it finds a virus, or any other aspect of the program's operation. Other VirusScan components, by contrast, operate automatically or according to a schedule you set. VirusScan software originally consisted solely of an on-demand scanner—features integrated into the program since then provide a cluster of anti-virus functions that give you maximum protection against virus infections and attacks from malicious software.

The VirusScan application operates in two modes: the VirusScan "Classic" interface gets you up and running quickly, with a minimum of configuration options, but with the full power of the VirusScan anti-virus scanning engine; the VirusScan Advanced mode adds flexibility to the program's configuration options, including the ability to run more than one scan operation concurrently.

To learn how to configure VirusScan properties and how to start and stop VirusScan software, see [Chapter 5, “Using the VirusScan application,”](#) in the *VirusScan User’s Guide*.

Scheduling scan tasks

The VirusScan Console runs scan operations and other tasks on the dates and at the times you choose, or at intervals you set. Use the Console to run a scan operation in your absence, when it causes the least disruption to your work, as part of a series of automated tasks, or in other ways that suit your needs.

To learn how to configure VirusScan Console properties, see [Chapter 6, “Creating and Configuring Scheduled Tasks,”](#) in the *VirusScan User’s Guide*.

Using specialized scanning tools

In addition to the continuous background scanning that the VShield scanner provides you with through its E-Mail Scan module, VirusScan software includes a Microsoft Outlook client extension designed specifically to look for viruses in your Microsoft Exchange and Microsoft Outlook mailboxes. The E-Mail Scan extension gives you the ability to scan your mail servers at your own initiative, and at times convenient for you. An unobtrusive plug-in architecture gives you access to the scanner from directly within your Exchange or Outlook client application.

To learn how to configure the E-Mail Scan extension and other specialized scanners, see [Chapter 8, “Using Specialized Scanning Tools,”](#) in the *VirusScan User’s Guide*.

Using the Alert Manager Client Configuration utility

All McAfee anti-virus software includes wide range of methods to alert you when it has detected a virus or other malicious software. These methods include:

- graphical and full-screen warnings that appear on your local computer, often with response options
- system beeps and custom messages that you can compose
- e-mail messages sent as replies to those who send you infected items, or as warnings to others that you've received an infected item
- log files that record VirusScan component actions, including virus detection and response events
- summary and real-time statistical displays that update detection and response events

Many of these methods alert you only if you are at your computer and watching as a scan operation runs. If you manage a network of workstations that you want to secure, however, you often need a method that will tell you about an infection if you are at any other workstation on your network, or even if you are not connected to the network at all. You also need a method to collect and manage alert messages from all over the network in a central repository so that you can respond whenever any workstation detects an infected file.

McAfee provides Alert Manager server software for just such a need. The software allows you to centralize alert message collection and processing, assign priority designations and custom messages to those messages, and designate any of up to 11 different methods to distribute them to you or to others. With the v4.5 anti-virus product series, the Alert Manager server now comes as an independent package bundled with McAfee NetShield anti-virus software. You can install this new Alert Manager server together with NetShield software, or by itself on a computer that you want to use as an alert collection point.

You can install multiple Alert Manager servers, one to a domain, perhaps, or one on each of the machines in a cluster server. If you do so, you can also forward alert messages among Alert Manager servers and, thereby, to other computers on your network or to centralized notification systems. This feature can allow MIS departments to keep close track of viruses and problem areas.

To learn how to install and configure the Alert Manager utility, see the *NetShield Administrator's Guide*.

VirusScan software as an Alert Manager Client

VirusScan software works as a client program with respect to NetShield software and an Alert Manager server. It can send alert “events” whenever it detects a virus or malicious software to any Alert Manager server you specify. The Alert Manager server then relays those events—and any others it receives from other workstations—as alert messages, via the methods you or your system administrator defined for alert distribution.

VirusScan software can instead send these same alert messages as text (.ALR) files to a Centralized Alerting directory visible to the Alert Manager server. The Alert Manager server checks the Centralized Alerting directory periodically, looking for any new .ALR files, and distributing the alert messages from any it finds.

-
- ❏ **NOTE:** McAfee recommends that you send alert events directly to an Alert Manager server rather than via Centralized Alerting, unless your network configuration does not permit you to use Alert Manager servers. The Alert Manager server can work in conjunction with Network Associates Event Orchestrator software to tie alert messages into the Network Associates Magic HelpDesk application for trouble-ticket generation and other features.

Alert Manager messages also contain much richer data than do those sent via Centralized Alerting. Enabling SNMP traps for Alert Manager will collect a host of information about the computer that generates the alert message and its software configuration.

The VirusScan client can supplement either method with Desktop Management Interface (DMI) alerts for network management software, such as Hewlett-Packard OpenView, to process.

Configuring the Alert Manager Client utility

VirusScan software includes a simple client configuration utility that allows you to choose the Alert Manager server that you want to receive alert events, designate a Centralized Alerting directory to receive alert messages, and specify the numeric value of DMI alert messages you want to send.

Setting up a complete alert system is a two-part process: First, you must enable the Alert Manager Client Configuration utility and point it to the correct Alert Manager server or Centralized Alerting location. Next, you must verify that you have selected the **Notify Alert Manager** checkbox in the VirusScan Advanced Alert property page, in the Alert page for the E-Mail Scan extension and in the Alert pages for each VShield module you have enabled.

This tells each VirusScan component to send an alert event to the Alert Manager client utility each time it detects a virus or malicious object. The client utility, in turn, passes the alert message to the Alert Manager server you designate. If you do not set your software to generate alert messages in the first place, the client utility will have nothing to pass to the Alert Manager server for distribution.

To start and configure the Alert Manager utility, follow these steps:

1. Click **Start** in the Windows taskbar, point to **Programs**, then to **Network Associates**. Next, choose **VirusScan Alerting Configuration**.


The Alert Manager Client Configuration page appears.



Figure 5-1. Alert Manager Client Configuration dialog box

2. Verify that the **Disable Alerting checkbox** is clear. This activates the remaining options in this dialog box.

Select this checkbox only if you want the Alert Manager Client Configuration utility *not* to pass alert messages from your anti-virus software to the Alert Manager server or to your Desktop Management Interface (DMI) administrative software. By default, this checkbox is clear. McAfee recommends that you leave it clear so that the client sends alert messages out.

 **NOTE:** If you use McAfee ePolicy Orchestrator software in your network environment, VirusScan software will still send alert messages to the ePolicy Orchestrator reporting component whether you activate or disable alerting here.

3. Select the alerting method you want to use. Your choices are:
 - **Enable Alert Manager alerting.** Click this button to send alert events to an Alert Manager server somewhere on your network. Choosing this option prevents you from sending alert events to a Centralized Alerting directory.

To choose the destination server, click **Configure** to open the Select Alert Manager Server dialog box.



Figure 5-2. Select Alert Manager Server dialog box

Next, enter the path to the directory that hosts the Alert Manager server you want to use, or click **Browse** to locate the server on your network.

You can use Universal Naming Convention (UNC) notation in the text box to designate the computer that hosts the Alert Manager server, or you can enter just the computer name. The Alert Manager Client Configuration utility will validate the form of the name you enter here, but will not verify that the Alert Manager server exists on the target computer. This allows laptop and other remote users to designate an Alert Manager server even when they are not connected to your network.

If you have Active Directory Services installed on your computer, clicking Browse displays a list of logical Alert Manager server names. If you do not have Active Directory installed, the display will show your entire directory tree. In that case, consult your system administrator to learn which computer hosts the Alert Manager server you want to use.

By default, the client utility will use Active Directory lookup to locate a published Alert Manager server if you have Active Directory Services installed on this computer and running on your network. To prevent the client utility from doing so, select the **Disable Active Directory Lookup** checkbox, when it appears.

When you've chosen a destination for your alert messages, click **OK** to close the dialog box.

- **Enable Centralized alerting.** Click this button to have VirusScan components send alert messages to a Centralized Alerting directory somewhere on your network. Choosing this option prevents you from sending alert events to an Alert Manager server.

To choose a destination directory, click **Configure** to open the Central Alerting Configuration dialog box.

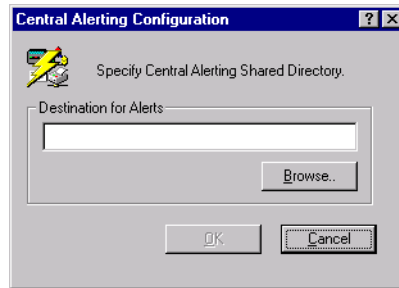


Figure 5-3. Central Alerting Configuration dialog box

Next, enter the path to the Centralized Alerting directory you want to use, or click **Browse** to locate the directory on your network. When you've chosen a destination, click **OK** to close the dialog box.

You can designate any directory on your network as a destination for Centralized Alerting messages, but the directory must contain a copy of the file CENTALRT.TXT in order for an Alert Manager server to relay the alert messages you send there.

If you enable Centralized Alerting, VirusScan software sends alert messages as text files with the extension .ALR to the target directory.

You can then point a designated Alert Manager server to the directory, if it contains the CENTALRT.TXT file, so that it checks periodically for .ALR files. If it finds one, it extracts the contents of the alert message from the file, distributes the message via one of its pre-configured notification methods, then deletes the .ALR file. It then steps up the frequency with which it checks the Centralized Alerting directory to capture any other alert messages that arrive.

- **Additionally Enable DMI Alerts.** Select this checkbox to supplement either of the other alerting methods. Next, click **Configure** to open the DMI Configuration dialog box, where you can enter the identifying number that your Desktop Management Interface (DMI) client application assigned to your VirusScan software when you installed it.

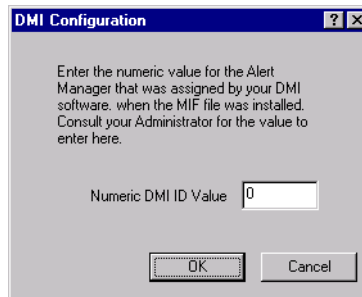


Figure 5-4. DMI Configuration dialog box

To use this option, you must have a DMI client application, such as Hewlett-Packard OpenView, already installed on your local computer and DMI administrative software running somewhere on your network.

VirusScan software comes packaged with a Management Information File (AMG.MIF) that identifies VirusScan alerting attributes to your DMI client application. The DMI client, in turn, assigns an identifying number to the VirusScan software, so that it can collect VirusScan alert events and send them to a DMI administrative application.

In order for VirusScan software to send alert messages with an identification number that the administrative application can recognize and process, you must enter the correct ID number here. Consult your system administrator for specific details that apply to your DMI software.

When you have entered a number, click **OK** to close the dialog box.

4. Click **OK** to save your changes and close the Alert Manager Client Configuration dialog box.

Developing an updating strategy

Make no mistake about it: virus writers are electronic vandals who can destroy your data, cause system instability, and cost you time and money. The overwhelming majority of them are relatively inept programmers who rely on virus “kits,” or other pre-made tools, to introduce small variations in existing viruses or other malicious software. But some virus writers do introduce new twists or unexpected attack strategies into their creations. To counter these threats, McAfee Anti-Virus Emergency Response Team (AVERT) researchers must release frequent updates to the virus definitions database and technical enhancements or upgrades to the scan engine that VirusScan software uses. Without updated files, VirusScan software might not recognize new forms of malicious software or detect new virus strains when it encounters them.

What are .DAT files?

Virus definition, or .DAT, files contain up-to-date virus signatures and other information that McAfee anti-virus products use to protect your computer against the thousands of computer viruses in circulation. McAfee releases new .DAT files weekly to provide protection against the approximately 500 new viruses that appear each month.

With this VirusScan release, McAfee has introduced a new incremental .DAT, or iDAT, technology that consists of small file collections that contain only the virus definitions that have changed between weekly .DAT file releases—*not* the entire .DAT file set. This development means that you can download .DAT file updates much faster, and at a far lower cost in bandwidth, than ever before. To learn more about the new technology, see [Appendix F, “Understanding iDAT Technology.”](#)

What is the scan engine?

The McAfee scan engine is at the heart of McAfee anti-virus software. The engine contains the program logic necessary to scan files at particular points, process and pattern-match virus definitions with data it finds in your files, decrypt and run virus code in an emulated environment, apply heuristic techniques to recognize new viruses, and remove infectious code from legitimate files. The remaining parts of the VirusScan package help to feed files to the engine for processing, integrate with various parts of your computer’s operating system to intercept files as they execute or as you work with them, and provide an interface you can use to configure various scan settings.

Update and upgrade methods

Because new .DAT and program files are crucial to ensuring your anti-virus security, McAfee incorporates a range of updating options into the VirusScan product package. These include:

- **SecureCast service broadcasts.** The McAfee SecureCast service uses BackWeb “push” technology to send out automatic .DAT file updates, product upgrades, virus alerts and other useful items to subscribers. McAfee recommends using a combination of this service and the mechanisms provided in VirusScan software to update and upgrade your software. To learn more about the SecureCast service, see [Appendix D, “Using the SecureCast Service to Get New Data Files.”](#)
- **Scheduled automatic update and upgrade operations.** VirusScan software includes two utilities that you can use to schedule regular .DAT file updates and product file upgrades directly from the VirusScan Console: AutoUpdate and AutoUpgrade. McAfee recommends that you use these utilities as your primary methods to update or upgrade your software for workstations on your network, after you download your files from the McAfee “b2b” website or receive them through the SecureCast service. To learn more, see [“Understanding the AutoUpdate utility” on page 108](#) and [“Understanding the AutoUpgrade utility” on page 118](#).
- **Incremental .DAT file updates.** The new McAfee iDAT, technology works transparently with the included AutoUpdate version. The new iDAT files consist of .UPD parcels and a DELTA.INI file that tracks what has changed between weekly .DAT file releases. The AutoUpdate utility uses the DELTA.INI file to determine files to download and install.

By default, the AutoUpdate utility will download iDAT files unless the .DAT files or scan engine you have installed on your computer is significantly out of date. In that case, the AutoUpdate utility automatically downloads and installs the full .DAT package. You do not need to configure the utility for this purpose—it can choose which route it must take based on what it finds on your system. To learn more about how iDAT files work, see [Appendix F, “Understanding iDAT Technology.”](#)

- **SuperDAT scan engine and .DAT file updates.** McAfee releases a weekly SuperDAT package of current .DAT file updates and the current Olympus scan engine, together with a Setup feature that makes updating and upgrading a snap.

The SuperDAT utility minimizes the need for complex software deployments each time you receive upgrade components. It takes care of shutting down any active scan operations, services, or other memory-resident software components that might interfere with your updates, then copies the new files to their proper locations and enables your software to use them immediately.

The current VirusScan release can download and install new .DAT and engine files from a SuperDAT package, on any supported Windows platform, without requiring you to restart your computer. You can download and run SuperDAT packages separately to update and update your software, or you can use the SuperDAT utility in conjunction with the AutoUpgrade utility to automate updates to a significant degree. To learn how to combine the two utilities, see [“Using the AutoUpgrade and SuperDAT utilities together” on page 128.](#)

In addition to the weekly SuperDAT package that contains both current .DAT files and a current scan engine, McAfee will make available a SuperDAT package that consists only of .DAT files. This executable file minimizes the need for you to closely manage your .DAT file updates. It takes care of shutting down any active scan operations, services, or other memory-resident software components that might interfere with your updates. It then copies the new files to their proper locations and enables your software to use them immediately.

- **Packaged .DAT file updates.** McAfee also releases weekly .DAT file stand-alone packages that you can download, extract, and copy to the program directory for your software. A .DAT package consists of an archived .ZIP file named DAT-XXXX.ZIP. The XXXX in the file name is a series number that changes with each .DAT file release. McAfee does not recommend this method to update your software, but you can do so when necessary. To learn more about how to use these packages for your updates, see the README.TXT file that accompanies each weekly package.
- **EXTRA.DAT files.** Regular McAfee virus definition (.DAT) file releases protect you quite well against new and still-circulating malicious code. But even weekly .DAT releases can't always protect you against a swift virus outbreak, especially in the wake of such e-mail borne viruses as W97M/MELISSA.

McAfee anti-virus software anticipates exactly this situation. It allows you to take advantage of capabilities built into the McAfee scan engine to deploy a small, supplemental virus definition file in between .DAT file releases. This small EXTRA.DAT file holds the absolutely latest available virus signature data for viruses that McAfee AVERT researchers have identified as high-risk contaminants.

The file can help to identify several viruses at once, but because AVERT researchers ordinarily publish an EXTRA.DAT file as soon as they identify a high-risk virus, the file frequently targets one or two highly prevalent agents. AVERT researchers then add the virus definitions they included in any EXTRA.DAT releases to the following week's regular .DAT file release. To learn how to deploy the EXTRA.DAT file, see [“Deploying an EXTRA.DAT file” on page 130.](#)

- **Emergency .DAT files.** VirusScan software includes an Emergency Disk utility you can use to create a bootable floppy disk to start your computer in a virus-free environment. The Emergency Disk you create uses specialized .DAT files that target boot-sector and memory-resident viruses, which pose the greatest infection risk to software if they activate before your anti-virus software can. McAfee provides updates for these files that you can download directly from the AVERT website at:

http://www.mcafee2b.com/asp_set/anti_virus/avert/tools.asp

McAfee recommends that you download these files directly to a virus-free computer, then extract them to an Emergency Disk you've created. To learn more about creating an Emergency Disk, see [“Using the Emergency Disk Creation utility” on page 47](#). To learn how to use the Emergency Disk to scan your system, see [“If you suspect you have a virus...” on page 71](#).

Understanding the AutoUpdate utility

The AutoUpdate utility is the principle method McAfee recommends that you use to update your .DAT files. The utility runs exclusively as a task from within the VirusScan Console. To use it to update your VirusScan software, you must:

- Set a schedule for the AutoUpdate task, and enable it to run
- Set a password to protect your configuration settings, if you wish
- Configure the task to download new files from a specific location on your network, or on the Internet

By default, the AutoUpdate task included with VirusScan Console comes configured to download the most recent .DAT file updates directly from the Network Associates FTP site. This configuration can make administration simple and straightforward for small networks or individual VirusScan installations. If you have a large network, however, retaining this configuration can severely tax your external bandwidth if, as will happen if you leave the default configuration enabled, each network node tries to update its .DAT files at once.

Instead, McAfee recommends that you use AutoUpdate in conjunction with its companion service, the Enterprise SecureCast channel, in an efficient “push-pull” arrangement. Once you install its client software on an administrative server, the SecureCast service can send, or “push,” updated files to you automatically, as soon as McAfee makes them available on its servers. To learn more about the SecureCast service, see [Appendix D, “Using the SecureCast Service to Get New Data Files”](#) or visit the McAfee website at:

http://www.mcafee2b.com/asp_set/anti_virus/securecast/enterprise.asp

If you make the files you download files available on one or more central servers on your network, then configure your remaining network nodes to “pull” the updated files from those servers, you can

- Schedule network-wide .DAT file roll-outs for convenient times and with minimal intervention from either administrators or network users. Use the AutoUpdate Task Properties dialog box to determine when each network node will check your network server for updated files.

