

McAfee VirusScan
Anti-Virus Software

User's Guide

Version 4.5

COPYRIGHT

Copyright © 1995-2000 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
What happened?	vii
Why worry?	vii
Where do viruses come from?	viii
Virus prehistory	viii
Viruses and the PC revolution	ix
On the frontier	xii
Where next?	xiv
How to protect yourself	xv
How to contact McAfee and Network Associates	xvi
Customer service	xvi
Technical support	xvii
Download support	xviii
Network Associates training	xviii
Comments and feedback	xviii
Reporting new items for anti-virus data file updates	xix
International contact information	xx
Chapter 1. About VirusScan Software	23
Introducing VirusScan anti-virus software	23
How does VirusScan software work?	25
What comes with VirusScan software?	27
What's new in this release?	31
Chapter 2. Installing VirusScan Software	35
Before you begin	35
System requirements	35
Other recommendations	35
Preparing to install VirusScan software	36
Installation options	36
Installation steps	37
Using the Emergency Disk Creation utility	49
Determining when you must restart your computer	55

Testing your installation	56
Modifying or removing your VirusScan installation	57
Chapter 3. Removing Infections From Your System	61
If you suspect you have a virus... ..	61
Deciding when to scan for viruses	64
Recognizing when you don't have a virus	65
Understanding false detections	66
Responding to viruses or malicious software	67
Submitting a virus sample	78
Using the SendVirus utility to submit a file sample	78
Capturing boot sector, file-infesting, and macro viruses	81
Chapter 4. Using the VShield Scanner	87
What does the VShield scanner do?	87
Why use the VShield scanner?	88
Browser and e-mail client support	89
Enabling or starting the VShield scanner	90
Using the VShield configuration wizard	95
Setting VShield scanner properties	99
Using the VShield shortcut menu	155
Disabling or stopping the VShield scanner	155
Tracking VShield software status information	161
Chapter 5. Using theVirusScan application	163
What is the VirusScan application?	163
Why use the VirusScan application?	164
Starting the VirusScan application	165
Configuring the VirusScan Classic interface	171
Configuring the VirusScan Advanced interface	176
Chapter 6. Creating and Configuring Scheduled Tasks	193
What does VirusScan Console do?	193
Why schedule scan operations?	193
Starting the VirusScan Console	194

Using the Console window	196
Working with default tasks	198
Working with the VShield task	200
Working with the AutoUpgrade and AutoUpdate tasks	201
Creating new tasks	202
Enabling tasks	206
Checking task status	208
Configuring VirusScan application options	210
Chapter 7. Updating and Upgrading VirusScan Software	229
Developing an updating strategy	229
Update and upgrade methods	230
Understanding the AutoUpdate utility	232
Configuring the AutoUpdate Utility	233
Understanding the AutoUpgrade utility	242
Configuring the AutoUpgrade utility	243
Using the AutoUpgrade and SuperDAT utilities together	252
Deploying an EXTRA.DAT file	254
Chapter 8. Using Specialized Scanning Tools	257
Scanning Microsoft Exchange and Outlook mail	257
When and why you should use the E-Mail Scan extension	257
Using the E-Mail Scan extension	258
Configuring the E-Mail Scan extension	259
Scanning cc:Mail	273
Using the ScreenScan utility	273
Chapter 9. Using VirusScan Utilities	281
Understanding the VirusScan control panel	281
Opening the VirusScan control panel	281
Choosing VirusScan control panel options	282
Using the Alert Manager Client Configuration utility	285
VirusScan software as an Alert Manager client	286
Configuring the Alert Manager client utility	286

Appendix A. Default Vulnerable and Compressed File Extensions	..291
Adding file name extensions for scanning	..291
Current list of vulnerable file name extensions	..292
Current list of compressed files scanned	..296
Appendix B. Network Associates Support Services299
Adding value to your McAfee product299
PrimeSupport options for corporate customers299
Ordering a corporate PrimeSupport plan302
PrimeSupport options for home users304
How to reach international home user support306
Ordering a PrimeSupport plan for home users306
Network Associates consulting and training307
Professional Services307
Total Education Services308
Appendix C. Using the SecureCast Service to Get New Data Files	..309
Introducing the SecureCast service309
Why should I update my data files?310
Which data files does the SecureCast service deliver?310
Installing the BackWeb client and SecureCast service311
System requirements311
Troubleshooting the Enterprise SecureCast service321
Unsubscribing from the SecureCast service321
Support resources321
SecureCast service321
BackWeb client322
Index323

Preface

What happened?

If you've ever lost important files stored on your hard disk, watched in dismay as your computer ground to a halt only to display a prankster's juvenile greeting on your monitor, or found yourself having to apologize for abusive e-mail messages you never sent, you know first-hand how computer viruses and other harmful programs can disrupt your productivity. If you haven't yet suffered from a virus "infection," count yourself lucky. But with more than 50,000 known viruses in circulation capable of attacking Windows- and DOS-based computer systems, it really is only a matter of time before you do.

The good news is that of those thousands of circulating viruses, only a small proportion have the means to do real damage to your data. In fact, the term "computer virus" identifies a broad array of programs that have only one feature in common: they "reproduce" themselves automatically by attaching themselves to host software or disk sectors on your computer, usually without your knowledge. Most viruses cause relatively trivial problems, ranging from the merely annoying to the downright insignificant. Often, the primary consequence of a virus infection is the cost you incur in time and effort to track down the source of the infection and eradicate all of its traces.

Why worry?

So why worry about virus infections, if most attacks do little harm? The problem is twofold. First, although relatively few viruses have destructive effects, that fact says nothing about how widespread the malicious viruses are. In many cases, viruses with the most debilitating effects are the hardest to detect—the virus writer bent on causing harm will take extra steps to avoid discovery. Second, even "benign" viruses can interfere with the normal operation of your computer and can cause unpredictable behavior in other software. Some viruses contain bugs, poorly written code, or other problems severe enough to cause crashes when they run. Other times, legitimate software has problems running when a virus has, intentionally or otherwise, altered system parameters or other aspects of the computing environment. Tracking down the source of resulting system freezes or crashes can drain time and money from more productive activities.

Beyond these problems lies a problem of perception: once infected, your computer can serve as a source of infection for other computers. If you regularly exchange data with colleagues or customers, you could unwittingly pass on a virus that could do more damage to your reputation or your dealings with others than it does to your computer.

The threat from viruses and other malicious software is real, and it is growing worse. Some estimates have placed the total worldwide cost in time and lost productivity for merely detecting and cleaning virus infections at more than \$10 billion per year, a figure that doesn't include the costs of data loss and recovery in the wake of attacks that destroyed data.

Where do viruses come from?

As you or one of your colleagues recovers from a virus attack or hears about new forms of malicious software appearing in commonly used programs, you've probably asked yourself a number of questions about how we as computer users got to this point. Where do viruses and other malicious programs come from? Who writes them? Why do those who write them seek to interrupt workflows, destroy data, or cost people the time and money necessary to eradicate them? What can stop them?

Why did this happen to me?

It probably doesn't console you much to hear that the programmer who wrote the virus that erased your hard disk's file allocation table didn't target you or your computer specifically. Nor will it cheer you up to learn that the virus problem will probably always be with us. But knowing a bit about the history of computer viruses and how they work can help you better protect yourself against them.

Virus prehistory

Historians have identified a number of programs that incorporated features now associated with virus software. Canadian researcher and educator Robert M. Slade traces virus lineage back to special-purpose utilities used to reclaim unused file space and perform other useful tasks in the earliest networked computers. Slade reports that computer scientists at a Xerox Corporation research facility called programs like these "worms," a term coined after the scientists noticed "holes" in printouts from computer memory maps that looked as though worms had eaten them. The term survives to this day to describe programs that make copies of themselves, but without necessarily using host software in the process.

A strong academic tradition of computer prank playing most likely contributed to the shift away from utility programs and toward more malicious uses of the programming techniques found in worm software. Computer science students, often to test their programming abilities, would construct rogue worm programs and unleash them to "fight" against each other, competing to see whose program could "survive" while shutting down rivals. Those same students also found uses for worm programs in practical jokes they played on unsuspecting colleagues.

Some of these students soon discovered that they could use certain features of the host computer's operating system to give them unauthorized access to computer resources. Others took advantage of users who had relatively little computer knowledge to substitute their own programs—written for their own purposes—in place of common or innocuous utilities. These unsophisticated users would run what they thought was their usual software only to find their files erased, to have their account passwords stolen, or to suffer other unpleasant consequences. Such “Trojan horse” programs or “Trojans,” so dubbed for their metaphorical resemblance to the ancient Greek gift to the city of Troy, remain a significant, and growing, threat to computer users today.

Viruses and the PC revolution

What we now think of as true computer viruses first appeared, according to Robert Slade, soon after the first personal computers reached the mass market in the early 1980s. Other researchers date the advent of virus programs to 1986, with the appearance of the “Brain” virus. Whichever date has the better claim, the link between the virus threat and the personal computer is not coincidental.

The new mass distribution of computers meant that viruses could spread to many more hosts than before, when a comparatively few, closely guarded mainframe systems dominated the computing world from their bastions in large corporations and universities. Nor did the individual users who bought PCs have much use for the sophisticated security measures needed to protect sensitive data in those environments. As further catalyst, virus writers found it relatively easy to exploit some PC technologies to serve their own ends.

Boot-sector viruses

Early PCs, for example, “booted” or loaded their operating systems from floppy disks. The authors of the Brain virus discovered that they could substitute their own program for the executable code present on the boot sector of every floppy disk formatted with Microsoft's MS-DOS, whether or not it included system files. Users thereby loaded the virus into memory every time they started their computers with any formatted disk in their floppy drives. Once in memory, a virus can copy itself to boot sectors on other floppy or hard disks. Those who unintentionally loaded Brain from an infected floppy found themselves reading an ersatz “advertisement” for a computer consulting company in Pakistan.

With that advertisement, Brain pioneered another characteristic feature of modern viruses: the payload. The payload is the prank or malicious behavior that, if triggered, causes effects that range from annoying messages to data destruction. It's the virus characteristic that draws the most attention—many virus authors now write their viruses specifically to deliver their payloads to as many computers as possible.

For a time, sophisticated descendants of this first boot-sector virus represented the most serious virus threat to computer users. Variants of boot sector viruses also infect the Master Boot Record (MBR), which stores the partition information your computer needs to figure out where to find each of your hard disk partitions and the boot sector itself.

Realistically, nearly every step in the boot process, from reading the MBR to loading the operating system, is vulnerable to virus sabotage. Some of the most tenacious and destructive viruses still include the ability to infect your computer's boot sector or MBR among their repertoire of tricks. Among other advantages, loading at boot time can give a virus a chance to do its work before your anti-virus software has a chance to run. Many McAfee anti-virus products anticipate this possibility by allowing you to create an emergency disk you can use to boot your computer and remove infections.

But most boot sector and MBR viruses had a particular weakness: they spread by means of floppy disks or other removable media, riding concealed in that first track of disk space. As fewer users exchanged floppy disks and as software distribution came to rely on other media, such as CD-ROMs and direct downloading from the Internet, other virus types eclipsed the boot sector threat. But it's far from gone—many later-generation viruses routinely incorporate functions that infect your hard disk boot sector or MBR, even if they use other methods as their primary means of transmission.

Those same viruses have also benefitted from several generations of evolution, and therefore incorporate much more sophisticated infection and concealment techniques that make it far from simple to detect them, even when they hide in relatively predictable places.

File infector viruses

At about the same time as the authors of the Brain virus found vulnerabilities in the DOS boot sector, other virus writers found out how to use other software to help replicate their creations. An early example of this type of virus showed up in computers at Lehigh University in Pennsylvania. The virus infected part of the DOS command interpreter COMMAND.COM, which it used to load itself into memory. Once there, it spread to other uninfected COMMAND.COM files each time a user entered any standard DOS command that involved disk access. This limited its spread to floppy disks that contained, usually, a full operating system.

Later viruses quickly overcame this limitation, sometimes with fairly clever programming. Virus writers might, for instance, have their virus add its code to the beginning of an executable file, so that when users start a program, the virus code executes immediately, then transfers control back to the legitimate software, which runs as though nothing unusual has happened. Once it activates, the virus "hooks" or "traps" requests that legitimate software makes to the operating system and substitutes its own responses.

Particularly clever viruses can even subvert attempts to clear them from memory by trapping the CTRL+ALT+DEL keyboard sequence for a warm reboot, then faking a restart. Sometimes the only outward indication that anything on your system is amiss—before any payload detonates, that is—might be a small change in the file size of infected legitimate software.

Stealth, mutation, encryption, and polymorphic techniques

Unobtrusive as they might be, changes in file size and other scant evidence of a virus infection usually gives most anti-virus software enough of a scent to locate and remove the offending code. One of the virus writer's principal challenges, therefore, is to find ways to hide his or her handiwork. The earliest disguises were a mixture of innovative programming and obvious giveaways. The Brain virus, for instance, redirected requests to see a disk's boot sector away from the actual location of the infected sector to the new location of the boot files, which the virus had moved. This "stealth" capability enabled this and other viruses to hide from conventional search techniques.

Because viruses needed to avoid continuously reinfecting host systems—doing so would quickly balloon an infected file's size to easily detectable proportions or would consume enough system resources to point to an obvious culprit—their authors also needed to tell them to leave certain files alone. They addressed this problem by having the virus write a characteristic byte sequence or, in 32-bit Windows operating systems, create a particular registry key that would flag infected files with the software equivalent of a "do not disturb" sign. Although that kept the virus from giving itself away immediately, it opened the way for anti-virus software to use the "do not disturb" sequence itself, along with other characteristic patterns that the virus wrote into files it infected, to spot its "code signature." Most anti-virus vendors now compile and regularly update a database of virus "definitions" that their products use to recognize those code signatures in the files they scan.

In response, virus writers found ways to conceal the code signatures. Some viruses would "mutate" or transform their code signatures with each new infection. Others encrypted themselves and, as a result, their code signatures, leaving only a couple of bytes to use as a key for decryption. The most sophisticated new viruses employed stealth, mutation and encryption to appear in an almost undetectable variety of new forms. Finding these "polymorphic" viruses required software engineers to develop very elaborate programming techniques for anti-virus software.

Macro viruses

By 1995 or so, the virus war had come to something of a standstill. New viruses appeared continuously, prompted in part by the availability of ready-made virus “kits” that enabled even some non-programmers to whip up a new virus in no time. But most existing anti-virus software easily kept pace with updates that detected and disposed of the new virus variants, which consisted primarily of minor tweaks to well-known templates.

But 1995 marked the emergence of the Concept virus, which added a new and surprising twist to virus history. Before Concept, most virus researchers thought of data files—the text, spreadsheet, or drawing documents created by the software you use—as immune to infection. Viruses, after all, are programs and, as such, needed to run in the same way executable software did in order to do their damage. Data files, on the other hand, simply stored information that you entered when you worked with your software.

That distinction melted away when Microsoft began adding macro capabilities to Word and Excel, the flagship applications in its Office suite. Using the stripped-down version of its Visual Basic language included with the suite, users could create document templates that would automatically format and add other features to documents created with Word and Excel. Other vendors quickly followed suit with their products, either using a variation of the same Microsoft macro language or incorporating one of their own. Virus writers, in turn, seized the opportunity that this presented to conceal and spread viruses in documents that you, the user, created yourself.

The exploding popularity of the Internet and of e-mail software that allowed users to attach files to messages ensured that macro viruses would spread very quickly and very widely. Within a year, macro viruses became the most potent virus threat ever.

On the frontier

Even as viruses grew more sophisticated and continued to threaten the integrity of computer systems we all had come to depend upon, still other dangers began to emerge from an unexpected source: the World Wide Web. Once a repository of research papers and academic treatises, the web has transformed itself into perhaps the most versatile and adaptable medium ever invented for communication and commerce.

Because its potential seems so vast, the web has attracted the attention and the developmental energies of nearly every computer-related company in the industry.

Convergences in the technologies that have resulted from this feverish pace of invention have given website designers tools they can use to collect and display information in ways never previously available. Websites soon sprang up that could send and receive e-mail, formulate and execute queries to databases using advanced search engines, send and receive live audio and video, and distribute data and multimedia resources to a worldwide audience.

Much of the technology that made these features possible consisted of small, easily downloaded programs that interact with your browser software and, sometimes, with other software on your hard disk. This same avenue served as an entry point into your computer system for other—less benign—programs to use for their own purposes.

Java, ActiveX, and scripted objects

These programs, whether beneficial or harmful, come in a variety of forms. Some are special-purpose miniature applications, or “applets,” written in Java, a programming language first developed by Sun Microsystems. Others are developed using ActiveX, a Microsoft technology that programmers can use for similar purposes.

Both Java and ActiveX make extensive use of prewritten software modules, or “objects,” that programmers can write themselves or take from existing sources and fashion into the plug-ins, applets, device drivers and other software needed to power the web. Java objects are called “classes,” while ActiveX objects are called “controls.” The principle difference between them lies in how they run on the host system. Java applets run in a Java “virtual machine” designed to interpret Java programming and translate it into action on the host machine, while ActiveX controls run as native Windows software that links and passes data among other Windows programs.

The overwhelming majority of these objects are useful, even necessary, parts of any interactive website. But despite the best efforts of Sun and Microsoft engineers to design security measures into them, determined programmers can use Java and ActiveX tools to plant harmful objects on websites, where they can lurk until visitors unwittingly allow them access to vulnerable computer systems.

Unlike viruses, harmful Java and ActiveX objects usually don’t seek to replicate themselves. The web provides them with plenty of opportunities to spread to target computer systems, while their small size and innocuous nature makes it easy for them to evade detection. In fact, unless you tell your web browser specifically to block them, Java and ActiveX objects download to your system automatically whenever you visit a website that hosts them.

Instead, harmful objects exist to deliver their equivalent of a virus payload. Programmers have written objects, for example, that can read data from your hard disk and send it back to the website you visited, that can “hijack” your e-mail account and send out offensive messages in your name, or that can watch data that passes between your computer and other computers.

Even more powerful agents have begun to appear in applications that run directly from websites you visit. JavaScript, a scripting language with a name similar to the unrelated Java language, first appeared in Netscape Navigator, with its implementation of version 3.2 of the Hyper Text Markup Language (HTML) standard. Since its introduction, JavaScript has grown tremendously in capability and power, as have the host of other scripting technologies that have followed it—including Microsoft VBScript and Active Server Pages, Allaire Cold Fusion, and others. These technologies now allow software designers to create fully realized applications that run on web servers, interact with databases and other data sources, and directly manipulate features in the web browser and e-mail client software running on your computer.

As with Java and ActiveX objects, significant security measures exist to prevent malicious actions, but virus writers and security hackers have found ways around these. Because the benefits these innovations bring to the web generally outweigh the risks, however, most users find themselves calculating the tradeoffs rather than shunning the technologies.

Where next?

Malicious software has even intruded into areas once thought completely out of bounds. Users of the mIRC Internet Relay Chat client, for example, have reported encountering viruses constructed from the mIRC scripting language. The chat client sends script viruses as plain text, which would ordinarily preclude them from infecting systems, but older versions of the mIRC client software would interpret the instructions coded into the script and perform unwanted actions on the recipient’s computer.

The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it. Late in 1999, another virus writer demonstrated this rule yet again with a proof-of-concept virus called VBS/Bubbleboy that ran directly within the Microsoft Outlook e-mail client by hijacking its built-in VBScript support. This virus crossed the once-sharp line that divided plain-text e-mail messages from the infectable attachments they carried. VBS/Bubbleboy didn’t even require you to open the e-mail message—simply viewing it from the Outlook preview window could infect your system.

How to protect yourself

McAfee anti-virus software already gives you an important bulwark against infection and damage to your data, but anti-virus software is only one part of the security measures you should take to protect yourself. Anti-virus software, moreover, is only as good as its latest update. Because as many as 200 to 300 viruses and variants appear each month, the virus definition (.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 means that the files you need to combat new viruses appear as soon as—and often before—you need them.

Most other security measures are common sense—checking disks you receive from unknown or questionable sources, either with anti-virus software or some kind of verification utility, is always a good idea. Malicious programmers have gone so far as to mimic the programs you trust to guard your computer, pasting a familiar face on software with a less-than-friendly purpose. Neither McAfee nor any other anti-virus software, however, can detect when someone substitutes an as-yet unidentified Trojan horse or other malicious program for one of your favorite shareware or commercial utilities—that is, until after the fact.

Web and Internet access poses its own risks. VirusScan* anti-virus software gives you the ability to block dangerous web sites so that users can't inadvertently download malicious software from known hazards; it also catches hostile objects that get downloaded anyway. But having a top-notch firewall in place to protect your network and implementing other network security measures is a necessity when unscrupulous attackers can penetrate your network from nearly any point on the globe, whether to steal sensitive data or implant malicious code. You should also make sure that your network is not accessible to unauthorized users, and that you have an adequate training program in place to teach and enforce security standards. To learn about the origin, behavior and other characteristics of particular viruses, consult the Virus Information Library maintained on the AVERT website.

McAfee can provide you with other powerful software in the Active Virus Defense* (AVD) and Total Virus Defense (TVD) suites, the most comprehensive anti-virus solutions available. Related companies within the Network Associates family provide other technologies that also help to protect your network, including the PGP Security CyberCop product line, and the Sniffer Technologies network monitoring product suite. Contact your Network Associates representative, or visit the Network Associates website, to find out how to enlist the power of these security solutions on your side.

How to contact McAfee and Network Associates

Customer service

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

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

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

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

Network Associates Customer Service
4099 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 B, "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 Southeast Asia

International contact information

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

Network Associates Australia

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

Network Associates Austria

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

Network Associates Belgique

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

Network Associates do Brasil

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

Network Associates Canada

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

Network Associates People's Republic of China

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 Hong Kong

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

Network Associates Japan, Inc.

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

**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
Deutschland GmbH**

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

Network Associates Srl

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

Network Associates Latin America

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

**Network Associates
International B.V.**

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

**Network Associates
Portugal**

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

**Net Tools Network Associates
South Africa**

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 31](#).

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. See “Using the VirusScan application” on page 163 for details.
- **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. See [“Creating and Configuring Scheduled Tasks”](#) on page 193 for details.

- **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. See [“Using the VShield Scanner”](#) on page 87 for details.

- **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. See [“Scanning Microsoft Exchange and Outlook mail”](#) on page 257 for details.
- **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 v8.x or earlier. See [“Choosing Detection options”](#) on page 118 for details.
- **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. See [“Using the Alert Manager Client Configuration utility”](#) on page 285 for details.
- **The ScreenScan utility.** This optional component scans your computer as your screen saver runs during idle periods. See [“Using the ScreenScan utility”](#) on page 273 for details.

- **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. See [“Using the SendVirus utility to submit a file sample” on page 78](#) for details.
- **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. See [“Using the Emergency Disk Creation utility” on page 49](#) for details.
- **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 25, 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 anti-virus software 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. You can secure this control panel with a password to prevent unauthorized users from disabling VirusScan software.

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

McAfee distributes VirusScan software in two ways: 1) as an archived file that you can download from the McAfee website; and 2) on CD-ROM. Although the method you use to transfer VirusScan files from an archive you download differs from the method you use to transfer files from a CD-ROM you place in your CD-ROM drive, the installation steps you follow after that are the same for both distribution types. Review the system requirements shown below to verify that VirusScan software will run on your system, then move to [“Preparing to install VirusScan software” on page 36.](#)

System requirements

VirusScan software will install and run on any IBM PC or PC-compatible computer equipped with:

- A processor equivalent to at least an Intel Pentium-class or compatible processor. McAfee recommends an Intel Pentium processor or Celeron processor running at a minimum of 166 MHz.
- A CD-ROM drive. If you downloaded your copy of VirusScan software, this is an optional item.
- 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 at least 20MB.
- Microsoft Windows 95, Windows 98, Windows NT Workstation v4.0 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.


Other recommendations

To take full advantage of VirusScan software’s automatic update features, you should have an Internet connection, either through your local-area network, or via a high-speed modem and an Internet service provider.

Preparing to install VirusScan software


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 61](#).

- **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 39](#) 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 37](#).

 **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 options

The [“Installation steps”](#) section describes how to install VirusScan software with its most common options on a single computer or workstation. You can choose to do a Typical setup—which installs commonly used VirusScan components but leaves out some VShield modules and the ScreenScan utility—or you can choose to do a Custom setup, which gives you the option to install all VirusScan components.

To learn how to install VirusScan software on more than one computer at a time, or to modify your installation to implement a corporate anti-virus policy, see the *VirusScan Administrator's Guide*, which describes how to install and configure VirusScan software to meet nearly any business contingency. You can also use McAfee ePolicy Orchestrator software to distribute and configure VirusScan software on thousands of network desktop computers. See the *ePolicy Orchestrator Administrator's Guide* for details.

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).

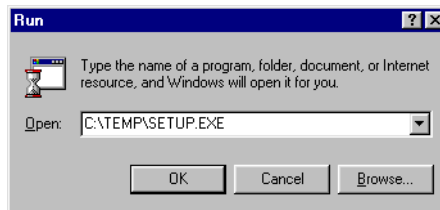


Figure 2-1. Run dialog box

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 whether it should check to see whether you have previous VirusScan versions installed on your computer (see [Figure 2-2 on page 38](#)).

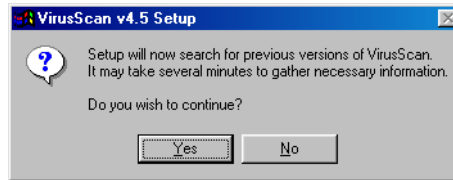


Figure 2-2. Previous versions dialog box

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 40](#)) 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 55](#).

When your computer restarts, Setup will continue from where it left off. The Setup welcome panel will appear (see [Figure 2-3 on page 39](#)).

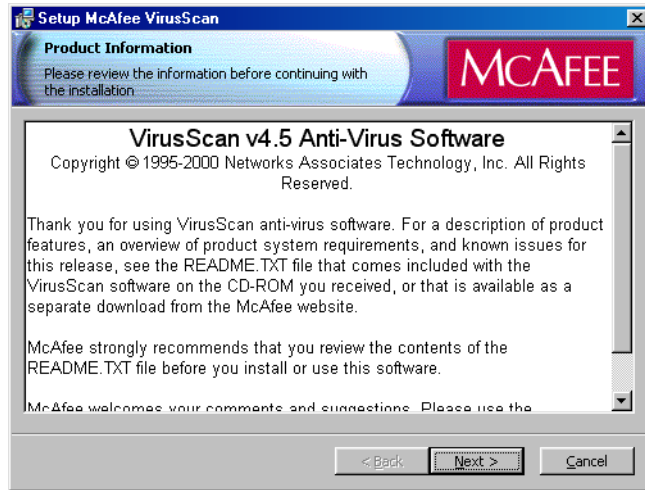


Figure 2-3. Setup welcome panel

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 41](#) or [Figure 2-7 on page 42](#)). Skip to [Step 9 on page 42](#) 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 (see [Figure 2-4 on page 40](#)).

-
- ❏ **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 38](#), but will *not* preserve any previous VShield scanner settings.
-

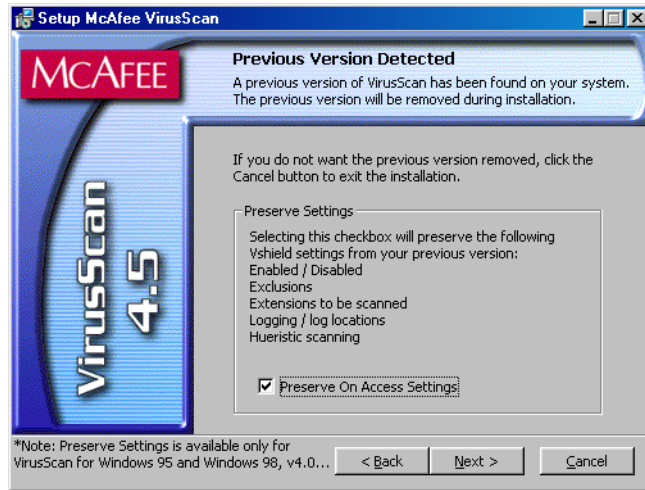


Figure 2-4. Previous Version Detected panel

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 (Figure 2-5).

If you have no incompatible software on your system and your computer runs Windows 95 or Windows 98, skip to [Step 10 on page 42](#) 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 42](#) 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 41](#)).

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.”](#)

- **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 (see [Figure 2-7 on page 42](#)).

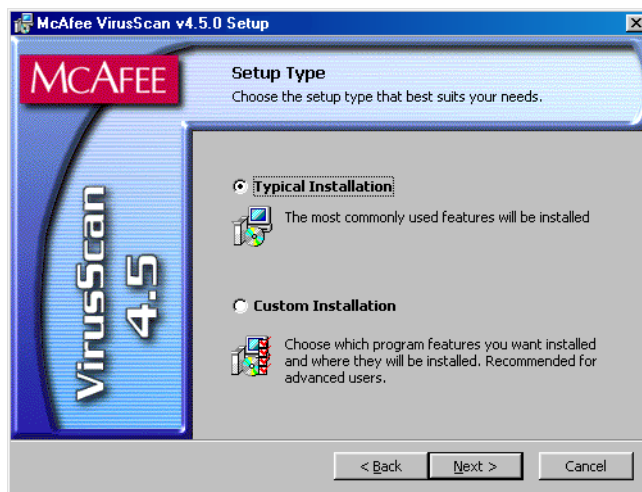


Figure 2-7. Setup Type panel

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 27.

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 45](#) to continue with your installation.

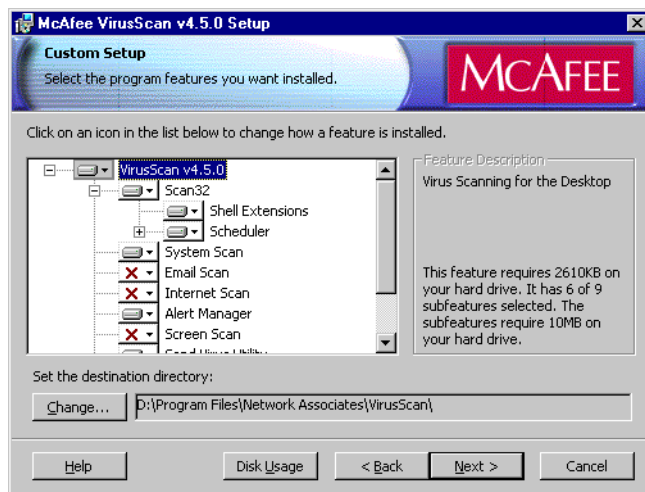







Figure 2-8. Custom Setup panel

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](#)).

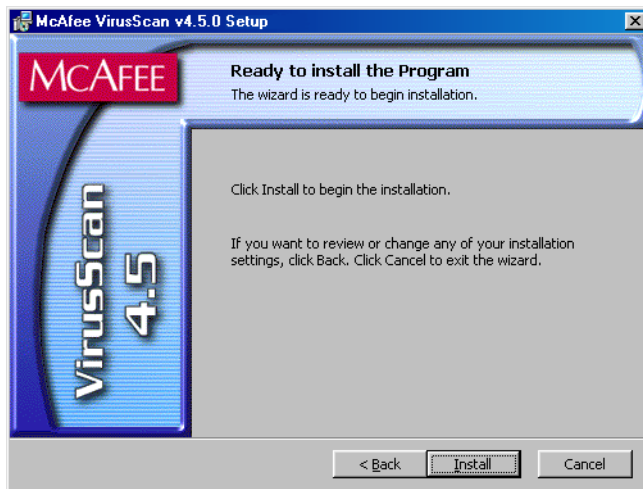


Figure 2-9. Ready to Install panel

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 (Figure 2-10).