You might, for example, specify one convenient update time when you first deploy VirusScan software, but set the AutoUpdate utility to trigger at a random interval within 60 minutes of that time, or set a schedule that phases in or rotates .DAT file updates among different parts of the network. To learn how to schedule the AutoUpdate task or other tasks, see [“Enabling tasks” on page 208](#) of the *VirusScan User’s Guide*.

- Split roll-out administration duties among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.
- Reduce the likelihood that you will need to wait to download new .DAT files. Traffic on McAfee servers increases dramatically on regular .DAT file publishing dates. Avoiding the competition for network bandwidth enables you to deploy your update with minimal interruptions.

Other advanced AutoUpdate options allow you to back up existing .DAT files, install the .DAT file update, reboot the updated computer, if necessary, or run particular programs after successful updates.

Configuring the AutoUpdate Utility

To configure the AutoUpdate utility so that it runs properly as a task within the VirusScan console, you must tell it:

- which update sites have the new files you want to download
- which transfer method you want it to use for the download
- whether you use a proxy server and, if so, what port you have assigned to it
- whether you want it to back up your existing .DAT files
- what you want it to do with the files it downloads-install them, save them for future use, or both
- what you want it to do after it downloads the files-force an update, reboot your system after an update, or run a program after an update
- whether you want it to keep track of its actions in a log file

Property pages in the Automatic Update Properties dialog box control the options for your update task. You can click each tab in turn to configure this task.

To display the Automatic Update dialog box, follow these steps:

1. Double-click the **AutoUpdate** task in the Console task list to open its Task Properties dialog box (see [Figure 6-4 on page 203](#) of the *VirusScan User's Guide*).

To learn how to set a password for this task, see [“Working with the AutoUpgrade and AutoUpdate tasks” on page 203](#) of the *VirusScan User's Guide*. To learn how to set a schedule for the task, see [“Enabling tasks” on page 208](#) of the *User's Guide*.

2. Click **Configure**.

The Automatic Update dialog box appears with the Update Sites property page selected (see [Figure 6-1 on page 110](#)).

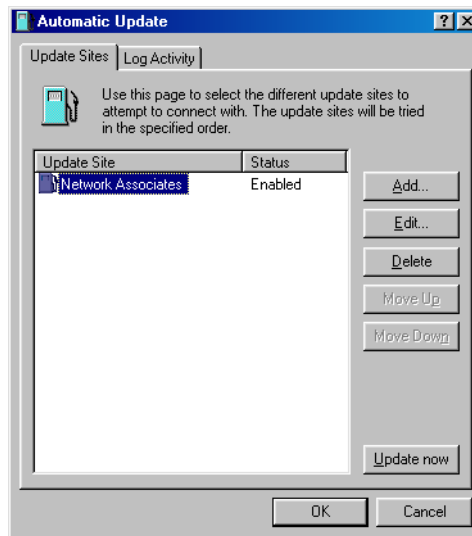


Figure 6-1. Automatic Update dialog box - Update Sites page

Here, the AutoUpdate utility lists the sites from which it will download new .DAT files. It also reports each site's current status as Enabled or Disabled. A site is enabled if you have selected the **Enabled** checkbox in the Automatic Update Properties dialog box. A site is disabled if you clear this checkbox. This designation does not change whether or not the AutoUpdate utility can connect with the site.

Initially, the utility comes configured to connect only to the Network Associates FTP site. You can add as many different sites as you need, and alter the order in which AutoUpdate tries to connect to them, from this dialog box. The utility will try each site in turn, starting from the top of the list, until it successfully downloads new files or determines that no new files exist.

3. From here, you can:

- Add a new site. Click **Add** to open the Automatic Update Properties dialog box (Figure 6-2 on page 111). To learn how to specify options for your new site, see “Configuring update options” on page 113.



Figure 6-2. Automatic Update Properties dialog box - Update Options page

- Change definitions for an existing update site. Select a site shown in the update site list, then click **Edit** to open the Automatic Update Properties dialog box (Figure 6-2). Make the changes you want to make, then click **OK** to save them and return to this dialog box. To see descriptions and instructions for configuring the available options, see “Configuring update options” on page 113.
- Remove an existing site from the update site list. Select a site shown in the update site list, then click **Delete**.
- Specify the order in which the AutoUpdate utility should connect to the listed sites. To position a site so that the utility tries it earlier, select the site, then click **Move Up**. To designate a site as lower in priority, select the site, then click **Move Down**.

- Update your files immediately from the sites listed in the update list, using default configuration options or the options you chose for this task. Click **Update now**.

To use this function, you must have configured enough of the necessary options for the AutoUpdate utility to locate the listed site and, if necessary, log on to it. See [“Configuring update options” on page 113](#) to learn how to specify the options you need.

If AutoUpdate cannot connect to the listed site after three attempts, or if it does not find new .DAT files, it will connect to each of the other sites listed until it finds the most current .DAT files available.

If you have the **Force Update** option selected, AutoUpdate will download any .DAT files it finds on the first site to which it can connect successfully. See [“Configuring advanced update options” on page 115](#) for more details.

4. Click the Log Activity tab to display the next property page ([Figure 6-3](#)).

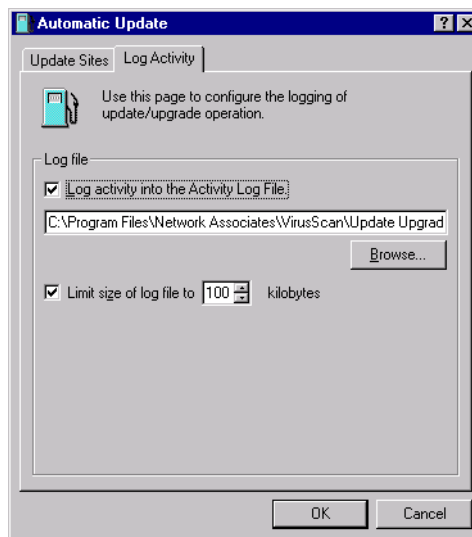



Figure 6-3. Automatic Update dialog box - Log Activity page

5. Select the **Log activity into the Activity Log File** checkbox.

By default, the AutoUpdate utility records what happens during update attempts and saves the record in the file UPDATE UPGRADE ACTIVITY LOG.TXT in the VirusScan program directory whenever you stop the task or when you shut your system down.

If you would prefer to log this data to a different text file, enter its path and filename in the text box provided, or click **Browse** to locate the file. The AutoUpdate utility will not generate a text file—it will write only to an existing file.

6. To minimize the log file size, select the **Limit size of log file to** checkbox. Next click  to set a size, or enter a value between 10KB and 999KB. By default, the AutoUpdate utility limits the file size to 100KB.

If you clear this checkbox, the log file can grow until disk space or file system limitations stop it. When the file reaches the maximum size you set, the AutoUpdate utility first clears it, then starts the log again from where it left off.

To see the contents of the log file from VirusScan Console, select the AutoUpdate task in the task list, then choose **View Activity Log** from the **Task** menu.

7. Click **OK** to save your changes and close the Automatic Update dialog box. Click **Cancel** to close the dialog box without saving your changes.

Configuring update options

To create a new update site or change the settings for an existing site, click **Add** in the Automatic Update dialog box (see [Figure 6-1 on page 110](#)), or select a listed site, then click **Edit**. Either action will open the Automatic Update Properties dialog box ([Figure 6-4](#)).

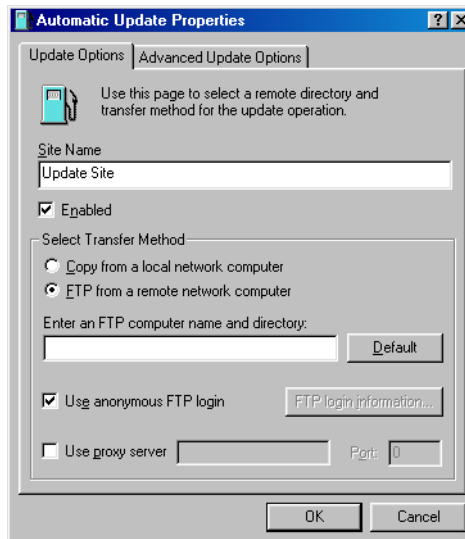


Figure 6-4. Automatic Update Properties dialog box - Update Options page

Next, follow these steps:

1. Enter a descriptive name in the Site Name text box that clearly identifies the new site.

An example might be Internal DAT File Update Site.

2. Select the **Enabled** checkbox to approve this site for the AutoUpdate utility's use.


Clearing this checkbox preserves the options you've chosen, but causes the utility to skip this site when it tries to download new .DAT files.

The AutoUpdate utility will make a maximum of three connection attempts for the site during each scheduled update operation. When it does connect and download the new .DAT file package, the utility also extracts the files and installs them into the correct directory.

3. Specify which transfer method the utility must use to download new files. Your choices are:
 - **Copy from a local network computer.** Click this button to tell the AutoUpdate utility to use your standard network configuration to look for new files on your local computer or on a computer elsewhere on your network. Your network settings will govern how the utility attempts the connection and how long it waits before it stops the connection attempt.

Next, use Universal Naming Convention (UNC) notation to enter the path to the computer that holds the new files you want to download in the text box labeled Select a Computer and Directory. You can also click **Browse** to locate the directory you want.

To use UNC notation, you must either use the same account you used to log into your network, or specify a user name and password to log into your network. To use the current account, select the **Use Logged In Account** checkbox.

 **NOTE:** On Windows NT Workstation v4.0 and Windows 2000 Professional systems, selecting the **Use Logged In Account** checkbox has slightly different effects. If you've scheduled your file update, the AutoUpdate utility will use its own service account to log on to the upgrade server and download new files. If you click **Update now**, the AutoUpdate utility will use the same account you used to log on to your network to connect to the upgrade server.

To use a custom account, clear the **Use Logged In Account** checkbox, then click **UNC login information** to enter a user name and password for an account that has access rights to the target server.

- **FTP from a remote network computer.** Click this button to tell the AutoUpdate utility to look for new files on an FTP site you designate. To use this option, the target server must have an FTP service enabled.

By default, the utility will download new files from the Network Associates FTP site, which accepts anonymous FTP logins. You can click **Default** to specify this site at any time.

The AutoUpdate utility uses its own FTP implementation to connect to the server, but the timeout period for the connection attempt will depend on your existing network protocol settings.

To use a different FTP site, enter the URL for the site you want to use in the text box labeled Enter an FTP Computer Name and Directory. You must either connect to a site set for anonymous FTP login, or you must designate the user name and password for an account on the site.

To have the utility use an anonymous login, select the **Use anonymous FTP login** checkbox.

To specify an account, clear the **Use anonymous FTP login** checkbox, then click **FTP login information** to enter a user name and password for an account that has access rights to the target server.

If your network uses a proxy server, select the **Use proxy server checkbox**, then enter the server name and the logical port it uses in the text boxes provided. You can enter the name in UNC notation or as a domain name, whichever is appropriate for your environment.

-
- ☐ **NOTE:** The AutoUpdate utility will not allow proxy connections that require challenge-response proxy authentication.
-

Configuring advanced update options

To complete your AutoUpdate task, you need to enter only a target server, a connection method, and any necessary login information. Once you enable the task and set a schedule for it, the AutoUpdate utility will download the correct files from the target server for you, extract them from their .ZIP archives, then install them into the VirusScan program directory.

To have AutoUpdate do additional pre- or post-processing on the files, or to have it take other actions, click the Advanced Update Options tab to display the property page shown in [Figure 6-5 on page 116](#).

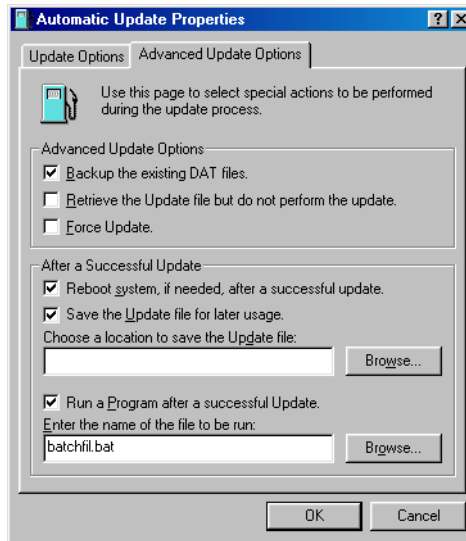


Figure 6-5. Automatic Update Properties dialog box - Advanced Update Options page

Next, follow these steps:

1. Tell the AutoUpdate utility what you want it to do before or as it performs an update. Your options are:
 - **Backup the existing .DAT files.** Select this checkbox to have the AutoUpdate utility rename existing VirusScan .DAT files before it installs new files. To rename each file, the utility appends the extension .SAV to the existing file name and extension. CLEAN.DAT, for example, will become CLEAN.DAT.SAV.
 - **Retrieve the Update file but do not perform the update.** Select this checkbox to have the utility download the .ZIP archive that contains the new .DAT files, then save it in a location you specify instead of extracting it and installing it.


Selecting this checkbox also selects the **Save the Update file for later usage** checkbox in the After a Successful Update area. To tell AutoUpdate where to save the .DAT file package, enter a path and folder name in the text box below this checkbox, or click **Browse** to locate a suitable folder.

Selecting this checkbox also makes the **Backup the existing DAT files**, the **Force Update**, and the **Reboot system, if needed, after a successful update** checkboxes unavailable.

You might want to use this option if you download new .DAT files to a central server on your network and want individual client computers to download, extract and install the new files locally.

- **Force Update.** Select this checkbox to tell the AutoUpdate utility to download and install whichever .DAT file package it finds on the target server, whether that package is more recent than your existing .DAT files or not.

You might use this option to “refresh” .DAT files stored in your VirusScan program directory periodically, in case your existing files have become corrupted. This option will also circumvent any error messages that VirusScan software might return if it doesn’t find new files on the target server at the time you have your update task scheduled.

 **WARNING:** McAfee recommends that you use this option with extreme caution. If you have configured your AutoUpdate task to connect to a server that stores older .DAT file versions, you can reduce the effectiveness of your VirusScan software and expose your computer or network to infection from newly emerging viruses and other malicious software. Upgrades to VirusScan program components can also cause incompatibilities with older .DAT file versions. These incompatibilities can, in turn, cause VirusScan software to behave unpredictably.

2. Tell the AutoUpdate utility what you want it to do after it successfully downloads, extracts, and installs new .DAT files. Your options are:
 - **Reboot system, if needed, after a successful update.** Select this checkbox to have the AutoUpdate utility restart your system after it installs new .DAT files.

In most cases, you will not need to restart in order for VirusScan software to use new .DAT files, but some systems will require that you do so in order for the new files to activate. If you want to restart your system at a more convenient time, clear this checkbox. If you plan to run a program after updating your .DAT files, you should also leave this checkbox clear.

- **Save the Update file for later usage.** Select this checkbox to have the AutoUpdate utility save an unextracted copy of the .DAT file package in a location you specify. The utility then extracts the .DAT files from the update package and continues with the installation.

By contrast, the **Retrieve the Update file but do not perform the update** option saves the unextracted file, but does not install the new .DAT files.

To tell the AutoUpdate utility where to save the .DAT file package, enter a path and folder name in the text box below this checkbox, or click **Browse** to locate a suitable folder.

- **Run a Program after a successful Update.** Select this checkbox to tell the utility to start another program after it installs new .DAT files. You might want to use this option, for example, to start an e-mail client program or a network message utility that notifies a system administrator that the update operation completed successfully.

Next, enter the path and file name for the program you want to run, or click **Browse** to locate the program on your hard disk.

3. To save your changes and return to the Automatic Update dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

Understanding the AutoUpgrade utility

McAfee revises VirusScan software and the Olympus scan engine regularly to add new detection and repair capabilities, new features for manageability and flexibility, and other enhancements that make it a better anti-virus security tool. VirusScan software's AutoUpgrade utility is designed specifically to look for and download these new versions as they become available. You can use this utility in conjunction with the SuperDAT utility to automate scan engine upgrades. To learn how to do so, see [“Using the AutoUpgrade and SuperDAT utilities together” on page 128](#).

The AutoUpgrade utility runs exclusively as a task from within the VirusScan Console. To use it to upgrade your VirusScan software, you must:

- Set a schedule for the AutoUpgrade task, and enable it to run
- Set a password to protect your configuration settings, if you wish
- Configure the task to download new files from a specific location on your network, or on the Internet

By default, the AutoUpgrade task included with VirusScan Console does not come configured with any default upgrade site. Instead, McAfee recommends that you use other mechanisms, such as the Enterprise SecureCast service, to receive new SuperDAT or program files, then place those files on a central server within your network. Next, you would configure the AutoUpgrade utility on each of your network workstations to “pull” the new files from the location you specify. To learn more about the SecureCast service, see [Appendix D, “Using the SecureCast Service to Get New Data Files”](#) or visit the Network Associates website at:

http://www.mcafee2b.com/asp_set/anti_virus/securecast/enterprise.asp

Making new files available on one or more central servers on your network allows you to:

- Schedule network-wide program file roll-outs for convenient times and with minimal intervention from either administrators or network users. Use the AutoUpgrade Task Properties dialog box to determine when each network node will check your network server for updated files.

You might, for example, specify one convenient update time when you first deploy VirusScan software, but set the AutoUpgrade utility to trigger at a random interval within 60 minutes of that time, or set a schedule that phases in or rotates program file upgrades among different parts of the network. To learn how to schedule the AutoUpdate task or other tasks, see [“Enabling tasks” on page 208](#) of the *VirusScan User’s Guide*.

- Split roll-out administration duties among different servers or domain controllers, among different regions of wide-area networks, or across other network divisions. Keeping update traffic primarily internal can also reduce the potential for network security breaches.
- Reduce the likelihood that you will need to wait to download new program files. Traffic on McAfee servers increases dramatically whenever new program files appear. Avoiding the competition for network bandwidth enables you to deploy your update with minimal interruptions.

Configuring the AutoUpgrade utility

To update program files for your VirusScan software, you must tell the AutoUpgrade utility:

- which update sites have the new files you want to download
- which transfer method you want it to use for the download
- whether you use a proxy server and, if so, what port you have assigned to it
- what you want it to do with the files it downloads—install them, save them for future use, or both

- whether you want it to reboot your system after an upgrade
- whether you want it to keep track of its actions in a log file

Property pages in the Automatic Upgrade Properties dialog box control the options for your upgrade task. You can click each tab in turn to configure this task.

To display the Automatic Upgrade dialog box, follow these steps:

1. Double-click the AutoUpgrade task in the Console task list to open its Task Properties dialog box ([Figure 6-6](#)).

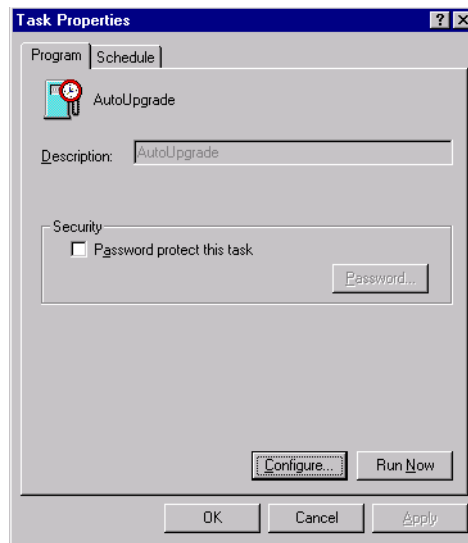


Figure 6-6. AutoUpgrade Task Properties dialog box

To learn how to set a password for this task, see [“Working with the AutoUpgrade and AutoUpdate tasks” on page 203](#) of the *VirusScan User’s Guide*. To learn how to set a schedule for the task, see [“Enabling tasks” on page 208](#) of the *User’s Guide*.