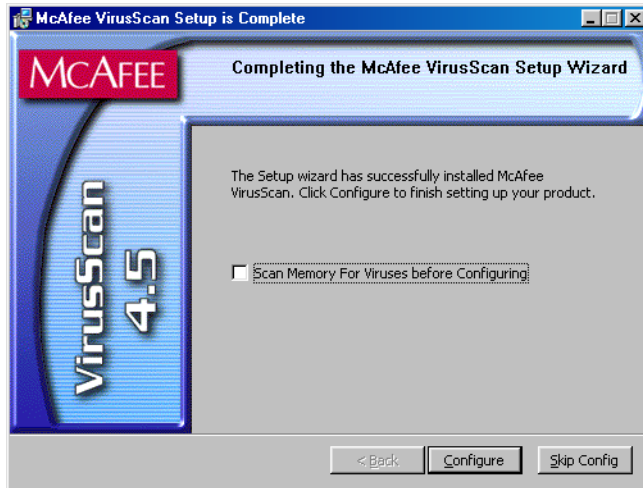


Figure 2-10. Completing Setup panel

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 ([Figure 2-11](#)).

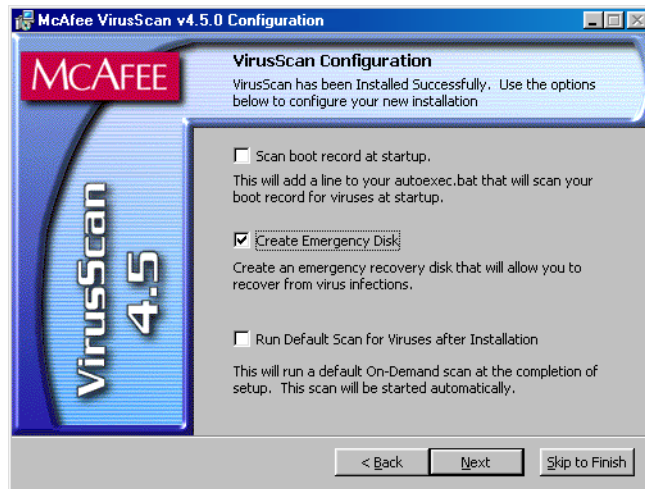


Figure 2-11. Configuration panel

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 49](#).

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).

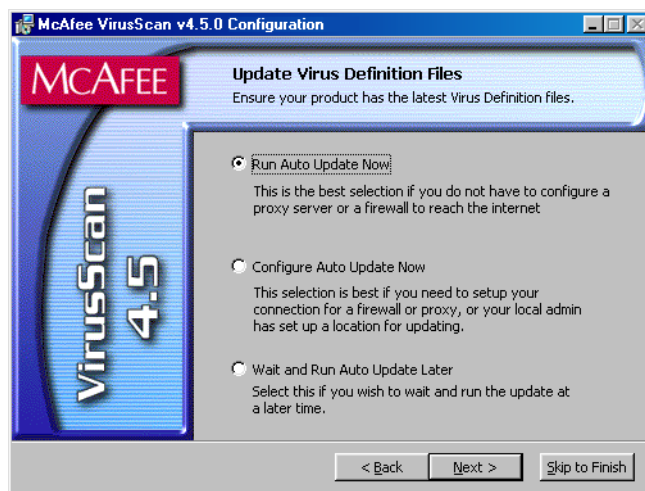


Figure 2-12. Update Virus Definition Files panel

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 237](#).

- **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.”](#)

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 ([Figure 2-13](#)).

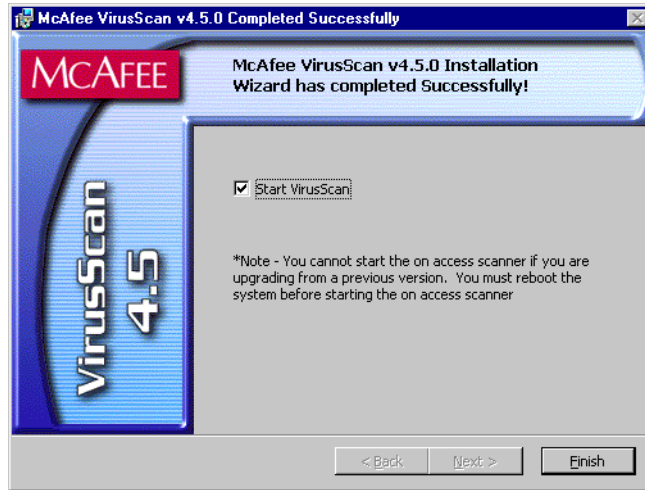


Figure 2-13. Successful Installation panel

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 51](#). 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.

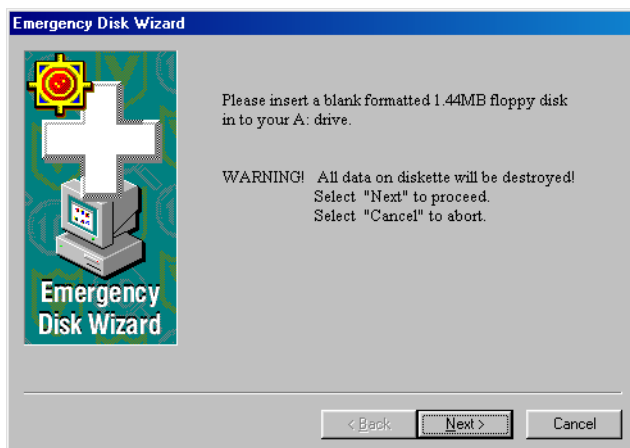


Figure 2-16. Emergency Disk informational panel

- If you chose to format your disk with the NAI-OS, the wizard displays an informational panel (see [Figure 2-16 on page 51](#)).

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 (see [Figure 2-17 on page 52](#)).

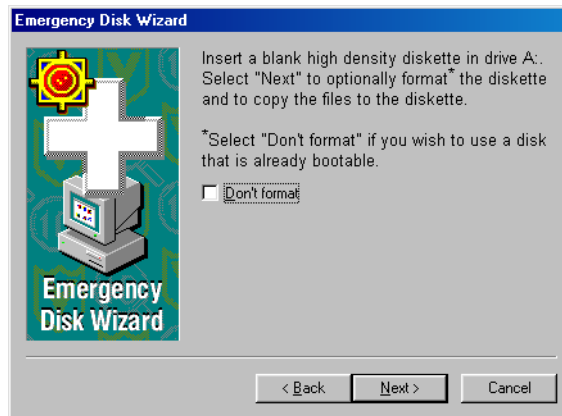


Figure 2-17. Third Emergency Disk panel

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 53](#) 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 (see [Figure 2-18 on page 53](#)).

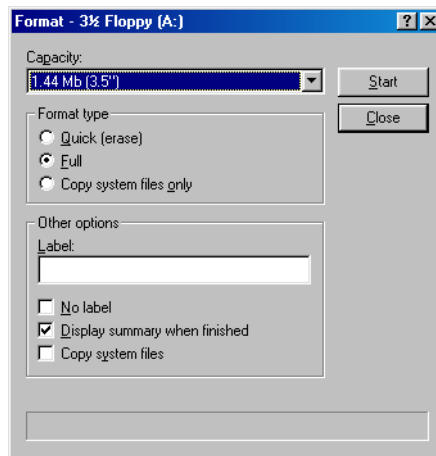


Figure 2-18. Windows Format dialog box

- 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 ([Figure 2-19](#)).

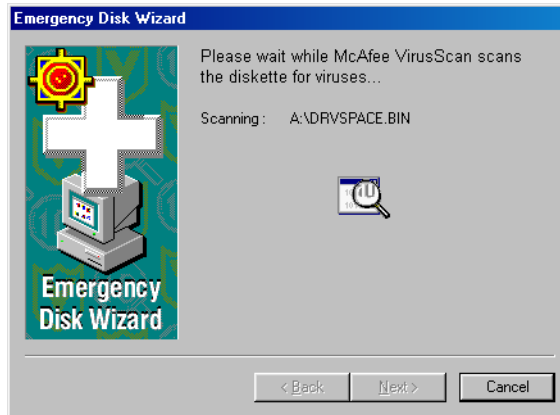


Figure 2-19. Scanning Emergency Disk for viruses

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 61 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 VirusScan installation

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

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).

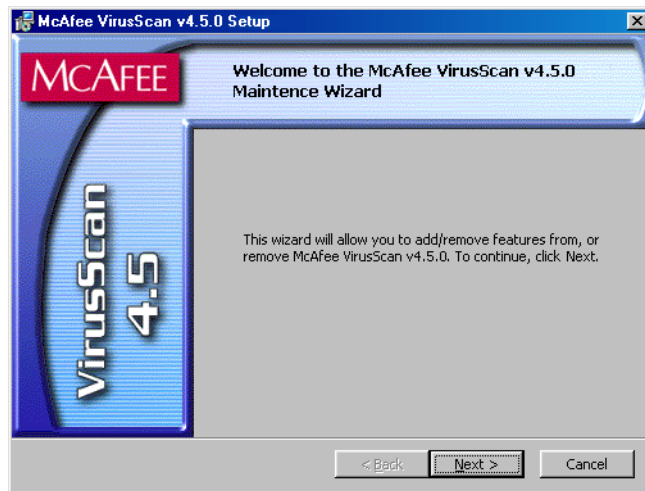


Figure 2-21. First maintenance panel

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

Setup displays the Program Maintenance wizard panel (see [Figure 2-22 on page 58](#)).

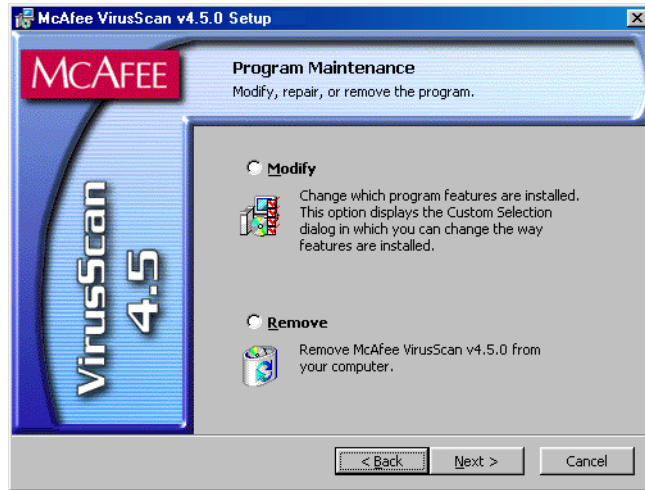


Figure 2-22. Program Maintenance panel

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 43](#)). Start with [Step 12 on page 44](#) to choose the components you want to add or remove.

 - ☐ **NOTE:** This panel differs from the one shown on [page 44](#): 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 59](#)).

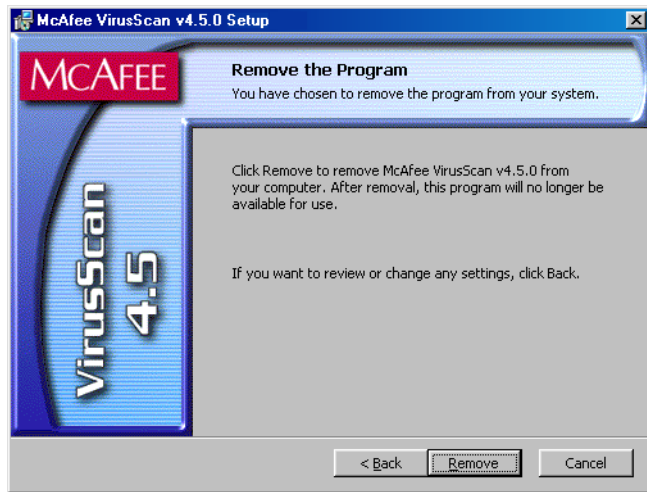


Figure 2-23. Remove the Program panel

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.

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 5, "Using the VirusScan application,"](#) 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 62](#).

 **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 49](#).

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 7, “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 xix.

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 the VShield Scanner,”](#) 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. To learn more about these options, see [“Choosing Action options” on page 107](#).

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 77](#)). 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.

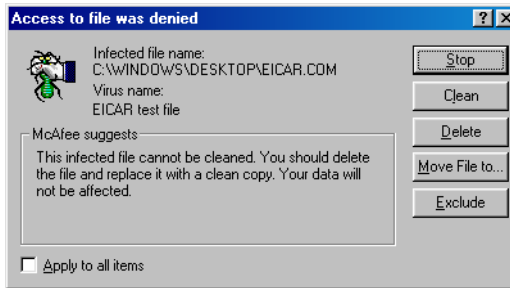


Figure 3-1. Initial System Scan response options

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).

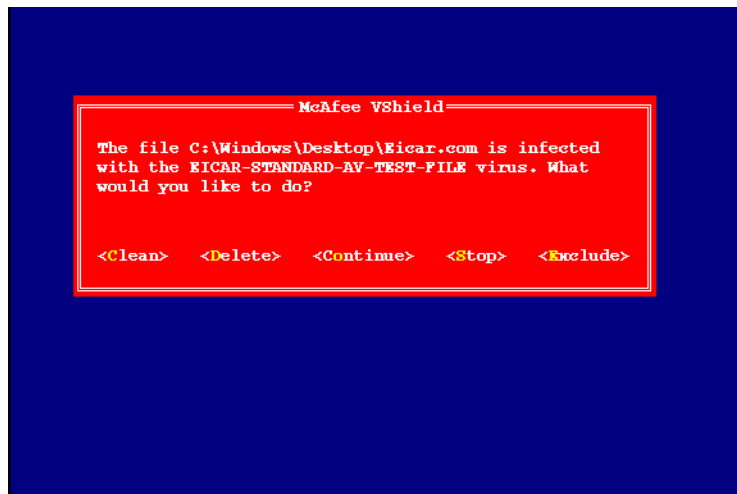


Figure 3-2. Full-screen Warning - System Scan response options

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).

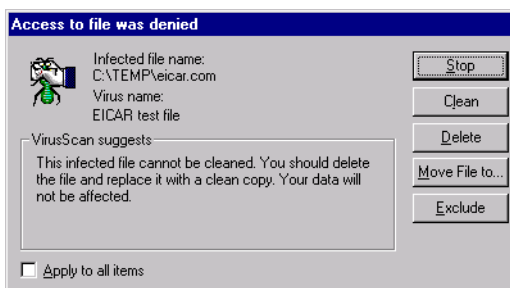


Figure 3-3. E-mail Scan module response options

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.

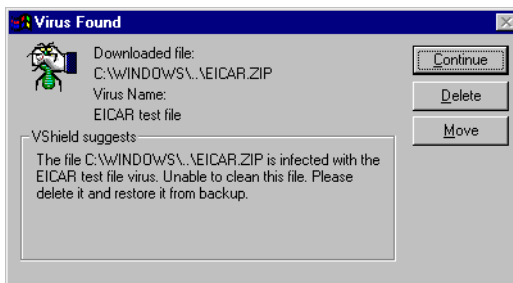


Figure 3-4. Download Scan response options

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).

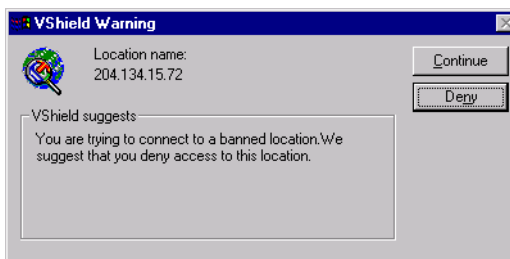


Figure 3-5. Internet Filter response options

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).

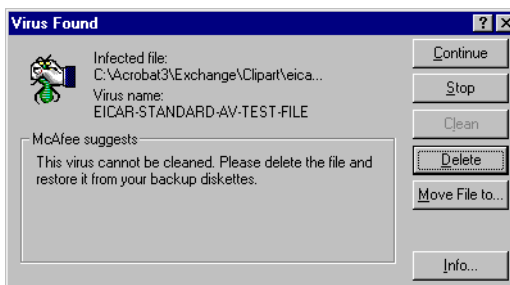


Figure 3-6. VirusScan response options

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.

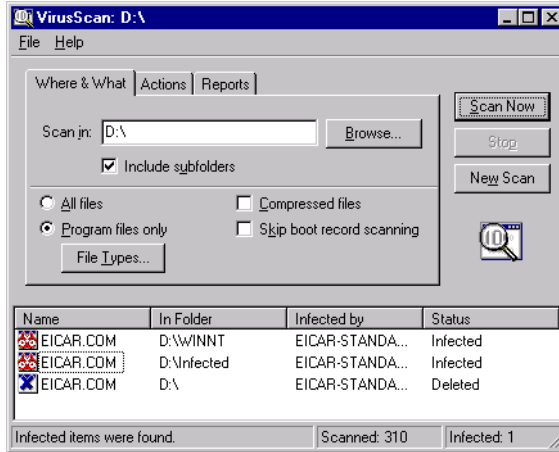


Figure 3-7. VirusScan main window

- **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 72, 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 76 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).

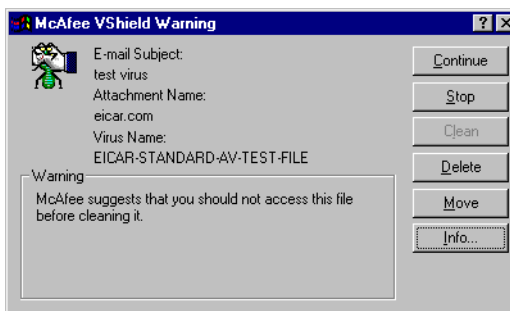


Figure 3-8. E-Mail Scan response options

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.

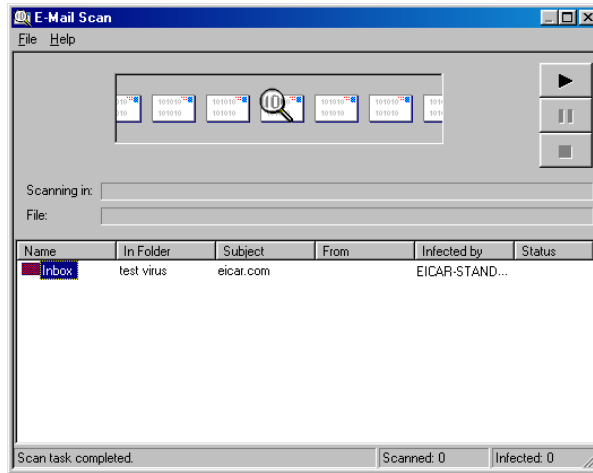


Figure 3-9. E-Mail Scan extension window

- 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).

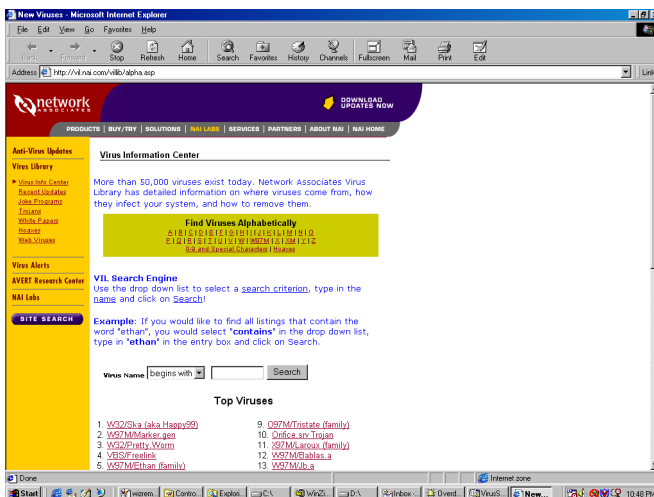


Figure 3-10. Network Associates Virus Information Library page

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.”](#)

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 75](#)), 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](#)).

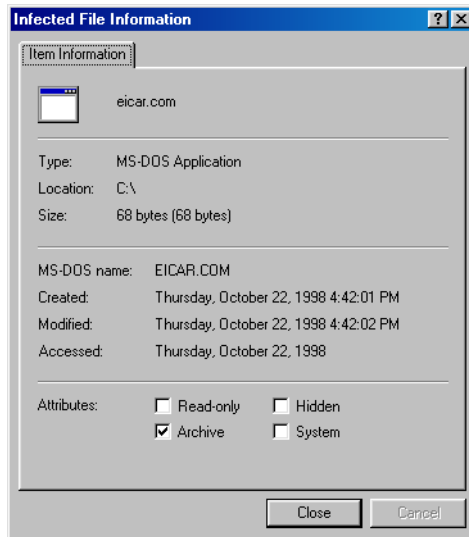


Figure 3-11. Infected File Information property page

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.

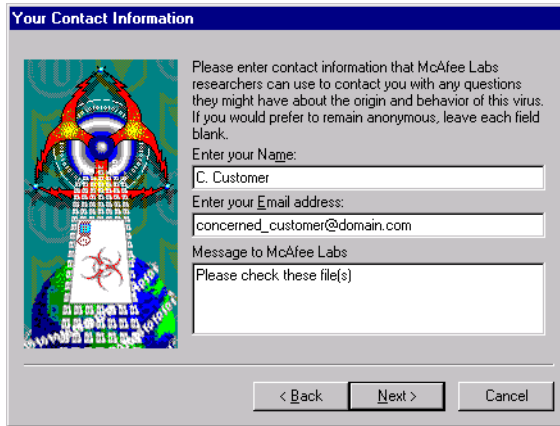


Figure 3-13. Your Contact Information panel

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).

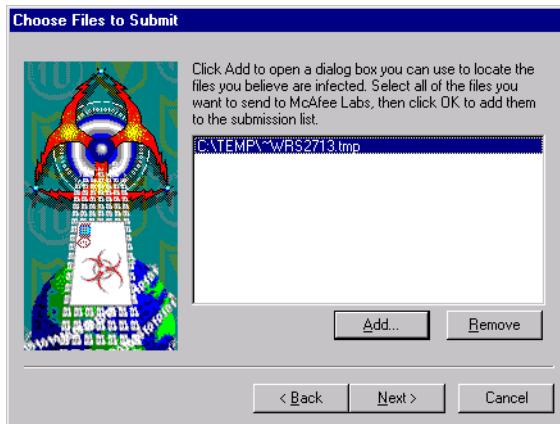


Figure 3-14. Choose Files to Submit panel

- 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).

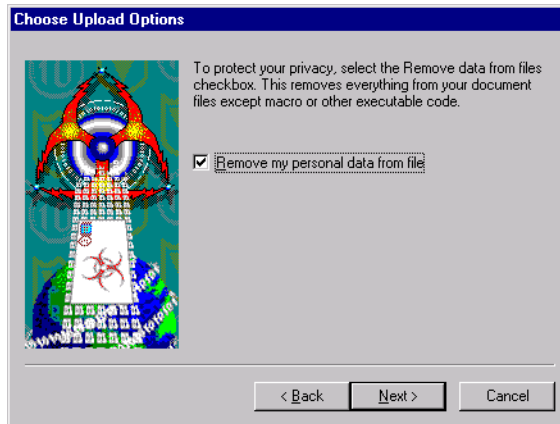


Figure 3-15. Choose Upload options panel

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).

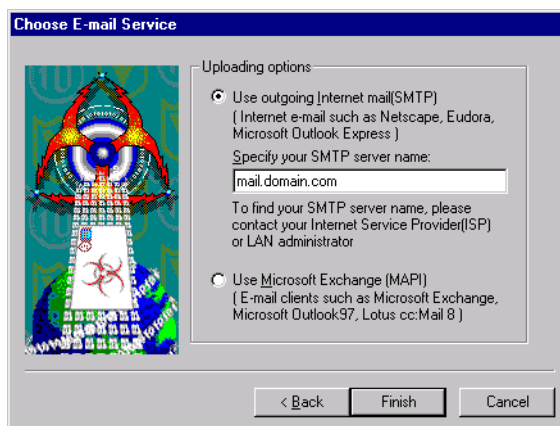


Figure 3-16. Choose E-mail Service panel

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	<code>virus_research@nai.com</code>
In the United Kingdom	<code>vsample@nai.com</code>
In Germany	<code>virus_research_de@nai.com</code>
In Japan	<code>virus_research_japan@nai.com</code>
In Australia	<code>virus_research_apac@nai.com</code>
In the Netherlands	<code>virus_research_europe@nai.com</code>

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 Toranomom Mori-bldg. 33
 3-8-21 Toranomom, 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.

What does the VShield scanner do?

McAfee desktop anti-virus products use two general methods to protect your system. The first method, background scanning, operates continuously, watching for viruses as you use your computer for everyday tasks. In the VirusScan product, the VShield scanner performs this function. A second method allows you to initiate your own scan operations. The VirusScan application generally handles these tasks. To learn more about the application, see [Chapter 5, “Using the VirusScan application.”](#)


Depending on how you configure it, the VShield scanner can monitor any file that arrives on or leaves your system, whether on floppy disk, over your network, in file attachments that accompany e-mail messages, or from the Internet. The scanner looks for viruses as you open, save, copy, rename or otherwise modify your files, and it probes your computer's memory during any file activity. The scanner starts when you start your computer, and stays in memory until you shut it or your system down. The scanner also includes optional features that guard against hostile Java applets and ActiveX controls, and that keep your computer from connecting to dangerous Internet sites.

The VShield scanner consists of five related modules, each of which has a specialized function. You can configure settings for all of these modules in the VShield Properties dialog box. The VShield modules are:


- **System Scan.** This module looks for viruses on your hard disk as you work with your computer. It tracks files as your system or other computers read files from your hard disk or write files to it. It can also scan floppy disks and network drives mapped to your system.
- **E-Mail Scan.** This module scans e-mail messages and message attachments that you receive via intraoffice e-mail systems, and via the Internet. It scans your Microsoft Exchange or Outlook mailbox on your Microsoft Exchange server, and older cc:Mail e-mail systems.

It works in conjunction with the Download Scan module to scan Internet mail that arrives via Simple Mail Transfer Protocol (SMTP) or Post Office Protocol (POP-3) sources.

- **Download Scan.** This module scans files that you download to your system from the Internet. If you have enabled the Internet mail option in the E-Mail Scan module, this will include e-mail and file attachments that arrive via SMTP or POP-3 e-mail systems, which include such e-mail client programs as Eudora Pro, Microsoft Outlook Express, NetScape mail, and America Online mail.
- **Internet Filter.** This module looks for and blocks hostile Java classes and ActiveX controls from downloading to and executing from your system as you visit Internet sites. It can also block your browser from connecting to potentially dangerous Internet sites that harbor malicious software.

 **IMPORTANT:** To use the E-Mail Scan, Download Scan or Internet Filter modules, you must install them from the Custom option in Setup. To learn how to do so, see [Chapter 2, "Installing VirusScan Software."](#)

- **Security.** This module provides password protection for the remaining VShield modules. You can protect any or all individual module property pages and set a password to prevent unauthorized changes.

 **NOTE:** Because the VShield scanner runs continuously, you should not install or run more than one VShield scanner on the same workstation. Doing so can cause the scanners to interfere with each others' operations.

Why use the VShield scanner?

The VShield scanner has unique capabilities that make it an integral part of the VirusScan comprehensive anti-virus software security package. These capabilities include:

- **On-access scanning.** This means that the scanner looks for viruses in files that you open, copy, save, or otherwise modify, and files that you read from or write to floppy disks and network drives. It therefore can detect and stop viruses as soon as they appear on your system, including those that arrive via e-mail or as downloads from the Internet. This means you can make the VShield scanner both your first line of anti-virus defense, and your backstop protection in between each scan operation that you perform. The VShield scanner detects viruses in memory and as they attempt to execute from within infected files.

- **Malicious object detection and blocking.** The VShield scanner can block harmful ActiveX and Java objects from gaining access to your system, before they pose a threat. The scanner does this by scanning the hundreds of objects you download as you connect to the web or to other Internet sites, and the file attachments you receive with your e-mail. It compares these items against a current list of harmful objects that it maintains, and blocks those that could cause problems.
- **Internet site filtering.** The VShield scanner comes with a list of dangerous web- or Internet sites that pose a hazard to your system, usually in the form of downloadable malicious software. You can add any other site that you want to keep your browser software from connecting to, either by listing its Internet Protocol (IP) address or its domain name.
- **Automatic operation.** The VShield scanner integrates with a range of browser software and e-mail client applications. This allows the scanner to log on to and scan your e-mail attachments for viruses before they ever reach your computer.

If you connect to the Internet or work on a network in any capacity, leaving this component running at all times can significantly improve your ability to detect and dispose of harmful software before it has a chance to damage your system.

Browser and e-mail client support

The VShield scanner works seamlessly with many of the most popular web browsers and e-mail client software available for the Windows platform. To work with your browser, the scanner requires no setup beyond what you have already done to connect your computer to the Internet. You must configure the scanner, however, to work correctly with your e-mail client software. See [“Using the VShield configuration wizard” on page 95](#) or [“Setting VShield scanner properties” on page 99](#) to learn how to do the required setup.

McAfee has tested these web browsers and verified that they work correctly with the VShield scanner:

- Netscape Navigator v3.x
- Netscape Navigator v4.0.x (not including v4.0.6)
- Microsoft Internet Explorer v3.x
- Microsoft Internet Explorer v4.x

McAfee has also tested these e-mail clients and verified that they work with the VShield Download Scan module:

- Microsoft Outlook Express
- Qualcomm Eudora v3.x and v4.x
- Netscape Mail (included with most versions of Netscape Navigator and Netscape Communicator)
- America Online mail v3.0 and v4.0

In order to work with the VShield E-mail Scan module, your corporate e-mail system must use Lotus cc:Mail, Microsoft Exchange, or Microsoft Outlook client. McAfee has tested these clients and has verified that they work correctly with the E-mail Scan module:

- Microsoft Exchange v4.0, v5.0 and v5.5
- Microsoft Outlook 97 and Outlook 98
- Lotus cc:Mail v6.x, v7.x, and v8.x (not MAPI-compliant)


McAfee does not certify VShield software compatibility with client software not listed above.

Enabling or starting the VShield scanner

At the end of the VirusScan installation, Setup asks if you want to enable the VShield scanner at that time. If you agree, the VShield scanner should load into memory immediately and begin working with a default set of options that give you basic anti-virus protection. If you do not agree, the VShield scanner will load automatically the next time you restart your computer.

When the VShield scanner first starts, it displays an icon in the Windows system tray that indicates which of its modules are active. To learn what each icon state means, see [“Understanding the VShield system tray icon states” on page 94](#).

At first, the scanner enables only its System Scan module, which scans viruses that arrive on your system from floppy disks and other removable media, from local-area network connections, and similar areas. The System Scan module also scans files that arrive via your e-mail system and from the Internet, but to do so, it requires the aid of the other VShield modules: E-Mail Scan, Download Scan, and Internet Filter.