2. Click **Configure**.

The Automatic Upgrade dialog box appears with the Upgrade Sites property page selected (see [Figure 6-7 on page 121](#)).

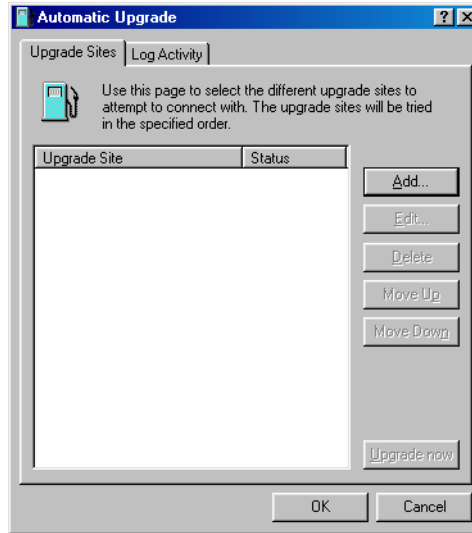


Figure 6-7. Automatic Upgrade dialog box - Upgrade Sites page

Here, the AutoUpgrade utility lists the sites from which it will download new VirusScan program files. It also reports each site's current status as Enabled or Disabled. A site is enabled if you have selected the **Enabled** checkbox in the Automatic Upgrade Properties dialog box. A site is disabled if you clear this checkbox. This designation does not change whether or not the AutoUpgrade utility can connect with the site.

You will not see any sites listed initially, because the AutoUpgrade utility does not come configured to connect to any upgrade site. You must add the sites you need from the information you received when you purchased VirusScan software. The AutoUpgrade utility can download new program files from any network share or FTP site that you specify.

You can add as many different sites as you need, and alter the order in which the utility tries to connect to them. The utility will try each site in turn, starting from the top of the list, until it successfully downloads new files or determines that no new files exist.

3. From this dialog box, you can:

- Add a new site. Click **Add** to open the Automatic Upgrade Properties dialog box (Figure 6-2 on page 111). To learn how to specify options for your new site, see “Configuring upgrade options” on page 124.

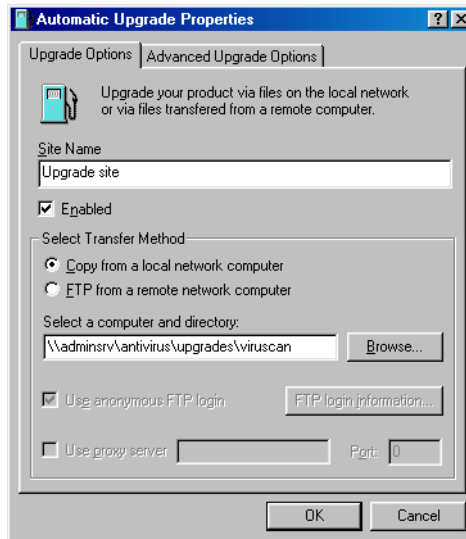


Figure 6-8. Automatic Upgrade Properties dialog box - Upgrade Options page

- Change definitions for an existing upgrade site. Select a site shown in the upgrade site list, then click **Edit** to open the Automatic Upgrade Properties dialog box (Figure 6-8). Make the changes you want to make, then click **OK** to save them and return to this dialog box. To see descriptions and instructions for configuring the available options, see “Configuring upgrade options” on page 124.
- Remove an existing site from the update site list. Select a site shown in the upgrade site list, then click **Delete**.
- Specify the order in which the AutoUpgrade utility should connect to the listed sites. To position a site so that the utility tries it earlier, select the site, then click **Move Up**. To designate a site as lower in priority, select the site, then click **Move Down**.
- Update your files immediately from the sites listed in the update list, using default configuration options or the options you chose for this task. Click **Upgrade now**.

To use this function, you must have configured enough of the necessary options for the AutoUpgrade utility to locate the listed site and, if necessary, log on to it. See [“Configuring upgrade options” on page 124](#) to learn how to specify the options you need.

If AutoUpgrade cannot connect to a listed site after three tries, or if it does not find new program files, it will connect to each of the other sites listed until it finds the most current program files available.

4. Click the Log Activity tab to display the next property page ([Figure 6-9](#)).

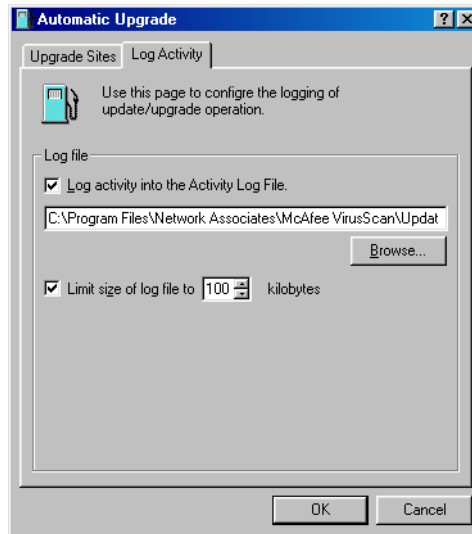



Figure 6-9. Automatic Upgrade dialog box - Log Activity page

5. Select the **Log activity into the Activity Log File** checkbox.

By default, the AutoUpgrade utility records what happens during update attempts and saves the record in the file UPDATE UPGRADE ACTIVITY LOG.TXT in the VirusScan program directory whenever you stop the task or when you shut your system down.

If you would prefer to log this data to a different text file, enter its path and filename in the text box provided, or click **Browse** to locate the file. The AutoUpgrade utility will not generate a text file—it will write only to an existing file.

6. To minimize the log file size, select the **Limit size of log file to** checkbox. Next click  to set a size, or enter a value between 10KB and 999KB. By default, the AutoUpgrade utility limits the file size to 100KB.

If you clear this checkbox, the log file can grow until disk space or file system limitations stop it. When the file reaches the maximum size you set, the AutoUpgrade utility first clears it, then starts the log again from where it left off.

To see the contents of the log file from VirusScan Console, select the AutoUpgrade task in the task list, then choose **View Activity Log** from the **Task** menu.

7. Click **OK** to save your changes and close the Automatic Upgrade dialog box. Click **Cancel** to close the dialog box without saving your changes.

Configuring upgrade options

To create a new update site or change the settings for an existing site, click **Add** in the Automatic Upgrade dialog box (see [Figure 6-7 on page 121](#)), or select a listed site, then click **Edit**. Either action will open the Automatic Upgrade Properties dialog box ([Figure 6-10](#)).

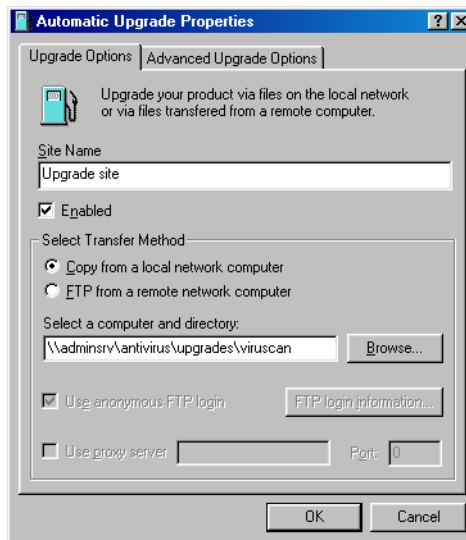


Figure 6-10. Automatic Upgrade Properties dialog box - Upgrade Options page

Next, follow these steps:

1. Enter a descriptive name in the Site Name text box that clearly identifies the new site.

An example might be Internal Program File Upgrade Site.

2. Select the **Enabled** checkbox to approve this site for the AutoUpgrade utility's use.

Clearing this checkbox preserves the options you've chosen, but causes the utility to skip this site when it tries to download new .DAT files.

The AutoUpgrade utility will make a maximum of three connection attempts for the site during each scheduled update operation. When it does connect and download new program files, the utility also extracts the files and installs them into the correct directory.

3. Specify which transfer method the utility must use to download new files. Your choices are:
 - **Copy from a local network computer.** Click this button to tell the AutoUpgrade utility to use your standard network configuration to look for new files on your local computer or on a computer elsewhere on your network. Your network settings will govern how the utility attempts the connection and how long it waits before it stops the connection attempt.

Next, use Universal Naming Convention (UNC) notation to enter the path to the computer that holds the new files you want to download in the text box labeled Select a Computer and Directory. You can also click **Browse** to locate the directory you want.

To use UNC notation, you must either use the same account you used to log into your network, or specify a user name and password to log into your network. To use the current account, select the **Use Logged In Account** checkbox.

-
- ☐ **NOTE:** On Windows NT Workstation v4.0 and Windows 2000 Professional systems, selecting the **Use Logged In Account** checkbox has slightly different effects. If you've *scheduled* your file update, the AutoUpgrade utility will use its own service account to log on to the upgrade server and download new files. If you click **Update now**, the AutoUpgrade utility will use the same account you used to log on to your network to connect to the upgrade server.

Either account must have administrative rights on your local computer—or, in other words, be a part of the Local Administrators group—to install new scan engine or any program files that replace existing VirusScan services.

To use a custom account, clear the **Use Logged In Account** checkbox, then click **UNC login information** to enter a user name and password for an account that has access rights to the target server.

- **FTP from a remote network computer.** Click this button to tell the AutoUpgrade utility to look for new files on an FTP site you designate. To use this option, the target server must have an FTP service enabled.


The AutoUpgrade utility uses its own FTP implementation to connect to the server, but the timeout period for the connection attempt will depend on your existing network protocol settings.

To use a different FTP site, enter the URL for the site you want to use in the text box labeled Enter an FTP Computer Name and Directory. You must either connect to a site set for anonymous FTP login, or you must designate the user name and password for an account on the site.

To have the utility use an anonymous login, select the **Use anonymous FTP login** checkbox.

To specify an account, clear the **Use anonymous FTP login** checkbox, then click **FTP login information** to enter a user name and password for an account that has access rights to the target server.

If your network uses a proxy server, select the **Use proxy server checkbox**, then enter the server name and the logical port it uses in the text boxes provided. You can enter the name in UNC notation or as a domain name, whichever is appropriate for your environment.

 **NOTE:** The AutoUpgrade utility will not allow proxy connections that require challenge-response proxy authentication.

Configuring advanced upgrade options

To complete your AutoUpgrade task, you need to enter only a target server, a connection method, and any necessary login information. Once you enable the task and set a schedule for it, the AutoUpgrade utility will download the correct files from the target server for you, extract them, then install them into the VirusScan program directory.

To have AutoUpgrade do additional pre- or post-processing on the files, or to have it take other actions, click the Advanced Upgrade Options tab to display the property page shown in [Figure 6-5 on page 116](#).

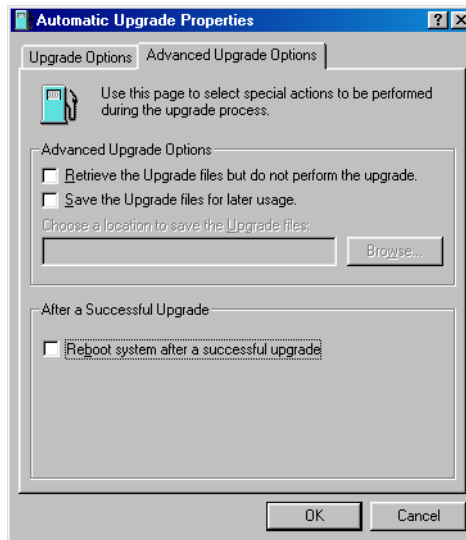


Figure 6-11. Automatic Update Properties dialog box - Advanced Update Options page

Next, follow these steps:

1. Tell the AutoUpgrade utility what you want it to do before or as it performs an update. Your options are:
 - **Retrieve the Upgrade files but do not perform the upgrade.** Select this checkbox to have the utility download the archive that contains new program files, then save it in a location you specify instead of extracting it and installing it.

Selecting this checkbox also selects the **Save the Upgrade files for later usage** checkbox. To tell AutoUpgrade where to save the program file archive, enter a path and folder name in the text box below this checkbox, or click **Browse** to locate a suitable folder.

You might want to use this option if you download new program files to a central server on your network and want individual client computers to download, extract and install the new files locally.
2. Tell the AutoUpgrade utility what you want it to do after it successfully downloads, extracts, and installs new .DAT files. Your options are:
 - **Reboot system, if needed, after a successful update.** Select this checkbox to have the AutoUpgrade utility restart your system after it installs new program files.

In most cases, you will not need to restart in order for VirusScan software to use new program files, but some systems will require that you do so in order for the new files to activate. If you want to restart your system at a more convenient time, clear this checkbox.

3. To save your changes and return to the Automatic Upgrade dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

Using the AutoUpgrade and SuperDAT utilities together

For this release, you must modify the SuperDAT package you download from the McAfee website in order to use it with the AutoUpgrade utility.

-
- ☐ **NOTE:** VirusScan v4.5 and later releases require you to use the SuperDAT v1.2 or later utility.
-

To modify the SuperDAT package, follow these steps:

1. Rename SDATXXXX.EXE to SETUP.EXE. Here, the XXXX refers to the SuperDAT version number included as part of the file name.
2. Download the file AUTOUPG.ZIP, which you will find on the Network Associates FTP site in this location:

```
ftp://<username>:<password>@ftp.nai.com/licensed/antivirus  
/superdat/tools/
```

-
- ☐ **NOTE:** Here, <username> is your Network Associates corporate site access username, and <password> is your corporate site access password. To download these files, you must have access to the site as a licensed McAfee customer.
-

AUTOUPG.ZIP contains the file PKGDESC.INI. Extract PKGDESC.INI from the .ZIP archive, then copy both the extracted file and the renamed SETUP.EXE package to the server from which you want other computers on your network to download updated files. Both PKGDESC.INI and SETUP.EXE must be present for AutoUpgrade to download update files correctly.

-
- ☐ **NOTE:** If your upgrade server runs UNIX or another case-sensitive operating system, verify that you have named the PKGDESC.INI file correctly. The AutoUpdate version included with VirusScan anti-virus software expects to find a lower-case filename: pkgdesc.ini.
-

3. If you want to, create and copy a SETUP.ISS file into the directory from which you tell AutoUpgrade to download new files.

SETUP.ISS is a simple text file that governs how the AutoUpgrade utility upgrades your software. You can use any standard text editor to create and save this file.

To specify configuration options in your SETUP.ISS file, use the example shown below to learn which options you may use. You can cut and paste this example directly into a text file, then edit and save the file as SETUP.ISS.

```
[SuperDATOptions]

bReboot=1

bPrompt=1

szLogFile=C:\temp\mylog.txt
```

Here's a description of what each statement in the file does:

- **bReboot=1**

This statement tells the SuperDAT utility to restart the target computer if it must do so in order to finish updating or upgrading your anti-virus software. If you do not want the target computer to restart after it updates your files, set the value of `bReboot=` to zero, or remove the statement from SETUP.ISS.

If you do not tell the SuperDAT utility to restart the target computer, either with this statement in the SETUP.ISS file, from the command line, or in an update script, it will *not* do so under any circumstances. VirusScan software does not require you to restart your system after you upgrade your engine files or update your .DAT files.

- **bPrompt=1**

This tells the SuperDAT utility to display only the Shut Down Windows dialog box when it has updated or upgraded your software.

- **szLogFile=<PATH\FILENAME>**

This option tells the SuperDAT utility to save a log file with the file name you specify and in the location you specify. By default, the SuperDAT utility creates a log file in the current working directory.

When you have placed the PKGDESC.INI file, the SETUP.EXE file, and any SETUP.ISS file you want to use on a central server, configure the AutoUpgrade utility copies on your workstation computers to download new files from the share you created on that central server. The AutoUpgrade utilities will download and install the new files from this package.

To learn more about how the SuperDAT utility works, download the *SuperDAT User's Guide* from the McAfee website at:

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

Otherwise, consult the README.TXT file that comes with each weekly SuperDAT release.


Deploying an EXTRA.DAT file

The McAfee AVERT research organization will sometimes provide EXTRA.DAT files to combat high-risk viruses between regular .DAT and SuperDAT releases. In ordinary circumstances, McAfee researchers publish these files when they determine that these situations warrant one:

- A virus presents a “medium on-watch” or “high” risk threat of infection. To learn about what constitutes a medium on-watch or high risk, or about McAfee AVERT risk assessment in general, visit the AVERT website at:

http://www.mcafeeb2b.com/asp_set/anti_virus/alerts/ara.asp

- A high-prevalence virus threatens an outbreak situation

 **IMPORTANT:** AVERT does *not* guarantee that it will make EXTRA.DAT files available in all such situations. AVERT researchers reserve the right to assess each situation and determine an appropriate course of action.

When AVERT does publish an EXTRA.DAT file, it will announce its availability—and a location where you can download the file—when it publishes a virus alert for a medium on-watch or high-risk virus. If you subscribe to the Enterprise SecureCast update service, you can receive all such alert messages if you wish. To learn more, see [Appendix D, “Using the SecureCast Service to Get New Data Files.”](#)

Once you download an EXTRA.DAT file, you need only copy the file to a particular directory to have VirusScan software use it immediately. Each time you start a scan session or a VirusScan application scan operation, the software checks to see if you have an EXTRA.DAT file located in the correct directory. If such a file exists, the software will add the EXTRA.DAT virus definitions to those in its other .DAT files automatically.

For VirusScan v4.5 and later releases, copy any EXTRA.DAT files you download to this directory:

C:\Program Files\Common Files\Network Associates\VirusScan Engine
\4.0.xx

Understanding the VirusScan control panel

The VirusScan control panel serves as the graphical front end for the VirusScan management service, which initiates and controls all top-level component processes, including the VirusScan application, the Console, and the VShield scanner. The VirusScan management service also provides a common memory structure for all VirusScan components, which allows the components to share data between themselves, and to act on that data.

In practical terms, you can use the control panel to:

- start and stop all VirusScan components with a single button
- tell the VShield scanner and VirusScan Console to load as soon as your computer starts
- set a ceiling for the number of scan targets the VirusScan application can examine or exclude during a scan session
- limit the number of scan tasks that you can create, configure, and run from the VirusScan Console

You can also choose whether you want to have the VirusScan management service load itself when your computer starts.


-
- ☐ **NOTE:** McAfee strongly recommends that you set the VirusScan management service to load at startup. If you do not, you might not be able to start some VirusScan components, and you will lose the benefit of data sharing between components.
-

Opening the VirusScan control panel

The VirusScan control panel operates much as a standard Windows control panel does.