 **IMPORTANT:** To use the E-Mail Scan, Download Scan or Internet Filter modules, you must install them from the Custom option in Setup. To learn how to do so, see [Chapter 2, “Installing VirusScan Software.”](#)

If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, the VShield scanner loads as a Windows NT service called McShield, which you can see in the Windows Services control panel.


- ❑ **NOTE:** McAfee recommends that you do not start or stop the McShield service from the Windows control panel. Instead, you can stop and restart the scanner from the provided VirusScan control panel. To learn more about how to use the VirusScan control panel, see [“Understanding the VirusScan control panel” on page 281](#)

If your computer runs Windows 95 or Windows 98, the scanner loads in a way that mimics a Windows service on that platform. This service is not visible in the Windows user interface.

Starting the scanner automatically

If the VShield scanner does not start automatically, you can set it to do so in the VirusScan 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  to open it. If you have assigned a password to protect your VShield settings, the control panel will ask for that password in order to give you access. Enter the correct password in the text box that appears, then click the Components tab ([Figure 4-1](#)).

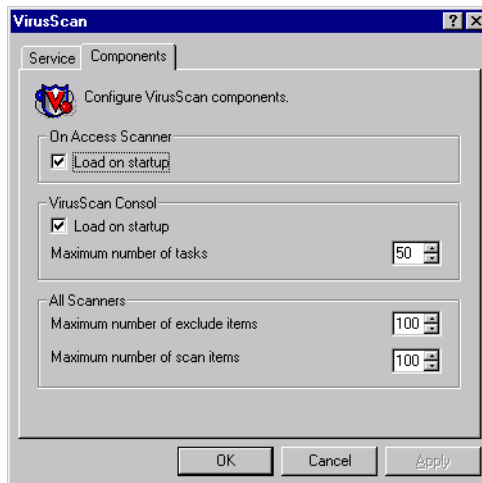


Figure 4-1. VirusScan control panel - Components page

3. Select the **Load VShield on startup** checkbox at the top of the Components property page, then click **OK** to close the control panel.


Enabling the VShield scanner and its modules

Once you have all VShield components installed, you can use any of four methods to enable them, in various combinations.

- ❏ **NOTE:** Enabling a module means activating it and loading it into your computer's memory for use. The VShield scanner can start and remain active in memory even with none of its modules enabled.

Method 1: Use the VShield shortcut menu


Follow these steps:

1. Right-click the VShield icon  in the Windows system tray to display its shortcut menu.
2. Point to **Quick Enable**.
3. Choose one of the module names shown without a check mark. Module names that have a check mark beside them are active. Those without a check mark are inactive. If you use this method to enable a module, it remains enabled until you restart your VirusScan software or your computer. At that point, its state will depend on whether you have enabled or disabled the module in the VirusScan Properties dialog box.

Depending on which combination of modules you enable, the VShield icon will display a different state. To learn what the different icon states mean, see [“Understanding the VShield system tray icon states”](#) on page 94.

Method 2: Use the System Scan Status dialog box

Follow these steps:

1. Double-click the VShield icon  in the Windows system tray to open the System Scan Status dialog box ([Figure 4-1](#)).

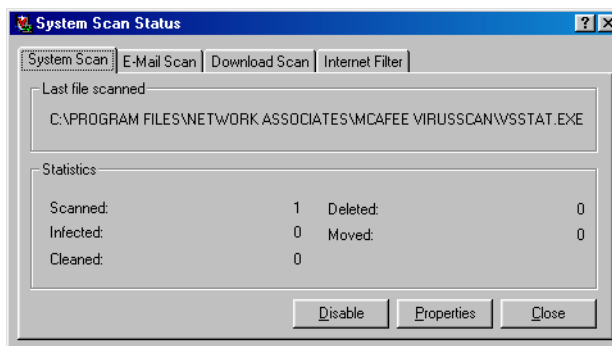



Figure 4-1. System Scan Status dialog box

- For each module that you want to enable, click the corresponding tab, then click **Enable**. The same button in the property page for active modules will read **Disable**.
- Click **Close** to close the dialog box.

Depending on which combination of modules you enable, the VShield icon will display a different state.

Method 3: Use the VShield Properties dialog box

Follow these steps:

- Right-click the VShield icon  in the Windows system tray to display the VShield shortcut menu, point to **Properties**, then choose **System Scan** to open the VShield Properties dialog box.

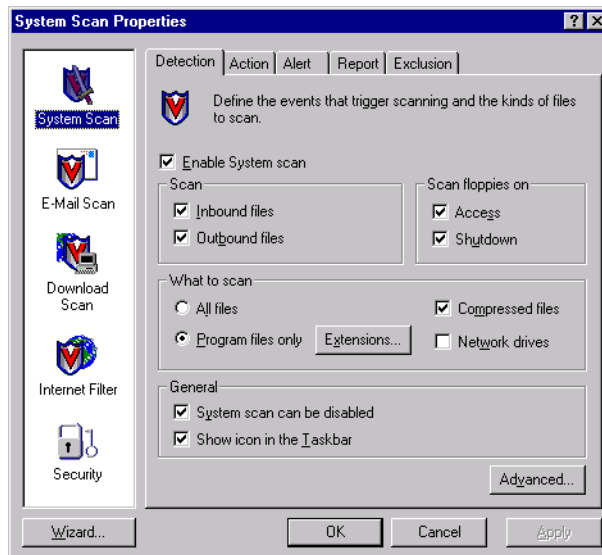



Figure 4-2. VShield Properties dialog box


- For each module that you want to enable, click the corresponding icon along the left side of the dialog box, then click the Detection tab.
- Select the **Enable** checkbox at the top of each page.

As you do so, the scanner enables that module. Depending on which combination of modules you enable, the VShield icon displays a different state.

If you enable all of its modules, the scanner will display  in the Windows system tray, unless you clear the **Show icon in the taskbar** checkbox in the System Scan Detection property page.

Method 4: Use the VirusScan Console

Follow these steps:

1. Double-click the VirusScan Console icon  in the Windows system tray to bring the Console window to the foreground.
2. Select VShield in the task list, then choose **Enable** from the **Task** menu.

the Console will enable the System Scan module and any other module you had enabled previously. You cannot use this method to enable individual modules other than the System Scan module.
3. Click the minimize or the close button in the upper-right corner of the Console window to shrink the Console window back to a system tray icon.

NOTE: Do *not* choose **Exit** from the **Task** menu. This will shut the Console down and unload it from memory. To run any tasks you have scheduled, the Console must be active.

Understanding the VShield system tray icon states

The VShield scanner displays four different icon states in the Windows system tray to indicate which, if any, of its modules are active. An active module is one that the VShield scanner has enabled, or loaded into memory, and that is ready to scan inbound and outbound files. An inactive module is one that the VShield scanner has disabled. Such modules do not scan files.

The following table shows and describes each icon state:



This icon means that the VShield scanner has started and all VShield modules are active



This icon means that the System Scan module is active, but one or more of the other VShield modules is inactive



This icon means that the System Scan module is inactive, but one or more of the other VShield modules is active



This icon means that all VShield modules are inactive

Using the VShield configuration wizard

After you install VirusScan software and restart your computer, the VShield scanner loads into memory immediately and begins working with a default set of options that give you basic anti-virus protection. Unless you disable it or one of its modules—or stop it entirely—you never have to worry about starting the scanner or scheduling scan tasks for it.

To ensure more than a minimal level of security, however, you should configure the scanner to work with your e-mail client software and have it examine your Internet traffic closely for viruses and malicious software. The VShield configuration wizard can help you set up many of these options right away—you can then tailor the program to work better in your environment as you become more familiar with the scanner and your system's susceptibility to harmful software.

To start the VShield configuration wizard:


1. Right-click the VShield icon  in the Windows system tray to display the VShield shortcut menu, point to **Properties**, then choose **System Scan** to open the VShield Properties dialog box (see [Figure 4-2 on page 93](#)).
2. Click **Wizard** in the lower-left corner of the dialog box to display the configuration wizard welcome panel ([Figure 4-3](#)).



Figure 4-3. VShield configuration wizard - Welcome panel

3. Click **Next>** to display the System Scan configuration panel (see [Figure 4-4 on page 96](#)).



Figure 4-4. VShield configuration wizard - System Scan panel

Here you can tell the VShield scanner to look for viruses in files susceptible to infection whenever you open, run, copy, save or otherwise modify them. Susceptible files include various types of executable files and document files with embedded macros, such as Microsoft Office files. The System Scan module will also scan files stored on floppy disks whenever you read from or write to them, or when you shut down your computer.

If it finds a virus, the module will sound an alert and prompt you for a response. The module will also record its actions and summarize its current settings in a log file that you can review later.

4. To enable these functions, click **Yes**, then click **Next>**. Otherwise, click **No**, then click **Next>** to continue.

The E-mail Scan wizard panel will appear ([Figure 4-5](#)).



Figure 4-5. VShield configuration wizard - E-mail Scan panel

5. Select the **Enable e-mail scanning** checkbox, then select the checkbox that corresponds to the type of e-mail client you use. Your choices are:
- **Internet e-mail clients.** Select this checkbox if you use a Post Office Protocol (POP-3) or Simple Mail Transfer Protocol (SMTP) e-mail client that sends and receives standard Internet mail directly or through a dial-up connection. If you send and receive e-mail from home and use Netscape Mail, America Online, or such popular clients as Qualcomm's Eudora or Microsoft's Outlook Express, be sure to select this option.
 - **Enable Corporate Mail.** Select this checkbox if you use a proprietary e-mail system at work or in a networked environment. Most such systems use a central network server to receive and distribute mail that individual users send to each other from client applications. Such systems might send and receive mail from outside the network or from the Internet, but they usually do so through a "gateway" application run from the server.

The E-Mail Scan module supports corporate e-mail systems that fall into two general categories:

- **Lotus cc:Mail.** Select this button if you use cc:Mail versions 6.x and later, which use a proprietary Lotus protocol for sending and receiving mail.
- **MAPI-compliant e-mail client.** Select this button if you use Microsoft Exchange or Microsoft Outlook, as your corporate e-mail system.

Specify which e-mail system you use, then click **Next>** to continue.

-
- NOTE:** If you use both types of mail systems, select both checkboxes. Note that the E-Mail Scan module supports only one type of *corporate* e-mail system at a time, however. If you need to verify which e-mail system your office uses, check with your network administrator.

Be sure to distinguish between Microsoft Outlook and Microsoft Outlook Express. Although the two programs share similar names, Outlook 97 and Outlook 98 are MAPI-compliant corporate e-mail systems, while Outlook Express sends and receives e-mail through the POP-3 and SMTP protocols. To learn more about these programs, consult your Microsoft documentation.

The next wizard panel sets options for the VShield Download Scan module (Figure 4-6).



Figure 4-6. VShield Configuration Wizard - Download Scan panel

6. To have the Download Scan module look for viruses in each file that you download from the Internet, select the **Yes, do scan my downloaded files for viruses** checkbox, then click **Next>** to continue.

The module will look for viruses in those files most susceptible to infection and will scan compressed files as you receive them.

Otherwise, select the **No, do not enable download scanning** checkbox, then click **Next>** to continue.

The next wizard panel sets options for the VShield Internet Filter module (Figure 4-7).



Figure 4-7. VShield configuration wizard - Internet Filter panel

7. To have the Internet Filter module block hostile Java and ActiveX objects or dangerous Internet sites that can cause your system harm, select **Yes, enable hostile applet protection and access prevention to unsafe websites**, then click **Next>**.

The Internet Filter module maintains a list of harmful objects and sites that it uses to check the sites you visit and the objects you encounter. If it finds a match, it can either block it automatically, or offer you the chance to allow or deny access.

To disable this function, select **No, do not enable hostile applet protection and access prevention to unsafe websites**, then click **Next>** to continue.

The final wizard panel summarizes the options you chose (Figure 4-8).




Figure 4-8. VShield configuration wizard - summary panel

8. If the summary list accurately reflects your choices, click **Finish** to save your changes and return to the VShield Properties dialog box. Otherwise, click **<Back** to change any options you chose, or **Cancel** to return to the VShield Properties dialog box without saving any of your changes.

Setting VShield scanner properties

To ensure its optimal performance on your computer or in your network environment, the VShield scanner needs to know what you want it to scan, what you want it to ignore, what you want it to do if it finds a virus or other malicious software, and how it should let you know when it has. You can use the configuration wizard to enable most of the scanner's protective options, but if you want complete control over the program and the ability to adapt it to your needs—including the ability to protect your settings with a password—choose your options in the VShield Properties dialog box.

The VShield Properties dialog box consists of a series of property pages that control the settings for each program module. To choose your options, click the icon for the appropriate program module, then click each tab in the VShield Properties dialog box in turn.

To open the VShield Properties dialog box, right-click the VShield icon  in the Windows system tray to display the VShield shortcut menu, point to **Properties**, then choose **System Scan**.

The dialog box appears with the System Scan icon selected ([Figure 4-9](#)).

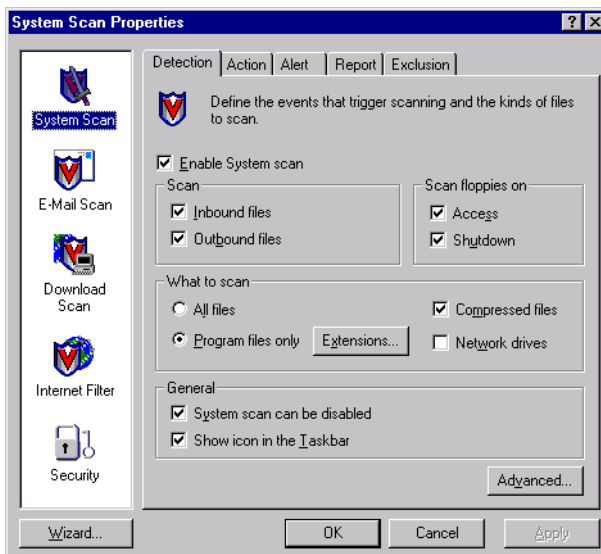



Figure 4-9. System Scan Properties dialog box - Detection page

Configuring the System Scan module



The VShield System Scan module is at the heart of the VShield scanner. It scans files that come from any source, including those that the other VShield modules direct to it from Internet downloads and e-mail messages. The module can check your system for viruses each time you open, run, copy, save, rename or otherwise modify files on your hard disk, on any removable media attached to your computer, or on network drives mapped to your system. It can also detect viruses each time you read from or write to a floppy disk. As an advanced option, you can activate heuristic scanning, which gives the scanner the capability to detect unidentified or unclassified viruses.

The module can take a variety of automatic actions to respond to any viruses it finds, and can report what it has done either with an alert message when it takes the action or in a log file you can examine at your leisure. You can also set it to ask you what to do when it finds a virus.

Elsewhere in this module, you can choose options that tell the VShield scanner to display a state icon  in the Windows taskbar that tells you at a glance which, if any, VShield modules are active. Another option lets you disable the System Scan module. This option might not be available if you run the VirusScan software in secure mode.

To choose your options, click the System Scan icon at the left side of the System Scan Properties dialog box to display the property pages for this module. The next sections describe each of the configuration options for this module.

Choosing Detection options

When you first activate it, the System Scan module initially assumes that you want it to scan for viruses each time you work with any file susceptible to virus infection, whether on your hard disk or on floppy disks, and whether you read the file from or write the file to your hard disk. The module will also examine compressed files by default, but will not use heuristic scanning unless you activate it.

-
- NOTE:** This property page will vary its appearance and have a different option set, depending on which operating system your computer runs.
-

To modify these settings, follow these steps:

1. Verify that the **Enable System Scan** checkbox is selected.

Selecting this checkbox activates the remaining options in this property page. Clear the checkbox to disable all configuration options in this page and to prevent the System Scan module from scanning your system.

2. Tell the module when and where you want it to look for viruses. You can have it
 - **Scan files as you work with them.** Each time you open, run, copy, save, rename, or otherwise use files on your hard disk, virus code can execute and spread infections to other files.

To prevent this on computers that run Windows NT Workstation v4.0 or Windows 2000 Professional, select both the **Inbound files** and the **Outbound files** checkboxes. On computers that run Windows 95 or Windows 98, select each of the **Run, Copy, Create,** and **Rename** checkboxes for full coverage.

“Inbound” files are files that your computer or another system on the network saves or writes to local hard disks attached to your computer or to any network hard disks you have mapped to your system. To include network drives mapped to your system for a scan session, you must also select the **Network drives** checkbox.

Your system can receive data from your computer's memory, from a floppy disk in your computer's floppy drive, from other systems, from e-mail, or from other sources, then write that data to a file on your hard disk. The VShield scanner treats all such data as “inbound.”

“Outbound” files, meanwhile, are files that your computer or other systems on the network read from local hard disks attached to your system or from network disks mapped to your system. To include network drives mapped to your system for a scan session, here too you must select the **Network drives** checkbox.

Whenever your computer or another system reads data from a file stored on a local hard disk attached to your system or a network disk mapped to your system, the System Scan module treats that data as “outbound.”

-
- ❑ **NOTE:** If you have network drives mapped to your computer from which you copy files, or if other network users copy files from your computer, McAfee strongly recommends that you have the VShield scanner installed both on your computer and on the computer that “owns” the network drive. You should also select all checkboxes in the Scan area in the Detection page, plus the **Network drives** checkbox in the What to Scan area.

Your copy of the System Scan module will then examine files as your computer reads them from your hard disk, then again as it writes them to the destination computer's hard disk. If the destination computer has its own copy of the System Scan module active, it too will scan the file as you write it to the network drive if that System Scan module has the **Inbound files** checkbox selected.

If you tend to copy files from one server that does not copy files from your computer, and if other network users do the same, you might want to configure your computers to scan only files that they write to their hard disks—or only files that they read from their hard disks—in order to prevent two computers from scanning the same file. If you do so, however, you should configure each computer identically. Otherwise, one computer that scans only outbound files could copy an infected file from a server that scans only inbound files.

- **Scan files on floppy disks.** Boot-sector viruses can hide in the boot blocks of any formatted floppy disk, then load into memory as soon as your computer reads your floppy drive. Select the **Access** checkbox to have the System Scan module examine floppy disks each time your computer reads from them or writes to them. Select the **Shutdown** checkbox to have the module scan any floppy disks that you leave in your drive as you shut down your computer. This ensures that no viruses can load when your computer reads your floppy drive at startup.
3. Specify the types of files you want the System Scan module to examine. You can
- **Scan compressed files.** Select the **Compressed files** checkbox to have the module look for viruses in compressed files or in file archives. This option ensures that viruses do not spread from compressed files, but because the module uncompresses these files before it scans them, choosing this option can lengthen the time it takes to scan a given set of files as you work with your computer.
-
- NOTE:** When the System Scan module examines a file archive, it will scan only the file archive itself, not the compressed files within the archive. To learn which files and archives the module scans, see [“Current list of compressed files scanned” on page 296](#).
-
- **Choose file types for scanning.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan sessions so that the module examines only those files most susceptible to virus infection. To do so, select the **Program files only** button.

To see or designate the file name extensions that the System Scan module will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 4-10).

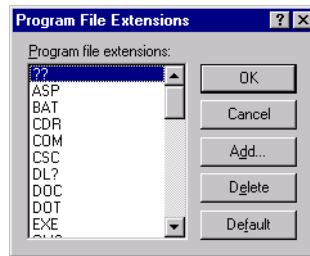


Figure 4-10. Program File Extensions dialog box

See “Adding file name extensions for scanning” on page 291 and “Current list of vulnerable file name extensions” on page 292 to learn which file name extensions this module scans by default and how to add to or change this list.


- **Scan all files.** Select the **All files** button to have the System Scan module examine any file, whatever its extension, whenever you or a system process modifies it in any way.
- **Scan networked drives.** To have the System Scan module look for viruses on any drives mapped to your system that you use in any way, select the **Network drives** checkbox.

NOTE: If you have network disks mounted on your system, the System Scan module treats any files your system writes to such drives as “inbound” files and any files your system reads from such drives as “outbound” files. To ensure complete coverage, select both of these checkboxes in the Scan area when you select the **Network drives** checkbox.

4. Choose VShield software management options. These options let you control your interaction with the VShield scanner. You can
 - **Disable the System Scan module at will.** Select the **System Scan can be disabled** checkbox in order to have the option to disable this module. Note that McAfee recommends that you leave the System Scan module enabled for maximum protection. Clearing this checkbox removes the **Exit** and **System Scan** items from the VShield shortcut menu and the **Disable** button from the VShield Status dialog box.

TIP: To ensure that nobody else who uses your computer will disable the VShield scanner, or to enforce an anti-virus security policy among VirusScan users on your network, clear this checkbox, then protect the settings with a password. This will keep other users from disabling the scanner from within the VirusScan Console, or from the VShield Properties dialog box. See “Configuring the Security module” on page 151 for details.

You can also run the entire VirusScan product in secure mode, which disables access to all configurable options. See “Installation steps” on page 37 to learn how to install VirusScan software so that it uses this mode.

- **Display the VShield icon in the Windows system tray.** Select the **Show icon in the Taskbar** checkbox to have the VShield scanner display this icon  in the system tray. The particular state in which the icon appears depends on which VShield modules you have enabled. See [“Understanding the VShield system tray icon states” on page 94](#) for details.

Double-clicking the icon opens the VShield Status dialog box. Right-clicking the icon displays a shortcut menu. See [“Using the VShield shortcut menu” on page 155](#) and [“Tracking VShield software status information” on page 161](#) for more details.

5. Turn on heuristic scanning. Click **Advanced** to open the Advanced Scan Settings dialog box ([Figure 4-11](#)).

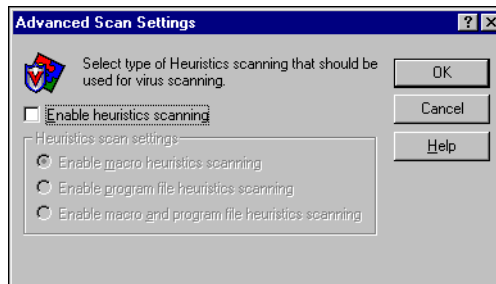


Figure 4-11. Advanced Scan Settings dialog box

Heuristic scanning technology enables the System Scan module to recognize new viruses based on their resemblance to similar viruses that the module already knows. To do this, the module looks for certain “virus-like” characteristics in the files you’ve asked it to scan. The presence of a sufficient number of these characteristics in a file leads the module to identify the file as potentially infected with a new or previously unidentified virus.

Because the System Scan module looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat “potential” infections with the same caution you would confirmed infections.

The System Scan module starts out without any heuristic scan options active. To activate heuristics scanning, follow these substeps:

- a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.
- b. Select the types of heuristics scanning you want the System Scan module to use. Your choices are:

- **Enable macro heuristics scanning.** Choose this option to have the System Scan module identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that contain embedded macros, then compare the macro code to its virus definitions database. The module will identify exact matches with the virus name; code signatures that resemble existing viruses cause the module to tell you it has found a potential macro virus.
- **Enable program file heuristics scanning.** Choose this option to have the System Scan module locate new viruses in program files by examining file characteristics and comparing them against a list of known virus characteristics. The module will identify files with a sufficient number of these characteristics as potential viruses.
- **Enable macro and program file heuristics scanning.** Choose this option to have the module use both types of heuristics scanning. McAfee recommends that you use this option for complete anti-virus protection.

NOTE: The System Scan module will use heuristic scanning techniques only on the file types you designate in the Program File Extensions dialog box. If you choose to scan **All files**, the module will use heuristic scanning for all file types.

- c. Click **OK** to save your settings and return to the VShield Properties dialog box.
6. Click the Action tab to choose additional System Scan module options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When the System Scan module detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want the module to give you when it finds a virus, or which actions you want it to take on its own.

- **NOTE:** This property page will vary its appearance and have a different option set, depending on which operating system your computer runs.

Follow these steps:

1. Click the Action tab in the System Scan module to display the correct property page (Figure 4-12).

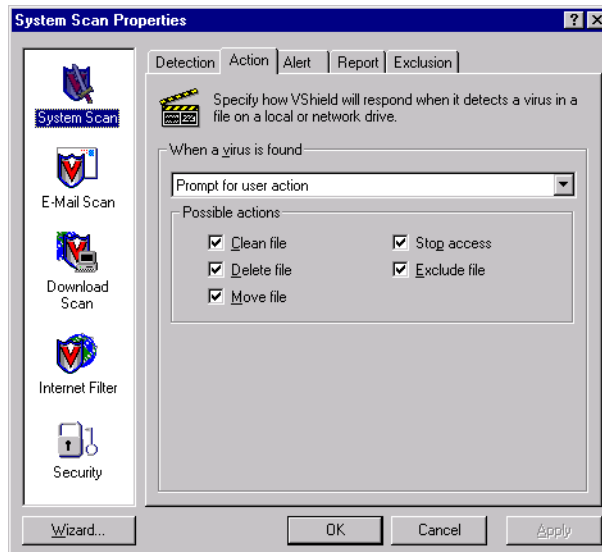


Figure 4-12. System Scan Properties dialog box - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each choice.

- **NOTE:** If you choose **Prompt for user action** from the list, click the Alert tab to specify whether you want the System Scan module to prompt you with a message, a beep, or both. See [“Choosing Alert options” on page 110](#) for details. To learn how to respond to these messages, see [“Responding when the VShield scanner detects malicious software” on page 67](#).

3. The items you can choose from the list are:

- **Prompt for user action.** Choose this response to have the System Scan module ask you what to do when it finds a virus—the module will display an alert message and offer you a set of possible responses.

If your computer runs Windows 95 or Windows 98, choosing this response displays the Prompt Type option (Figure 4-13). Here you can choose the method you want the System Scan module to use to alert you when it finds a virus.

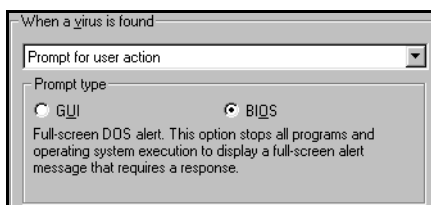


Figure 4-13. Prompt Type area

Your choices are:

- **BIOS.** Click this button to see a full-screen text-mode alert message that offers you a range of response options, including the option to continue without any action against the virus. This mode also brings your system to a complete halt until you choose a response option.
- **GUI.** Click this button to see a standard graphical alert message that also offers a range of response options. This range will not include Continue access. As the prompt awaits your choice, your system will continue with normal operations in the background.

Next, choose which response options you want to see in that alert message from the Possible Actions area at the bottom of the property page. Each of the checkboxes you choose here causes an option button to appear in an alert message that the module displays when it finds a virus. Selecting **Delete file**, here, for example, causes a **Delete** button or option to appear in the alert message. Your choices are:

- **Clean file.** This option tells the module to try to remove the virus code from the infected file. If you have its reporting function enabled, it will record a log event each time it successfully cleans, or fails to clean, an infected file.
- **Delete file.** This option tells the module to delete the infected file immediately.

- **Move file.** This option tells the module to move the infected file to a quarantine folder. The GUI version of the alert message will display a **Move file to** button that allows you to locate a quarantine folder to use.
- **Stop access.** This option tells the module to prevent you or anyone else who tried to modify this file from working with it in any way at all.
- **Exclude file.** This option tells the module to skip the file during this and later scan sessions.
- **Continue access.** This option leaves the file intact and in its original location on your computer and does not prevent you from opening, copying, renaming, or otherwise modifying the file in the future. Use this option only when you know positively that the file the System Scan module flagged is not infected. To preserve files as virus samples, McAfee recommends moving infected files to a quarantine folder instead.

NOTE: The option is available only on computers that run Windows 95 or Windows 98 and only when you choose the **BIOS** prompt mode.

- **Move infected files automatically.** Choose this response to have the module move infected files to a quarantine folder as soon as it finds them.

By default, the module moves these files to a folder named \infected located in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.

- **Clean infected files automatically.** Choose this response to tell the module to remove the virus code from the infected file as soon as it finds it. If the module cannot remove the virus, it will deny access to the file and note the incident in its log file. See [“Choosing Report options” on page 112](#) for details.
- **Delete infected files automatically.** Choose this option to have the module delete every infected file it finds immediately. Be sure to enable the reporting feature so that you have a record of which files the module deleted. You will need to restore deleted files from backup copies. If the module cannot delete an infected file, it will note the incident in its log file.

- **Deny access to infected files and continue.** Choose this response to have the module mark the file “off limits” and continue with its normal scanning operations. Choose this response only if you plan to leave your computer unattended for long periods.

If you also activate the module’s reporting feature (see “[Choosing Report options](#)” on page 112 for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

4. Click the Alert tab to choose additional System Scan module options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want in the Action page, you can let the System Scan module look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. But if you want the module to tell you as soon as it finds a virus so you can take appropriate action, have it send an alert message to you or to others.

Follow these steps:

1. Click the Alert tab in the System Scan module to display the correct property page ([Figure 4-14](#)).

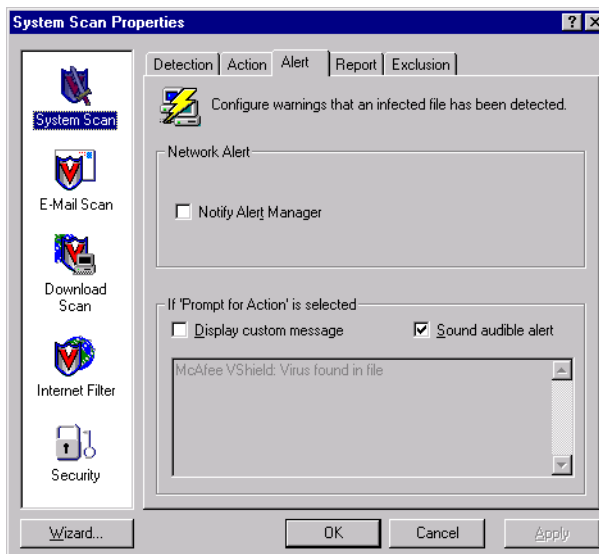


Figure 4-14. System Scan Properties dialog box - Alert page

2. Select the **Notify Alert Manager** checkbox to have the module send alert messages to Alert Manager for distribution.

Alert Manager is a separate McAfee software component that collects alert messages and uses a variety of methods to send them to recipients that you specify. To have the System Scan module send these alert messages successfully, you must also set up the Alert Manager Client Configuration utility. See [“Using the Alert Manager Client Configuration utility” on page 285](#) for details.

You can pass alert messages directly to an Alert Manager server, or you can send alert messages as text (.ALR) files to a Centralized Alerting directory that the Alert Manager server checks periodically.

NOTE: Clearing this checkbox tells the System Scan module not to send an alert message via Alert Manager, but does not affect other alert messages that you configure in this property page.

3. Select the **Sound audible alert** checkbox to have the module beep when it finds an infected file.

You can change the setting for this option only if you select **Prompt for user action** in the Action property page. Otherwise, the checkbox will display and use the setting it had when you last chose the **Prompt for user action** item. The module will sound the standard system warning beep or .WAV file you have your computer set to play.

4. Select the **Display custom message** checkbox to have the module add a custom message to the alert box it displays when it finds an infected file.

As with the audible alert, you can change the setting for this option only if you choose **Prompt for user action** in the Action property page. If you do not choose that item in the Action page, no alert box will appear and you will not see a custom message even if you select this checkbox.

5. Enter the message you want the module to display in the text box provided. You can enter a maximum of 250 characters here.
6. Click the Report tab to choose additional System Scan module options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

The System Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSHLOG.TXT. You can have the module write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor.

The VSHLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections the System Scan module found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Report property page to determine which information the module will include in its log file.

To set the System Scan module to record its actions in a log file, follow these steps:

1. Click the Report tab in the System Scan module to display the correct property page (Figure 4-15).

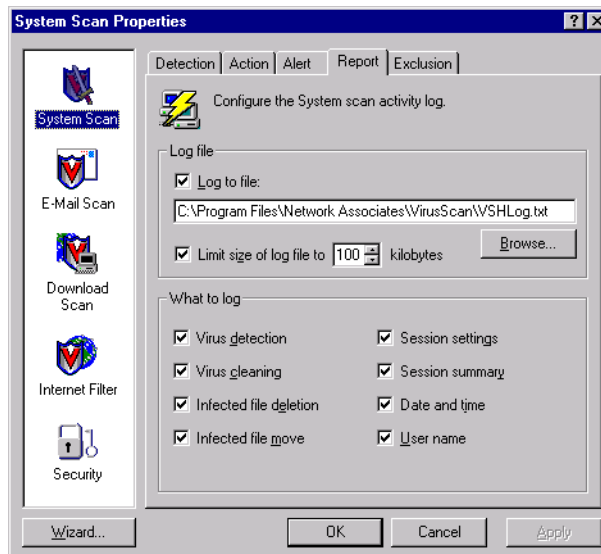


Figure 4-15. System Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

By default, the System Scan module writes log information to the file VSHLOG.TXT in the VirusScan program directory.

You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network. You may use a different file, but the text file must already exist. The module will not create a new file.

3. Select the **Limit size of log file to** checkbox to minimize the log file size, then enter a value for the file size, in kilobytes, in the text box provided. If you do not select this checkbox, the log file can grow to as large a size as your disk space or file system permits.

Enter a value between 10KB and 999KB. By default, the System Scan module limits the file size to 100KB. If the data in the log exceeds the file size you set, the module erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want the module to record in its log file. The module usually will record the data when the scan session ends or when you shut your system down.

You can choose to record any of this information:

- **Virus Detection.** Select this checkbox to have the log file record how many viruses the module finds during each scan session. Clear the checkbox to leave this information out of the log file.
- **Virus Cleaning.** Select this checkbox to have the log file record how many infected files the module cleans-or tries to clean-during each scan session. Clear this checkbox to leave this information out of the log file.
- **Infected file deletion.** Select this checkbox to have the log file record how many viruses the module deletes during each scan session. Clear this checkbox to leave this information out of the log file.
- **Infected file move.** Select this checkbox to have the log file record how many viruses the module moves to a quarantine folder during each scan session. Clear this checkbox to leave this information out of the log file.
- **Session settings.** Select this checkbox to have the log file record the configuration settings you used for the module during each scan session. Clear this checkbox to leave this information out of the log file.
- **Session summary.** Select this checkbox to have the log file summarize the actions that the module took during each scan session.

If you choose this option, the log will record:

- How many files the module examined.
- How many infected files the module cleaned.
- How many infected files the module deleted.
- How many infected files the module moved to a quarantine folder.
- Your System Scan module settings.

Clear the checkbox to leave this information out of the log file.

5. **Date and time.** Select this checkbox to have the log file record the date and time at which the module starts each scan session. Clear this checkbox to leave this information out of the log file.
6. **User name.** Select this checkbox to have the log file record the name of the user logged into the workstation as the module starts each scan session. Clear this checkbox to leave this information out of the log file.
7. Click the Exclusion tab to choose additional System Scan module options. To save your changes without closing the System Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Having the System Scan module examine these files can take a long time and produce few results. You can reduce the time the System Scan module spends looking at each file you modify by restricting it to examining only susceptible file types. You can also tell the module to ignore entire files or folders that you know cannot become infected.

The exclusion list identifies which disks, folders, or individual files you want to exclude from VShield scan sessions. By default, the System Scan module does not scan the Recycle Bin because Windows will not run items stored there. This item will appear in the list when you first open the window.

Each entry in the exclusion list displays the path to the item, notes whether the module will also exclude any nested folders within the target, and explains whether the application will exclude the item when it scans files, when it scans your hard disk boot sector, or both.

Once you use VirusScan software to scan your system thoroughly, you can tell the System Scan module to ignore those files and folders that do not change or that are not normally vulnerable to virus infection.

To choose your options, follow these steps:

1. Click the Exclusion tab in the System Scan module to display the correct property page (Figure 4-16).

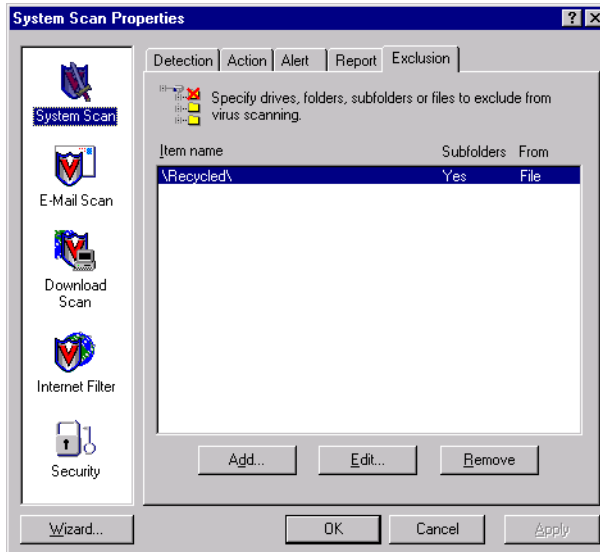


Figure 4-16. System Scan Properties dialog box - Exclusion page

2. Specify the items you want to exclude. You can
 - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 4-17).

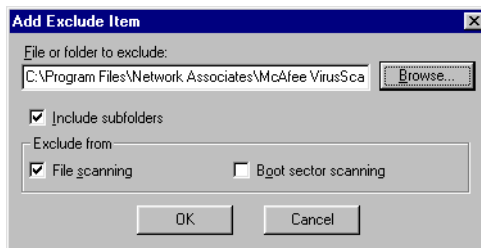


Figure 4-17. Add Exclude Item dialog box

Next, follow these substeps to add items to the list:

- a. Enter a path to a folder or a file name in the text box provided, or click **Browse** to locate the item you want the module to exclude.

NOTE: If you have chosen to move infected files to a quarantine folder automatically, the module excludes that folder from scan operations.

- b. Select the **Include subfolders** checkbox to tell the module to ignore files stored in any subfolders within the folder you specified in [Step a](#).

NOTE: Choosing **Include subfolders** causes the module to ignore only those files stored in the subfolders themselves. The module will still scan files stored at the root level of the folder you designate. To exclude the files at the folder root level, clear the **Include subfolders** checkbox.

- c. Select the **File scanning** checkbox to exclude the item you specified in the first step when the module looks for file-infecting viruses. These viruses usually appear in files stored in the visible portions of your hard disk.
- d. Select the **Boot sector scanning** checkbox to exclude the item you specified in the first step from scan operations when the module looks for boot-sector viruses.

These viruses usually appear in memory or in files that reside in your hard disk's boot sector or master boot record. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

 **WARNING:** McAfee recommends that you do *not* exclude your system files during a scan session.

- e. Repeat [Step a](#). through [Step d](#). until you have listed all of the files and folders you do not want scanned.
- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.

- **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. This means that the System Scan module *will* scan this file or folder during this scan session.
3. Click a different tab to change any of your System Scan settings, or click one of the icons along the side of the System Scan Properties dialog box to choose options for a different module.

To save your changes in the System Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

-
- NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.
-

Configuring the E-mail Scan module



The VShield E-mail Scan module looks for viruses in files attached to e-mail messages that you receive via corporate e-mail systems that adhere to the Messaging Application Programming Interface (MAPI) standard, such as Microsoft Exchange and Outlook, or later versions of Lotus cc:Mail. It also includes a special scan mode that looks for viruses in earlier cc:Mail versions.

This module can work with the Download Scan module to examine messages that arrive via POP-3 or SMTP e-mail client programs such as Eudora, Netscape Mail, or Outlook Express. The module pays particular attention to attachments that come with your e-mail, which are the biggest potential source of viruses. Because it can scan e-mail as soon as it appears on your desktop, the module can intercept viruses before they have a chance to spread.

When it finds a virus, the module can ask you what you want it to do, or it can take a variety of automatic actions in response. You can have it report what it has done either with an alert message when it takes the action, or in a log file you can examine at your leisure. It can even send a message to the person who sent an infected e-mail message, which makes tracking the source of virus infections relatively simple.

-
- NOTE:** The E-Mail Scan module will not appear in the VShield Properties dialog box unless you used the Custom Setup option when you installed VirusScan software and specified that you wanted to install the E-Mail Scan module.

By default, the VShield scanner does *not* enable the E-Mail Scan module when it first starts—you must tell the module which e-mail systems you use before it can activate.

Choosing Detection options

The VShield scanner does not start with the E-mail Scan module enabled by default because it needs to know which e-mail system you use. Once you configure it for use with your regular e-mail client, the module will use your MAPI profile, or your cc:Mail user name and password, to log on to your mail account whenever it starts a scan session.

If you have already started and logged into your e-mail system, the module will simply work within the session you've created. If, however, you have not yet logged into your e-mail system, the module will prompt you to choose a profile or enter account information as soon as a scan session starts, even before you've logged into your e-mail account. This also can occur when you start your computer, if you do not have your e-mail client program set to load at startup.

If you switch profiles or log into a different account—perhaps in another domain—the module will ask you to choose the profile you want to use or to supply a new user name and password to log on to the mail system.


To choose configuration options for this page, follow these steps

1. Select the **Enable Scanning of e-mail attachments** checkbox.

The options in the rest of the property page activate (Figure 4-18).



Figure 4-18. E-mail Scan Properties dialog box - Detection page

-
2. Select the type of e-mail system you use. Your options are:
- **Enable Corporate Mail.** Select this checkbox to have the E-Mail Scan module scan mail attachments you receive via a mail system that runs within your office network. Usually such systems use a proprietary mail protocol and have a central mail server to which you send mail for delivery. Often such systems send and receive Internet mail, but they usually do so through a gateway application. The E-mail Scan module supports two types of corporate e-mail systems:
 - **Microsoft Exchange (MAPI).** Select this button if you use an e-mail system that sends and receives mail via Microsoft's Messaging Application Programming Interface (MAPI), a Windows mail protocol. Examples include Microsoft Exchange and Microsoft Outlook 97 and Outlook 98.
 - **Lotus cc:Mail.** Select this button if you use cc:Mail 6.x or 7.x. These systems use a proprietary Lotus protocol to send and receive e-mail. You can also install cc:Mail version 8.0 or later so that it uses the same protocol as earlier cc:Mail versions. To verify which system you use, check with your network administrator.
-
- NOTE:** You can select only one *corporate* e-mail system at a time, but you can have the E-Mail Scan module scan all attachments that arrive via both corporate and Internet e-mail systems, if you use both.
-
- **Internet Mail (Requires Download Scan).** Select this checkbox to have the E-Mail Scan module scan Internet mail attachments that you send and receive via the Post Office Protocol (POP-3) or the Simple Mail Transfer Protocol (SMTP). Choose this option if you work from home or through a dial-up Internet service provider with such software as Qualcomm's Eudora Pro, Microsoft's Outlook Express, or Netscape Mail.
-
-  **IMPORTANT:** Because you receive Internet mail and other files that you download from websites and other sources through the same "pipe," the E-Mail Scan module uses the detection, action, alerting and reporting options you set in the Download Scan module to determine how to respond to incoming Internet mail. To scan Internet mail attachments, therefore, you must also enable the Download Scan module and use those property pages to choose the settings you want.
-

3. Tell the E-Mail Scan module which mail sources it should monitor:
 - If you chose **Microsoft Exchange (MAPI)** as your corporate e-mail system, the Folders area shows **All incoming mail**, which means that the module will look for viruses in files attached to each e-mail message as it arrives in your MAPI mailbox or via other MAPI services.
 - If you chose **Lotus cc:Mail** as your corporate e-mail system, you'll need to tell the module how often to scan your cc:Mail Inbox ([Figure 4-19](#)).

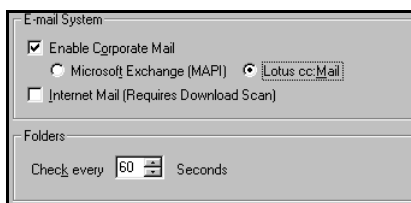



Figure 4-19. Detection page with cc:Mail option chosen

In the Folders area, enter the number of seconds the E-Mail Scan module should wait before it checks your cc:Mail Inbox for new mail. By default, the module checks once every minute. Be sure to set an interval shorter than the interval you set to receive your e-mail so that module has an opportunity to detect any viruses before they reach your computer.

4. Specify the types of e-mail attachments you want the E-Mail Scan module to examine. You can
 - **Scan compressed files.** Select the **Compressed files** checkbox to have the module look for viruses in compressed files or in file archives. This option ensures that viruses do not spread from compressed files, but because the module uncompresses these files before it scans them, choosing this option can lengthen the time it takes to scan a given set of files as you work with your computer.

 **NOTE:** When the E-Mail Scan module examines a file archive, it will scan only the file archive itself, not the compressed files within the archive. To learn which files and archives the module scans, see [“Current list of compressed files scanned” on page 296](#).

- **Choose file types for scanning.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan sessions so that the module examines only those files most susceptible to virus infection. To do so, select the **Program files only** button.

To see or designate the file name extensions that the E-Mail Scan module will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 4-10).

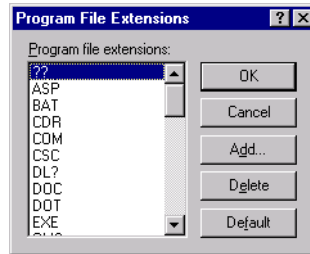


Figure 4-20. Program File Extensions dialog box

See “Adding file name extensions for scanning” on page 291 and “Current list of vulnerable file name extensions” on page 292 to learn which file name extensions this module scans by default and how to add to or change this list.

- **Scan all files.** Select the **All files** button to have the E-Mail Scan module examine any file, whatever its extension, whenever you or a system process modifies it in any way.
5. Turn on heuristic scanning. Click **Advanced** to open the Advanced Scan Settings dialog box (Figure 4-11).

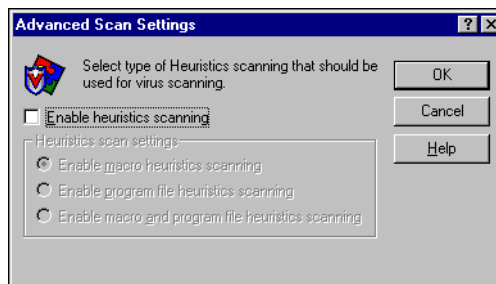


Figure 4-21. Advanced Scan Settings dialog box

Heuristic scanning technology enables the E-Mail Scan module to recognize new viruses based on their resemblance to similar viruses that the module already knows.

To do this, the module looks for certain “virus-like” characteristics in the files you’ve asked it to scan. The presence of a sufficient number of these characteristics in a file leads the module to identify the file as potentially infected with a new or previously unidentified virus.

Because the E-Mail Scan module looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat “potential” infections with the same caution you would confirmed infections.

The E-Mail Scan module starts out without any heuristic scan options active. To activate heuristics scanning, follow these substeps:

- a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.
- b. Select the types of heuristics scanning you want the E-Mail Scan module to use. Your choices are:
 - **Enable macro heuristics scanning.** Choose this option to have the E-Mail Scan module identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that contain embedded macros, then compare the macro code to its virus definitions database. The module will identify exact matches with the virus name; code signatures that resemble existing viruses cause the module to tell you it has found a potential macro virus.
 - **Enable program file heuristics scanning.** Choose this option to have the E-Mail Scan module locate new viruses in program files by examining file characteristics and comparing them against a list of known virus characteristics. The module will identify files with a sufficient number of these characteristics as potential viruses.
 - **Enable macro and program file heuristics scanning.** Choose this option to have the module use both types of heuristics scanning. McAfee recommends that you use this option for complete anti-virus protection.

NOTE: The module will use heuristic scanning techniques only on the file types you designate in the Program File Extensions dialog box. If you choose to scan **All files**, the module will use heuristic scanning for all file types.

- Click the Action tab to choose additional E-Mail Scan module options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When the E-Mail Scan module detects a virus in an e-mail attachment, it can respond either by asking you what it should do with the infected file, or by taking an action that you determine ahead of time. Use the Action property page to specify which response options you want the module to give you when it finds a virus, or which actions you want it to take on its own.

NOTE: The E-Mail Scan module can respond to viruses only if you select a corporate e-mail system for it to scan. If you select only Internet Mail, the options here will be unavailable. If you receive only Internet mail, you must choose your responses in the Action property page for the Download Scan module.

Follow these steps:

- Click the Action tab in the E-mail Scan module to display the correct property page (Figure 4-22).

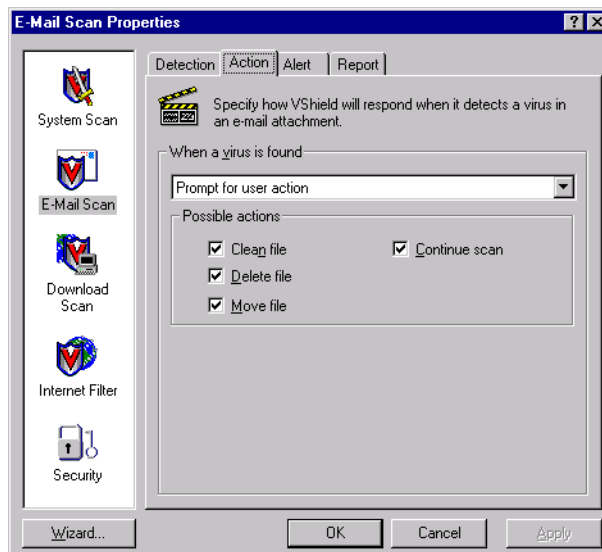


Figure 4-22. E-mail Scan Properties dialog box - Action page

2. Choose a response from the **When a virus is found** list. The area beneath the list will change to show you additional options for each response. Your choices are:

- **Prompt for user action.** Choose this response if you want the E-Mail Scan module to ask you what to do when it finds a virus—the module will display an alert message and offer you a range of possible responses.

NOTE: If you choose **Prompt for user action** from the list, click the Alert tab to specify whether you want the E-Mail Scan module to prompt you with a message, a beep, or both.

Select the options you want to see in the alert message. Each of the checkboxes you select here causes an option button to appear in an alert message that the module displays when it finds a virus. Selecting **Delete file** here, for example, causes a **Delete** button to appear in the alert message.

You can choose from these options:

- **Clean file.** This option tells the module to try to remove the virus code from the infected file. If you have its reporting function enabled, it will record a log event each time it successfully cleans, or fails to clean, an infected file.

NOTE: The E-Mail Scan module does *not* support this option for Lotus cc:Mail v7.x and earlier e-mail systems. The option will not appear here if you selected Lotus cc:Mail in the E-Mail Scan Detection page.

- **Delete file.** This option tells the module to delete the infected attachment immediately. The module will, however, preserve the e-mail message it came in.
 - **Move file.** This option tells the module to move the infected file to a quarantine folder. The alert message will display a **Move file to** button that allows you to locate a quarantine folder.
 - **Continue scan.** This option tells the module to continue scanning, but to take no other actions. If you have its reporting options enabled, the module records the incident in its log file.
- **Move infected files to a folder.** Choose this response to have the module move infected files to a quarantine folder as soon as it finds them. The module moves these files to a folder named **Infected** located in the VirusScan program directory.

You can change the name and location of the folder into which the module deposits infected Internet mail, but to do so, you must switch to the Download Scan module and click the Action tab there. See [“Choosing Action options” on page 136](#) for details.

- **Clean infected files.** Choose this response to tell the module to remove the virus code from the infected file as soon as it finds it. If the module cannot remove the virus, it will note the incident in its log file.

NOTE: The E-Mail Scan module does *not* support this option for Lotus cc:Mail v7.x and earlier e-mail systems. The option will not appear here if you selected Lotus cc:Mail in the E-Mail Scan Detection page.

- **Delete infected files.** Choose this response to have the E-Mail Scan module delete every infected file it detects immediately. Be sure to enable its reporting feature so that you have a record of which files the module deleted. You will need to restore deleted files from backup copies. See [“Choosing Report options” on page 129](#) for details.
- **Continue scanning.** Choose this response to have the module continue scanning without taking any action against the virus it finds. If you also activate the E-Mail Scan reporting feature (see [“Choosing Report options” on page 129](#) for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

Use this option only if you plan to leave your computer unattended while the module checks for viruses.

3. Click the Alert tab to choose additional E-Mail Scan module options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want in the Action page, you can let the E-Mail Scan module look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. But if you want the module to tell you as soon as it finds a virus so you can take appropriate action, configure it to send an alert message to you or to others.

Follow these steps:

1. Click the Alert tab in the E-mail Scan module to display the correct property page (Figure 4-23).

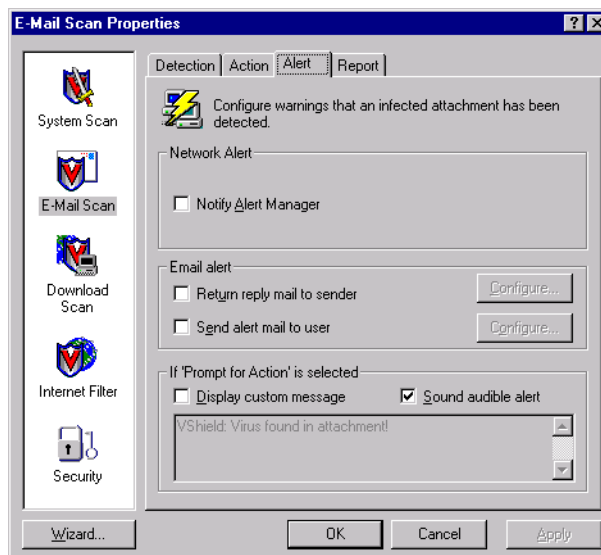


Figure 4-23. E-mail Scan Properties dialog box - Alert page

2. Select the **Notify Alert Manager** checkbox to have the module send alert messages to Alert Manager for distribution.

Alert Manager is a separate McAfee software component that collects alert messages and uses a variety of methods to send them to recipients that you specify. To have the E-Mail Scan module send these alert messages successfully, you must also set up the Alert Manager Client Configuration utility. See [“Using the Alert Manager Client Configuration utility”](#) on page 285 for details.

You can pass alert messages directly to an Alert Manager server, or you can send alert messages as text (.ALR) files to a Centralized Alerting directory that the Alert Manager server checks periodically.

-
- NOTE:** Clearing this checkbox tells the E-Mail Scan module not to send an alert message via Alert Manager, but does not affect other alert messages that you configure in this property page.
-

As part of your anti-virus warning system, the E-Mail Scan module can reply directly with an alert message to anybody who sends you an infected message or attachment. You can copy that message to any other recipient in your organization, or any number of other recipients. If you prefer not to send a reply, you can simply have the module send an e-mail notification, perhaps to a system administrator, whenever it detects a virus.

Sending reply messages can aid your ability to track virus sources and pinpoint where infectious agents enter your network; copies of these messages sent to system administrators can help them track how infections spread.

You can also choose to send a messages to any recipient without replying to the source of the infected attachment. The E-Mail Scan module can draw recipients directly from your Microsoft Exchange, Microsoft Outlook, or other MAPI-compliant address book, or from an equivalent Lotus cc:Mail directory. You can also enter recipient addresses directly.

The message you create for a response is a template—the module will send the message you compose automatically to each recipient you designate, so McAfee recommends that you enter a message that all recipients can read and understand. Apart from the steps you take to compose this template message, the module will not give you an opportunity to edit the message before it sends it.

You may send one message to reply to the source of the infected message and a different message to other recipients, but you cannot tailor the same message for different recipients.

3. To compose your template messages, follow these substeps:
 - a. Select the **Return reply mail to sender** checkbox in the Alert property page, then click **Configure** to open a standard mail message form.

Because the module will send this message directly back to the source of the infected e-mail message, the **To:** button and text box are unavailable.

- b. To send a copy of this message to someone else, enter an e-mail address in the text box labeled Cc; or click **Cc:** to choose a recipient from your mail system's user directory or address book.

NOTE: To find an e-mail address in your mail system's user directory, you must store address information in a MAPI-compliant user directory, database, or address book, or in an equivalent Lotus cc:Mail directory. If you have not yet logged onto your e-mail system, the E-Mail Scan module tries to use your default MAPI profile to log onto MAPI-compliant mail systems, or asks you to supply a user name, password and path to your Lotus cc:Mail mailbox. Enter the information the module requires, then click **OK** to continue.

- c. Enter a subject for the message that conveys its urgency, then add any comments you want to make in the body of the message, below a standard infection notice that the module itself will supply. You may add up to 1024 characters of text.
- d. Click **OK** to save the message.

Whenever it detects a virus, the module will send a copy of this message to each person who sends you e-mail with an infected attachment. It fills in the recipient's address with information found in the original message header, and identifies the virus and the affected file in the area immediately below the subject line. If you have activated its report feature, the module also logs each instance when it sends an alert message.

- e. To send an e-mail message to warn others—a network administrator, for example—about an infected attachment, select the **Send alert mail to user** checkbox in the Alert property page. You can then compose a standard reply in the same way you did in [Step a](#) through [Step d](#) above. In this case, however, you can fill out both the To: and the Cc: text boxes.

Whenever it detects a virus, the E-Mail Scan module sends a copy of this message to all of the addresses that you entered for this message.

- 4. Select the **Sound audible alert** checkbox to have the module beep when it finds an infected file.

You can change the setting for this option only if you select **Prompt for user action** in the Action property page. Otherwise, the checkbox will display and use the setting it had when you last chose the **Prompt for user action** item.

The module will sound the standard system warning beep or .WAV file you have your computer set to play.

5. Select the **Display custom message** checkbox to have the module add a custom message to the alert box it displays when it finds an infected file.

As with the audible alert, you can change the setting for this option only if you choose **Prompt for user action** in the Action property page. If you do not choose that item in the Action page, no alert box will appear and you will not see a custom message even if you select this checkbox.

6. Enter the message you want the module to display in the text box provided. You can enter a maximum of 250 characters here.
7. Click the Report tab to choose additional E-Mail Scan module options. To save your changes without closing the E-mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

The E-mail Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called WEBEMAIL.TXT. You can have the module write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor.

The WEBEMAIL.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections the module found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Report property page to determine which information the module will include in its log file.

To set the E-Mail Scan module to record its actions in a log file, follow these steps:

1. Click the Report tab in the E-mail Scan module to display the correct property page (see [Figure 4-24 on page 130](#)).

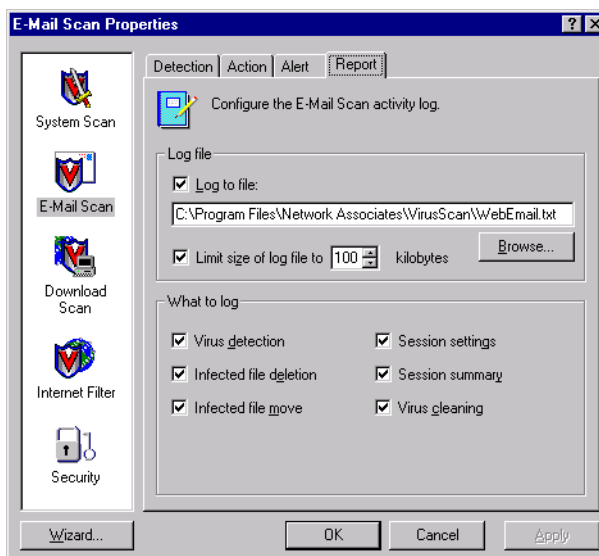


Figure 4-24. E-mail Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

By default, the module writes log information to the file WEBEMAIL.TXT in the VirusScan program directory. you can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. Select the **Limit size of log file to** checkbox to minimize the log file size, then enter a value for the file size, in kilobytes, in the text box provided. If you do not select this checkbox, the log file can grow to as large a size as your disk space or file system permits.

Enter a value between 10KB and 999KB. By default, the System Scan module limits the file size to 100KB. If the data in the log exceeds the file size you set, the module erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want the module to record in its log file. The module usually will record the data when the scan session ends or when you shut your system down.

You can choose to record any of this information:

- **Virus Detection.** Select this checkbox to have the log file record how many viruses the module finds during each scan session. Clear the checkbox to leave this information out of the log file.

- **Infected file deletion.** Select this checkbox to have the log file record how many viruses the module deletes during each scan session. Clear this checkbox to leave this information out.
- **Infected file move.** Select this checkbox to have the log file record how many viruses the module moves to a quarantine folder during each scan session. Clear this checkbox to leave this information out.
- **Session settings.** Select this checkbox to have the log file record the configuration settings you used for the module during each scan session. Clear this checkbox to leave this information out.
- **Session summary.** Select this checkbox to have the log file summarize the actions that the module took during each scan session. The log will record:
 - How many files the module examined.
 - How many infected files the module cleaned (MAPI e-mail systems only).
 - How many infected files the module deleted.
 - How many infected files the module moved to a quarantine folder.
 - Your E-Mail Scan module settings.

Clear the checkbox to leave this information out.

- **Virus Cleaning.** Select this checkbox to have the log file record how many infected files the module cleans-or tries to clean-during each scan session. Clear this checkbox to leave this information out.

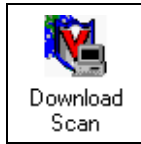
NOTE: The E-Mail Scan module does *not* support this option for Lotus cc:Mail v7.x and earlier e-mail systems. The option will not appear here if you selected Lotus cc:Mail in the E-Mail Scan Detection page.

5. Click a different tab to change any of your E-mail Scan settings, or click one of the icons along the side of the E-mail Scan Properties dialog box to choose options for a different module.

To save your changes in the E-mail Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Configuring the Download Scan module



The Download Scan module can check files you download from the Internet as you visit websites, FTP sites, and other Internet sites. This module is also where you set the options you want to use to respond to infected e-mail attachments you receive via POP-3 or SMTP e-mail client programs such as Eudora, Netscape Mail, or Microsoft Outlook Express. To activate this function, you must also choose an appropriate mail system in the E-mail Scan module's Detection page. See ["Choosing Detection options" on page 118](#) for details.

When it finds a virus, the module can ask you what you want it to do, or it can take a variety of automatic actions in response. You can have it report what it has done either with an alert message when it takes the action or in a log file you can examine at your leisure. It can even send a message to the person who sent an infected e-mail message, which makes tracking the source of virus infections relatively simple.

-
- **NOTE:** The Download Scan module will *not* appear in the VShield Properties dialog box unless you used the Custom Setup option when you installed VirusScan software and specified that you wanted to install the Internet Scan component.
-

Choosing Detection options

The Download Scan module initially assumes that you want it to scan for viruses each time you download any file susceptible to virus infection from the Internet (Figure 4-25). These default options provide excellent security, but your environment might require different settings.