To open the control panel, follow these steps:

1. Click **Start** in the Windows taskbar, point to **Settings**, then choose **Control Panel**.

2. Locate and double-click the VirusScan control panel icon  to open the control panel itself.

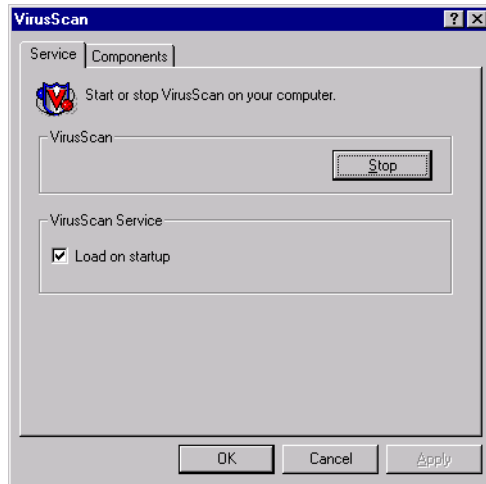


Figure A-1. VirusScan control panel - Service page

Choosing VirusScan control panel options

The control panel consists of two tabbed property pages that set out its options.

To choose your options, follow these steps:

1. Open the control panel, then click the Service tab.
2. To stop all active VirusScan components, click **Stop**.

If all VirusScan components that normally load into memory—the Console and the VShield scanner, normally—are inactive, this button will read **Start**. Click it to reload inactive VirusScan components.

You can also restart the VirusScan application and the Console individually from the Windows **Start** menu.

3. Select the **Load on startup** checkbox in the VirusScan Service area to start the VirusScan management service (AVSYNMGR.EXE) as soon as you start your computer.

The management service oversees all communications between VirusScan program components, determines which components must load to accomplish program tasks, and allows you to start or stop all program components at once.

If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, this service appears in the Services dialog box as AvSync Manager. If your computer runs Windows 95 or Windows 98, this service is not directly accessible.

-
- ☐ **NOTE:** McAfee strongly recommends that you set the VirusScan management service to load at startup. If you do not, you might not be able to start some VirusScan components, and you will lose the benefit of data sharing between components.
-

4. Click the Components tab to continue.

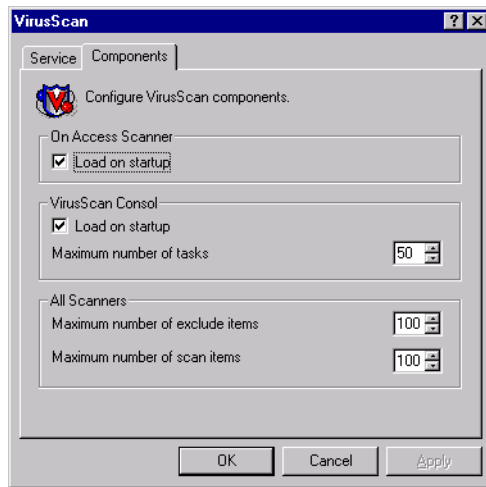



Figure A-2. VirusScan control panel - Components page

5. To have the VShield scanner load when you start your computer, select the **Load VShield on startup** checkbox. This same setting appears in the System Scan module's Detection page. Either setting will load the scanner when you start your computer.

-
- ☐ **NOTE:** McAfee recommends that you leave this checkbox selected. The VShield scanner is your best continuous defense against virus infections.
-

6. Click  or enter a figure in the Exclude Items text box to specify how many items can appear in the VShield System Scan module's exclusion list. This setting also determines how many items can appear in the exclusion list for any VirusScan application scan task or any scan task you configure from within the VirusScan Console.


By default, 100 items can appear in the list. You may not set the value here to fewer than five items.

7. Click  or enter a figure in the Scan Items text box to specify how many targets the VirusScan application can examine at one time.

This setting sets a maximum number of items that can appear as scan targets for any default scan task-or any task you configure-from within the VirusScan Console. By default, 100 items can appear in the list. If you add more than 100 unique items to the exclusion list, the VirusScan application might affect your system performance. You may not set the value here to fewer than five items.


8. Select the **Load on startup** checkbox in the Console area to have the VirusScan Console start as soon as you start your computer.

The Console must be running in order to execute any tasks you have scheduled, including scan tasks, AutoUpgrade tasks, and AutoUpdate tasks. You do not need to start the Console to start the VShield scanner, however.

9. Click  or enter a figure in the Maximum Number of Tasks text box how many scan tasks can appear in the VirusScan Console window.

By default, 50 items can appear in the list. If you add more than 50 items, task execution might affect your system performance. You may not set the value here to fewer than five items.

10. Click **Apply** to save the changes you make to these settings without closing the control panel. Click **OK** to save your changes and close the control panel. Click **Cancel** to close the control panel without saving your changes.

 **NOTE:** The VirusScan management service must restart itself and all active VirusScan components in order to implement any changes you make.

What’s in this appendix?

The VirusScan installation procedure places essential program files on the VirusScan client workstation. This section provides an overview of the files installed. Some of the files are associated with a particular component while others are in common use, called by program functions as needed.

VShield scanner

The VShield scanner runs as a Windows NT service on Windows NT and Windows 2000 systems, and as a virtual device driver on Windows 95 and Windows 98 systems. It requires a number of support files to function, including some that enable its various modules. This table lists VShield scanner and related files:

Program files

These files run directly as VShield components or are dedicated VShield library or support files.

Table B-1. VShield scanner program files

File	Function	Location
VSTAT.EXE	Handles program communication among VShield components, displays VShield icon	C:\Program Files\Network Associates\VirusScan
VSCONFIG.EXE	Configures VShield settings, displays the VShield Properties dialog box	C:\Program Files\Network Associates\VirusScan
MFLDR.DLL	Library file for use with MessagingApplication Programming Interface (MAPI) e-mail systems; handles access and export functions	C:\Program Files\Network Associates\VirusScan

Table B-1. VShield scanner program files

CONFWIZ.EXE	VShield configuration wizard file	C:\Program Files\Network Associates\VirusScan
VSHWIN32.EXE	Communicates between VSSTAT.EXE and the VShield System Scan module	C:\Program Files\Network Associates\VirusScan
MCSHIELD.EXE	System Scan module. Runs as a Windows NT Service on Windows NT and Windows 2000 systems	C:\Program Files\Common Files\Network Associates\McShield
NAIEVENT.DLL	Event logging resource. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Common Files\Network Associates\McShield
MCSHIELD.DLL	Resource file for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Common Files\Network Associates\McShield\Res09
NAIANN.DLL	Support file for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Common Files\Network Associates\McShield
NAIFILTR.SYS	Filter driver for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Common Files\Network Associates\McShield
NAIFSREC.SYS	File system redirector for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Winnt\System32\drivers

Table B-1. VShield scanner program files

NTCLIENT.DLL	Support file for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Network Associates\VirusScan
SCANSERV.DLL	Support file for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Common Files\Network Associates\McShield
VSHIELD.VXD	VShield System Scan module. Runs as a Windows virtual device driver only on Windows 95 and Windows 98 systems	C:\Windows\System
VSHINIT.VXD	VShield support file. Initializes services for DOS protected-mode interface. Runs only on Windows 95 and Windows 98 systems	C:\Windows\System
MCSCAN32.VXD	McAfee scan engine. Runs only on Windows 95 and Windows 98 systems	C:\Windows\System
MCUTIL.VXD	Support file for System Scan module. Runs only on Windows 95 and Windows 98 systems	C:\Windows\System
MCKRNL.VXD	Support file for System Scan module. Runs only on Windows 95 and Windows 98 systems	C:\Windows\System

Table B-1. VShield scanner program files

EMALSCAN.DLL	Scans e-mail you receive from the Internet or from your network via Messaging Application Programming Interface (MAPI) e-mail systems	C:\Program Files\Network Associates\VirusScan
CCM_SCAN.EXE	Scans e-mail you receive via Lotus cc:Mail v7.x and earlier cc:Mail systems	C:\Program Files\Network Associates\VirusScan
WEBSCANX.EXE	Provides functionality for VShield Download Scan and Internet Filter modules. Initializes WBHOOK32.DLL	C:\Program Files\Network Associates\VirusScan
WBHOOK32.DLL	Provides functionality for VShield Download Scan, and Internet Filter modules. Intercepts files downloaded through web browsers for scan engine to examine	C:\Program Files\Network Associates\VirusScan

Dependent files

VShield requires these files to run, but these are not VShield program files, or are not dedicated solely to VShield support.

Table B-2. VShield scanner dependent files

File	Function	Location
AVSYNMGR.EXE	VirusScan management service. Initializes, starts and stops all VirusScan services and components. Must run to enable all VirusScan components.	C:\Program Files\Network Associates\VirusScan
AVSYNCH.DLL	Handles inter-component communication through shared memory	C:\Program Files\Network Associates\VirusScan
SYNCUTIL.DLL	Stores data shared between components	C:\Program Files\Network Associates\VirusScan
VSUTIL.DLL	Provides common utilities for components	C:\Program Files\Network Associates\VirusScan
AVSMCPA.CPL	VirusScan control panel applet	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	Resource file for all components	C:\Program Files\Common Files\Network Associates\McPal
MCSCAN32.DLL	McAfee Scan engine file	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS16.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS32.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates VirusScan Engine\4.0.xx
MESSAGES.DAT	Support file for scan engine. Provides virus detection messages to engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

Temporary files

The VShield scanner and its related files use these files as “memory maps” to store configuration options copied from the Windows registry when the program runs. These files start out with a standard file size and minimal data, and grow or shrink as necessary to accommodate configuration data.

Table B-3. VShield scanner temporary files

File	Function	Location
SYNC_MAP.MMF	Memory map file for AVSYNCH.DLL	C:\Program Files\Network Associates\VirusScan
AVCONSOLE.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_CONS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_SCAN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DEXCLDEF.MFF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DSCANDEF.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DVS_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANGEN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANOAS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANODS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan

Dependent and related files for the VirusScan application

The VirusScan application runs as a stand-alone executable file that you can start yourself, or that the VirusScan Scheduler can start according to a schedule you set. The application requires a number of support files to function, including some related to the McAfee scan engine. This table lists VirusScan application and related files:

Program files

These files run directly as VirusScan application files or are dedicated VirusScan application library or support files

Table B-4. VirusScan application program files

File	Function	Location
SCAN32.EXE	VirusScan application executable file. Runs in all Windows 32-bit environments	C:\Program Files\Network Associates\VirusScan
ADVGUI.DLL	VirusScan application library file. Provides user interface elements for the VirusScan Advanced interface	C:\Program Files\Network Associates\VirusScan

Dependent files

The VirusScan application requires these files to run at various points during its operation, but these are not VirusScan application program files, or are not dedicated solely to VirusScan application support.

Table B-5. VirusScan application dependent files

File	Function	Location
AVSYNMGR.EXE	VirusScan management service. Initializes, starts and stops all VirusScan services and components. Must run to enable all VirusScan components.	C:\Program Files\Network Associates\VirusScan
AVSYNCH.DLL	Handles inter-component communication through shared memory	C:\Program Files\Network Associates\VirusScan
SYNCUTIL.DLL	Stores data shared between components	C:\Program Files\Network Associates\VirusScan
VSUTIL.DLL	Provides common utilities for components	C:\Program Files\Network Associates\VirusScan
AVSMCPA.CPL	VirusScan control panel applet	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	Resource file for all VirusScan components	C:\Program Files\Common Files\Network Associates\McPal
MCSCAN32.DLL	McAfee Scan engine file	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS16.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS32.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

Table B-5. VirusScan application dependent files

MESSAGES.DAT	Support file for scan engine. Provides virus detection messages to engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
S95EXT.DLL	Shell extension file. Allows you to right-click .VSC settings files you saved and start scan operations or view scan task properties.	C:\Program Files\Network Associates\VirusScan

Temporary files

The VirusScan application and its related files use these files as “memory maps” to store configuration options copied from the Windows registry when the program runs. These files start out with a standard file size and minimal data, and grow or shrink as necessary to accommodate configuration data.

Table B-6. VirusScan application temporary files

File	Function	Location
SYNC_MAP.MMF	Memory map file for AVSYNCH.DLL	C:\Program Files\Network Associates\VirusScan
AVCONSOLE.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_CONS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_SCAN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DEXCLDEF.MFF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DSCANDEF.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DVS_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANGEN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan

Table B-6. VirusScan application temporary files

VSCANOAS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANODS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan

Alert Manager

The Alert Manager client configuration utility requires these files to run.

Table B-7. Alert Manager files

File	Function	Location
ADSLOOKUP.DLL	Library file. Allows client utility to locate Alert Manager server through Microsoft Active Directory services	C:\Program Files\Common Files\Network Associates\McPal
AMG.MIF	Management Information File for use with Desktop Management Interface client application software	C:\Program Files\Common Files\Network Associates\McPal
NAARCHIV.DLL	Library file for VirusScan data compression routines	C:\Program Files\Common Files\Network Associates\McPal
NAEVENT.DLL	Library file. Handles event processing from desktop client anti-virus software to Alert Manager utility and McAfee ePolicy Orchestrator software	C:\Program Files\Common Files\Network Associates\McPal
NAGUI32.DLL	Graphical library file for various VirusScan utilities	C:\Program Files\Common Files\Network Associates\McPal

Table B-7. Alert Manager files

NAKRNL32.DLL	Library file for various VirusScan utilities	C:\Program Files\Common Files\Network Associates\McPal
NAUTIL32.DLL	Library file for various VirusScan utilities	C:\Program Files\Common Files\Network Associates\McPal

VirusScan control panel files

As the initial process for all VirusScan components, the VirusScan management service does not depend on other VirusScan components. It does depend on some Windows system components to run, however.

This table lists VirusScan control panel files and points to where you can find them.

Table B-8. VirusScan control panel files

File	Function	Location
AVSYNMGR.EXE	The VirusScan management service. Initializes, starts and stops all VirusScan services and components. Must run to enable all VirusScan components.	C:\Program Files\Network Associates\VirusScan
AVSYNCH.DLL	Handles inter-component communication through shared memory	C:\Program Files\Network Associates\VirusScan
SYNCUTIL.DLL	Stores data shared between components	C:\Program Files\Network Associates\VirusScan
VSUTIL.DLL	Provides common utilities for components	C:\Program Files\Network Associates\VirusScan
AVSMCPA.CPL	VirusScan control panel applet	C:\Windows\System or C:\Winnt\System 32

Temporary files

The VirusScan control panel and its related files use these files as “memory maps” to store configuration options copied from the Windows registry when the program runs. These files start out with a standard file size and minimal data, and grow or shrink as necessary to accommodate configuration data.

Table B-9. VirusScan control panel temporary files

File	Function	Location
SYNC_MAP.MMF	Memory map file for AVSYNCH.DLL	C:\Program Files\Network Associates\VirusScan
AVCONSOLE.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_CONS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_SCAN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DEXCLDEF.MFF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DSCANDEF.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DVS_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANGEN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANOAS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANODS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan

ScreenScan

The ScreenScan utility runs as an executable file that starts whenever your screen saver runs. The utility requires a number of support files to function, including some related to the McAfee scan engine. This table lists ScreenScan utility and related files:

Program files

These files run directly as ScreenScan files or are dedicated ScreenScan library or support files

Table B-10. ScreenScan program files

File	Function	Location
SCRSCAN.EXE	ScreenScan utility executable file. Runs the actual scan operation	C:\Program Files\Network Associates\VirusScan
SCRSCANP.DLL	ScreenScan control panel extension. Provides the ScreenScan configuration property page in the Windows Display Properties dialog box	C:\Program Files\Network Associates\VirusScan

Dependent files

The ScreenScan utility requires these files to run at various points during its operation, but these are not ScreenScan program files, or are not dedicated solely to ScreenScan utility support.

Table B-11. ScreenScan dependent files

File	Function	Location
RESDLL.DLL	Resource file for all VirusScan components	C:\Program Files\Common Files\Network Associates \McPal
MCSCAN32.DLL	McAfee Scan engine file	C:\Program Files\Common Files\Network Associates \VirusScan Engine\4.0.xx
RWABS16.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates \VirusScan Engine\4.0.xx
RWABS32.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates \VirusScan Engine\4.0.xx
MESSAGES.DAT	Support file for scan engine. Provides virus detection messages to engine	C:\Program Files\Common Files\Network Associates \VirusScan Engine\4.0.xx

VirusScan Emergency Disk files

The Emergency Disk wizard will copy files you need to start your computer and scan your hard disk for boot-sector viruses. These files include a reduced-footprint command line scanner, a set of emergency virus definition (.DAT) files, and boot files that enable you to start your computer from the Emergency Disk.

This table lists the files that appear on the Emergency Disk when you create it:

Table B-12. VirusScan Emergency Disk files

File	Function	Location
AUTOEXEC.BAT	MS-DOS batch file. This file leads you through an immediate scan operation, as soon as the Emergency Disk finishes starting your computer	A:\
BIOS.SYS	System file	A:\
BOOTSCAN.EXE	McAfee command-line scanner. This file conducts the scan operation on your hard disk	A:\
CLEAN.DAT	McAfee virus definition file. This file is a smaller, specialized version of the CLEAN.DAT file that other VirusScan components use. You may <i>not</i> use a CLEAN.DAT file from the VirusScan program directory for the Emergency Disk.	A:\
COMMAND.COM	Command interpreter. This file is a command shell that responds to command-line input	A:\

Table B-12. VirusScan Emergency Disk files

GETREPLY.EXE	Application file. This file processes output from the scan operation	A:\
KERNEL.SYS	System file	A:\
LICENSE.DAT	McAfee License file. The command-line scanner uses this to track use eligibility for this product	A:\
MESSAGES.DAT	McAfee resource file. This file stores application messages for use during scan operations	A:\
NAMES.DAT	McAfee virus definition file. This file is a smaller, specialized version of the NAMES.DAT file that other VirusScan components use. You may not use a NAMES.DAT file from the VirusScan program directory for the Emergency Disk	A:\
SCAN.DAT	McAfee virus definition file. This file is a smaller, specialized version of the NAMES.DAT file that other VirusScan components use. You may not use a NAMES.DAT file from the VirusScan program directory for the Emergency Disk	A:\

Dependent and related files for the E-Mail Scan extension

The E-Mail Scan extension runs as an add-in to your MAPI e-mail system. If you use a Microsoft Exchange or Outlook client, the extension loads into the client application and appears as menu items in the **Tools** menu and as buttons in the application toolbar. You can use the extension to run scan operations whenever you wish. The extension requires a number of support files to function, including some related to the McAfee scan engine. This table lists extension and related files:

Program files

Table B-13. E-Mail Scan program files

File	Function	Location
EMALSCAN.DLL	Scans e-mail on your Microsoft Exchange server or other Messaging Application Programming Interface (MAPI) e-mail system. This file runs as an Exchange or Outlook extension that loads into the e-mail client application. This same file provides scan services for the VShield E-Mail Scan module.	C:\Program Files\Network Associates\VirusScan

Dependent files

The E-Mail Scan extension requires these files to run at various points, but these are not extension files, or are not dedicated solely to support the E-Mail Scan extension.