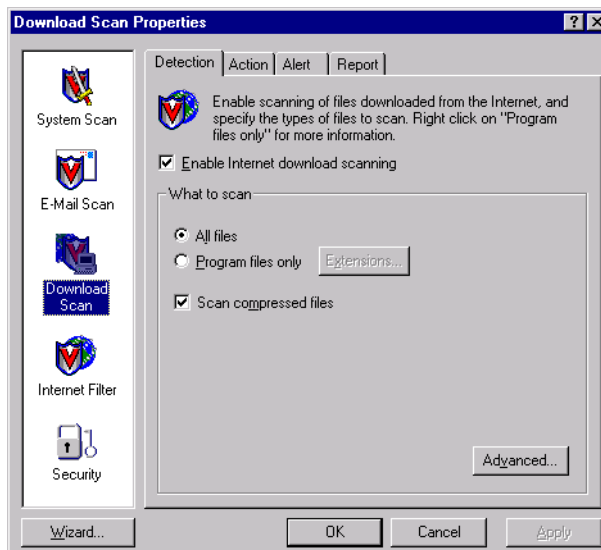


Figure 4-25. Download Scan Properties dialog box - Detection page

To modify the settings in this property page, follow these steps:

1. Select the **Enable Internet download scanning** checkbox.

The options in the rest of the property page activate.

2. Specify the types of files you want the Download Scan module to examine. You can:

- **Choose file types for scanning.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan sessions so that the module examines only those files most susceptible to virus infection. To do so, select the **Program files only** button.

To see or designate the file name extensions that the Download Scan module will examine, click **Extensions** to open the Program File Extensions dialog box (Figure 4-10).

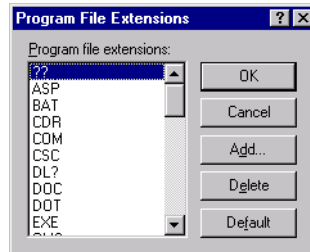


Figure 4-26. Program File Extensions dialog box

See “Adding file name extensions for scanning” on page 291 and “Current list of vulnerable file name extensions” on page 292 to learn which file name extensions this module scans by default and how to add to or change this list.

- **Scan all files.** Select the **All files** button to have the Download Scan module examine any file, whatever its extension, whenever you or a system process modifies it in any way.
- **Scan compressed files.** Select the **Compressed files** checkbox to have the module look for viruses in compressed files or in file archives.

This option ensures that viruses do not spread from compressed files, but because the module uncompresses these files before it scans them, choosing this option can lengthen the time it takes to scan a given set of files as you work with your computer.

-
- NOTE:** When the Download Scan module examines a file archive, it will scan only the file archive itself, not the compressed files within the archive. To learn which files and archives the module scans, see [“Current list of compressed files scanned”](#) on page 296.
-

3. Turn on heuristic scanning. Click **Advanced** to open the Advanced Scan Settings dialog box (Figure 4-11).

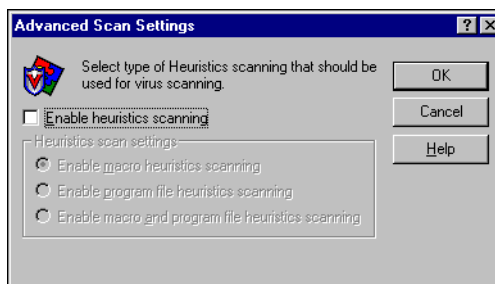


Figure 4-27. Advanced Scan Settings dialog box

Heuristic scanning technology enables the Download Scan module to recognize new viruses based on their resemblance to similar viruses that the module already knows. To do this, the module looks for certain “virus-like” characteristics in the files you’ve asked it to scan. The presence of a sufficient number of these characteristics in a file leads the module to identify the file as potentially infected with a new or previously unidentified virus.

Because the Download Scan module looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat “potential” infections with the same caution you would confirmed infections.

The Download Scan module starts out without any heuristic scan options active. To activate heuristics scanning, follow these substeps:

- a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.
- b. Select the types of heuristics scanning you want the Download Scan module to use. Your choices are:

- **Enable macro heuristics scanning.** Choose this option to have the Download Scan module identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that contain embedded macros, then compare the macro code to its virus definitions database. The module will identify exact matches with the virus name; code signatures that resemble existing viruses cause the module to tell you it has found a potential macro virus.
- **Enable program file heuristics scanning.** Choose this option to have the Download Scan module locate new viruses in program files by examining file characteristics and comparing them against a list of known virus characteristics. The module will identify files with a sufficient number of these characteristics as potential viruses.
- **Enable macro and program file heuristics scanning.** Choose this option to have the module use both types of heuristics scanning. McAfee recommends that you use this option for complete anti-virus protection.

NOTE: The Download Scan module will use heuristic scanning techniques only on the file types you designate in the Program File Extensions dialog box. If you choose to scan **All files**, the module will use heuristic scanning for all file types.

- c. Click **OK** to save your settings and return to the VShield Properties dialog box.
4. Click the Action tab to choose additional Download Scan module options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When the Download Scan module detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want the module to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the Download Scan module to display the correct property page (Figure 4-28).

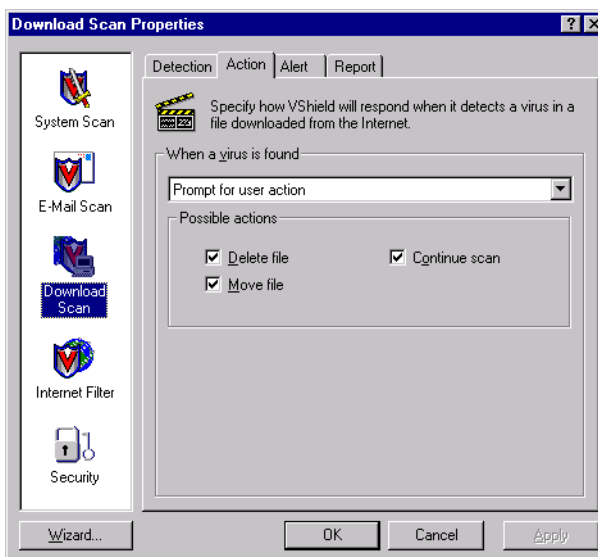



Figure 4-28. Download Scan Properties dialog box - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each choice. Your choices are:
 - **Prompt for user action.** Choose this response if you want the Download Scan module to ask you what to do when it finds a virus—the module will display an alert message and offer you a range of possible responses.

 **NOTE:** If you choose **Prompt for user action** from the list, click the Alert tab to specify whether you want the Download Scan module to prompt you with a message, a beep, or both.

Select the options you want to see in the alert message. Each of the checkboxes you select here causes an option button to appear in an alert message that the module displays when it finds a virus. Selecting **Delete file** here, for example, causes a **Delete** button to appear in the alert message.

You can choose from these options:

- **Delete file.** This option tells the module to delete the infected attachment immediately. The module will, however, preserve the e-mail message it came in.
 - **Move file.** This option tells the module to move the infected file to a quarantine folder. The alert message will display a **Move** button that tells the module to move the infected file to a preselected quarantine directory. By default, this directory is a folder named Infected in the VirusScan program directory.
 - **Continue scan.** This option tells the module to continue with its scan operation, but not take any other actions. If you have its reporting options enabled, the module records the incident in its log file.
- **Move infected files to a folder.** Choose this response to have the module move infected files to a quarantine folder as soon as it finds them. The module moves these files to a folder named Infected located in the VirusScan program directory.
 - **Delete infected files.** Choose this response to have the Download Scan module delete every infected file it detects immediately. Be sure to enable its reporting feature so that you have a record of which files the module deleted. You will need to restore deleted files from backup copies. See [“Choosing Report options” on page 140](#) for details.
 - **Continue scanning.** Choose this response to have the module continue scanning without taking any action against the virus it finds. If you also activate the Download Scan reporting feature (see [“Choosing Report options” on page 140](#) for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

Use this option only if you plan to leave your computer unattended while the module checks for viruses.

3. Click the Alert tab to choose additional Download Scan module options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want in the Action page, you can let the Download Scan module look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. But if you want the module to tell you as soon as it finds a virus so you can take appropriate action, have it send an alert message to you or to others.

Follow these steps:

1. Click the Alert tab in the Download Scan module to display the correct property page (see [Figure 4-29 on page 138](#)).

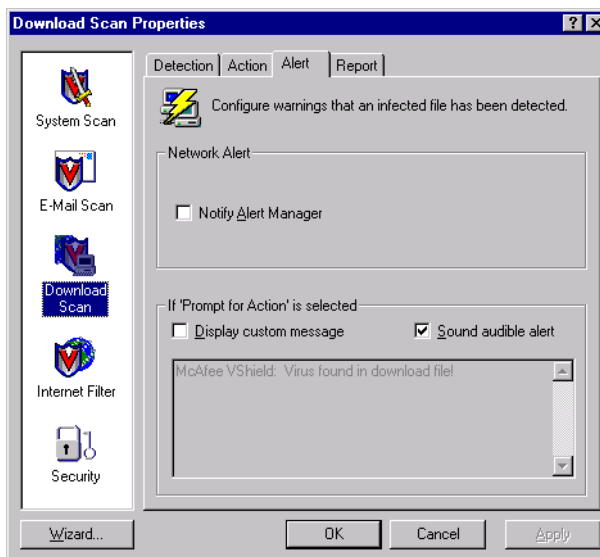


Figure 4-29. Download Scan Properties dialog box - Alert page

2. Select the **Notify Alert Manager** checkbox to have the module send alert messages to Alert Manager for distribution.

Alert Manager is a separate McAfee software component that collects alert messages and uses a variety of methods to send them to recipients that you specify. To have the Download Scan module send these alert messages successfully, you must also set up the Alert Manager Client Configuration utility. See [“Using the Alert Manager Client Configuration utility”](#) on page 285 for details.

You can pass alert messages directly to an Alert Manager server, or you can send alert messages as text (.ALR) files to a Centralized Alerting directory that the Alert Manager server checks periodically.

-
- NOTE:** Clearing this checkbox tells the Download Scan module not to send an alert message via Alert Manager, but does not affect other alert messages that you configure in this property page.
-

3. Select the **Sound audible alert** checkbox to have the module beep when it finds an infected file.

You can change the setting for this option only if you select **Prompt for user action** in the Action property page. Otherwise, the checkbox will display and use the setting it had when you last chose the **Prompt for user action** item. The module will sound the standard system warning beep or .WAV file you have your computer set to play.

4. Select the **Display custom message** checkbox to have the module add a custom message to the alert box it displays when it finds an infected file.

As with the audible alert, you can change the setting for this option only if you choose **Prompt for user action** in the Action property page. If you do not choose that item in the Action page, no alert box will appear and you will not see a custom message even if you select this checkbox.

5. Enter the message you want the module to display in the text box provided. You can enter a maximum of 250 characters here.
6. Click the Report tab to choose additional Download Scan module options. To save your changes without closing the Download Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

-
- NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.
-

Choosing Report options

The Download Scan module lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called WEBINET.TXT. You can have the module write its log to this file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor. Use the Report property page to determine which information the module will include in its log file.

The WEBINET.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections the Download Scan module found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer.

To set the Download Scan module to record its actions in a log file, follow these steps:

1. Click the Report tab in the Download Scan module to display the correct property page (Figure 4-30).

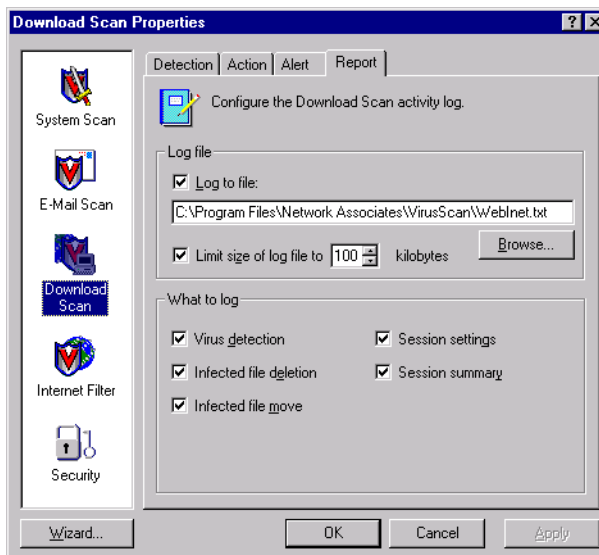


Figure 4-30. Download Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

By default, the Download Scan module writes log information to the file WEBINET.TXT in the VirusScan program directory.

You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network. You may use a different file, but the text file must already exist. The module will not create a new file.

3. Select the **Limit size of log file to** checkbox to minimize the log file size, then enter a value for the file size, in kilobytes, in the text box provided. If you do not select this checkbox, the log file can grow to as large a size as your disk space or file system permits.

Enter a value between 10KB and 999KB. By default, the Download Scan module limits the file size to 100KB. If the data in the log exceeds the file size you set, the module erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want the module to record in its log file. The module usually will record the data when the scan session ends or when you shut your system down.

You can choose to record any of this information:

- **Virus Detection.** Select this checkbox to have the log file record how many viruses the module finds during each scan session. Clear the checkbox to leave this information out.
- **Infected file deletion.** Select this checkbox to have the log file record how many viruses the module deletes during each scan session. Clear this checkbox to leave this information out.
- **Infected file move.** Select this checkbox to have the log file record how many viruses the module moves to a quarantine folder during each scan session. Clear this checkbox to leave this information out.
- **Session settings.** Select this checkbox to have the log file record the configuration settings you used for the module during each scan session. Clear this checkbox to leave this information out.
- **Session summary.** Select this checkbox to have the log file summarize what the module did during each scan session.

If you choose this option, the log will record:

- How many files the module examined.
- How many infected files the module cleaned.
- How many infected files the module deleted.
- How many infected files the module moved to a quarantine folder.
- Your Download Scan module settings.

Clear the checkbox to leave this information out.

5. Click a different tab to change any of your Download Scan settings, or click one of the icons along the side of the Download Scan Properties dialog box to choose options for a different module.

To save your changes in the Download Scan module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

-
- NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.
-

Configuring the Internet Filter module



Although both Java and ActiveX objects include safeguards designed to prevent harm to your computer system, determined programmers have developed objects that exploit arcane Java or ActiveX features to cause various sorts of harm to your system.

Dangerous objects such as these can often lurk on websites until you visit and download them to your system, usually without realizing that they exist. Most browser software includes a feature that allows you to block Java applets or ActiveX controls altogether, or to turn on security features that authenticate objects before downloading them to your system. But these approaches can deprive you of the interactive benefits of websites you visit by indiscriminately blocking all objects, dangerous or not.

The Internet Filter module allows a more judicious approach. It uses an up-to-date database of objects known to cause harm to screen Java classes and ActiveX controls you encounter as you browse.

When it finds a virus, the module can ask you what you want it to do, or it can block the dangerous object or site automatically. You can have it report what it has done either with an alert message when it takes the action or in a log file you can examine at your leisure.

To choose your options, click the Internet Filter icon at the left side of the VShield Properties dialog box to display the property pages for this module.

-
- NOTE:** The Internet Filter icon will not appear here unless you used the Custom Setup option to install the VirusScan software and specified that you wanted to install the Internet Scan component.
-

Choosing Detection options

The Internet Filter module starts by assuming that you want to block all of the harmful objects and sites it has listed in its database in order to prevent you from accidentally encountering them (Figure 4-31). This option provides you with the tightest security against harmful objects, but allows you to make use of other objects on the Internet sites you visit.

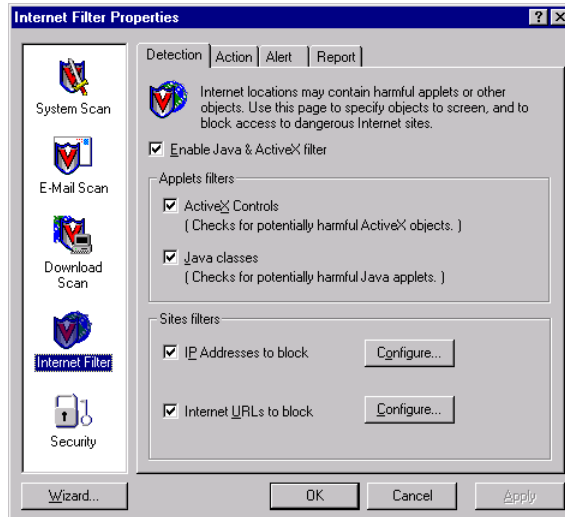


Figure 4-31. Internet Filter Properties - Detection page

To change configuration options, follow these steps:

1. Verify that the Enable Java & ActiveX filter checkbox is selected.
This activates the options in the rest of the property page.
2. Specify which objects you want the Internet Filter module to examine. Your options are:
 - **ActiveX Controls.** Select this checkbox to have the module look for and block harmful ActiveX or .OCX controls.
 - **Java classes.** Select this checkbox to have the module look for and block harmful Java classes, or applets written in Java.

The Internet Filter module will compare the objects you encounter as you visit Internet sites with an internal database that lists the characteristics of objects known to cause harm. When it finds a match, the module can alert you and let you decide what to do, or it can automatically keep the object from downloading. See “Choosing Action options” on page 147 for more details.

3. Tell the module which sites to filter. The program uses a list of dangerous Internet sites to decide which ones to prevent your browser from visiting. You can enable this function and add to the list of “banned” sites in two ways:
 - **IP Addresses to block.** Select this checkbox to tell the module to identify dangerous Internet sites by using their Internet Protocol (IP) addresses. To see or designate which addresses you want the module to ban, click **Configure** to open the Banned IP Addresses dialog box (Figure 4-32).

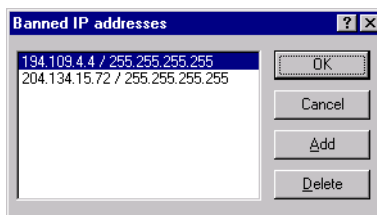


Figure 4-32. Banned IP addresses dialog box

The Banned IP Addresses dialog box identifies which Internet Protocol (IP) addresses you want the Internet Filter module to block whenever you or someone else tries to connect to them.

By default, the list includes two sites that download hostile Java or ActiveX objects to your machine as soon as you connect. You can add other sites, then password-protect your settings to ensure that users do not delete them.

Each address consists of four numeric groups of one to three digits each, formatted in this manner:

123.123.123.123

The Internet Filter module can use this number to identify a specific computer or network of computers on the Internet and prevent your browser from connecting to it. Each group of numbers can range between zero and 255. The first number series is the banned site's domain address—the number you use to find it on the Internet—and the second is a “subnet mask.”

A subnet mask is a way to “remap” a range of computer addresses within an internal network. The module lists a default subnet mask of 255.255.255.255. In most circumstances, you will not need to change this number, but if you know that a particular network node at the site you visit is the source of danger, you might need to enter a subnet mask to preserve your access to other machines at this site.

To change the list, you can:

- Click **Add** to open the Add IP Address dialog box (Figure 4-33).

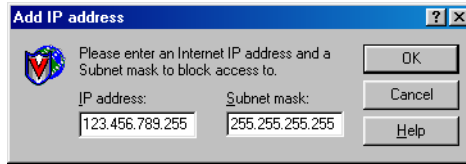


Figure 4-33. Add IP address dialog box

Next, follow these substeps:

- Type the Internet Protocol (IP) address you want to add to the Banned IP Addresses list in the text box on the left. Be sure to format the address with periods between each number group.
 - Type the subnet mask associated with the IP address you want to add to the Banned IP Addresses list in the text box on the right, if you know the correct subnet mask value for the site you want to avoid. Otherwise, leave the default value shown.
 - Click **OK** to return to the Banned IP addresses dialog box.
- Select one of the items shown, then click **Delete** to remove the item from the list.

When you changed the banned list so that it has all of the addresses you want to block, click **OK** to return to the Internet Filter Properties dialog box.

- **Internet URLs to block.** Select this checkbox to tell the module to identify dangerous Internet sites by using their Uniform Resource Locator designation. To see or choose which addresses you want the module to ban, click **Configure** to open the Banned URLs dialog box (Figure 4-34).

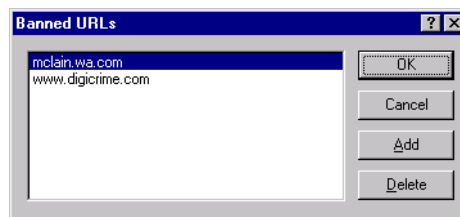


Figure 4-34. Banned URLs dialog box

The Banned URLs dialog box identifies which Uniform Resource Locators you want the Internet Filter module to block whenever you or someone else tries to connect to them.

By default, the list includes two domain names that download hostile Java or ActiveX objects to your machine as soon as you connect. You can add other domain names, then password-protect your settings to ensure that users do not delete them.

URLs specify the domain name and location of a computer on the Internet, usually together with the “transport protocol” you want to use to request a resource from that computer. A complete URL for a website, for instance, would look like:

http://www.domain.com

The complete URL tells your browser to request the resource via the Hyper Text Transport Protocol (“http://”) from a computer named “www” on a network domain named “domain.com.” Other transport protocols include “ftp://” and “gopher://.” The Internet’s Domain Name System translates URLs into IP addresses using an up-to-date, centralized, and cross-referenced database.

To add a site to this list, you must enter the domain name by itself, since the module will assume you mean the Hyper Text Transport Protocol (HTTP). To change the list, you can:

- Click **Add** to open the Add URL dialog box. Next, type the URL you want to add to the Banned URLs list in the in the dialog box that appears (Figure 4-35). Click **OK** to return to the Banned IP addresses dialog box.

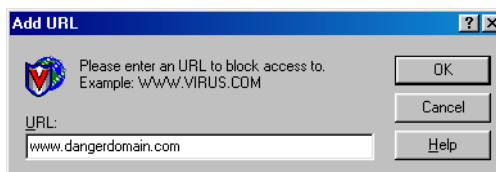


Figure 4-35. Add URL dialog box

- Select one of the items shown, then click **Delete** to remove the item from the list.

When you have changed the banned list so that it has all of the addresses you want to block, click **OK** to return to the Internet Filter Properties dialog box.

- Click the Action tab to choose additional Internet Filter module options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When the Internet Filter module encounters a dangerous object or a banned site, it can respond either by asking you whether it should block the object or site, or by automatically blocking it. Use the Action property page to specify which of these courses you want the module to take.

By default, the module lets you decide what you want to do (Figure 4-36).

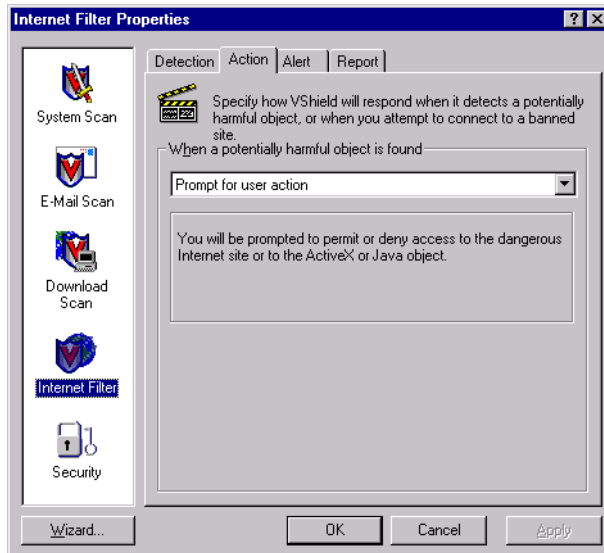


Figure 4-36. Internet Filter Properties dialog box - Action page

Choose a response from the **When a potentially harmful object is found** list. Your choices are:

- **Prompt for user action.** Choose this response to have the module ask you whether to block a harmful object or site, or to permit access to it.

NOTE: If you choose **Prompt for user action** from the list, click the Alert tab to specify whether you want the Internet Filter module to prompt you with a message, a beep, or both.

- **Deny access to objects.** Choose this response to have the module block harmful objects or sites automatically. The program will do so based on the contents of its own database, plus whatever site information you added. See “Choosing Detection options” on page 143 for details.

Click the Alert tab to choose additional Internet Filter module options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want in the Action page, you can let the Internet Filter module look for and block harmful objects or dangerous Internet sites away from your system automatically, as it finds them, with almost no further intervention. But if you want the module to tell you as soon as it finds a harmful object so you can take appropriate action, configure it to send an alert message to you or to others.

Follow these steps:

1. Click the Alert tab in the Internet Filter module to display the correct property page (Figure 4-37).

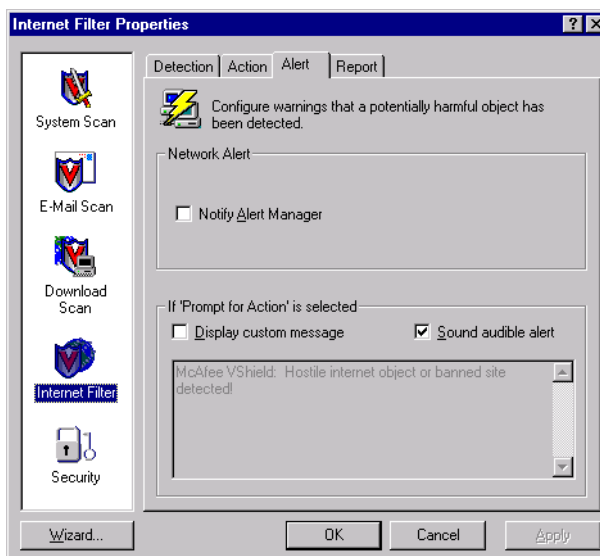


Figure 4-37. Internet Filter Properties dialog box - Alert page

2. Select the **Notify Alert Manager** checkbox to have the module send alert messages to Alert Manager for distribution.

Alert Manager is a separate McAfee software component that collects alert messages and uses a variety of methods to send them to recipients that you specify. To have the Internet Filter module send these alert messages successfully, you must also set up the Alert Manager Client Configuration utility. See [“Using the Alert Manager Client Configuration utility” on page 285](#) for details.

You can pass alert messages directly to an Alert Manager server, or you can send alert messages as text (.ALR) files to a Centralized Alerting directory that the Alert Manager server checks periodically.

NOTE: Clearing this checkbox tells the Internet Filter module not to send an alert message via Alert Manager, but does not affect other alert messages that you configure in this property page.

3. Select the **Sound audible alert** checkbox to have the module beep when it finds an infected file.

You can change the setting for this option only if you select **Prompt for user action** in the Action property page. Otherwise, the checkbox will display and use the setting it had when you last chose the **Prompt for user action** item. The module will sound the standard system warning beep or .WAV file you have your computer set to play.

4. Select the **Display custom message** checkbox to have the module add a custom message to the alert box it displays when it finds an infected file.

As with the audible alert, you can change the setting for this option only if you choose **Prompt for user action** in the Action property page. If you do not choose that item in the Action page, no alert box will appear and you will not see a custom message even if you select this checkbox.

5. Enter the message you want the module to display in the text box provided. You can enter a maximum of 250 characters here.
6. Click the Report tab to choose additional Internet Filter module options. To save your changes without closing the Internet Filter Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

The Internet Filter module records how many Java and ActiveX objects it scanned, and how many it blocked from access to your computer in a log file called WEBFLTR.TXT. The same file records the number of Internet sites you visited while the module was active, and how many dangerous sites the program kept your browser from visiting.

You can have the module write its log to its default file, or you can use any text editor to create a text file for it to use. You can then open and print the log file for later review from any text editor. Use the Report property page to designate the file you want to serve as the Internet Filter log, and to determine that file's permissible size.

The WEBFLTR.TXT file can serve as an important management tool for you to track malicious software activity on your system and to note which settings you used to detect and block the harmful objects or sites that the module found.

To set the Internet Filter module to record its actions in a log file, follow these steps:

1. Click the Report tab in the Internet Filter module to display the correct property page (Figure 4-38).

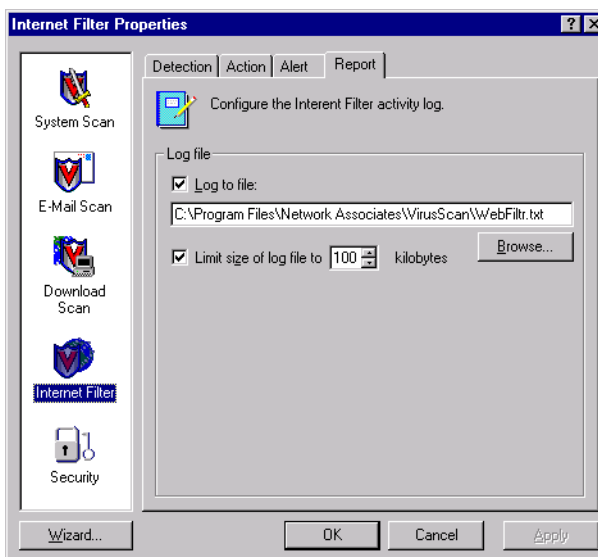


Figure 4-38. Internet Filter Properties dialog box - Report page

2. Select the **Log to file** checkbox.

By default, the module writes log information to the file WEBFILTR.TXT in the VirusScan program directory. You can enter a different name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

Enter a value between 10KB and 999KB. By default, the module limits the file size to 100KB. If the data in the log exceeds the file size you set, the module erases the existing log and begins again from the point at which it left off.

4. Click a different tab to change any of your Internet Filter settings, or click one of the icons along the side of the Internet Filter Properties dialog box to choose options for a different module.

To save your changes in the Internet Filter module without closing its dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

-
- NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.
-

Configuring the Security module



To keep the settings you chose for each VShield module safe from unauthorized changes, you can protect any or all module property pages with a password. System administrators can prevent network users from disabling the VShield scanner (see [Step 4 on page 104](#) for details), then protect that setting with a password, to can enforce a strict anti-virus security policy easily and effectively.

Use the Security module to assign a password and to choose which pages to protect.

Enabling password protection

The VShield Security module does not come enabled by default, because it needs to know which password you want to assign to your settings.

To activate and configure Security module password protection, follow these steps:

1. Select the **Enable password protection** checkbox.


The options in the rest of the property page activate (Figure 4-39).



Figure 4-39. Security Properties dialog box - Password page

2. Decide whether to protect the property pages for all VShield modules, or whether to protect individual pages. Your choices are:
 - **Password-protect all options on all property pages.** Select this button to lock everything all at once.
 - **Password-protect selected property pages only.** Select this button to choose which property pages in individual modules you want to lock. The other tabs in the Security Properties dialog box let you designate individual pages.

3. Enter a password to use to lock your settings. Type any combination of up to 20 characters in the upper text box in the Password area, then enter the exact same combination in the text box below to confirm your choice.

 **IMPORTANT:** The password protection in the VShield scanner is different from the password protection you can assign to tasks in the VirusScan Console or to settings in the VirusScan application. Choosing a password for one component does not assign that password to the other component—you must choose passwords for each independently.

The password you set here also protects the VirusScan control panel from tampering. This prevents unauthorized users from disabling VirusScan components through the control panel. To use this feature, you must clear the **System Scan can be disabled** checkbox in the System Scan Properties dialog box, then protect at least the System Scan property page in your security settings. See [“Protecting individual property pages” on page 154](#) for details.

4. Click any of the other Security module tabs to protect individual property pages. To save your password without closing the Security Properties dialog box, click **Apply**. If you chose to protect all property pages in all modules and want to close the dialog box, click **OK**. To close the dialog box without saving any changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Entering your password to configure settings

Once you have protected your settings with a password, the Security module will ask you to enter that password whenever you open the VShield Properties dialog box (Figure 4-40).