Table B-14. E-Mail Scan dependent files

File	Function	Location
AVSYNMGR.EXE	VirusScan management service. Initializes, starts and stops all VirusScan services and components. Must run to enable all VirusScan components.	C:\Program Files\Network Associates\VirusScan
AVSYNCH.DLL	Handles inter-component communication through shared memory.	C:\Program Files\Network Associates\VirusScan
SYNCUTIL.DLL	Stores data shared between components.	C:\Program Files\Network Associates\VirusScan
VSUTIL.DLL	Provides common utilities for components.	C:\Program Files\Network Associates\VirusScan
AVSMCPA.CPL	VirusScan control panel applet.	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	Resource file for all VirusScan components.	C:\Program Files\Common Files\Network Associates\McPal
MCSCAN32.DLL	McAfee Scan engine file.	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS16.DLL	Support file for scan engine.	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS32.DLL	Support file for scan engine.	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
MESSAGES.DAT	Support file for scan engine. Provides virus detection messages to engine.	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

Temporary files

The E-Mail Scan extension and its related files use the files listed in this table as “memory maps” to store configuration options copied from the Windows registry when the program runs. These files start out with a standard file size and minimal data, and grow or shrink as necessary to accommodate configuration data.

Table B-15. E-Mail Scan temporary files

File	Function	Location
SYNC_MAP.MMF	Memory map file for AVSYNCH.DLL	C:\Program Files\Network Associates\VirusScan
AVCONSOLE.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_CONS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DAV_SCAN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DEXCLDEF.MFF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DSCANDEF.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DVS_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANGEN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANOAS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANODS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan

Using VirusScan Command-line Options



Adding advanced VirusScan engine options

The following table lists all of the command-line options that can be communicated directly to the scanning engine via the Advanced Scan Settings dialog box provided by most Detection property pages. These command-line options (that you specify in the Advanced Scan Settings dialog box), will supplement, and can overwrite, the options selected in the VShield and VirusScan Detection property pages.

For additional information about adding advanced engine options:

- for VShield, see “Using the VShield scanner,” in Chapter 4 of your *VirusScan User’s Guide*.
- for VirusScan software, see “Using the VirusScan application,” in Chapter 5 of your *VirusScan User’s Guide*, or “Creating and Configuring Scheduled Tasks,” in Chapter 6 of your *VirusScan User’s Guide*.

Running the VirusScan Command Line program

A typical installation of VirusScan software includes the VirusScan Command Line program. You can run VirusScan Command Line either from a Windows MS-DOS Prompt window, or by restarting your computer in DOS mode. Network Associates recommends restarting in DOS mode for best results. To learn how to restart your computer in DOS mode, see your Microsoft Windows documentation. To run the program, change to the directory in which the file SCAN.EXE is located, and type `scan` followed by the scanning options you want to use (see [Table C-1, “VirusScan command-line scanner options,”](#) on page 156 for details).

To run the VirusScan Command Line program, follow these steps:

1. Open an MS-DOS Prompt window from within Windows, or restart your computer in DOS mode.
2. Change to the VirusScan program directory, in which the file SCAN.EXE is located. If you installed VirusScan with its default options, type this line at your command prompt to locate the correct directory:

```
C:\progra~1\networ~1\virus~1
```

3. Type `scan`, followed by the scan options you want to use, at the command prompt.

VirusScan Command Line will start immediately and begin scanning your system with the options you choose. When it has finished, it will display the results of its scan operation, then return to the command prompt.

4. To run another scan operation, repeat [Step 3](#). To close the MS-DOS Prompt window, type `exit` at the command prompt. If you restarted your computer in DOS mode, type `win` to start Windows, or restart your computer as you would normally.

The tables on the following pages list all of the VirusScan options available.

- ❏ **NOTE:** When you specify a file name as part of a command-line option, you must include the full path to the file if it is not located in the VirusScan program directory.

The following table lists the options that can be added to the `SCAN` command.

Table C-1. VirusScan command-line scanner options

Command-line Option	Limitations	Description
<code>/?</code> or <code>/HELP</code>	None	Displays a list of VirusScan command-line options, each with a brief description.
<code>/ADL</code>	On-demand scanning only	Scan all local drives—including compressed drives and PC cards, but not disks—in addition to any other drive specified on the command line. To scan both local and network drives, use the <code>/ADL</code> and <code>/ADN</code> commands together in the same command line. OS/2: <code>/ADL</code> includes the CD-ROM drive in the scan, when used with <code>/NODDA</code> .
<code>/ADN</code>	On-demand scanning only	Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command line. To scan both local drives and network drives, use the <code>/ADL</code> and <code>/ADN</code> commands together in the same command line.
<code>/ALERTPATH <dir></code>	On-demand scanning only	Designates the directory <code><dir></code> as a network path for Centralized Alerting alert messages.

Table C-1. VirusScan command-line scanner options

/ALL	On-demand scanning only	<p>Overrides the default scan setting by scanning all infectable files—regardless of extension.</p> <p>Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect that you have one.</p>
/ANALYZE	On-demand scanning only	Sets scanner to use its full heuristics, both program and macro.
	Extended memory required.	<p>/MANALYZE targets macro viruses only.</p> <p>/PANALYZE targets program viruses only.</p>
/ANYACCESS	On-access scanning only	<p>Scans:</p> <ul style="list-style-type: none"> • the boot sector whenever a disk is either read or written to • executables • any newly created files
/APPEND	On-demand scanning only	Used with /REPORT to append report message text to the specified report file instead of overwriting it.
/BOOT	On-demand scanning only	Scan boot sector and master boot record only.
/BOOTACCESS	On-access scanning only	Scans a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/CLEAN	On-demand scanning only	Clean viruses from all infected files and system areas.
/CLEANDOCALL	On-demand scanning only	<p>As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents.</p> <p>This option deletes all macros, including macros not infected by a virus.</p>
/CONTACT <message>	On-access scanning only	Displays specified message when a virus is detected. This message cannot exceed 255 characters.

Table C-1. VirusScan command-line scanner options

<code>/CONTACTFILE <filename></code>	None	<p>Display the contents of <filename> when a virus is found. Use this to provide contact information and instructions to the user when the scanner finds a virus.</p> <p>This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation.</p> <p>Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/) or a hyphen (-) should be placed in quotation marks.</p>
<code>/DEL</code>	On-demand scanning only	<p>Deletes infected files permanently.</p>
<code>/EXCLUDE <filename></code>	On-demand scanning only	<p>Do not scan or add validation codes to the files listed in <filename>.</p> <p>Use this option to exclude specific files from a scan operation. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?</p>
<code>/FILEACCESS</code>	On-access scanning only	<p>Scans executable files when you modify them in any way, including executing them.</p> <p>This scan operation will not check the boot sector.</p>
<code>/FREQUENCY <n></code>	On-demand scanning only	<p>Do not scan <n> hours after the previous scan operation.</p> <p>In environments where the risk of viral infection is very low, use this option to prevent unnecessary scan operations.</p> <p>Note that the greater the scan frequency, the greater your protection against infection.</p>
<code>/HELP or /?</code>	None	<p>Displays a list of VirusScan scanner command-line options, each with a brief description.</p>
<code>/IGNORE <drive(s)></code>	On-access scanning only	<p>Does not check any files loaded from the specified drive(s).</p>
<code>/LOAD <filename></code>	On-demand scanning only	<p>Load scanning options from the named file.</p> <p>Use this option to perform a scan you've already configured by loading custom settings saved in an ASCII-formatted file.</p>

Table C-1. VirusScan command-line scanner options

/LOCK	Not available in low-memory environments	<p>With this /LOCK option enabled, VirusScan will halt and lock your system if it finds a virus.</p> <p>/LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs.</p> <p>McAfee recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system.</p>
/MANALYZE	On-demand scanning only Extended memory required	<p>Sets the scanner's heuristic scanning features to target macro viruses only.</p> <p>/PANALYZE targets program viruses only.</p> <p>/ANALYZE targets both program and macro viruses.</p>
/MANY	On-demand scanning only	<p>Scans multiple disks consecutively in a single drive. The scanner will prompt you for each disk.</p> <p>Use this option to check multiple floppy disks quickly.</p> <p>You cannot use the /MANY option if you run the scanner from a boot disk and you have only one floppy drive.</p>
/MAXFILESIZE <xxx.x>	On-demand scanning only	Scan only files no larger than <xxx.x> megabytes.
/MEMEXCL	On-demand scanning only Not available for Windows	Excludes the memory address A0000:0000 from scanning.
/MOVE <dir> or *.???	On-demand scanning only	<p>/MOVE <directory>:</p> <p>Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure.</p> <p>This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.</p> <p>/MOVE*.???:</p> <p>The scanner will change the extension of infected files, but not move them. For example, using the /MOVE*.BAD option will result in any infected files being simply renamed with the extension .BAD but not physically moved.</p>
/NOBEEP	On-demand scanning only	Disables the tone that sounds whenever the scanner finds a virus.

Table C-1. VirusScan command-line scanner options

/NOBREAK	On-demand scanning only	<p>Disables CTRL-C and CTRL-BREAK during scans.</p> <p>Users will not be able to halt scans in progress with /NOBREAK in use.</p> <p>Use this option with /LOG to create a meaningful audit trail of regularly scheduled scans.</p>
/NOCOMP	On-demand scanning only Extended memory required.	<p>Skips checking of compressed executables created with the LZEXE or PkLite file compression programs.</p> <p>This reduces scanning time when you do not need to run a full operation. Otherwise, by default, the scanner checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for virus signatures.</p> <p>The scanner will still check for modifications to compressed executables if they contain VirusScan validation codes.</p>
/NODDA	On-demand scanning only	<p>No direct disk access. This prevents the scanner from examining the boot record.</p> <p>This feature has been added to allow the scanner to run under Windows NT.</p> <p>You might need to use this option on some device-driven drives.</p> <p>Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.</p>
/NODISK	On-access scanning only	Does not scan boot sector while loading the VShield scanner.
/NODOC	On-demand scanning only	Does not scan Microsoft Office files.
/NOEMS	On-access scanning only	Keeps the VShield scanner from using extended memory (XMS).
/NOEXPIRE	On-demand scanning only	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMEM	None	<p>Does not scan memory for viruses.</p> <p>This greatly reduces scan time.</p> <p>Use /NOMEM only when you are absolutely certain that your computer is virus-free.</p>

Table C-1. VirusScan command-line scanner options

/NOREMOVE	On-access scanning only	Prevents users from removing the VShield scanner from memory with the /REMOVE switch.
/NOWARMBOOT	On-access scanning only	Does not check the disk boot sector of the floppy disk in drive A: for viruses during warm boot (system reset or CTRL+ALT+DEL).
/NOXMS	On-access scanning only	Does not use extended memory (XMS).
/ONLY <drive(s)>	On-access scanning only	Checks only files loaded from the specified drive(s).
/PANALYZE	On-demand scanning only	Sets the VirusScan scanner to use program heuristics.
	Extended memory required	/MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.
/PAUSE	On-demand scanning only	Enables screen pause.
		The <code>Press any key to continue</code> prompt will appear when the scanner fills a screen with messages. Otherwise, by default, the scanner fills and scrolls a screen continuously without stopping, which allows it to run on PCs with multiple drives or that have severe infections, without needing your input. McAfee recommends omitting /PAUSE when using the report options (/REPORT, /RPTCOR, and /RPTERR)
/PLAD	On-demand scanning only	Preserves the last access dates on Novell NetWare drives.
		Normally, proprietary network drives update the last access date when the scanner opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning
/RECONNECT	On-access scanning only	Restores the VShield scanner after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	On-access scanning only	Unloads the VShield scanner from memory.

Table C-1. VirusScan command-line scanner options

<code>/REPORT <filename></code>	On-demand scanning only	<p>Creates a report of infected files and system errors, and saves the data to <filename> in ASCII text file format.</p> <p>If <filename> already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: The scanner will instead add report information to the end of the file, instead of overwriting it.</p> <p>You can also use /RPTALL, /RPTCOR, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report.</p> <p>You can include the destination drive and directory (such as D:\VSREPT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive.</p> <p>McAfee recommends omitting /PAUSE when using any report option.</p>
<code>/RPTALL</code>	On-demand scanning only	<p>Include all scanned files in the /REPORT file.</p> <p>When used with /REPORT, this option adds the names of corrupted files to the report file.</p> <p>McAfee recommends omitting /PAUSE when using any report option.</p>
<code>/RPTERR</code>	On-demand scanning only	<p>Include errors in /REPORT file.</p> <p>When used with /REPORT, this option adds a list of system errors to the report file.</p> <p>/LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs.</p> <p>System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.</p> <p>McAfee recommends omitting /PAUSE when using any report option.</p>
<code>/SAVE</code>	On-access scanning only	<p>Saves the command-line options to the VSHIELD.INI file.</p>

Table C-1. VirusScan command-line scanner options

/SUB	On-demand scanning only	<p>Scans subdirectories inside a directory.</p> <ul style="list-style-type: none"> • By default, when you specify a directory to scan rather than a drive, the scanner will examine only the files it contains, not its subdirectories. • Use /SUB to scan all subdirectories within any directories you have specified. • It is not necessary to use /SUB if you are scanning an entire drive.
/UNZIP	On-demand scanning only Extended memory required	Scan inside compressed files.
/VIRLIST	On-demand scanning only	<p>Displays the name and a brief description of each virus that the scanner detects.</p> <p>You may use the /PAUSE option on the same command line as /VIRLIST to read the virus list one screen at a time.</p> <p>To redirect the /VIRLIST output to a text file:</p> <p>At the command prompt, type</p> <pre>scan /VIRLIST <filename>.txt</pre> <p>Because the scanner can detect many viruses, this file will be over 250 pages long. This is too large for the MS-DOS Edit program to open; McAfee recommends using Notepad or another text editor to open the virus list.</p>
/XMSDATA	On-access scanning only	Loads VShield data files into XMS memory.

Running the on-demand scanner with command-line arguments

You can run the VirusScan on-demand scanner with command-line arguments either from a Windows MS-DOS Prompt window, or by restarting your computer in DOS mode. (You can also run the scanner without command-line arguments, either from a Windows MS-DOS Prompt window or from the **Start** menu's Run dialog box.) Network Associates recommends restarting in DOS mode for best results. To learn how to restart your computer in DOS mode, see your Microsoft Windows documentation. To run the program, change to the directory in which the file SCAN32.EXE is located, and type `scan32` followed by the scanning options you want to use (see [Table C-2, "SCAN32.EXE command-line options,"](#) on page 165 for details).

To run the VirusScan on-demand scanner, follow these steps:

1. Open an MS-DOS Prompt window from within Windows, or restart your computer in DOS mode.
2. Change to the VirusScan program directory, in which the file SCAN32.EXE is located. If you installed VirusScan with its default options, type this line at your command prompt to locate the correct directory:

```
C:\progra~1\networ~1\virus~1
```

3. Type `scan32`, followed by the scan options you want to use, at the command prompt.

The VirusScan on-demand scanner will start immediately and begin scanning your system with the options you choose. When it has finished, it will display the results of its scan operation, then return to the command prompt.

4. To run another scan operation, repeat [Step 3](#). To close the MS-DOS Prompt window, type `exit` at the command prompt. If you restarted your computer in DOS mode, type `win` to start Windows, or restart your computer as you would normally.

The following table lists the arguments that can be added to the SCAN32 command.

Table C-2. SCAN32.EXE command-line options

Option	Use
/SPLASH	This option tells the VirusScan application to display its identity or “splash” screen when it starts.
/NOSPLASH	This option tells the VirusScan application to hide its identity or “splash” screen when it starts.
/AUTOSCAN	This option tells the VirusScan application to run a scan operation immediately, with the configuration options currently set, and without further user interaction. To have the application begin scanning immediately, you must start it with either the /UIEXONLY or the /UINONE options on the same command line. If you start it with the /UICONFIG option, you must click the Scan Now button in the application window to begin the scan operation.
/NOAUTOSCAN	<p>This option tells the VirusScan application not to start its scan operation automatically. Instead, depending on the user-interface options you’ve entered on the command line, the application window will open for you to set configuration options.</p> <ul style="list-style-type: none"> • If you set the user-interface option to /UICONFIG, the application will default to /NOAUTOSCAN. • If you set the user-interface option to /UINONE, the application will run with /AUTOSCAN enabled. Enter NOAUTOSCAN to suppress this behavior. • If you set the user-interface option to /UIEXONLY, the application will run with /AUTOSCAN enabled. Enter NOAUTOSCAN to suppress this behavior.
/AUTOEXIT	This option tells the VirusScan application to quit as soon as it completes a scan operation during which it finds no viruses.
/NOAUTOEXIT	This option tells the VirusScan application not to quit after a scan operation in which it finds no viruses. Instead, the VirusScan application window will remain open if you have told the application to run with it open.
/ALWAYSEXIT	This option tells the VirusScan application to quit immediately after it completes a scan operation, whether it found a virus, encountered an error, or finished without incident.
/NOALWAYSEXIT	This tells the VirusScan application not to quit immediately after it completes a scan operation. Instead, any other command-line options you’ve chosen will determine what it does when it finishes.

Table C-2. SCAN32.EXE command-line options

/UICONFIG	<p>This option tells the VirusScan application to open its main window and await configuration option changes. To start a scan operation after you change configuration options, click the Scan Now button in the application window.</p> <p>Setting this option will disable the /AUTOSCAN option if you use it in the same command line.</p>
/UIEXONLY	<p>This option prevents you from making changes to configuration options or scan targets you've set previously. Instead, it tells the VirusScan application to open its Scan Only window and begin a scan operation immediately.</p>
/UINONE	<p>This option tells the VirusScan application to run a scan task immediately with no visible interface. You must tell the application on the same command line which scan targets it must examine. Enter the drive designation, or a complete path to a file or directory you want it to scan.</p>
/SUB	<p>This option tells the VirusScan application to look for viruses in any subfolders inside the directory you specified as your scan target.</p> <p>Note: This option causes the application to scan only those files stored in the subfolders themselves. The application will not scan files stored at the root level of the folder you designate. To scan those files, run the application with the /NOSUB option.</p>
/NOSUB	<p>This option tells the VirusScan application not to look for viruses in any subfolders inside the directory you specified as your scan target.</p> <p>Note: This option causes the application to scan only those files stored at the root level of the folder you designate. The application will not scan files stored in any subfolder beneath that level. To scan those files, run the application with the /SUB option.</p>
/ALL	<p>This option tells the VirusScan application to scan all of the files stored on the drive or in the folder you specified as your scan target, whatever their extensions.</p>
/NOALL	<p>This option tells the VirusScan application to scan only those files stored on the drive or in the folder you specified as your scan target that have the extensions predefined in the application's default program extension list.</p> <p>Use the /EXT option to replace the default extension list with a set of extensions you specify on the same command line. Use the /DEFEXT option to supplement the default extension list with extensions you add on the same command line.</p>
/COMP	<p>This option tells the VirusScan application to scan files saved in compressed file archives. Examples of such archives include .ZIP, .CAB, .LZH, and .UUE files. This can slow down scan operations, but gives your system better protection.</p>

Table C-2. SCAN32.EXE command-line options

/NOCOMP	This option tells the VirusScan application not to scan any files in compressed file archives. This can speed up scan operations.
/CONTINUE	This option tells the VirusScan application to continue the scan operation automatically when it detects a virus.
/PROMPT	This option tells the VirusScan application to ask you what to do when it finds a virus. The application will display an alert message that gives you several options from which to choose.
/NOPROMPT	This option tells the VirusScan application not to ask what to do when it finds a virus. Instead, it will automatically take the actions you've specified elsewhere in the command line. You can specify these automatic responses: /CONTINUE, /CLEAN, /DELETE, /MOVE
/CLEAN	This option tells the VirusScan application to automatically clean any infected files it finds. The application "cleans" a file by removing virus code from it.
/DELETE	This option tells the VirusScan application to automatically delete any infected files it finds.
/MOVE	This option tells the VirusScan application to automatically move any infected files it finds to a predefined quarantine directory.
/BEEP	This option tells the VirusScan application to beep when it finds a virus. Your computer will play the default alert beep or .WAV file you've assigned.
/NOBEEP	This option tells the VirusScan application not to beep when it finds a virus. This option does not affect any other alert methods you've configured.
/RPTSIZE	This option tells the VirusScan application how large it can let the VSCLOG.TXT file get. You must specify a value, in kilobytes, on the same command line.
/BOOT	This option tells the VirusScan application to look for viruses in your hard disk's boot sector, or in the boot sector of any floppy disk you have in your drive.
/NOBOOT	This option tells the VirusScan application not to look for viruses in your hard disk boot sector or in the boot sectors of any floppy disk you have in your drive.
/EXT	This option tells the VirusScan application to replace the default program extension list it uses to narrow the scope of its scan operations with a list made up of the extensions you specify on the same command line. During the scan operation, the application will look for viruses only in files that have the extensions you specify.

Table C-2. SCAN32.EXE command-line options

/DEFEXT	This option tells the VirusScan application to add to its default program extension list those extensions you specify on the same command line. During the scan operation, the application will use the combined list to govern which files it examines.
/TASK	<p>This option tells the VirusScan application to start a specific task listed in the VirusScan Scheduler task list. You must specify an ID for the task you want to run on the same command line.</p> <p>To see the set of current task IDs available in the Scheduler, look in the Windows registry for this key:</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\VirusScan\AVConsole\ScanTasks</p> <p>That location lists each task available in the Scheduler by an item number. Within each item number folder, the Item_# of the registry key gives you the task ID number.</p>
/SERVER	This option tells the VirusScan application on which computer you want it to start or stop a scan task. Specify the computer name following the /SERVER option on the same command line.
/CANCEL	This option adjusts the Windows registry so that it correctly records that a task is no longer running. Use this option if your task fails, but the VirusScan Scheduler still shows it as running.
/LOG	<p>This option tells the VirusScan application to record its actions in a predefined log file. By default, that log file is VSCLOG.TXT, which you will find in the VirusScan program directory.</p> <p>The application records each action it takes as a single “event.” The information the application records depends on the type of event. If you tell the application to note whenever it deletes an infected file, it will record a “one” each time it does so. If you tell the application to note the date on which it started a scan operation, it will record the current date.</p>
/NOLOG	This option tells the VirusScan application not to record its actions in a log file.
/LOGALL	This option tells the VirusScan application to record an event in the log file each time it responds to a virus. The application will do so whenever it cleans, deletes, or moves a virus, or whenever it prompts you for a response.
/LOGDETECT	This option tells the VirusScan application to record an event in the log file each time it finds a virus.
/NOLOGDETECT	This option tells the VirusScan application to leave virus detection events out of the log file.
/LOGCLEAN	This option tells the VirusScan application to record an event in the log file each time it cleans, or fails to clean, an infected file.

Table C-2. SCAN32.EXE command-line options

/NOLOGCLEAN	This option tells the VirusScan application not to record an event when it cleans or fails to clean an infected file.
/LOGDELETE	This option tells the VirusScan application to record an event in the log file each time it deletes an infected file.
/NOLOGDELETE	This option tells the VirusScan application to leave virus deletion events out of the log file.
/LOGMOVE	This option tells the VirusScan application to record an event in the log file each time it moves an infected file to the quarantine folder.
/NOLOGMOVE	This option tells the VirusScan application not to record an event when it moves an infected file to a quarantine folder.
/LOGSETTINGS	This option tells the VirusScan application to record in the log file the current configuration options you've chosen for this task.
/NOLOGSETTINGS	This option tells the VirusScan application not to record the current task configuration options in the log file.
/LOGSUMMARY	This option tells the VirusScan application to summarize the results of all the events it has recorded for each virus detection and response event.
/NOLOGSUMMARY	This option tells the VirusScan application not to summarize the results of all the events it has recorded for each virus detection and response event.
/LOGDATETIME	This option tells the VirusScan application to note in the log file the date and the time at which it began the current scan operation.
/NOLOGDATETIME	This option tells the VirusScan application to leave the time when it began the current scan operation out of the log file.
/LOGUSER	This option tells the VirusScan application to note in the log file the name of the user logged into your computer at the time the scan task began.
/NOLOGUSER	This option tells the VirusScan to leave out of the log file the name of the user logged into your computer when the scan task began.
/PRIORITY	<p>This option tells VirusScan to give a higher or lower priority to this scan task relative to other system operations. You must specify a priority level within the range 1 to 5 on the same command line.</p> <p>A value of 1 assigns priority to all other system processes. A value of 5 assigns the highest priority to the scan task.</p>

Using the SecureCast Service to Get New Data Files



Introducing the SecureCast service

The Network Associates SecureCast service provides a convenient method you can use to receive the latest virus definition (.DAT) file updates automatically, as they become available, without your having to download them. The SecureCast service makes use of BackWeb “push” technology to send out new files, alert messages, and other information via the Enterprise SecureCast channel, to which you can subscribe when you register with Network Associates.

To use this option, you must download the BackWeb client software available from the Network Associates website at:

http://www.nai.com/asp_set/anti_virus/alerts/register.asp

-
- ❑ **NOTE:** If you are a corporate customer, you must first have a grant number or product serial number to subscribe to the Enterprise SecureCast channel.

If you do not have a grant number, please contact your purchasing agent, your Value Added Reseller, or Network Associates Customer Care at (972) 308-9960 for assistance.

If you are already a registered Network Associates customer and do not know your grant number, submit the grant-number request form online:

http://www.nai.com/asp_set/anti_virus/alerts/grantreq.asp

OR

Send an e-mail message to the appropriate address:

entsecast@nai.com (United States)

esc_registration_Europe@nai.com (Europe)


esc_registration_asia@nai.com (Asia)

Network Associates provides an extensive Frequently Asked Questions section that can answer most of your questions concerning SecureCast downloading and configuration. To see this FAQ list, visit the Network Associates website at:

http://www.nai.com/asp_set/anti_virus/alerts/faq.asp

Why should I update my data files?

Your software relies on information in its virus definition files (.DAT) files to identify viruses. More than 200 new viruses appear each month, however, and older .DAT files might not recognize them. To meet this challenge, McAfee releases new .DAT files each week. You are entitled to these free data file updates for use with your version of the software. If you do not use current .DAT files you may compromise your anti-virus security. Network Associates strongly recommends that you update your .DAT files on a regular basis.

 **IMPORTANT:** Using current virus identification files is only one element of an effective virus protection program. It is equally important to use a scanning engine that incorporates current advances in virus detection and cleaning. Periodically, Network Associates releases an upgrade of its scan engine that incorporates these advances.

Earlier .DAT files, however, may not function properly with newer scan engines. When the older scan engine version becomes obsolete, Network Associates will discontinue development of .DAT files for it. You should upgrade your software before your current version becomes obsolete.

Which data files does the SecureCast service deliver?

With the SecureCast service, you'll receive automatic downloads of these files:

- **New product upgrades.** The products upgrades you will receive via SecureCast depends on the terms of your license or grant.
- **Virus definition updates.** You will receive weekly .DAT file updates for your product version.
- **SuperDAT package updates.** SuperDAT packages consist of .DAT file updates—exactly the same updates you receive via your regular weekly package—and scan engine upgrades, as they become available. The SuperDAT utility also features an easy-to-use Setup architecture for quick .DAT file and scan engine updating and upgrading.
- **Virus alert messages.** McAfee AVERT researchers publish virus alert messages to warn customers about potential high-risk virus threats. These messages connect you directly with the AVERT website, where you can download EXTRA.DAT files, if available, to counter the threat, and learn about the characteristics of the new virus.

Installing the BackWeb client and SecureCast service

Setting up SecureCast service and the BackWeb client is a two-phase process:

1. Download and install the BackWeb client
2. Register to receive SecureCast service InfoPaks

To get started with the SecureCast service, review the system requirements shown below, then follow the steps outlined in each section.

System requirements

The BackWeb client software will install and run on any personal computer equipped with:

- An Intel processor or a compatible processor
- Windows 95, Windows 98, Windows NT or Windows 2000
- At least 10MB free hard disk space, plus sufficient space for product and other downloads
- An active Internet connection—direct or dial-up—for a minimum of one hour per week.

Phase 1: Download and install BackWeb

1. To download the BackWeb client software, connect to the Network Associates website at:

http://www.nai.com/asp_set/anti_virus/alerts/register.asp

Next, download the file ESC_501.EXE to a temporary directory on your hard disk.

If your product came on CD-ROM, select the SecureCast service from the choices on the installation CD-ROM, or locate the file ESC_501.EXE on your CD-ROM.

2. Double-click the program icon to start.

As soon as Setup has extracted the necessary installation files, the first BackWeb Setup panel appears (see [Figure D-1 on page 174](#)).

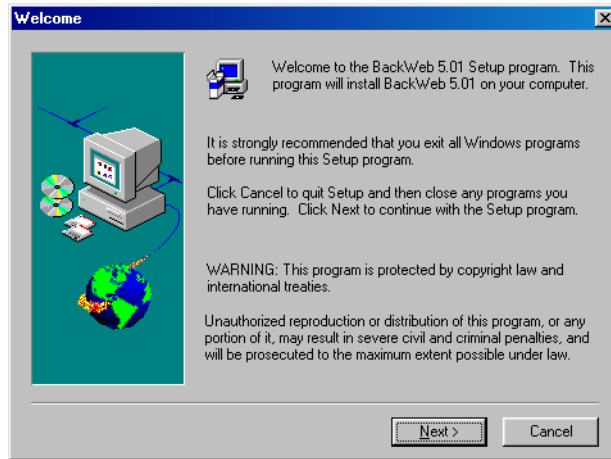


Figure D-1. BackWeb client welcome panel

3. Read the instructions and warnings on this panel, then click **Next>** to continue.
4. The BackWeb license agreement appears (Figure D-2).

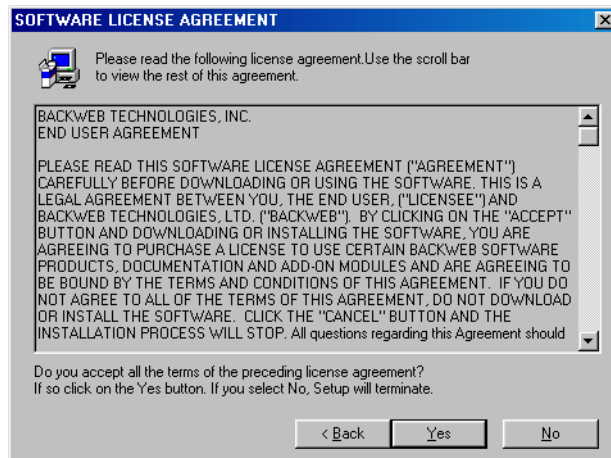


Figure D-2. BackWeb Software License Agreement panel

5. Click **Yes** to continue.
6. The Choose Destination Location panel appears (Figure D-3 on page 175).

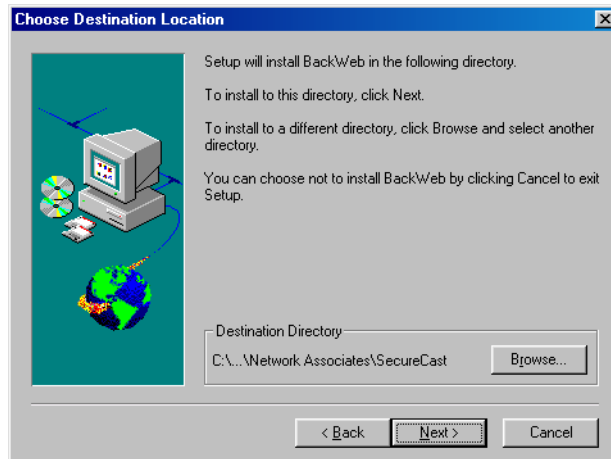


Figure D-3. Choose Destination Location panel

7. Enter a new location for Setup to install the client software, if you wish, or click **Browse** to locate a suitable folder. Click **Next>** to continue.

Setup will begin to copy BackWeb program files to your computer. As it does so, it displays its progress. When it has finished, Setup displays the Connection Type panel (Figure D-4).

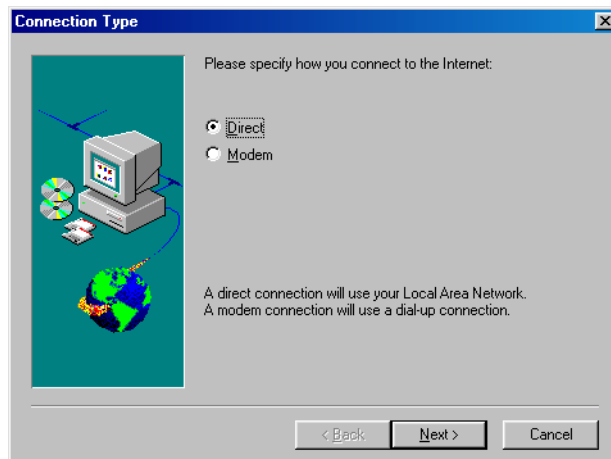


Figure D-4. Connection Type panel

8. Specify the type of connection your computer has to the Internet. Your choices are:
 - **Direct.** Choose this option if you connect to the Internet through a local-area network, a high-bandwidth connection such as a cable modem or digital subscriber line (DSL) connection. Continue with [Step 9](#).
 - **Modem.** Choose this option if you dial up to connect to an Internet service provider, or into your corporate network. Skip to [Step 13](#).

The Communication Method panel appears ([Figure D-5](#)).

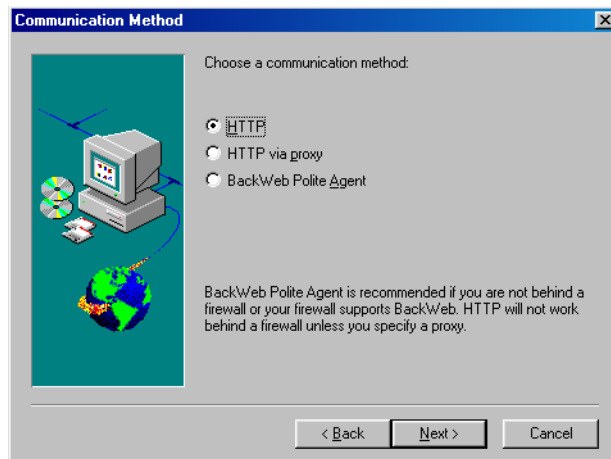


Figure D-5. Communication Method panel

9. Choose a communication method. Your choices are:
 - **HTTP.** Choose this option if you can connect directly to the Internet without going through a proxy server. Skip to [Step 13](#).
 - **HTTP via proxy.** Choose this option if you connect to the Internet through a proxy server on your network. Continue with [Step 10](#).
 - **BackWeb Polite Agent.** Choose this option to connect to the Internet through a Universal Datagram Protocol (UDP) connection. This allows you to control how the BackWeb client behaves with respect to other applications you might have running when SecureCast InfoPaks arrive at your desktop. For more information, see the BackWeb online help at <http://www.backweb.com/>.

Next, skip to [Step 13](#).

10. If you chose **HTTP via proxy** as your connection method, the HTTP Proxy Setup panel appears (Figure D-6).

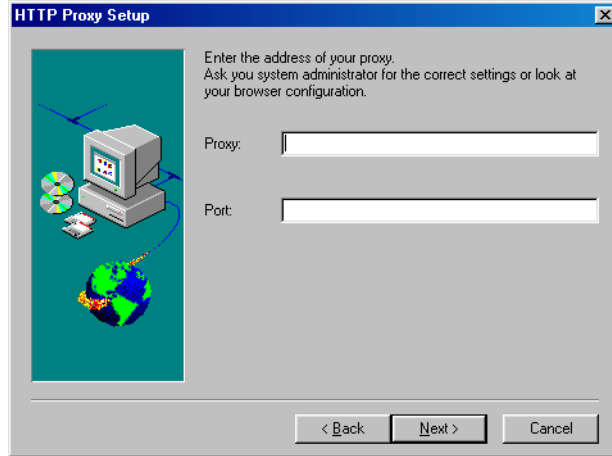


Figure D-6. HTTP Proxy Setup panel

11. Enter the name of your proxy server in the Proxy text box, then enter the port the server uses for communication in the Port text box.

When you have finished, click **Next>** to continue. The Proxy Authentication panel appears (Figure D-7 on page 177).

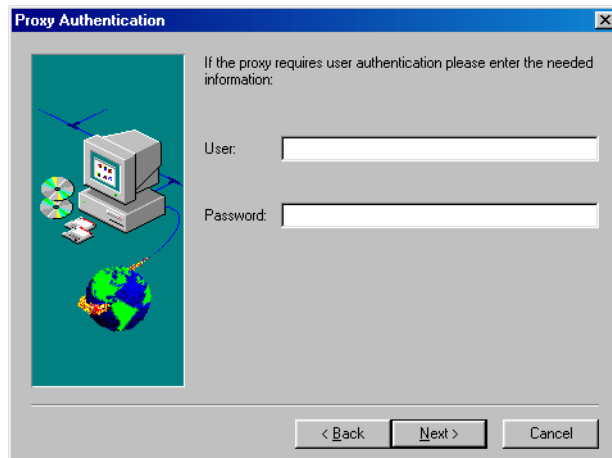


Figure D-7. Proxy Authentication panel

12. If the proxy server requires user authentication, enter in the text boxes provided a user name and password with sufficient rights to permit you to connect, then click **Next>** to continue.

The Setup Complete panel appears (Figure D-8).