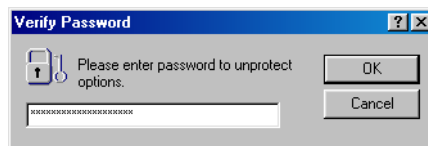




Figure 4-40. Verify Password dialog box

Enter the password you chose in the text box provided, then click **OK** to get access to the VShield Properties dialog box.

Protecting individual property pages

If you chose **Password-protect selected property pages only** in the Security module's Password page, you can choose which configuration options you want to lock for individual modules.

Follow these steps:

1. Click the tab for the *module* whose settings you want to protect. If you don't see the tab you want, click  or  to bring it into view. A representative page appears in [Figure 4-41](#).

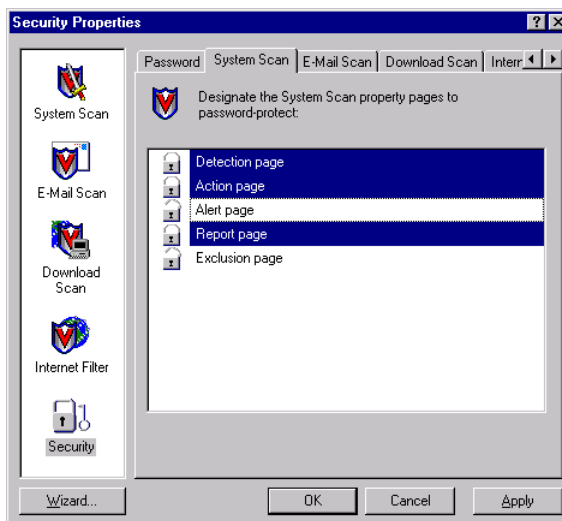




Figure 4-41. Security Properties dialog box - System Scan page


2. Select the settings you want to protect in the list shown.

You may protect any or all of a module's property pages. Protected property pages display a locked padlock icon  in the security list shown in [Figure 4-41](#). To remove protection from a property page, click the locked padlock icon to unlock it .

3. Select as many property pages as you want to protect in each module.
4. To save your password without closing the Security Properties dialog box, click **Apply**. To save your changes close the dialog box, click **OK**. To close the dialog box without saving any changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.


Using the VShield shortcut menu

The VShield scanner groups several of its common commands in a shortcut menu associated with its system tray icon . Double-click this icon to display the VShield Status dialog box. Right-click the icon to display these commands:


- **Status.** Choose this to open the VShield Status dialog box.
- **Properties.** Point to this, then choose one of the modules listed to open the VShield Properties dialog box to the property page for that module.
- **Quick Enable.** Point to this, then choose one of the VShield modules listed to activate or deactivate it. Those modules displayed in the menu with check marks are active; those without are inactive. If you use this method to disable a module, it stays disabled until you restart your computer.
- **About.** Choose this to display the VShield scanner's version number and serial number, the version number and creation date for the current .DAT files in use, and a Network Associates copyright notice.
- **Exit.** Choose this to stop all VShield modules and to unload the entire VShield scanner from memory.

Disabling or stopping the VShield scanner

At the end of the VirusScan installation, Setup asks if you want to enable the VShield scanner at that time. If you agree, the VShield scanner should load into memory immediately and begin working with a default set of options that give you basic anti-virus protection. If you do not agree, the VShield scanner will load automatically the next time you restart your computer.

When the VShield scanner first starts, it displays an icon  in the Windows system tray that indicates which of its modules are active. To learn what each icon state means, see [“Understanding the VShield system tray icon states” on page 94](#).

You can stop the scanner completely, which means deactivating all VShield modules and removing the scanner from memory. The VShield icon will disappear from the system tray. At that point, you may restart the scanner only from the VirusScan control panel, from the VirusScan Console, or by restarting your computer if you have VShield set to load at startup.

This differs from disabling the scanner, which means deactivating one or more of its modules and preventing those modules from running during a scan session. It does not mean stopping the scanner and unloading it from your computer's memory. The VShield scanner can remain active in memory even with none of its modules enabled. In this state, the scanner still leaves an icon  in the Windows system tray that you can use to enable it again.

Preventing the scanner from starting automatically

If you do not want the VShield scanner to start automatically, you can use the VirusScan control panel to prevent it from doing so.

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 to open it. If you have assigned a password to protect your VShield settings, the control panel will ask for that password in order to give you access. Enter the correct password in the text box that appears.
3. Click the Components tab.
4. Clear the **Load VShield on startup** checkbox at the top of the Components property page.
5. Click **OK** to close the control panel.


The VShield scanner will not stop or unload at this point, but it will not start when you next start your computer.

Stopping the VShield scanner completely

You can stop the VShield scanner completely—that is, deactivate it and remove it from memory—in any of three ways. Once you stop the scanner, you can reactivate it only by restarting it or restarting your computer. To learn how to start or restart the scanner, see [“Enabling or starting the VShield scanner” on page 90](#).

Method 1: Use the VShield shortcut menu


Follow these steps:

1. Right-click the VShield icon  in the Windows system tray to display its shortcut menu.
2. Choose **Exit**.

The VShield scanner will stop and unload itself from memory. The VShield icon will disappear from the Windows taskbar.

Method 2: Use the VirusScan Console

Follow these steps:

1. Double-click the VirusScan Console icon  in the Windows system tray to bring the Console window to the foreground (Figure 4-42).

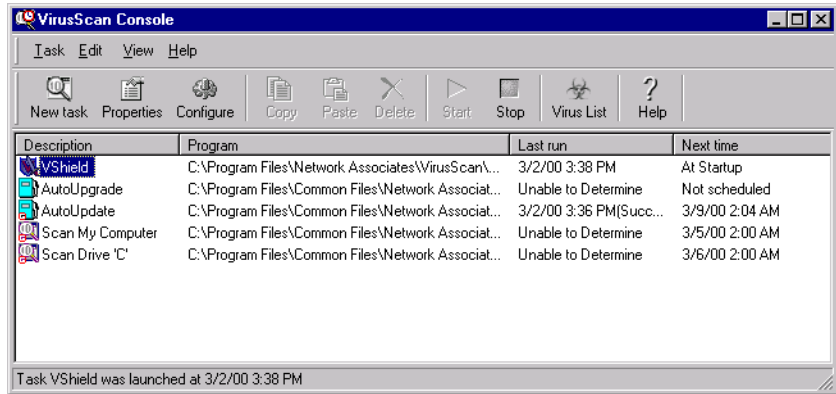




Figure 4-42. VirusScan Console window

2. Select VShield in the task list, then choose **Disable** from the **Task** menu. the Console will stop the VShield scanner and all of its modules, and unload them from memory. The VShield icon will disappear from the Windows taskbar.
3. Click the minimize or the close button in the upper-right corner of the Console window to shrink it back to a system tray icon.

 **NOTE:** Do not choose **Exit** from the **Task** menu. This will shut the Console down and unload it from memory. To run any tasks you have scheduled, the Console must be active.

Method 3: Use the VirusScan 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  to open it (Figure 4-43). If you have assigned a password to protect your VShield settings, the control panel will ask for that password in order to give you access. Enter the correct password in the text box that appears.

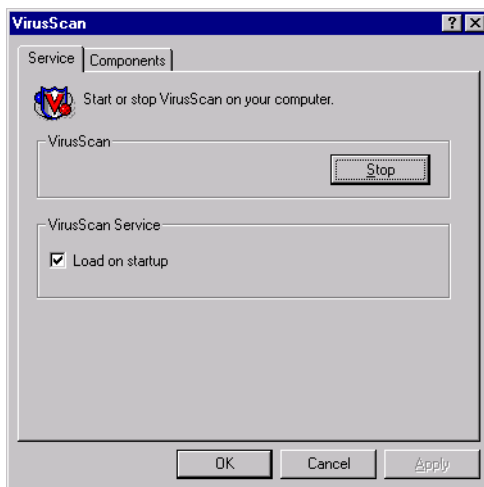


Figure 4-43. VirusScan control panel - Service page

3. Click **Stop** in the Service page.

All active VirusScan components will stop, close all open windows or dialog boxes, remove their icons from the Windows system tray, and unload from memory.


4. Click **OK** to close the control panel.

Disabling the VShield scanner and its modules

You can use any of three methods to disable any of the VShield modules—that is, deactivate the module, but do not remove the scanner from memory—in any of three ways. Once you disable a module, you can reactivate it in much the same way you disabled it. To learn how to enable modules, see [“Enabling or starting the VShield scanner” on page 90](#).

Method 1: Use the VShield shortcut menu


Follow these steps:

1. Right-click the VShield icon  in the Windows system tray to display its shortcut menu.
2. Point to **Quick Enable**.
3. Choose one of the module names shown with a check mark beside it to deactivate it. Module names that have a check mark beside them are active. Those without a check mark are inactive. This method disables a module only for the length of a scan session, or until you enable it again. The module will start again when you restart your computer.

Depending on which combination of modules you enable, the VShield icon will display a different state. To learn what each icon state means, see [“Understanding the VShield system tray icon states”](#) on page 94.

Method 2: Use the System Scan Status dialog box

Follow these steps:

1. Double-click the VShield icon  in the Windows system tray to open the System Scan Status dialog box ([Figure 4-44](#)).

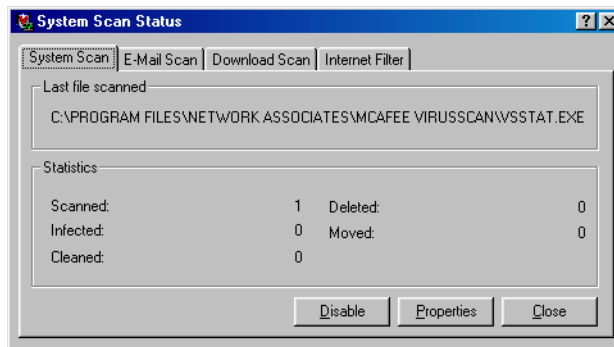



Figure 4-44. VShield System Scan Status dialog box

2. For each module that you want to disable, click the corresponding tab, then click **Disable**. The same button in the property page for inactive modules will read **Enable**.
3. Click **Close** to close the dialog box.

Depending on which combination of modules you enable, the VShield icon will display a different state. To learn what each icon state means, see [“Understanding the VShield system tray icon states”](#) on page 94.

Method 3: Use the VShield Properties dialog box

Follow these steps:

1. Right-click the VShield icon  in the Windows system tray to display the VShield shortcut menu.
2. Point to **Properties**, then choose a module name to open the VShield Properties dialog box (Figure 4-45).

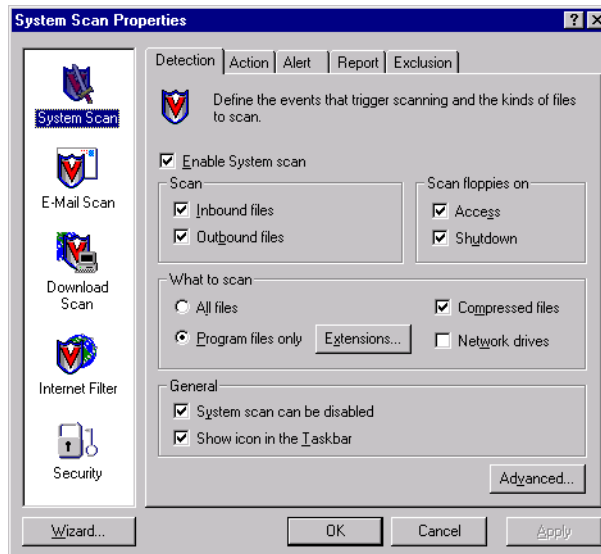



Figure 4-45. VShield Properties dialog box

3. For each module that you want to disable, click the corresponding icon along the left side of the dialog box, then click the Detection tab.
4. Clear the **Enable** checkbox at the top of each module page.

As you do so, the scanner will disable that module and make all of the configuration options in that page unavailable. Depending on which modules you disable, the VShield icon will display a different state.


If you disable all of its modules, the scanner will display  in the Windows system tray, unless you clear the **Show icon in the taskbar** checkbox in the System Scan Detection property page. In that case, VShield will not display an icon in the system tray.

Using this method to disable the module makes the disabled state the module's "default" state. If you later use the shortcut menu to enable the module, it will stay enabled only until you restart your VirusScan software or your computer.

Tracking VShield software status information

Once you activate and configure the VShield scanner, it operates continuously in the background, watching for and then scanning e-mail you receive, files you run or download, or Java and ActiveX objects you encounter.

To see a real-time summary of its progress:

1. Double-click the VShield system tray icon  to open the Status dialog box.
2. Click the tab that corresponds to the program module whose progress you want to check.

The information each module will report is:

- **System Scan.** This module reports the number of files it has scanned, the number of infected files it found, and the number it cleaned, moved or deleted.
- **E-mail Scan.** This module reports the number of files it scanned, the number of infections it found, and the number it moved or deleted.
- **Download Scan.** This module reports the number of files it scanned, the number of infections it found, and the number it moved or deleted.
- **Internet Filter.** This module reports the number of Java and ActiveX objects or Internet sites it has scanned and the number it has “banned,” or kept you from encountering.

To see a short description of each of the items that appears in this page, right click a figure or label, then choose **What's This?** from the shortcut menu that appears, or click the **?** button in the upper-right corner of the dialog box, then click the item you want described.

If you have activated its reporting feature, the VShield scanner also records the same information in the log file for each module.



Other functions available in this dialog box are:

- **Enable or disable modules.** Click the tab that corresponds to the program component you want to enable or disable, then click **Enable** to start the program component. Click **Disable** to disable it.
- **Open the VShield Properties dialog box.** Click the tab that corresponds to the program component you want to configure, then click **Properties** to open the VShield Properties dialog box for that module.

Viewing VShield task status information

You can also see statistical information in the Task Properties dialog box for each VShield module.

To view this information, follow these steps:

1. Double-click the VirusScan Console icon  in the Windows system tray to bring the Console window to the foreground (see [Figure 4-42 on page 157](#)).
2. Double-click the McAfee VShield task  in the task list to display the Task Properties dialog box shown in [Figure 4-46](#).

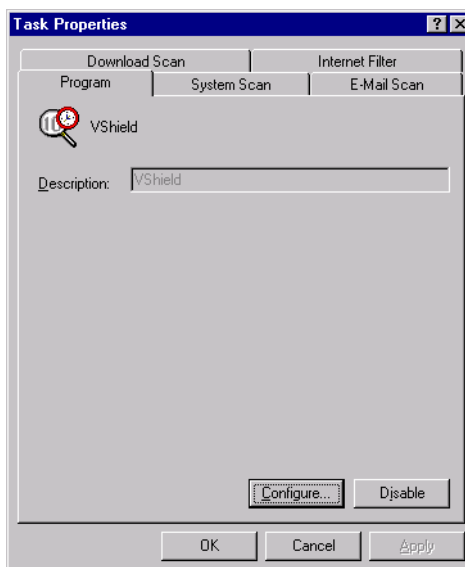


Figure 4-46. VShield Task Properties dialog box

3. Click the tab that corresponds to the program component that you want to enable or disable, or whose progress you want to check.

The status page will list the results of the last scan operation this task conducted, and the name of the last file it scanned. To see a short description of each of the items that appears in this page, right click a figure or label, then choose **What's This?** from the shortcut menu that appears, or click the **?** button in the upper-right corner of the dialog box, then click the item you want described. These displays will *not* update in real time.

If you have activated its reporting feature, the VShield scanner also records the same information in the log file for each module.

What is the VirusScan application?

McAfee desktop anti-virus products use two general methods to protect your system. The first method, background scanning, operates continuously, watching for viruses as you use your computer for everyday tasks. In the VirusScan product, the VShield scanner performs this function. To learn more about the VShield scanner, see [Chapter 4, “Using the VShield Scanner.”](#)

The second method puts you in charge. You decide when and where the software should look for viruses, then you tailor and run scan operations that suit your needs. You can run successive or concurrent scan operations, create different settings and specify different scan targets for each operation, and save your settings in exportable files for future use.

You might also see other materials identify this second method as “on-demand scanning.” The term “on demand” means that you as a user control when the application starts and ends a scan operation, which targets it examines, what it does when it finds a virus, or any other aspect of the scan operation. Other VirusScan components, by contrast, operate automatically or according to a schedule you set.

The VirusScan name applies both to the entire set of desktop anti-virus program components described in this *User’s Guide*, and to a particular component of that set: SCAN32.EXE, or the VirusScan application. The VirusScan application operates in two modes:

- **The VirusScan “Classic” interface.** This mode 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 interface.** This mode adds flexibility to the program’s configuration options, including the ability to run more than one scan operation concurrently.

This chapter describes how to use VirusScan software in both its Classic and Advanced modes.

Why use the VirusScan application?

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 scan your computer's memory and maintain a constant level of vigilance between scanning operations. Under most circumstances, this should protect your system's integrity. But good anti-virus security measures incorporate complete, regular system scans because:

- **Background scanning checks files as they execute.** The VShield scanner looks for virus code as executable files run or when you read a floppy disk, but the VirusScan application can check for code signatures in files stored on your hard disk. If you rarely run an infected file, the VShield scanner might not detect the virus until it deploys its payload. The VirusScan application, however, can detect a virus as it lies in wait for an opportunity to run.
- **Viruses are sneaky.** Accidentally leaving a floppy disk in your drive as you start your computer could load a virus into memory before the VShield scanner, particularly if you do not have the scanner configured to scan floppy disks. Once in memory, a virus can infect nearly any program, including the VShield scanner.
- **The VShield scanner requires time and resources.** Scanning for viruses as you run, copy or save files can delay, though very slightly, software launch times and other tasks. Depending on your situation, this could be time you might rather devote to important system operations. Although the impact is very slight, you might be tempted to disable the VShield scanner if you need every bit of available power for demanding tasks. In that case, performing regular scan operations during idle periods can guard your system against infection without compromising performance.
- **Good security is redundant security.** In the networked, web-centric world in which most computer users operate today, it takes only a moment to download a virus from a source you might not even realize you visited. If a software conflict has disabled background scanning for that moment, or if you have not configured background scanning to watch a vulnerable entry point, you could end up with a virus. Regular scan operations can often catch infections before they spread or do any harm.

If you connect to the Internet frequently or download files often, you might want to schedule regular scan operations that sweep your system at set intervals, so that you don't have to remember to start the VirusScan application. The VirusScan Console provides a very flexible set of options for this purpose. To learn more about scheduling VirusScan application tasks, see “Creating new tasks” on page 202.

Starting the VirusScan application

You can start the VirusScan application in its own window, or as part of a scheduled scan task. The method you choose depends on what sort of scan operation you want to run. When you first start it, the application window opens so that you can make changes to its configuration. You must click **Scan Now** or **Run Now** in a separate step to start an actual scan operation.

Four separate methods exist to start the VirusScan application—the fourth method involves running the application from the command line. The *VirusScan Administrator's Guide* lists the command-line options for this method.

The next sections describe each method.

Method 1: Displaying the VirusScan application main window

Follow these steps:

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

The VirusScan Classic main window appears (Figure 5-1).

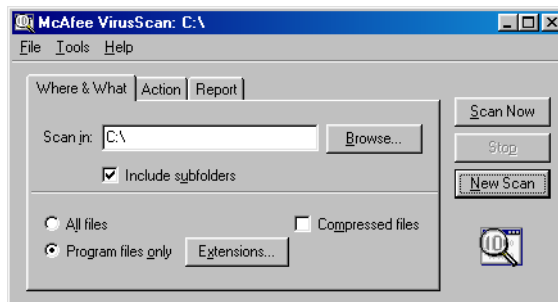


Figure 5-1. VirusScan Classic window

From here, you can:

- **Start scanning immediately.** Click **Scan Now** to have the application scan your system with the last configuration options you set, or with default options.
- **Switch between the Classic and Advanced interfaces.** Use the Classic interface for quick, uncomplicated scan operations that use default or restricted settings. To switch to the Advanced interface from there, choose **Advanced** from the **Tools** menu. Use the Advanced interface to control nearly all aspects of your scan operation. To return to the Classic interface from that point, choose **Classic** from the **Tools** menu.
- **Configure new scan options.** Specify which files you want to scan, then choose your response, reporting, alerting and exclusion options in each tabbed property page. To learn about Advanced options, see [“Configuring the VirusScan Advanced interface” on page 176.](#)

Next, click the **New Scan** button to the right of the window—or choose **Save As Default** from the **File** menu—to save the options you choose as the default options. The new settings will govern each new scan operation you run from that point forward. You can change your options as often as you want to, then save them again this same way to replace the old options with the new ones.

Choose **Save Settings** from the **File** menu to save your options to a settings file. You can use this file to run future scan operations or send it to other computers in order to control their scan operations.

- **View the VirusScan application activity log.** Choose **View Activity Log** from the **File** menu to open the VSCLOG.TXT file in a Notepad window.

```

VSCLog - Notepad
File Edit Search Help
8/18/98 4:58 PM Scan Started sbrennan On Demand Scan
8/18/98 4:58 PM Scan Settings sbrennan Current scan settings:
8/18/98 4:58 PM Scan Settings sbrennan Log file size is limited to 100 kilobytes.
8/18/98 4:58 PM Scan Settings sbrennan Action options
8/18/98 4:58 PM Scan Settings sbrennan Automatically clean : DISABLED
8/18/98 4:58 PM Scan Settings sbrennan Automatically delete : DISABLED
8/18/98 4:58 PM Scan Settings sbrennan Log options
8/18/98 4:58 PM Scan Settings sbrennan Virus detections : ENABLED
8/18/98 4:58 PM Scan Settings sbrennan Cleaned files : ENABLED
8/18/98 4:58 PM Scan Settings sbrennan Deleted files : ENABLED
8/18/98 4:58 PM Scan Settings sbrennan Moved files : ENABLED
8/18/98 4:58 PM Scan Settings sbrennan Scan Options
8/18/98 4:58 PM Scan Settings sbrennan Subdirectories : ENABLED
8/18/98 4:58 PM Scan Settings sbrennan All files : DISABLED
8/18/98 4:58 PM Scan Settings sbrennan Compressed files : DISABLED
8/18/98 4:58 PM Scan Settings sbrennan Skip memory scan : DISABLED
8/18/98 4:58 PM Scan Settings sbrennan Priority [1-5] : 0
8/18/98 4:58 PM Scan Settings sbrennan Program extensions : EXE COH DO? XL? HD?
8/18/98 4:58 PM Scan Settings sbrennan Scan targets
8/18/98 4:58 PM Scan Settings sbrennan All fixed disks
8/18/98 4:55 PM Scan Summary sbrennan Scan Summary
8/18/98 4:55 PM Scan Summary sbrennan Memory scan : No Viruses Found
8/18/98 4:55 PM Scan Summary sbrennan Boot sectors scanned : 2
8/18/98 4:55 PM Scan Summary sbrennan Boot sectors infected : 0
8/18/98 4:55 PM Scan Summary sbrennan Boot sectors cleaned : 0
8/18/98 4:55 PM Scan Summary sbrennan Files scanned : 2889
8/18/98 4:55 PM Scan Summary sbrennan Files infected : 0
8/18/98 4:55 PM Scan Summary sbrennan Files cleaned : 0
8/18/98 4:55 PM Scan Summary sbrennan Files deleted : 0
8/18/98 4:55 PM Scan Summary sbrennan Files Moved : 0
8/18/98 4:55 PM Scan Complete sbrennan On Demand Scan
8/18/98 8:25 PM Scan Started sbrennan On Demand Scan
  
```

Figure 5-2. VirusScan Activity Log

- **Protect your settings with a password.** Choose **Password Protect** from the **Tools** menu to open a dialog box you can use to lock any VirusScan application property page.

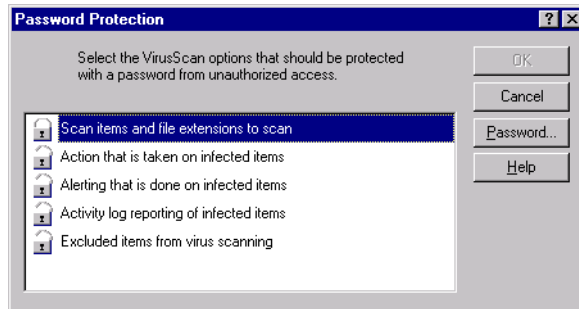


Figure 5-3. Password protection dialog box

Select each property page you want to protect, then click the **Password** button to the right to assign a password.

- **Open the online help file.** Choose **Help Topics** from the **Help** menu to see a list of VirusScan help topics. To see a context-sensitive description of buttons, lists and other items in the VirusScan window, choose **What's this?** from the **Help** menu, then click an item with your left mouse button after your mouse cursor changes to . You can see these same help topics if you right-click an element in the VirusScan window, then choose **What's This?** from the menu that appears.

2. Choose **Exit** from the **File** menu to quit the application.

Method 2: Starting a scan task from the VirusScan Console



Follow these steps:

1. Double-click the VirusScan Console icon in the Windows system tray to bring the Console window to the foreground.

If the icon does not appear in the system tray, click **Start** in the Windows taskbar, point to **Programs**, then to **Network Associates**. Next, choose **VirusScan Console**.

the Console comes with two preset tasks that use the VirusScan application to run—Scan My Computer and Scan Drive 'C'. To learn more about configuring and running scan tasks, see [“Creating new tasks” on page 202](#).

You can:

- **Start one of the preset tasks in its default configuration.** Select a task in the task list, then click  in the Console toolbar. If the scan task is set to start automatically, the VirusScan application window will open and the task will run immediately. If the task is not set to start automatically, the window will open, but you must click **Scan Now** to start the operation.
 - **Create and schedule a new task of your own.** Click  in the Console toolbar to open the Task Properties dialog box. Name your task, choose security options for it, specify how you want it to appear when it runs and what you want it to do when it finishes. To set configuration options for the task, click the **Configure** button at the bottom of the property page. To learn about how to configure your scan task, see [“Configuring VirusScan application options” on page 210](#).
2. Click the Schedule tab to specify when the task should run. Select the **Enable task** checkbox to ready it to run at the scheduled time. To learn how to set a schedule for the task, see [“Enabling tasks” on page 206](#).

Method 3: Starting a scan task from a settings file

You can use any settings file you've saved with your own configuration options to start the VirusScan application.

Follow these steps:

1. Locate and double-click a settings file that you saved from the VirusScan application window.

This reopens the VirusScan application window and loads the configuration options you saved ([Figure 5-4](#)).

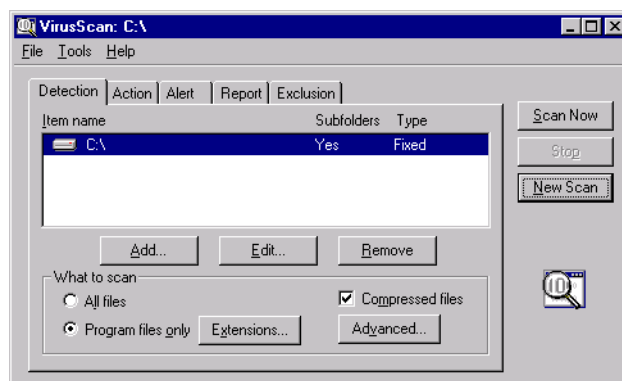


Figure 5-4. VirusScan Advanced window

You can also open this window and load your settings by right-clicking the settings file, then choosing **Start** from the shortcut menu that appears.

Ordinarily, you'll find your settings files in the VirusScan program directory, but you can save your settings files anywhere on your hard disk. VirusScan settings files have a .VSC extension.

2. Click **Scan Now** to start the scan operation with the settings you specified.

You can also change those settings on the fly before you run your scan task. To do so, either:

- Follow Step [Step 1](#) and [Step 2](#), above, to open the VirusScan application window, then change your configuration options in each property page; or
- Right-click the .VSC settings file, then choose **Properties** from the shortcut menu that appears.

This opens a Properties dialog box with configuration tabs similar to those available when you configure the VirusScan application from the VirusScan Console ([Figure 5-5](#)).

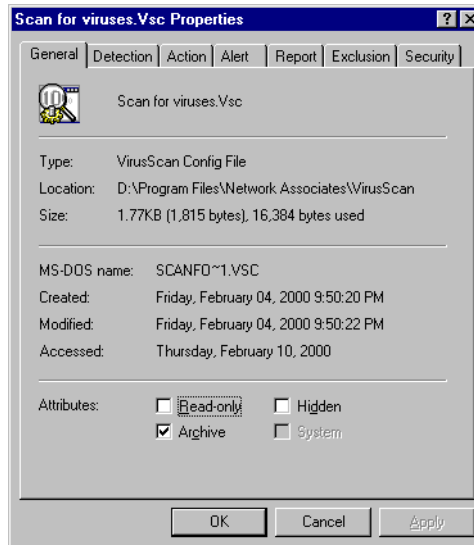


Figure 5-5. Example .VSC Properties dialog box

To learn how to configure the options in these property pages, “[Configuring VirusScan application options](#)” on page 210.

Method 4: Starting the application from the command line

Follow these steps:

1. Click **Start** in the Windows taskbar, point to **Programs**, then choose **MS-DOS Prompt** if your computer runs Windows 95 or Windows 98. If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, choose **Command Prompt** instead.

Windows displays a command-prompt window. If you installed the VirusScan software to its default location, change to this directory:

```
C:\Program Files\Common Files\Network Associates  
  \On Demand Scanner\Scan32
```

2. Type this line at the command prompt:

```
scan32.exe <scan target> /<configuration options>
```

Here, <scan target> means any drive, directory path, or filename you want the application to examine. Specify drives with DOS-style names—C: or D:, for example—and give complete path names for directories according to the conventions available for your operating system.

You may use long names on Windows NT Workstation v4.0 and Windows 2000 Professional systems, but you must use truncated names on Windows 95 and Windows 98 systems.

3. Follow the scan target with the set of configuration options, if any, that you want this scan operation to use as it runs. For a complete list of available options, see the VirusScan *Administrator's Guide*.

Precede each option with a /. Although the application will allow you to specify some options without the /, specifying others will result in an error. You may specify any necessary parameters for your options without special notation.

Depending on the command-line options you choose, starting the application this way can either run a scan operation or display the VirusScan application window, where you can choose configuration options for a scan operation.

Configuring the VirusScan Classic interface

For the VirusScan application to protect your system, you must tell it:

- what you want it to scan
- what you want it to do if it finds a virus
- how it should let you know when it finds a virus
- whether you want it to keep track of its actions

A series of property pages in the VirusScan window controls the options for each task—click each tab to set up the application for your task. To give yourself more configuration options, move to the VirusScan Advanced interface. Choose **Advanced** from the **Tools** menu in the VirusScan Classic window.

You can start a scan operation with the options you've chosen at any point—simply click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

The settings file you save will have your filename with a .VSC extension. To learn how to use this file to start a VirusScan application scan operation, see [“Method 3: Starting a scan task from a settings file” on page 168](#).

Choosing Where & What options

VirusScan software initially assumes that you want to scan your C: drive and all of its subfolders, and to restrict the files it scans only to those susceptible to virus infection ([Figure 5-6](#)).