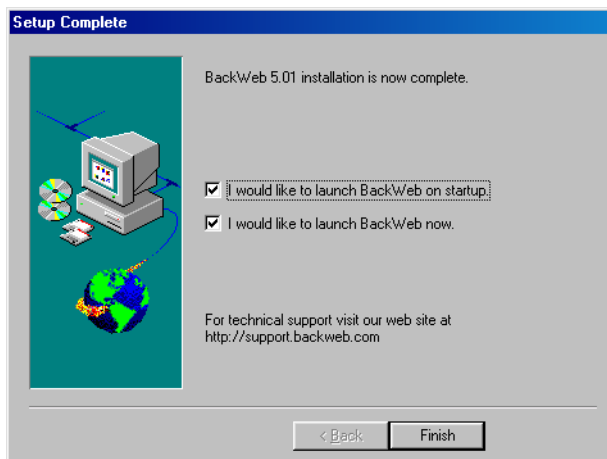


Figure D-8. Setup Complete panel

13. To start immediately, leave both checkboxes selected in this panel, then click **Finish** to complete your installation.

Phase 2: Register with the Enterprise SecureCast service

After you install the BackWeb client and start it, the SecureCast service immediately opens the client application and sends its first InfoPak: the SecureCast registration forms (Figure D-9).

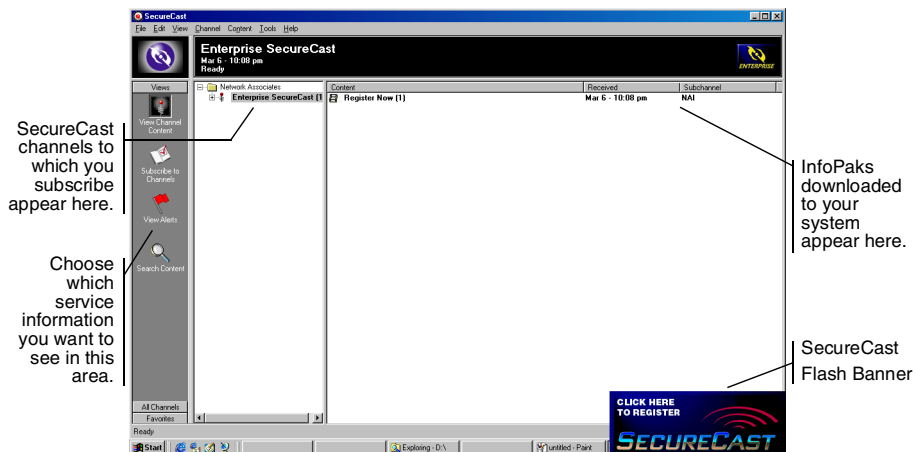



Figure D-9. The Enterprise SecureCast client window

The SecureCast service alerts you that an InfoPak has arrived with the Flash message shown at the bottom right corner of [Figure D-9](#).

-  **IMPORTANT:** If you are a corporate user and have a high-speed Internet connection, the window may list **Register Now** as an already received InfoPak. Continue with [Step 1](#).

If you have a slower connection, or if there is unusually heavy traffic at the SecureCast service site or your site, the window might not list any InfoPaks. In that case, minimize or close the BackWeb window. After some time, you will receive a Flash message. Click the flashing message, then continue with [Step 2](#).

To register for the Enterprise SecureCast channel, follow these steps:

1. If you see **Register Now** listed in the window, double-click it. The SecureCast service Flash banner appears ([Figure D-10](#)).



Figure D-10. SecureCast Flash banner

2. Click the banner. The Network Associates Welcome panel appears ([Figure D-11](#)).

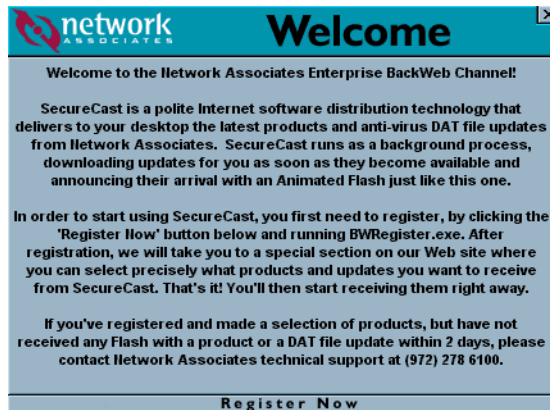
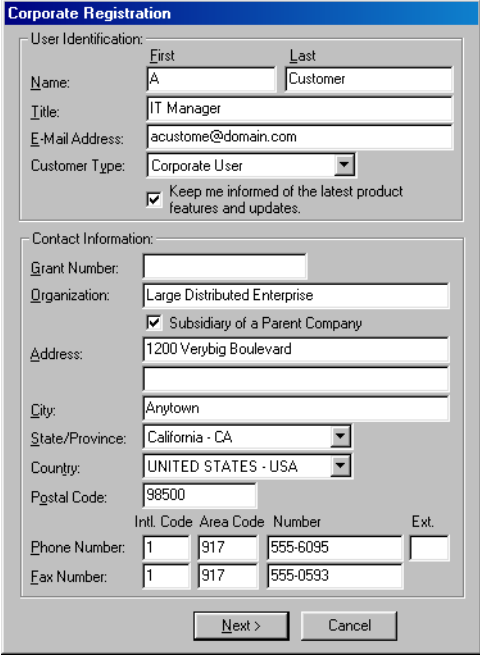


Figure D-11. Network Associates Welcome panel

3. Review the information shown, then click **Register Now** at the bottom of the panel.

4. Double-click the **BW Register** icon  in the window that opens next. A registration information form appears ([Figure D-12](#)).



The image shows a 'Corporate Registration' dialog box. It is divided into two main sections: 'User Identification' and 'Contact Information'.
User Identification:
 - Name: First (A), Last (Customer)
 - Title: IT Manager
 - E-Mail Address: acustome@domain.com
 - Customer Type: Corporate User (dropdown menu)
 - A checked checkbox: 'Keep me informed of the latest product features and updates.'
Contact Information:
 - Grant Number: (empty text box)
 - Organization: Large Distributed Enterprise
 - A checked checkbox: 'Subsidiary of a Parent Company'
 - Address: 1200 Verybig Boulevard
 - City: Anytown
 - State/Province: California - CA (dropdown menu)
 - Country: UNITED STATES - USA (dropdown menu)
 - Postal Code: 98500
 - Phone Number: Intl. Code (1), Area Code (917), Number (555-6095), Ext. (empty)
 - Fax Number: Intl. Code (1), Area Code (917), Number (555-0593), Ext. (empty)
 At the bottom are 'Next >' and 'Cancel' buttons.

Figure D-12. SecureCast User Registration Information form

5. Enter your name, title and company contact information in the text boxes provided. Here you will also need to enter the grant number you received when you purchased your software, or that you received from Network Associates Customer Service.

☐ **NOTE:** If your company is not a subsidiary of another company, clear the **Subsidiary of a Parent Company** checkbox before you continue.

When you have entered your information, click **Next>** to continue.

- If you did not clear the **Subsidiary of a Parent Company** checkbox, the **Parent Company Information** dialog box appears (see [Figure D-13 on page 181](#)). Skip to [Step 7 on page 181](#).
- If you have cleared the **Subsidiary of a Parent Company** checkbox, continue with [Step 6 on page 181](#).

Parent Company Information

Parent Company Name: EvenBigger MegaConglomerate, Inc.

Parent Address: 8000 West, 9000 South

Parent City: Erewhon

State/Province: Texas - TX

Parent Country: UNITED STATES - USA

Postal Code: 70700

< Back Next > Cancel

Figure D-13. SecureCast Parent Company Information form

6. If your company is the subsidiary of another company, enter contact information for your parent company in the text boxes provided.

When you have finished, click **Next>**. The **Proxy Communication Configuration** dialog box appears (Figure D-14).

Proxy Communication Configuration

HTTP proxy setup

☒ Use HTTP proxy at address: Port: 80

☐ Proxy requires user authentication

User Name: Password:

< Back Next > Cancel

Figure D-14. SecureCast Proxy Communication Configuration

7. If your network requires you to connect to the Internet through a proxy server, select the Use HTTP proxy at address checkbox, then enter the server name or its Internet Protocol (IP) address in the text box provided. Next, verify that the correct port number appears in the Port text box, or enter the correct port number.

If your proxy server requires you to sign on to use it, select the **Proxy requires users authentication** checkbox, then enter a user name and password with sufficient rights.

8. When you have finished, click **Next>**. The **Online Activity Status** panel appears displaying the progress of the registration process (Figure D-15 on page 182).

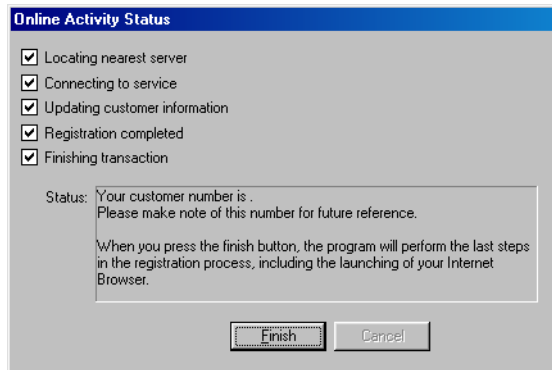


Figure D-15. SecureCast Online Activity Status panel

9. Click **Finish** after a check mark appears in all the boxes.

The setup process is complete. At that point, your web browser will connect to the Network Associates SecureCast service electronic customer care page. If you are a corporate user, the window resembles the one shown in Figure D-16:

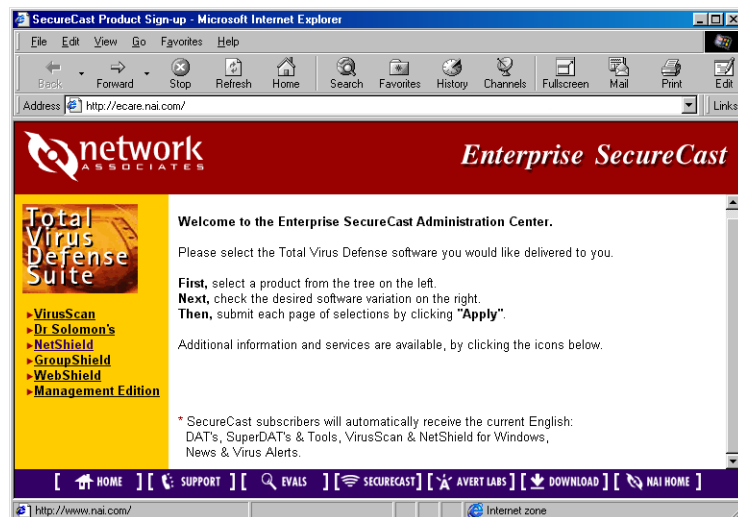


Figure D-16. SecureCast Electronic Corporate Customer Care


You can use this page to download product updates and upgrades, contact technical support, and get other information directly from Network Associates. The terms of your grant will determine what information you see here and what you can download.

Troubleshooting the Enterprise SecureCast service

Registration problems

If you try to register during a busy time of day on the web, you may encounter a delay while the server tries to process your registration request. If you receive the error message “1105 Error” or “Database Error: Unable to connect to the data source,” this means that there is a database problem on the server. Try submitting the form again, or try to register later. If you continue to have problems subscribing to the Enterprise SecureCast channel, contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central time) at (801) 492-2650.

Unsubscribing from the SecureCast service

You can stop the SecureCast service from delivering InfoPaks at any time you want to. To do so, right-click the BackWeb icon  in your Windows system tray, then choose **Start SecureCast** from the shortcut menu that appears.

Next, follow these steps:

1. In the list box on the left side of the BackWeb client window (see [Figure D-9 on page 178](#)), locate, then select, the listing for the SecureCast channel to which you now subscribe.
2. Right-click the channel icon, then choose **Unsubscribe** from the shortcut menu that appears.

All InfoPaks listed in the SecureCast service window will disappear. The SecureCast service will no longer deliver InfoPaks from that channel.

Support resources

SecureCast service

If you have additional questions about the SecureCast service, consult the SecureCast service FAQ on the Network Associates website at:

http://www.nai.com/asp_set/anti_virus/alerts/faq.asp

BackWeb client

- For a comprehensive guide to BackWeb, including additional troubleshooting advice, see the online BackWeb User's Manual:

<http://www.backweb.com/>

Adding value to your McAfee product

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

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from four levels of extended support under the Network Associates Corporate PrimeSupport* program. If you are a home user, you can choose a plan geared toward your needs from the Home User PrimeSupport program.

PrimeSupport options for corporate customers

The Corporate PrimeSupport program offers these four support plans:

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

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

The PrimeSupport KnowledgeCenter plan

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

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

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

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

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

With the PrimeSupport KnowledgeCenter plan, you get:

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

The PrimeSupport Connect plan

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

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

The PrimeSupport Priority plan

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

The PrimeSupport Priority plan has these features:

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


The PrimeSupport Enterprise plan

The PrimeSupport Enterprise plan gives you round-the-clock, personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products.

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

With the PrimeSupport Enterprise plan, you get:

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

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

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

Ordering a corporate PrimeSupport plan

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

- In North America, call Network Associates at (972) 308-9960, Monday through Friday from 8:00 a.m. to 7:00 p.m. Central time. Press 3 on your telephone keypad for sales assistance.
- In Europe, the Middle East, and Africa, contact your local Network Associates office. Contact information appears near the front of this guide.

Table E-1. Corporate PrimeSupport Plans at a Glance

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

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

PrimeSupport options for home users

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

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

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

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

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

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

To contact Network Associates electronic services

- Call the automated voice and fax system at (408) 346-3414
- Visit the Network Associates website at <http://support.nai.com>
- Visit the Network Associates CompuServe forum at GO NAI
- Visit Network Associates on America Online: keyword MCAFEE
- Free access to the PrimeSupport KnowledgeBase: online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes. Visit the KnowledgeBase at:

http://www.nai.com/asp_set/support/technical/intro.asp

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

(972) 855-7044

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

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

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

All McAfee products

(800) 950-1165

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

All products except PGP encryption
software

(900) 225-5624

- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via Network Associates online or electronic services.
- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot obtain product upgrades online. This service is available for McAfee VirusScan and NetShield software only.

How to reach international home user support

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

Table E-2. International home user support

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

* long distance charges might apply

Ordering a PrimeSupport plan for home users

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

- In North America, call Network Associates Customer Service at (972) 855-7044
- In international locations, contact the Network Associates retail technical support center closest to your location for more information. Some support options may not be available in some locations.

Network Associates consulting and training

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

Professional Services

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

Jumpstart Services

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

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

Network consulting

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

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

To learn more about the options available:

- Contact your regional sales representative.
- In North America, call Network Associates at (972) 308-9960, Monday through Friday from 8:00 a.m. to 7:00 p.m. Central time.
- Visit the Network Associates website at:

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

Total Education Services

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

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

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


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

Understanding incremental .DAT files

To function at peak efficiency, VirusScan software needs regular infusions of new virus definition data files (.DAT files). Without them, the software might not detect new virus strains or respond effectively to remove the threat from your system. Prior versions of the AutoUpdate utility required you to download and install the entire virus definition package each week. That package has grown steadily in size with each new virus definition addition and now includes more than 50,000 virus definitions.

With this VirusScan release, McAfee introduced a new incremental virus definition (.DAT or iDAT) technology that consists of small parcels that contain only the virus definitions that have changed between weekly .DAT file releases—*not* the entire .DAT file set. Instead of a weekly 3MB or larger .DAT file update, you can now download iDAT parcels that range in size from 100KB to 110KB, depending on how many virus definitions come included. This development means that you can download .DAT file updates much faster, and at a far lower cost in bandwidth, than ever before.

Better still, the AutoUpdate utility makes this process completely transparent—it will download as many incremental .DAT files as it needs to bring your software up to date. If your .DAT files are older than the backward range of iDAT packages available, or if an iDAT download fails for any reason, the utility will download the entire current .DAT file package. In either case, the AutoUpdate utility ensures that you have absolutely current .DAT files to protect your system, without the need to worry about which files to download. Simply point the utility to an update source, schedule a time for the AutoUpdate task to run, and let the utility do its work.

 **IMPORTANT:** Incremental updates apply only to .DAT files. McAfee does not provide incremental updates for scan engine files. To update your engine files, use the SuperDAT utility. The SuperDAT utility will download and install only full .DAT file updates.

Product requirements

To download and install iDAT parcels, you must have VirusScan v4.5 or later anti-virus software along with the corresponding AutoUpdate utility, and you must have already upgraded your Olympus scan engine to v4.0.50 or later. Incremental .DAT files do not work with earlier product or engine versions.

How does iDAT updating work?

The AutoUpdate utility downloads two types of files when it connects to the update site you specified:

- **.UPD files.** These update files contain only the virus definition changes between one weekly .DAT file release and the .DAT file release from the week immediately following. The names for these .UPD files consist of the version number of a .DAT file release—4053, for example—and the version number of the very next .DAT release in the sequence, or 4054 in this case. The complete filename for this .UPD file would therefore be 40534054.UPD.

If you updated your .DAT files every week, the AutoUpdate utility would simply download the weekly file, then install it alone to bring your .DAT files up to date. If you have not updated your software for three or four weeks, however, the AutoUpdate utility would need to download a number of .UPD packages from which it could extract and install all of the virus definition files it needed to bring your existing .DAT files up to date. The utility finds the information it needs to determine which packages to download in the DELTA.INI file.

- **DELTA.INI files.** These are text files that describe which weekly .UPD files the AutoUpdate utility needs to bring your .DAT files completely up to date. The DELTA.INI file consists of entries that list a number of previous .DAT file versions, along with the corresponding number of weekly .UPD files it would need to download from a given .DAT file version number in order to have all of the virus definitions that the current .DAT file release has. The file entries have the following format:

```
[Multiple Patch Table]
```

```
4053=10
```

```
4054=11
```

```
4055=12
```

```
[Incremental Resolver]
```

```
10=40534054.UPD
```


```
11=40544055.UPD
```

```
12=40554056.UPD
```


For this example, suppose you have .DAT version 4053 installed on your computer and the current .DAT file release is version 4056. The AutoUpdate utility can look in the DELTA.INI file to learn that it needs to download the 10th, 11th, and 12th .UPD file releases to have all of the virus definitions that the current .DAT file release does.

The entries in the Incremental Resolver table, meanwhile, translate the sequential numbers from the Multiple Patch Table into actual filenames that the AutoUpdate utility can download.

The DELTA.INI file also has checksum and other information that the AutoUpdate utility can use to verify that files it downloaded have not changed or become corrupted.

 **NOTE:** If an iDAT download fails for any reason, the AutoUpdate utility will download and install a full .DAT update.


After it downloads the correct .UPD file, the AutoUpdate utility decodes the existing .DAT files, patches the downloaded iDAT files into them, validates the data, then re-encodes the newly updated .DAT files for use with your software.

 **NOTE:** Because the iDAT files patch the existing .DAT files you may not download the iDAT files through the AutoUpdate utility and use the utility to save them for later updates. You can download the .UPD packages independently from the McAfee FTP site, however, and save these files for later distribution. See “[Best practices](#)” below for details.

What does McAfee post each week?

Each week McAfee posts a complete .DAT file update, along with a new weekly iDAT update, and a new DELTA.INI file that has updated Multiple Patch Table and Incremental Resolver entries. You can download these files independently of the AutoUpdate utility for posting on your internal servers from the McAfee FTP site at:

<ftp://ftp.nai.com/licensed/antivirus/datfiles/4.x/>

 **IMPORTANT:** To connect to this site you must have a licensed customer user name and password. The FTP site will not accept anonymous connections.

A typical file listing would be:

```
00_index.txt
40534054.UPD
40544055.UPD
40554056.UPD
```

dat-4056.zip

dat-4056.tar

DELTA.INI

README.TXT

Best practices

The following sections outline some suggestions for how to employ iDAT downloads in your updating strategy.

Three-stage updating

If you need to roll out new virus definitions to multiple workstations on your network, McAfee recommends a three-stage update strategy that will save you external network bandwidth, minimize your security risks, and give you more control over your internal updating strategy:

1. If the .DAT files installed on your network computers are very old, use a web browser or FTP client software to download a full .DAT file update or the SuperDAT utility to a central server on your network, then configure the AutoUpdate copies on your network computers to download and install the complete .DAT set and the current scan engine.

This brings your network to a workable baseline state. You can then download and install iDAT files to keep current.

2. From the baseline state, use a web browser or FTP client software each week to download new .UPD files directly from the McAfee FTP site to a central server on your network.

If you start from the baseline state described in [Step 1](#), you can simply download the most recent .UPD file posted on the McAfee FTP site. If you have not updated in a couple of weeks, open the DELTA.INI file online, and look at the entries in the Multiple Patch and the Incremental Resolver tables to see which .UPD files you must download to update the .DAT files installed on your network, then download each of the files you need, *including* the DELTA.INI file.

3. Install all of the .UPD files and the DELTA.INI file you downloaded to a central server on your network, then configure the AutoUpdate copies on your network computers to download and install the iDAT set. Do not mark these files read-only, as this could cause the target computer to report an error when it tries to delete old files later.

The AutoUpdate utility will download each file it needs, in sequence, to bring the .DAT files installed on its host computer up to date. From that point forward, your network computers will install iDAT files, which will reduce your update time and the demand on your network bandwidth.

Scheduling internal .DAT updates

The AutoUpdate utility has a built-in scheduling feature that lets you automate the entire update process. You can schedule updates for late nights, for times when network bandwidth demand is, low or at other convenient periods. The scheduling feature also allows you to set a “randomization window” centered on the time you schedule for your update. You can use this feature to send out a standard AutoUpdate configuration, with a standard update schedule, but still prevent network traffic bottlenecks that might otherwise result when all of the computers on your network simultaneously try to update their .DAT files.

If some of your client computers are off, or if they do not have the VirusScan Console running, the AutoUpdate utility will resume its scheduled task when you next start the computer or the VirusScan Console.

To learn how to use this feature, see [“Enabling tasks” on page 208](#) of the *VirusScan User’s Guide*.

-
- ❏ **NOTE:** Be sure to schedule your client computer updates for a time after you have downloaded and installed the update files on your central server. If you configure your computers to download iDAT files directly from the McAfee website, be sure to schedule your updates for a time after the regular weekly .DAT file postings.
-

Frequently asked questions

Connectivity issues

Q: What happens if my machine is off when a scheduled update is due?

A: If the AutoUpdate utility misses a scheduled task because your computer or the VirusScan Console were not running at the task’s scheduled time, the utility will run the task when it next starts.

Q: What happens if my Internet or network connection goes down during an update?

A: If the AutoUpdate utility downloaded one or more iDAT files before the connection loss, it will install them into your existing .DAT files and record its failure to download the remaining iDAT files in its activity log.

Corrupted data

Q: What happens if one of the iDAT files is corrupted during download?

A: Before the AutoUpdate utility installs any iDAT file, it checks the file against a verification checksum recorded in the DELTA.INI file. If the checksums do not match, the utility does not install that iDAT file or any subsequent files it downloads in that session. Instead, the utility will display an error message, then will download a full .DAT file set to update your software.

Incremental vs. full .DAT update

Q: What happens if my existing .DAT files are very old? Will incremental .DAT file updating still work?

A: The AutoUpdate utility decides which process to use. It downloads iDAT files only if your existing .DAT file set is no more than 15 weeks out of date. After that point, it becomes more efficient to download a full .DAT file set.

Network configuration issues

Q: Do all the machines I want to update need to be able to connect to the Internet?

A: No. You can configure one computer on your network to download the iDAT files from the Internet, then have other computers on your network download their files from this computer. To learn more, see [“Three-stage updating” on page 198](#).

Q: How can I prevent network bottlenecks when I update many workstations?

A: The AutoUpdate Task Properties dialog box has a randomization feature you can use to spread the network load. To learn how this works, see [“Enabling tasks” on page 208](#) of the *VirusScan User's Guide*.

Scheduling issues

Q: How often should I check for updates?

A: Normally, McAfee posts updated .DAT files on a weekly basis. You may, however, check more or less often as your network security needs require. Be aware that your risk of virus infection grows as the period between updates to the virus data files grows.

Index

A

- alarms, false, understanding, [76](#)
- Alert Manager
 - files, [146](#)
- America Online
 - technical support via, [xv](#)
- America Online, technical support via, [190](#)
- anonymous FTP, use of to log on to update and upgrade sites, [115](#), [126](#)
- anti-virus software
 - consequences of running multiple vendor versions, [76](#)
 - reporting new viruses not detected by to McAfee, [xvii](#)
- autoexe.bat, [64](#)
- AutoUpdate
 - advanced options for, configuring, [115](#) to [118](#)
 - Force Update, use of to replace corrupted .DAT files, [117](#)
 - number of connection attempts made for update sites, [114](#)
 - options for, configuring, [108](#) to [128](#)
 - use of in conjunction with SecureCast, [108](#), [119](#)
 - using iDAT files with, [195](#)
- AutoUpgrade
 - advanced options for, configuring, [126](#) to [128](#)
 - number of connection attempts made for update sites, [125](#)
 - options for, configuring, [118](#) to [128](#)
 - use of with SuperDAT utility, [128](#) to [130](#)

B

- batch files, running after successful updates, [118](#)
- BIOS
 - possible VirusScan conflicts with anti-virus features of, [76](#)
- BOOTSCAN.EXE
 - use of on Emergency Disk, [72](#)

C

- Command line options
 - silent, [59](#)
- command line options
 - on access scanner, [64](#)
 - preserving settings, [64](#)
 - rebooting, [63](#)
 - security, [63](#)
- command line scanner, [155](#)
- command-line scanner, [155](#)
- components, included with VirusScan, [25](#) to [29](#)
- CompuServe, technical support via, [xv](#), [190](#)
- computer problems, attributing to viruses, [71](#)
- consulting services, [193](#)
- crashes, when not attributable to viruses, [75](#)
- custom directory, [61](#)
- Customer Care
 - contacting, [xiv](#)

D

- .DAT file updates
 - reporting new items for, [xvii](#)
 - what they are, [105](#)
 - definition of and numbering convention for, [107](#)
- data files
 - common, delivered via SecureCast, [172](#)
- DELTA.INI files
 - description and use of, [196](#)
- deploy VirusScan, [65 to 66](#)
- descriptions, of VirusScan program
 - components, [25 to 29](#)
- detections, false, understanding, [76](#)
- distribution
 - of update files, recommended methods for, [108 to 119](#)
- double heuristics analysis, [24](#)
- Download Scan module
 - default response options for, [81 to 82](#)

E

- educational services, description of, [194](#)
- EICAR "virus," use of to test installation, [54](#)
- electronic services, contacting for technical support, [190](#)
- e-mail
 - addresses for reporting new viruses to McAfee, [xvii](#)
- E-Mail Scan
 - dependent files, [152](#)
 - program files, [152](#)
 - temporary files, [153](#)
- E-Mail Scan program component, default responses when virus found, [84 to 85](#)

Emergency .DAT files, location and use of, [108](#)

Emergency Disk

- creating
 - on uninfected computer, [72](#)
- use of BOOTSCAN.EXE on, [72](#)
- use of to reboot system, [72](#)

Enterprise SecureCast, [171](#)

- features of, [173](#)
- setting up, [183](#)
- support resources for, [183](#)
- system requirements for, [173](#)
- troubleshooting, [183](#)
- unsubscribing from, [183](#)

ePolicy Orchestrator

- deploy, [66](#)

EXTRA.DAT files, location, use, and description of, [107](#)

F

- false detections, understanding, [76](#)
- file information, viewing, [86 to 87](#)
- File Transfer Protocol (FTP)
 - use of to obtain VirusScan upgrades, [126](#)
- files
 - infected
 - cleaning yourself when VirusScan cannot, [73](#)
- files installed, [137](#)
- Force Update, use of to replace corrupted .DAT files, [117](#)
- FTP (File Transfer Protocol)
 - use of to obtain VirusScan upgrades, [126](#)

H

heuristic scanning

definition of, [24](#)

heuristics, [24](#)

Home SecureCast

features of, [173](#)

support resources for, [183](#)

system requirements for, [173](#)

I

iDAT files

use of DELTA.INI file for, [196](#)

using the AutoUpdate utility to download and install, [195](#)

what they are, [195](#)

iDAT files, understanding and

using, [195 to 200](#)

incompatible software, [63](#)

incremental .DAT (iDAT) files

what they are, [105](#)

incremental .DAT files

using the AutoUpdate utility to download and install, [195](#)

what they are, [195](#)

incremental .DAT files, understanding and

using, [195 to 200](#)

incremental DAT files

use of DELTA.INI file for, [196](#)

infected files

cleaning yourself when VirusScan cannot, [73](#)

removing viruses from, [71 to 85](#)

installation

aborting if virus detected during, [71](#)

logging, [60](#)

silent, [59](#)

specific features, [61](#)

testing effectiveness of, [54](#)

installation customization, [68](#)

installing to a custom directory, [61](#)

installing via SMS, [67](#)

installing via Tivoli, [67](#)

installing via ZENworks, [68](#)

Internet Filter module

default response options for, [82](#)

L

log file

limiting size of, [113, 123](#)

UPDATE UPGRADE ACTIVITY.TXT

as, [112, 123](#)

M

Management Edition

deploy, [65](#)

McAfee

contacting

via America Online, [xv](#)

via CompuServe, [xv](#)

within the United States, [xv](#)

McAfee Emergency Disk

creating

on uninfected computer, [72](#)

use of to reboot system, [72](#)

methods for updating and upgrading

VirusScan software, [106 to 108](#)

MSI_Inst.exe Customization, [68](#)

N

Network Associates

- consulting services from, [193](#)
- contacting
 - Customer Service, [xiv](#)
 - outside the United States, [xviii](#)
- educational services, [194](#)
- support services, [185](#)
- training, [xvi](#), [193](#)
- website address for software updates and upgrades, [190](#)

new viruses, reporting to McAfee, [xvii](#)

numbering conventions for .DAT files, [107](#)

O

Olympus scan engine

- what it is, [105](#)

ommand line options, [58](#)

on-demand scanner

- command-line, [164](#)

options

- command line scanner, [155](#)
- command-line scanner, [155](#)

P

panic, avoiding when your system is infected, [71](#)

PKGDESC.INI file, use of for SuperDAT utility upgrades, [130](#)

preserving settings, [64](#)

PrimeSupport

- corporate
 - at a glance, [189](#)
 - KnowledgeCenter, [185](#)
 - ordering, [188](#)

PrimeSupport Connect, [186](#)

PrimeSupport Connect 24-By-7, [187](#)

PrimeSupport Enterprise, [187](#)

for home users

Online Upgrades plan, [191](#)

ordering, [192](#)

Pay-Per-Minute plan, [191](#)

Quarterly Disk/CD plan, [191](#)

Small Office/Home Office Annual Plan, [191](#)

Professional Consulting Services

description of, [193](#)

program components, included with VirusScan, [25](#) to [29](#)

programs

running after successful updates, [118](#)

proxy servers, working through to obtain updates and upgrades, [115](#), [126](#)

R

rebooting, [63](#)

rebooting, with the McAfee Emergency Disk, [72](#)

registry keys installed, [137](#)

remover

actions available when VirusScan has none, [73](#)

report file

limiting size of, [113](#), [123](#)

UPDATE UPGRADE ACTIVITY.TXT as, [112](#), [123](#)

reporting viruses not detected to McAfee, [xvii](#)

response options

choosing

- when Download Scan module finds a virus, [81 to 82](#)

- when E-mail Scan module finds a virus, [80 to 81](#)

- when Internet Filter module finds harmful objects, [82](#)

- when System Scan module finds a virus, [77 to 79](#)

- when the E-Mail Scan program component detects a virus, [84 to 85](#)

- when VirusScan detects a virus, [82 to 84](#)

responses, default, when infected by viruses, [71 to 85](#)

restarting

- with the McAfee Emergency Disk, [72](#)

S

scan engine

- upgrading with AutoUpdate and the SuperDAT utility, [128 to 130](#)

- what it is, [105](#)

scan operations, deciding when to start, [74](#)

scan tasks

- scheduling and enabling

- as purpose of Scheduler, [98](#)

Scheduler

- purpose of, [98](#)

ScreenScan

- dependent files, [149](#)

- program files, [148](#)

SecureCast

- common data files delivered via, [172](#)

- Enterprise SecureCast, [171](#)

- setting up, [183](#)

- troubleshooting, [183](#)

- unsubscribing from, [183](#)

- features of, [173](#)

- support resources for, [183](#)

- system requirements, [173](#)

- use of in conjunction with AutoUpdate, [108, 119](#)

- using to update your software, [171](#)

- VirusScan channel for retail users, [173](#)

security, [63](#)

Sending, [99](#)

Setup

- "silent" and "record" modes, using, [59](#)

- aborting if virus detected during, [71](#)

SETUP.EXE, renaming SuperDAT packages for use with AutoUpgrade, [130](#)

SETUP.ISS file, use of for SuperDAT utility upgrades, [130](#)

software conflicts, as potential cause for computer problems, [75](#)

software updates and upgrades, website address for obtaining, [190](#)

SuperDAT utility

- use of for upgrade strategy, [106](#)

- use of in conjunction with the AutoUpgrade utility, [128 to 130](#)

support

corporate

at a glance, [189](#)

KnowledgeCenter, [185](#)

ordering, [188](#)

PrimeSupport Connect, [186](#)

PrimeSupport Connect 24-By-7, [187](#)

PrimeSupport Enterprise, [187](#)

for home users, [190](#)

Online Upgrades plan, [191](#)

Pay-Per-Minute plan, [191](#)

PrimeSupport

ordering, [192](#)

Small Office/Home Office Annual Plan, [191](#)

Quarterly Disk/CD plan, [191](#)

hours of availability, [190](#)

resources for SecureCast, [183](#)

via electronic services, [190](#)

system crashes, attributing to viruses, [71](#)

System Management Server(SMS)

installing VirusScan, [67](#)

system requirements

for VirusScan, [33](#)

SecureCast, [173](#)

System Scan module

default response options for, [77](#) to [79](#)

T

Task menu

View Activity Log, [113](#), [124](#)

technical support

corporate

at a glance, [189](#)

KnowledgeCenter, [185](#)

ordering, [188](#)

PrimeSupport Connect, [186](#)

PrimeSupport Connect 24-By-7, [187](#)

PrimeSupport Enterprise, [187](#)

e-mail address for, [xv](#)

for home users

PrimeSupport

Online Upgrades plan, [191](#)

Pay-Per-Minute plan, [191](#)

Quarterly Disk/CD plan, [191](#)

Small Office/Home Office Annual Plan, [191](#)

hours of availability, [190](#)

information needed from user, [xvi](#)

online, [xv](#)

phone numbers for, [xv](#)

PrimeSupport

for home users

ordering, [192](#)

via electronic services, [190](#)

testing your installation, [54](#)

Tivoli

installing VirusScan, [67](#)

Total Education Services

description of, [193](#)

Total Service Solutions

contacting, [193](#)

Total Virus Defense

VirusScan as component of, 22

training for Network Associates
products, xvi, 193

scheduling, xvi

troubleshooting SecureCast

firewall problems, 183

registration problems, 183

U

uninfected computer, use of to create
Emergency Disk, 72

Universal Naming Convention (UNC)
notation, use of to designate update and
upgrade sites, 114, 125

.UPD files

description and use of, 196

iDAT files

.UPD files as downloads, 196

incremental DAT files

UPD files as downloads, 196

update and upgrade methods

using with VirusScan
software, 106 to 108

UPDATE UPGRADE ACTIVITY.TXT

as AutoUpdate and AutoUpgrade log
file, 112, 123

updates

automatic, via AutoUpdate, 108 to 128

recommended method for downloading
and distributing, 108 to 119

updates and upgrades

use of anonymous FTP to log into sites
for, 115, 126

use of UNC notation to designate, 114,
125

updates and upgrades, website address for
obtaining, 190

updating strategies for VirusScan
software, 105

upgrades

automatic, via AutoUpgrade, 118 to 128

utilities, 133

V

View Activity Log

in **Task** menu, 113, 124

VirusLogic, "double heuristics"
technology, 24

Virus Information Library, connecting to
from VirusScan, 86 to 87

viruses

deciding when to start scan operations
for, 74

default response to

when E-Mail Scan program
component detects, 84 to 85

when VirusScan detects, 82 to 84

when VShield detects, 77 to 82

effects of, 71 to 85

false detections of, understanding, 76

recognizing when computer problems do
not result from, 75

removing

before installation, necessity of and
steps for, 71

from infected files, 71 to 85

reporting new strains to McAfee, xvii

viewing information about, 86 to 87

VirusScan

- as component of Total Virus Defense suite, [22](#)
- BIOS anti-virus features, potential conflicts with, [76](#)
- command line options, [155](#)
- command-line examples, [164](#)
- command-line options, [155](#)
- components included with, [25 to 29](#)
- default responses to virus detection, [82 to 84](#)
- description of program components, [25 to 29](#)
- installation
 - as best protection against infection, [71](#)
 - what to do when virus found during, [71](#)
- introducing, [21](#)
- main window
 - use of to select responses to infections, [83](#)
- overview of features, [21](#)
- updating via AutoUpdate, [108 to 128](#)
- upgrading via AutoUpgrade, [118 to 128](#)
- what it does, [97](#)

VirusScan application

- dependent files, [143](#)
- program files, [143](#)
- temporary files, [145](#)

VirusScan Command Line

- use of when booting with Emergency Disk, [72](#)

VirusScan control panel, [133](#)

- files, [147](#)
- options, [134](#)
- temporary files, [147](#)

VirusScan Emergency Disk

- files, [150](#)

VirusScan Scheduler

- purpose of, [98](#)

VShield

- default responses to virus detection, [77 to 82](#)
- Download Scan module
 - default response options for, [81 to 82](#)
- E-mail Scan module
 - default response options for, [80 to 81](#)
- Internet Filter module
 - default response options for, [82](#)
- System Scan module
 - default response options for, [77 to 79](#)
- what it does, [97](#)

Vshield

- components included with VirusScan, [25 to 29](#)

VShield scanner

- dependent files, [140](#)
- program files, [137](#)
- temporary files, [142](#)

W

- website, Network Associates technical support via, [190](#)

Z**ZENworks**

- installing VirusScan, [68](#)