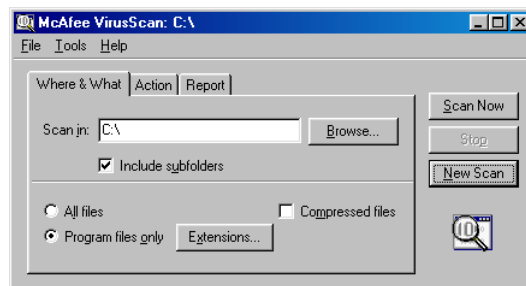


Figure 5-6. VirusScan Classic window - Where & What page

To modify these options, follow these steps:

1. Choose a volume or folder on your system or on your network that you want VirusScan software to examine for viruses.

Type a path to the target volume or folder in the text box provided, or click **Browse** to open the Browse for Folder dialog box (Figure 5-7).

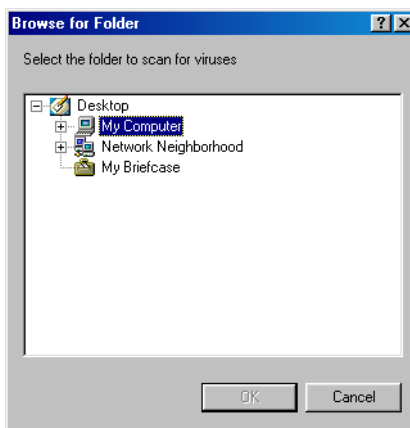


Figure 5-7. Browse for Folder dialog box

Click to expand the listing for an item shown in the dialog box. Click to collapse an item. You can select hard disks, folders or files as scan targets, whether they reside on your system or on other computers on your network. You cannot select My Computer, Network Neighborhood, or multiple volumes as scan targets from VirusScan Classic—to choose these items as scan targets, you must switch to VirusScan Advanced.

When you have selected your scan target, click **OK** to return to the VirusScan Classic window.

2. Select the **Include subfolders** checkbox to have the application look for viruses in any folders inside your scan target.

NOTE: Choosing **Include subfolders** 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, clear the **Include subfolders** checkbox.

3. Specify the types of files you want VirusScan software to examine. You can:

- **Scan compressed files.** Select the **Compressed files** checkbox to have VirusScan software look for viruses in compressed files and file archives. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

To see a list of the types of files and archives that the application scans, see [“Current list of compressed files scanned” on page 296](#).

- **Scan all files.** Select the **All Files** checkbox to have the application scan all of the files on the target you specified, whatever their extensions.

-
- NOTE:** McAfee recommends that you choose this option for your first scan operation, or periodically thereafter, to ensure that your system is virus-free. You can then limit the scope of later scan operations.
-

- **Choose file types.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection. To do so, click the **Program files only** button.

To see or designate the file name extensions the application will examine, click **Extensions**. This opens the Program File Extensions dialog box. To learn about how to change the files listed there, see [“Adding file name extensions for scanning” on page 291](#).

4. Click the Action tab to choose additional VirusScan options.

To start a scan operation immediately with just the options you’ve chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Action options

When VirusScan software detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VirusScan software to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the VirusScan Classic window to display the correct property page (Figure 5-8).

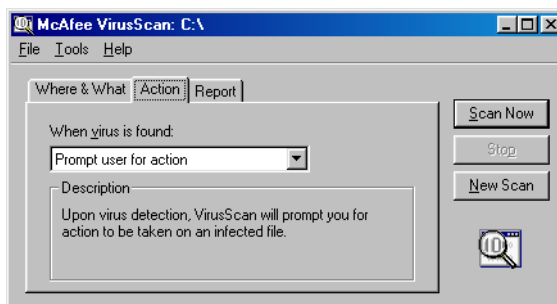


Figure 5-8. VirusScan Classic window - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each response. Your choices are:
 - **Prompt User for Action.** Choose this response if you expect to be at your computer when the VirusScan application scans your disk—the application will display an alert message when it finds a virus and offer you the full range of its available response options.
 - **Move infected files automatically.** Choose this response to have the application move infected files to a quarantine folder as soon as it finds them.

By default, the application moves these files to a folder named **Infected** located in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.

- **Clean infected files automatically.** Choose this response to tell the VirusScan application to remove the virus code from the infected file as soon as it finds it. If the application cannot remove the virus, it will note the incident in its log file. See [“Choosing Report options” on page 185](#) for details.
- **Delete infected files automatically.** Use this option to have the VirusScan application delete every infected file it finds immediately. Be sure to enable its reporting feature so that you have a record of which files the application deleted. You will need to restore deleted files from backup copies. If the application cannot delete an infected file, it will note the incident in its log file.

- **Continue scanning.** Use this option only if you plan to leave your computer unattended while the VirusScan application checks for viruses. If you also activate the application's feature (see [“Choosing Report options” on page 185](#) for details), the program will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Report tab to choose additional VirusScan options.

To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Report options

By default, the VirusScan application beeps to alert you when it finds a virus. You can use the Report page to enable or disable this alert, or to add an alert message to the Virus Found dialog box that appears when the application finds an infected file. This alert message can contain any information, from a simple warning to instructions about how to report the incident to a network administrator.

You can also set the size and location of the VirusScan log file here. By default, the application lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called VSCLOG.TXT. You can keep this file as your log file, or you can specify a different existing text file for the application to use. The application will not create a new text file itself.

You can then open and print the log file for later review from within the VirusScan application or from a text editor.

To choose VirusScan alert and log options, follow these steps:

1. Click the Report tab in the VirusScan Classic window to display the correct property page ([Figure 5-9](#)).

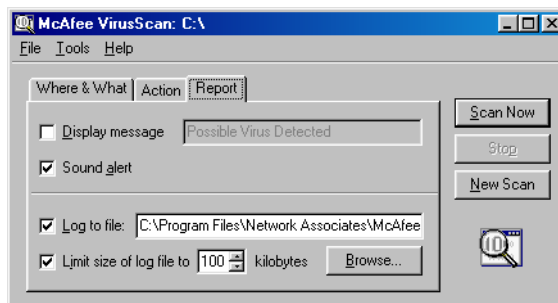


Figure 5-9. VirusScan Classic window - Report page

2. Choose the types of alert methods you want the VirusScan application to use when it finds a virus. You can have it:

- **Display a custom message.** Select the **Display message** checkbox, then enter the message you want to appear in the text box provided. You can enter a message up to 225 characters in length.

NOTE: To have the VirusScan application display your message, you must have selected **Prompt user for action** as your response in the Action page (see [“Choosing Action options” on page 182](#) for details).

- **Beep.** Select the **Sound alert** checkbox.
3. Select the **Log to file** checkbox.

By default, VirusScan software writes log information to the file VSCLOG.TXT in the VirusScan program directory. To specify a log file other than VSCLOG.TXT, enter a file name and path in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network.

4. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

Enter a value between 10KB and 999KB. By default, VirusScan software limits the file size to 100KB. If the data in the log exceeds the file size you set, VirusScan software erases the existing log and begins again from the point at which it left off.

5. Click a different tab to change any of your VirusScan settings.

To start a scan operation immediately with the options you’ve chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Configuring the VirusScan Advanced interface

The VirusScan Advanced interface offers you more flexibility in your configuration options than does the VirusScan Classic interface, including the ability to run more than one scan operation concurrently, the ability to exclude items from scan operations, and the ability to activate the application’s heuristic detection capability.

For the VirusScan application to protect your system, you must tell it:

- what you want it to scan
- what you want it to do if it finds a virus
- how it should let you know when it finds a virus
- whether you want it to keep track of its actions
- which items you don't want it to scan for viruses

A series of property pages in the VirusScan window controls the options for each task—click each tab to set up the application for your task. To choose from a simpler set of configuration options, move to the VirusScan Classic interface. Choose **Classic** from the **Tools** menu in the VirusScan Advanced window.

To protect the settings you've chosen from unauthorized changes, choose **Password Protect** from the **Tools** menu to open the Password Protection dialog box. To learn how to configure the settings for this dialog box, see [“Enabling password protection” on page 191](#).

You can start a scan operation with the options you've chosen at any point—simply click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Detection options

VirusScan software initially assumes that you want to scan all hard disks on your computer, including those mapped from network drives, and to restrict the files it scans only to those susceptible to virus infection ([Figure 5-10](#)).

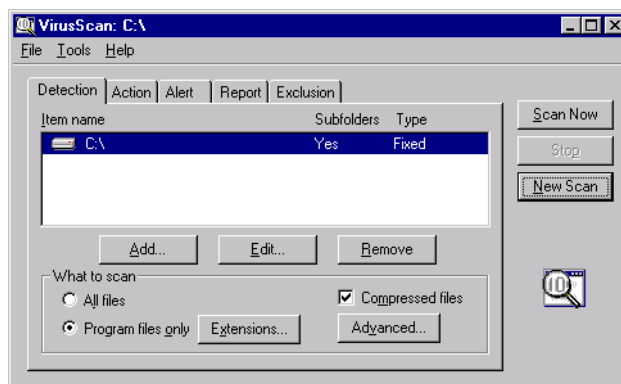


Figure 5-10. VirusScan Advanced window - Detection page

To modify these options and add others, follow these steps:

1. Choose which parts of your system or your network that you want VirusScan software to examine for viruses. You can:
 - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 5-11).

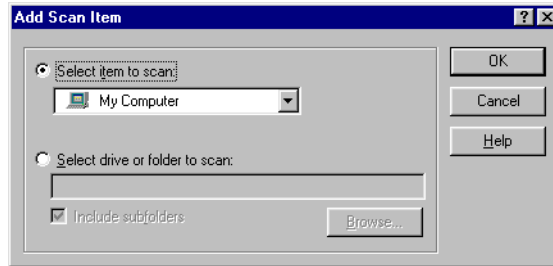


Figure 5-11. Add Scan Item dialog box

To scan your entire computer or a subset of the drives on your system or your network, click the **Select item to scan** button, then:

- a. Choose a scan target from the list provided. Your choices are:
 - **My Computer.** This tells the application to scan all drives physically attached to your computer or logically mapped via Windows Explorer to a drive letter on your computer.
 - **All removable media.** This tells the application to scan only floppy disks, CD-ROM discs, Iomega ZIP disks, or similar storage devices physically attached to your computer.
 - **All fixed disks.** This tells the application to scan hard disks physically connected to your computer.
 - **All network drives.** This tells the application to scan all drives logically mapped via Windows Explorer to a drive letter on your computer.
- b. When you've chosen your target, click **OK** to close the dialog box.

To scan a particular disk or folder on your system, click the **Select drive or folder to scan button**, then:

- a. Type in the text box provided the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer.

NOTE: You may not use Universal Naming Convention (UNC) notation to specify a network disk as a scan target for scheduled tasks. Doing so will result in an “Invalid Path” error. You may use UNC notation to specify scan targets for operations you run directly with the VirusScan application.

- b. Select the **Include subfolders** checkbox to have the VirusScan application also look for viruses in any folders inside your scan target.

NOTE: Choosing **Include subfolders** 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, clear the **Include subfolders** checkbox.

- c. Click **OK** to close the dialog box.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Item to Scan dialog box (Figure 5-12).

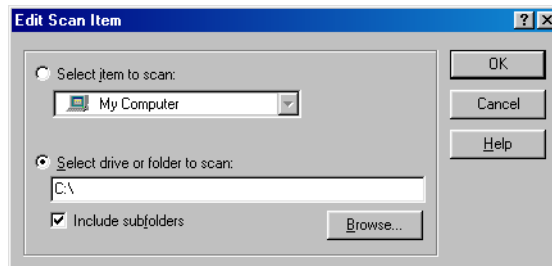


Figure 5-12. Edit Scan Item dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

- Specify the types of files you want the VirusScan application to examine. You can:

- Scan compressed files.** Select the **Compressed files** checkbox to have the VirusScan application look for viruses in compressed files and file archives. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

To see a list of the types of files and archives that the application scans, see [“Current list of compressed files scanned” on page 296](#).

- Scan all files.** Select the **All Files** checkbox to have the application scan all of the files on the target you specified, whatever their extensions.

-
- NOTE:** McAfee recommends that you choose this option for your first scan operation, or periodically thereafter, to ensure that your system is virus-free. You can then limit the scope of later scan operations.
-

- Choose file types.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection. To do so, click the **Program files only** button.

To see or designate the file name extensions the application will examine, click **Extensions**. This opens the Program File Extensions dialog box. To learn about how to change the files listed there, see [“Adding file name extensions for scanning” on page 291](#).

- Turn on heuristic scanning. Click **Advanced** to open the Advanced Scan Settings dialog box ([Figure 5-13](#)).

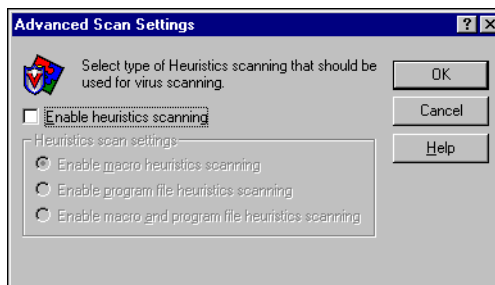


Figure 5-13. Advanced Scan Settings dialog box

Heuristic scanning technology enables the VirusScan application to recognize new viruses based on their resemblance to similar viruses that the module already knows. To do this, the application looks for certain “virus-like” characteristics in the files you’ve asked it to scan. The presence of a sufficient number of these characteristics in a file leads the application to identify the file as potentially infected with a new or previously unidentified virus.

Because the application looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat “potential” infections with the same caution you would confirmed infections.

The VirusScan application starts out without any heuristic scan options active. To activate heuristic scanning, follow these substeps:

- a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.
- b. Select the types of heuristics scanning you want the VirusScan application to use. Your choices are:
 - **Enable macro heuristics scanning.** Choose this option to have the application identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that contain embedded macros, then compare the macro code to its virus definitions database. The application will identify exact matches with the virus name; code signatures that resemble existing viruses cause it to tell you it has found a potential macro virus.
 - **Enable program file heuristics scanning.** Choose this option to have the VirusScan application locate new viruses in program files by examining file characteristics and comparing them against a list of known virus characteristics. The application will identify files with a sufficient number of these characteristics as potential viruses.
 - **Enable macro and program file heuristics scanning.** Choose this option to have the application use both types of heuristics scanning. McAfee recommends that you use this option for complete anti-virus protection.

NOTE: The application will use heuristic scanning techniques only on the file types you designate in the Program File Extensions dialog box. If you choose to scan **All files**, it will use heuristic scanning for all file types.

- c. Click **OK** to save your settings and return to the VShield Properties dialog box.
4. Click the Action tab to choose additional VirusScan application options.

To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Action options

When VirusScan software detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VirusScan software to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the VirusScan Advanced window to display the correct property page (Figure 5-14).

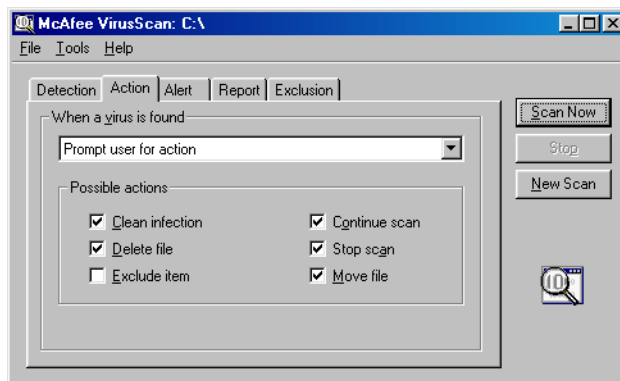


Figure 5-14. VirusScan Advanced - Action page

2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each response. Your choices are:
 - **Prompt user for action.** Choose this response if you expect to be at your computer when the VirusScan application examines your disk—the program will display an alert message when it finds a virus and offer you a range of possible responses.

Each of the checkboxes you select in the Action page causes an option button to appear in an alert message that the application displays when it finds a virus. Selecting **Delete file**, here, for example, causes a **Delete** button to appear in the alert message.

You can choose from these options:

- **Clean infection.** This option tells the application to try to remove the virus code from the infected file. If you have its reporting function enabled, it will record a log event each time it successfully cleans, or fails to clean, an infected file.
 - **Delete file.** This option tells the application to delete the infected file immediately.
 - **Exclude item.** This option tells the application to skip the file during later scan operations. This is the only option not selected by default.
 - **Continue scan.** This option tells the application to continue with its scan operation, but not take any other actions. If you have its reporting options enabled, the application records the incident in its log file.
 - **Stop scan.** This option tells the application to stop the scan operation immediately. To continue, you must click **Scan Now** to restart the operation.
 - **Move file.** This option tells the application to move the infected file to a quarantine folder. The alert message will display a **Move file to** button you can use to locate a quarantine folder.
- **Move infected files automatically.** Choose this response to have the application move infected files to a quarantine folder.

By default, the application moves these files to a folder named `\Infected` located in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.

- **Clean infected files automatically.** Choose this response to tell the application to remove the virus code from the infected file as soon as it finds it. If the application cannot remove the virus, it will note the incident in its log file.
- **Delete infected files automatically.** Choose this option to have the application delete every infected file it finds immediately. Be sure to enable the reporting feature so that you have a record of which files the application deleted. You will need to restore deleted files from backup copies. If the application cannot delete an infected file, it will note the incident in its log file.
- **Continue scanning.** Use this option only if you plan to leave your computer unattended while the application checks for viruses. If you also activate the reporting feature, the application will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

3. Click the Alert tab to choose additional VirusScan configuration options.

To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Alert options

Once you configure it with the response options you want, you can let the VirusScan application look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. To have the application tell you immediately when it finds a virus so that you can take appropriate action, however, configure it to send an alert message to you.

Follow these steps:

1. Click the Alert tab in the VirusScan Advanced window to display the correct property page ([Figure 5-15](#)).

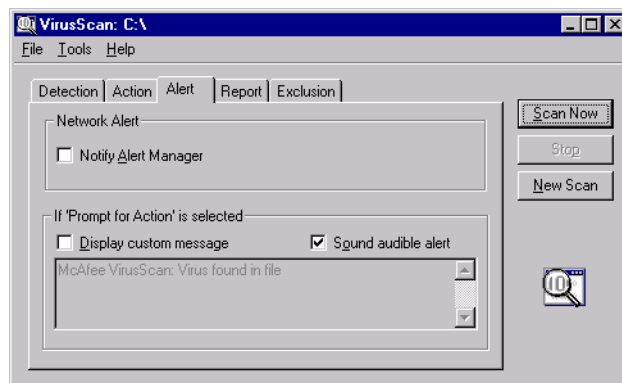


Figure 5-15. VirusScan Advanced - Alert page

2. Select the **Notify Alert Manager** checkbox to have the VirusScan application send alert messages to Alert Manager for distribution.

Alert Manager is a separate McAfee software component that collects alert messages and uses a variety of methods to send them to recipients that you specify. To have the VirusScan application send these alert messages successfully, you must also set up the Alert Manager Client Configuration utility. See [“Using the Alert Manager Client Configuration utility” on page 285](#) for details.

You can pass alert messages directly to an Alert Manager server, or you can send alert messages as text (.ALR) files to a Centralized Alerting directory that the Alert Manager server checks periodically.

-
- NOTE:** Clearing this checkbox tells the VirusScan application not to send an alert message via Alert Manager, but does not affect other alert messages that you configure in this property page.
-

3. Select the **Sound audible alert** checkbox to have the application beep when it finds an infected file.

You can change the setting for this option only if you select **Prompt for user action** in the Action property page. Otherwise, the checkbox will display and use the setting it had when you last chose the **Prompt for user action** item. The application will sound the standard system warning beep or .WAV file you have your computer set to play.

4. Select the **Display custom message** checkbox to have the application add a custom message to the alert box it displays when it finds an infected file.

As with the audible alert, you can change the setting for this option only if you choose **Prompt for user action** in the Action property page. If you do not choose that item in the Action page, no alert box will appear and you will not see a custom message even if you select this checkbox.

5. Enter the message you want the application to display in the text box provided. You can enter a maximum of 250 characters here.
6. Click the Report tab to choose additional VirusScan configuration options.

To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Report options

The VirusScan application lists its current settings and summarizes all of the actions it takes during its scan operations in a log file called VSCLOG.TXT. You can have the application write its log to this file, or you can use any text editor to create a text file for the application to use. You can then open and print the log file for later review from within the application or from your text editor.

The VSCLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections the VirusScan application found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Reports property page to determine which information the application will include in its log file.

To see the contents of the log file, choose **View Activity Log** from the **File** menu in the VirusScan application window.

To set VirusScan software to record its actions in a log file, follow these steps:

1. Click the Report tab in the VirusScan Advanced window to display the correct property page (Figure 5-16).

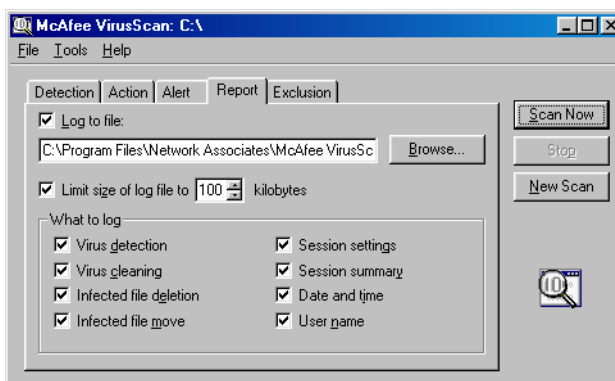


Figure 5-16. VirusScan Advanced - Report page

2. Select the **Log to file** checkbox.

By default, the VirusScan application writes log information to the file VSCLOG.TXT in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network. You may use a different file, but the text file must already exist. The application will not create a new file.

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided. If you do not select this checkbox, the log file can grow to as large a size as your disk space permits.

Enter a value between 10KB and 999KB. By default, the application limits the file size to 100KB. If the data in the log exceeds the file size you set, the application erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want the application to record in its log file. Each checkbox you select here causes the application to record this information, usually when the scan operation ends, or when you shut your system down:
 - **Virus detection.** Select this checkbox to have the log file record how many viruses the application finds during each scan operation. Clear the checkbox to leave this information out of the log file.
 - **Virus cleaning.** Select this checkbox to have the log file record how many infected files the application cleans—or tries to clean—during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Infected file deletion.** Select this checkbox to have the log file record how many viruses the application deletes during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Infected file move.** Select this checkbox to have the log file record how many viruses the application moves to a quarantine folder during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Session settings.** Select this checkbox to have the log file record the configuration settings you used for the application during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Session summary.** Select this checkbox to have the log file summarize the actions that the application took during each scan operation. The log will record:
 - How many files the application examined.
 - How many infected files the application cleaned.
 - How many infected files the application deleted.
 - How many infected files the application moved to a quarantine folder.
 - Your application settings.Clear the checkbox to leave this information out of the log file.
 - **Date and time.** Select this checkbox to have the log file record the date and time at which the software starts each scan operation. Clear this checkbox to leave this information out of the log file.

- **User name.** Select this checkbox to have the log file record the name of the user logged into the workstation as the software starts each scan operation. Clear this checkbox to leave this information out of the log file.
5. Click the Exclusion tab to choose additional VirusScan configuration options.

To start a scan operation immediately with just the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Choosing Exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling the VirusScan application to look only at susceptible file types (see [“Choosing Detection options” on page 177](#) for details), or you can tell the application to ignore entire files or folders that you know cannot become infected.

Once you scan your system thoroughly, you can exclude the files and folders that do not change or that are not normally vulnerable to virus infection. You can also rely on the VShield scanner to provide you with protection between scheduled scan operations. Regular scan operations that examine all areas of your computer, however, provide you with the best virus defense.

To prevent the application from scanning files that do not get infected, you can identify which disks, folders, or individual files you want to exclude from scan operations in an exclusion list. By default, the VirusScan application does not scan the Recycle Bin because Windows will not run items stored there. This item, therefore, will appear in the exclusion list when you first open the window.

Each entry in the exclusion list displays the path to the item, notes whether the application will also exclude any nested folders within the target, and explains whether the application will exclude the item when it scans files, when it scans your hard disk boot sector, or both.

By default, you can exclude up to 100 unique scan targets. To change this number, open the VirusScan control panel, click the Components tab, then enter a new figure in the **Maximum number of exclude items** text box. To learn more about how to use the VirusScan control panel, see [“Understanding the VirusScan control panel” on page 281](#).

To exclude files or folders from scan operations, follow these steps:

1. Click the Exclusion tab in the VirusScan Advanced window to display the correct property page (Figure 5-17).

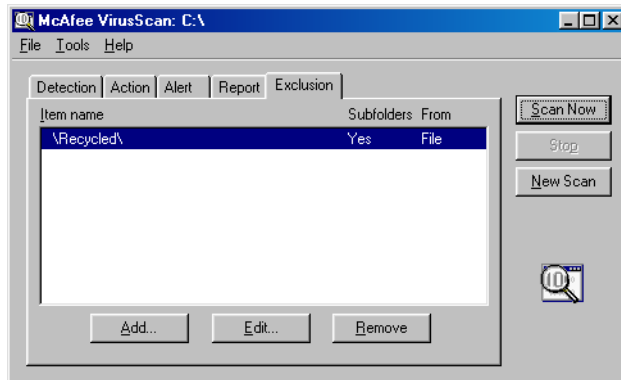


Figure 5-17. VirusScan Advanced window - Exclusion page

2. Specify the items you want to exclude. You can
 - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box (Figure 5-18).

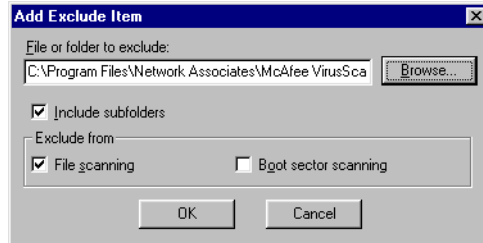



Figure 5-18. Add Exclude Item dialog box

Next, follow these substeps to add items to the list:

- a. Enter a path to a folder or a file name in the text box provided, or click **Browse** to locate the item you want the application to exclude.

 **NOTE:** If you have chosen to move infected files to a quarantine folder automatically, the application excludes that folder from scan operations.

- b. Select the **Include subfolders** checkbox to tell the application to ignore files stored in any subfolders within the folder you specified in [Step a](#).

NOTE: Choosing **Include subfolders** causes the application to ignore only those files stored in the subfolders themselves. The application will still scan files stored at the root level of the folder you designate. To exclude the files at the folder root level, clear the **Include subfolders** checkbox.

- c. Select the **File scanning** checkbox to exclude the item you specified in the first step from scan operations in which the application looks for file-infecting viruses. These viruses usually appear in files in the visible portions of your hard disk.
- d. Select the **Boot sector scanning** checkbox to exclude the item you specified in the first step from scan operations in which the application looks for boot-sector viruses.

These viruses usually appear in memory or in files that reside in your hard disk's boot sector or master boot record. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

 **WARNING:** McAfee recommends that you do *not* exclude your system files from scan operations.

- e. Repeat [Step a](#). through [Step d](#). until you have listed all of the files and folders you do not want scanned.
 - **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.
 - **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. This means that the VirusScan application *will* scan this file or folder during its next scan operation.
3. Click a different tab to change any of your VirusScan settings.

To start a scan operation immediately with the options you've chosen, click **Scan Now**. To save your changes as default scan options, choose **Save As Default** from the **File** menu or click **New Scan**. To save your settings in a new file, choose **Save Settings** from the **File** menu, name your file in the dialog box that appears, then click **Save**.

Enabling password protection

VirusScan software lets you set a password to protect the settings you choose in each property page from unauthorized changes. This feature is particularly useful for system administrators who need to keep users from tampering with their security measures by changing VirusScan settings. Use the Security property page to lock your settings.

To enable password protection for VirusScan Advanced, follow these steps:

1. Choose **Password Protect** from the **Tools** menu in the VirusScan Advanced window to open the Password Protection dialog box (Figure 5-19).

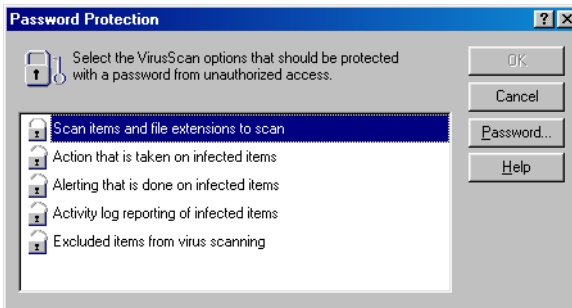




Figure 5-19. Password Protection dialog box

2. Select the settings you want to protect in the list shown.

You may protect any or all VirusScan property pages. Protected property pages display a locked padlock icon  in the security list shown in Figure 5-19. To remove protection from a property page, click the locked padlock icon to unlock it .

3. Click **Password** to open the Specify Password dialog box (Figure 5-20).

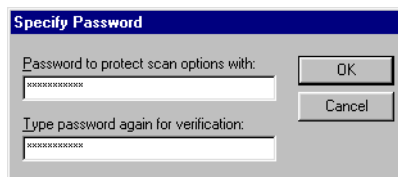


Figure 5-20. Specify Password dialog box

- a. Enter a password in the first text box shown, then enter the same password again in the text box below to confirm your choice.
 - b. Click **OK** to close the Specify Password dialog box.
4. Click **OK** to return to the VirusScan Advanced window.

What does VirusScan Console do?

The VirusScan Console exists primarily to run scan operations and other tasks on the dates and at the times you choose, or at intervals you set. You can 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. The VirusScan Console can become the cornerstone of your anti-virus security strategy if you set it up to run a number of interlocking or related tasks that provide coverage at idle or otherwise unproductive computer time. Separate tasks on individual cycles can scan different parts of your system, for instance, or provide coverage for regular and predictable work events.

the Console also allows you to start and stop a number of other important VirusScan operations, including VShield scan sessions, AutoUpdate, and AutoUpgrade operations. You can connect to the McAfee AVERT Labs website for virus information, open and view log files, and copy and paste task definitions within the Console window. For a complete overview of functions available from within the Console window, see [“Using the Console window” on page 196](#).

Why schedule scan operations?

Although VirusScan software includes components that look for viruses continuously or that allow you to scan your system whenever you want, you should schedule regular scan operations and other software activities to:

- **Set a periodic baseline for your system.** If you want to track your system or your network for recurring virus activity, schedule a full scan operation for your system at regular intervals. VirusScan software reporting features can provide you with a complete report on the number, type, size and other characteristics of any viruses it finds.
- **Supplement or replace on-access scanning.** McAfee recommends that you use VShield software to scan continuously for viruses, but if your environment doesn't permit you to use VShield software or if you have other concerns about system performance, schedule frequent scan operations to prevent infections. Even if you do use VShield software, scheduling periodic full scan operations for your system reduces the likelihood that infected files remain undetected.


- **Alternate between scan operations.** Scheduled scanning operations give you the flexibility to choose different operations for different purposes or different times. If, for example, you want to use VShield software to scan your own system continuously and scan mapped network drives less frequently, you can schedule a task for this purpose.

the Console comes with a default set of tasks already configured, but not yet scheduled. This set includes tasks that start the VShield scanner when you start your computer, that scan all drives included in the My Computer group, that scan your C: drive, and that update VirusScan software data files and program components. You can enable any of the default tasks to start, or you can create your own tasks to suit your work habits.

Starting the VirusScan Console

You must have the VirusScan Console running in order to run any tasks you have scheduled. McAfee recommends that you set the Console to start automatically, as soon as you start your computer.

To do so, 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  to open it. If you have assigned a password to protect your VShield settings, the control panel will ask for that password in order to give you access. Enter the correct password in the text box that appears, then click the Components tab (Figure 6-1).

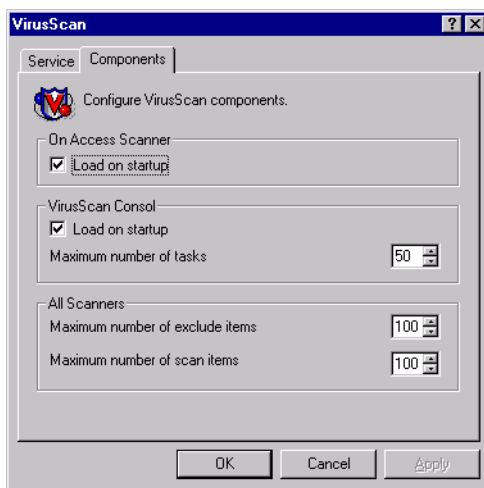


Figure 6-1. VirusScan control panel - Components page

3. Select the **Load on startup** checkbox in the VirusScan Console area in the Components page.
4. Click **OK** to close the control panel.

When you next restart your computer, the Console will also start, but it will remain minimized as an icon in the Windows system tray. To bring the Console window to the foreground, double-click the icon (Figure 6-2).

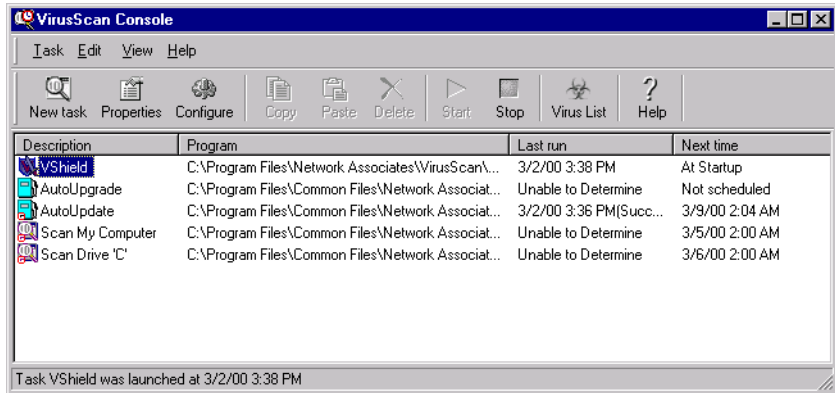


Figure 6-2. VirusScan Console window

If the icon does not appear in the system tray:

1. Click **Start** in the Windows taskbar, point to **Programs**, then to **Network Associates**.
2. Choose **VirusScan Console** to make the Console window appear.

Once you can display the Console window, you can also ensure that it will load automatically at startup by choosing **Load at startup** from the **View** menu.

the Console window initially shows a list of default tasks that come with the Console, pre-configured and ready to run. A “task” is a set of instructions to run a particular program, in a certain configuration, at a certain time. Along with a name for each task, the Console window shows the path and filename for the program that the task will run at the scheduled time. Tasks that you create will always run the VirusScan application. Your newly created tasks will appear at the bottom of the Console window. the Console also shows the time and date on which each task last ran, and the time and date on which it will next run.







The toolbar at the top of the Console window gives you quick access to the program’s most common commands. To have this toolbar display only its command buttons, click **View**, point to **Toolbar**, then choose **Standard Buttons**.

To add text captions to the buttons, click **View**, point to **Toolbar**, then choose **Text Labels**. You can have both options active at the same time—a check mark beside the menu item indicates which view is active. You'll find most of the same toolbar commands in the menus at the top of the Console window, and in shortcut menus that appear when you click a listed task with your right mouse button.






A status bar at the bottom of the Console window counts the number of listed tasks. When you select a listed task, the status bar tells you when the task last ran. The status bar also shows a brief description of each toolbar button as you pass your mouse cursor over it. Choose **Title Bar** or **Status Bar** from the **View** menu to display or hide each window element.


Using the Console window


From the Console window, you can:

- **Create a new task.** Choose **New Task** from the **Task** menu, or click  in the Console toolbar. A Task Properties dialog box will appear. To learn how to name and set other properties for your new task, see [“Creating new tasks” on page 202](#).
- **Schedule and enable a task.** Select one of the tasks listed in the Console window, then choose **Properties** from the **Task** menu, or click  in the Console toolbar. A Task Properties dialog box will appear. To learn how to schedule and enable a task, see [“Enabling tasks” on page 206](#).
- **Configure the task.** Select one of the tasks listed in the Console window, then click  in the Console toolbar to display a property page for the VirusScan component that will run the task. How this property page looks depends on which VirusScan component you run. To learn how to choose settings for the VirusScan application, see [“Configuring VirusScan application options” on page 210](#).
- **Copy a task.** Select one of the tasks listed in the Console window, then choose **Copy** from the **Edit** menu, or click  in the Console toolbar. This copies the task to the Windows clipboard. Next, click inside the Console window, then choose **Paste** from the **Edit** menu or click  in the Console toolbar to paste a copy of the task to the Console list. Use this feature to copy task settings for use as templates for similar tasks.
- **Delete a task.** Select one of the tasks listed in the Console window, then choose **Delete** from the **Task** menu, or click  in the Console toolbar.

NOTE: You can delete only tasks that you create—you may not delete any of the tasks from the default set that come with the Console. You can, however, disable any default task that you don't want to run. See [“Enabling tasks” on page 206](#) for details.

- **Start a task.** Select one of the tasks listed in the Console window, then choose **Start** from the **Task** menu, or click  in the Console toolbar. The task you selected will start immediately and will run with the options you've chosen. To enable the VShield scanner, select the VShield task, then choose **Enable** from the **Task** menu. To start the scanner and load it into memory, select the VShield task, then click  in the Console toolbar.
- **Stop a task.** Select one of the tasks listed in the Console window, then choose **Stop Now** from the **Task** menu, or click  in the Console toolbar. To stop the VShield scanner, select the VShield task, then click  in the Console toolbar or choose **Disable** from the **Task** menu. To learn other ways to stop or disable the VShield scanner, see [“Disabling or stopping the VShield scanner” on page 155](#).
- **Connect to the McAfee Virus Information Library.** Choose **Virus List** from the **View** menu, or click  in the Console toolbar. The Console will start your preferred browser application and connect to the AVERT website. See [“Viewing virus information” on page 76](#) to learn more about what information you'll find in the library.


 **NOTE:** To connect to the Virus Information Library, you must have an Internet connection and web browsing software available on your computer.

- **Open the online help file.** Choose **Help Topics** from the **Help** menu, or click  in the Console toolbar to see a list of VirusScan software help topics. You can also right-click most dialog box buttons, lists, menus, and other items to reveal context-sensitive help topics. Choose the **What's This?** item that appears when you right-click inside a dialog box to see the help topic. To learn more about VirusScan documentation, see [“What comes with VirusScan software?” on page 27](#).
- **View an Activity Log.** Select one of the tasks listed in the Console window, then choose **View Activity Log** from the **Task** menu. Not all tasks will have an associated log file, but VirusScan software will open the log file for those that do in a Notepad window. You can print, edit, copy, or otherwise treat this file as you would any ordinary text file. To learn more about what information each log file records, see [Chapter 4, “Using the VShield Scanner,”](#) and [Chapter 5, “Using the VirusScan application.”](#)
- **Protect tasks with a password.** Select any of the tasks listed in the Console window except the VShield task, then choose **Password Protect Task** from the **Task** menu to open the Specify Password dialog box. Enter a password of up to 20 characters in the text box provided, then enter the same password again in the text box below. Click **OK** to close the dialog box.

Whenever you or anyone else tries to configure task properties for the task you protected, the Console will ask for the password you specified. Choosing this option gives you the same results as selecting the **Password protect this task** checkbox in the Task Properties dialog box.

- **Start VirusScan Console automatically.** Choose **Load at Startup** from the **View** menu to have the VirusScan Console start whenever you start your computer. The Console has this option enabled by default. Because it must be running in order to execute any tasks you have scheduled, you should choose to have the Console start automatically so that your scheduled tasks will begin at their appointed times.

You can also control this option from the VirusScan control panel. To learn more about how to use the control panel, see [“Understanding the VirusScan control panel” on page 281](#).

- **Display the Console system tray icon.** Choose **Show System Tray Icon** from the **View** menu to have the Console display this icon  in the Windows system tray. Double-clicking this icon brings the Console window to the foreground. Right-clicking the icon displays a shortcut menu.
- **Quit VirusScan Console.** Choose **Exit** from the **Task** menu to quit the Console. If you have any tasks pending, you should minimize the Console rather than quit. To learn how to start the Console again, see [“Starting the VirusScan Console” on page 194](#).

Working with default tasks

As soon as you install VirusScan software on your computer and reboot, VShield software will immediately begin scanning your system, using a default configuration that provides you with a basic range of protection for your system. The other tasks listed in the Console window also have default configurations set up, but these tasks remain dormant until you activate them. See [“Enabling tasks” on page 206](#) for details.

the Console comes with five default tasks. These are:

- **VShield.** This task runs the VShield scanner. By default, it runs automatically as soon as you start your computer. You cannot schedule the VShield scanner to run any other time, but you can choose different scan options. You may not rename or delete this task, but you can see statistics from its most recent scan session, you can enable or disable it, and you can open up the VShield properties dialog box to configure it.

See [“Setting VShield scanner properties” on page 99](#) to learn which options you have available.

- **AutoUpgrade.** This task allows you to schedule automatic program upgrades for VirusScan software. These upgrades can consist of new scan engine files or other file upgrades. To get it to upgrade your files, you must configure this task to connect to a local network server or FTP site that you designate, then you must schedule and activate it. You may not rename or delete this task, but you can enable and disable it, schedule it, configure it, and protect its settings with a password.

To learn how to schedule and enable this task, see [“Enabling tasks” on page 206](#). To learn how to configure this task to suit your needs, see [Chapter 7, “Updating and Upgrading VirusScan Software.”](#)

- **AutoUpdate.** This task allows you to schedule automatic virus definition (.DAT) file updates. To get it to do so, you must configure the task to connect to a server or File Transfer Protocol (FTP) site that you designate. The task comes configured to connect to a McAfee server, but you may also set it to download files internally. You must also schedule and activate the task to get it to update your files. In other respects, this task closely resembles the AutoUpgrade task.

To learn how to schedule and enable this task, see [“Enabling tasks” on page 206](#). To learn how to configure this task to suit your needs, see [Chapter 7, “Updating and Upgrading VirusScan Software.”](#)

- **Scan My Computer.** This task runs a baseline scan operation on all hard disks and other drives connected to your computer, along with your RAM and hard disk or floppy disk boot sectors. You may not rename or delete this task, but you can modify its configuration, schedule it, see statistics from its most recent scan operation, and protect its settings with a password. You must activate this task to get it to run, but you can run it in its default configuration for nearly comprehensive protection.
- **Scan Drive ‘C’.** This task runs a baseline scan operation on your computer's C: drive. Otherwise, it closely resembles the Scan My Computer task.

Both the Scan My Computer and Scan Drive ‘C’ tasks require the VirusScan application to run. To learn how to configure the application for use with the VirusScan Console, see [“Configuring VirusScan application options” on page 210](#).

Working with the VShield task

The VShield task appears in the Console window primarily so that you can manage its operation. You can enable and disable it directly from the Console window, or double-click the task to open the Task Properties dialog box (Figure 6-3).

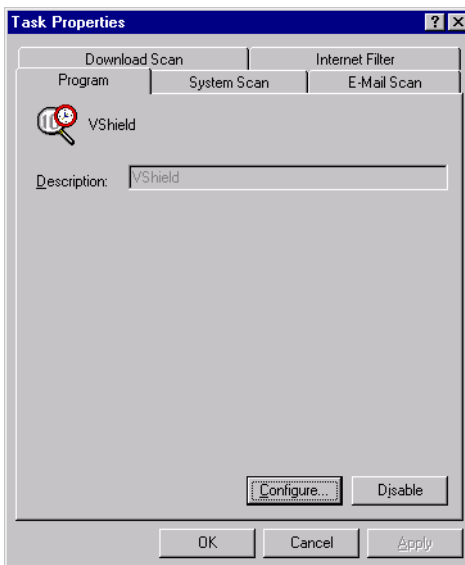


Figure 6-3. VShield scanner Task Properties dialog box

In this dialog box, you can:

- **Enable or disable the task.** Click the **Disable** button at the bottom of the Task Properties dialog box. If the scanner is inactive, this button will read **Enable**.
- **Open the VShield configuration property pages.** Click **Configure** to open the System Scan dialog box, where you can choose all of the configuration options available for the VShield scanner. To learn how to configure the scanner, see [“Setting VShield scanner properties” on page 99](#).
- **View statistics for VShield modules.** Each of the other property pages in the Task Properties dialog box shows summary statistics for the last scan session each ran. Click any other tab to see these statistics. To learn how to display a real-time update for these statistics, see [“Tracking VShield software status information” on page 161](#).

Working with the AutoUpgrade and AutoUpdate tasks

The AutoUpgrade task allows you to download and install new program files for your VirusScan software according to a schedule you set. The AutoUpdate task allows you to download and install new virus definition (.DAT) files. You may not rename, delete, or create other copies of these tasks, but you can configure them, protect them with a password, or run them immediately from the Task Properties dialog box.

To work with either task, open the Console window, then follow these steps:

1. Double-click the AutoUpgrade or the AutoUpdate task in the Console window.

The Task Properties dialog box will appear (Figure 6-4).

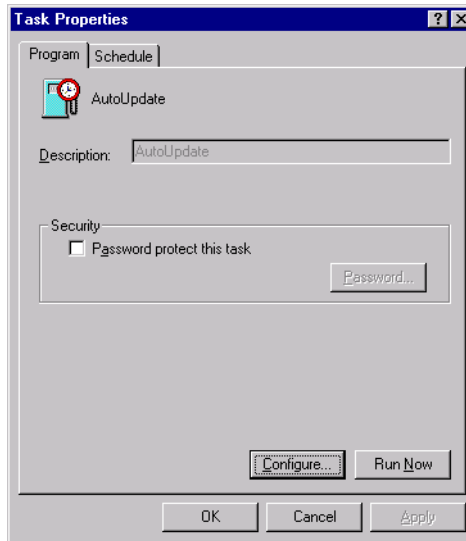


Figure 6-4. AutoUpdate utility Task Properties dialog box

You may not rename either the AutoUpgrade or AutoUpdate this task, so the Description text box will be unavailable.

2. Set a password to protect this task and prevent anyone else from making any changes to your AutoUpdate or AutoUpgrade settings. To do this, follow these substeps:
 - a. Select the **Password protect this task** checkbox, then click **Password** to open the Specify Password dialog box.
 - b. Enter a unique password in the text box provided.


You may enter a maximum of 20 characters of any type. Be sure to choose a password you will remember.

- c. Re-enter your password exactly as you typed it in the previous text box.
- d. Click **OK** to close the Specify Password dialog box.

The Console will ask for the password you entered whenever anybody tries to open the Task Properties dialog box for this task.

3. Next, you can:

- **Run this task with its existing configuration options.** Click **Run Now** to start an immediate AutoUpgrade or AutoUpdate operation.
- **Configure the AutoUpgrade or AutoUpdate task.** Click **Configure** to open either the Automatic Upgrade or the AutoUpdate dialog box. To learn how to configure the AutoUpgrade utility, see [“Configuring the AutoUpgrade utility” on page 243](#). To learn how to configure the AutoUpdate task, see [“Understanding the AutoUpdate utility” on page 232](#).
- Click **Apply** to save your changes without closing the Task Properties dialog box, then click the Schedule tab. To learn how to set a task schedule, see [“Enabling tasks” on page 206](#).
- Click **OK** to save your changes and return to the VirusScan Console window. You will need to set a task schedule later to get it to run.

To do so, select the task from the list in the Console window, then click  to open the Task Properties dialog box.

- Click **Cancel** to close the dialog box without creating a task.


Creating new tasks

Although the tasks that come in the default set can provide your system with nearly comprehensive anti-virus protection, you will probably want to create and run your own tasks after you have some experience with VirusScan software and have a good idea of what and when you want it to scan.

You can modify some aspects of the default tasks that come with the VirusScan Console, but you may not delete, rename or—with the exception of the Scan My Computer and Scan Drive ‘C’ tasks—create new instances of them. You may copy the existing configuration options from the Scan My Computer and Scan Drive ‘C’ tasks for use as foundation settings for your own new tasks.

The Console, however, allows you to create as many as 50 new tasks to suit your own needs. You can raise this limit by changing the number in the VirusScan control panel. To learn how to do so, see [“Understanding the VirusScan control panel”](#) on page 281.

To create a new task, follow these steps:

1. Choose **New Task** from the **Task** menu in the Console window, or click  in the Console toolbar.

The Task Properties dialog box will appear ([Figure 6-5](#)).

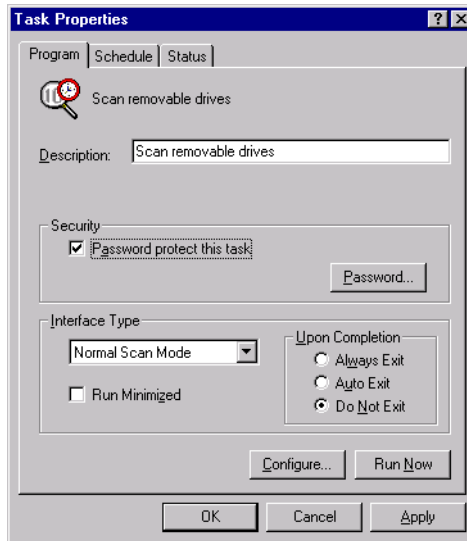


Figure 6-5. Task Properties dialog box - Program page

2. Type a name for the task in the Description text box.
Be sure that your name describes the task so that you can distinguish it from others in the Console window and so that you can tell at a glance what it does.
3. Set a password to protect this task and prevent anyone else from making any changes to your scan task settings. To do this, follow these substeps:
 - a. Select the **Password protect this task** checkbox, then click **Password** to open the Specify Password dialog box.
 - b. Enter a unique password in the text box provided.

You may enter a maximum of 20 characters of any type. Be sure to choose a password you will remember.

- c. Re-enter your password exactly as you typed it in the previous text box.
- d. Select the **Protect all options** checkbox to protect all of the options you set for this task.

Doing so locks all of the property pages for this task at once in the Security page in the VirusScan Properties dialog box. Clearing this checkbox allows you to choose different security settings for each page in the Security property page. To learn how to choose these options, see [“Choosing security options” on page 225](#).

- e. Click **OK** to close the Specify Password dialog box.

The Console will ask for the password you entered whenever anybody tries to open the Task Properties dialog box for this task.

4. Specify how you want the task interface to appear and the degree of control over the task you want to have as it runs. Your choices are:
 - **Normal Scan Mode.** This displays the VirusScan application main window during scan operations. This allows you or the user on whose computer the task runs to see—but not change—the configuration options the task uses as it runs, to see the results of the scan operation, or to stop the operation at any time. You can also choose any of the commands from the main window’s menus.

Select the **Run Minimized** checkbox to start the window out as a minimized button in the Windows taskbar.

- **Scan only mode.** This displays a minimal window that indicates that the task is running. You can stop, pause, or resume the task at any point.

Select the **Run Minimized** checkbox to start the window out as a minimized button in the Windows taskbar.

- **Hidden mode.** This displays no interface as the scan task runs. You cannot pause or stop the task unless you have the VirusScan Console or the Task Properties dialog box active. The VirusScan application will still notify you when it finds a virus, if you have configured any local alerting options for the task. This task always quits the application when the task finishes.

5. Specify what you want the task to do when it finishes. Your choices are:
 - **Always Exit.** Click this button to tell the VirusScan application to always quit immediately after it completes this scan task. If you choose **Hidden Mode** in the Interface Type list, this is your only option.

- **Auto Exit.** Click this button to tell the VirusScan application to quit automatically if it has not detected any viruses during this scan task. If the application does find a virus, it will remain open to display its scan results.

If you run the task in normal scan mode, it will also allow you to dispose of any viruses it detects, if you have not already set the application to dispose of them automatically.

- **Never Exit.** Click this button to specify that you want the VirusScan application to always remain open after it completes this scan task.

If you run the task in normal scan mode, it will display the results of the scan operation and allow you to dispose of any viruses it detected, if you have not already set it to dispose of them automatically. You can then run the task again immediately, if you wish.

6. At this point, you have entered enough information to create your task, but you have not yet chosen program options or scheduled it to run. You can:


- Click **Configure** to set the properties for this task.

This opens the VirusScan Properties dialog box. Here, you can tell the VirusScan application where and what to look for during this scan operation, how to respond to any viruses it finds, how to notify you when it finds a virus, what information to record in its activity log, what items to exclude from scan tasks, and whether to protect the configuration options you set for the task.

To learn how to set these options, see [“Configuring VirusScan application options” on page 210](#).

- Click **Run Now** to run this task immediately. The task will run with default configuration options or the configuration options you've defined for it. Here's what happens when you click the button:
 - If you have configured the task to start automatically, it will run immediately. For this to happen, you must have previously selected the **Start Automatically** checkbox in the VirusScan Properties dialog box. To see this checkbox, click **Configure**, immediately to the left, then locate the checkbox in the What to Scan area in the Detection property page.
 - If you chose a scan task that you have not set to start automatically, the VirusScan application window appears. Click **Scan Now** in this window to run the task.

- Click **Apply** to save your changes without closing the Task Properties dialog box, then click the Schedule tab. To learn how to set a task schedule, see [“Enabling tasks” on page 206](#).
- Click **OK** to save your changes and return to the VirusScan Console window. You will need to set a task schedule later to get it to run.

To do so, select the task from the list in the Console window, then click  to open the Task Properties dialog box.

- Click **Cancel** to close the dialog box without creating a task.


Enabling tasks

Enabling a task means choosing a schedule for it and activating that schedule so that the task runs when you need it. You can schedule any of the tasks shown in the VirusScan Console window, except the VShield task, which runs continuously from the time you start your computer or as soon as you start the task yourself.

In order for your task to run, you must also ensure that the VirusScan Console is active at the time you want your task to run. To learn how to start the Console, see [“Starting the VirusScan Console” on page 194](#).


To run a scan task that uses the VirusScan application, you must configure the scan operation to start automatically. You do not need to do this for the other default tasks. See [Step 5 on page 215](#) for more details.

To enable a task, follow these steps:

1. If you do not already have the Task Properties dialog box open, double-click one of the listed tasks in the Console window, or select a task, then click  in the Console toolbar.

The Task Properties dialog box will appear (see [Figure 6-5 on page 203](#)). If you chose the VShield, AutoUpdate, or AutoUpgrade tasks in the Console task list, the Task Properties dialog box will look different from that shown in [Figure 6-5](#).

2. Click the Schedule tab to display the correct property page (see [Figure 6-6 on page 207](#)).

 **NOTE:** The Task Properties dialog box for the VShield scanner will not include a Schedule property page—instead, it will include status pages for each of the scanner’s modules. The Task Properties dialog boxes for the AutoUpdate and AutoUpgrade tasks, meanwhile, will not include status pages.

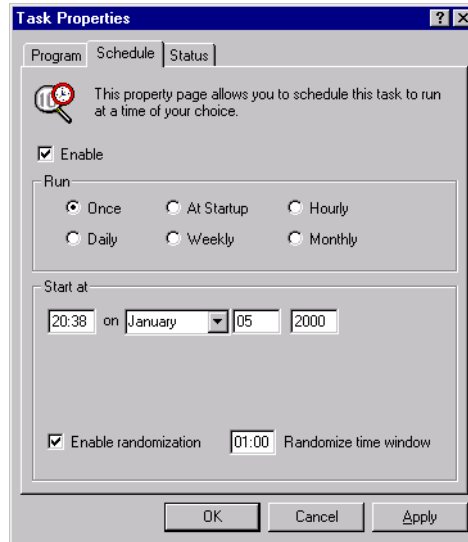


Figure 6-6. Task Properties dialog box - Schedule page

3. Select the **Enable** checkbox. The options in the Run and the Start At areas become active.
4. Choose how often you want the task to run in the Run area. Depending on which interval you select, the Start At area gives you a different set of choices for your task schedule. The choices are:
 - **Once.** This runs your task exactly once on the date and at the time you specify. Enter the time in the leftmost text box in the Start At area, then select a month from the list to the right. Next, enter the date and the year in the text boxes provided.
 - **Daily.** This runs your task once at the time and on the days you specify. Enter a time in the text box provided, then select the checkboxes in the Start At area for each day you want the task to run.
 - **At Startup.** Select this checkbox to run your task once each time you start your computer and the VirusScan Console. Specify in minutes how long after startup you want the Console to wait before it runs your task—you can have the task wait for up to 59 minutes. You may *not* randomize this schedule.

NOTE: Do not schedule both a scan task and an AutoUpdate task to run at startup. The AutoUpdate task will stop any scan task in progress to run its own operation.

- **Weekly.** This runs your task once each week on the day and at the time you specify. Enter the time in the text box provided, then choose a day from the list to the right.
- **Hourly.** This runs the task each hour as long as your computer and the Console are running. Specify in the text box provided how many minutes the Console should wait after each hour to run the task.
- **Monthly.** This runs your task once each month on the day and at the time you specify. Enter the time in the leftmost text box, then enter the day of the month on which you want the task to run.

NOTE: Enter all scheduled times, except for the hourly time interval, using a 24-hour clock. If you want the task to run at 9:30 p.m., for example, enter 21:30.

5. To have this task run within a random interval of the time you set, select the **Enable randomization** checkbox, then enter a time period of up to eight hours in the Randomize Time Window text box.

Unless you've set this task to run at startup, you can use this feature to reduce network traffic and other system overhead that might result from many computers running scan or update operations at the same time. The task will run at a random point within the time "window" you specify.

The window centers on the time you've scheduled for the task to run. If, for example, you set this task to run daily at 15:00, then you selected **Enable randomization** and specified a time window of one hour, the task would run at any point in the period between 14:30 and 15:30. You may set a window of up to 480 minutes, or eight hours.

6. You have now set a schedule for your task and readied it to run at the scheduled time. Click **OK** to close the Task Properties dialog box, or click **Apply** to save your settings without closing the dialog box. Click **Cancel** to close the dialog box without saving your changes.


NOTE: To start your task, your computer must be on and the VirusScan Console must be running. If your computer is off or if the Console is not running at the time your task should start, the task will start at the next scheduled time. You can minimize the Console so that appears only as an icon in the Windows taskbar.

If you plan to have the VirusScan application run a scan task on an unattended computer, you must also configure the program to start its scan operation automatically. See [Step 5 on page 215](#) for details.

Checking task status

The VirusScan Console window summarizes the time and date when your tasks last ran and when you have scheduled them to start again—look for this information to the right of each listed task. You can also see a summary of how many files each task scanned, whether it found any malicious agents, and what actions it took.

To see task results, follow these steps:

1. If you do not already have the Task Properties dialog box open, double-click one of the listed tasks in the Console window, or select a task, then click  in the Console toolbar.
2. The Task Properties dialog box will appear (see [Figure 6-5 on page 203](#)). Click the Status tab to display the correct property page ([Figure 6-7](#)).

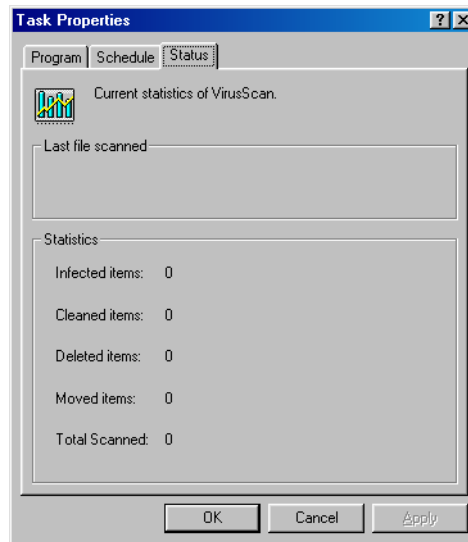


Figure 6-7. Task Properties dialog box - Status page

The status page will list the results of the last scan operation this task conducted, and the name of the last file it scanned. To see a short description of each of the items that appears in this page, right click a figure or label, then choose **What's This?** from the shortcut menu that appears, or click the **?** button in the upper-right corner of the dialog box, then click the item you want described. These displays will *not* update in real time.


-
- ❏ **NOTE:** The Task Properties dialog box for the VShield task will include status pages for all VShield modules. The Task Properties dialog box for AutoUpdate and AutoUpgrade will not include a status page. To learn more about how to find status information for the VShield scanner, see [“Tracking VShield software status information” on page 161](#).
-

Configuring VirusScan application options

To configure a VirusScan scan task that will run at a time you designate, you must tell the application:

- when you want it to run
- what you want it to scan
- what you want it to do if it finds a virus
- how it should let you know when it finds a virus
- whether you want it to keep track of its actions
- which items you don't want it to scan for viruses
- whether you want to protect the settings you chose from unauthorized changes

The VirusScan Console provides a series of property pages you can use to define your task. These property pages replicate many of the options you find in the VirusScan application main window, and add others that help you define a task you want to run regularly and repeatedly.

To configure the VirusScan application to run a scan task, select one of those listed in the Console window—including any task that you created yourself—then click  in the Console toolbar.

The VirusScan Properties dialog box will appear ([Figure 6-8](#)).



Figure 6-8. VirusScan Properties dialog box - Detection page

Choosing Detection options

If you chose to configure a task you just created, the VirusScan application initially assumes that you want to scan your C: drive and your computer's memory, to look for boot sector viruses, and to restrict the files it scans only to those susceptible to virus infection. If you chose to configure one of the default tasks, your initial options will vary.

To modify the initial task options, follow these steps:

1. Choose which parts of your system or your network you want the VirusScan application to examine for viruses. You can:
 - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 6-9).

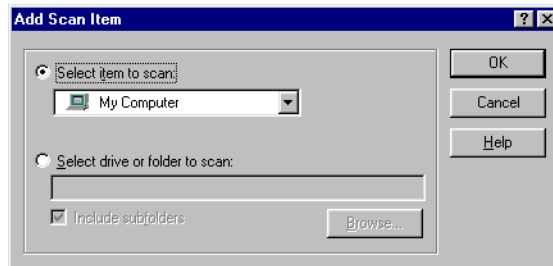


Figure 6-9. Add Scan Item dialog box

To scan your entire computer or a subset of the drives on your system or your network, click the **Select item to scan** button, then:

- a. Choose a scan target from the list provided. Your choices are:
 - **My Computer.** This tells the application to scan all drives physically attached to your computer or logically mapped via Windows Explorer to a drive letter on your computer.
 - **All removable media.** This tells the application to scan only floppy disks, CD-ROM discs, Iomega ZIP disks, or similar storage devices physically attached to your computer.
 - **All fixed disks.** This tells the application to scan hard disks physically connected to your computer.
 - **All network drives.** This tells the application to scan all drives logically mapped via Windows Explorer to a drive letter on your computer.
- b. Click **OK** to close the dialog box.

To scan a particular disk or folder on your system, click the **Select drive or folder to scan button**, then:

- a. Type in the text box provided the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer.

NOTE: You may not use Universal Naming Convention (UNC) notation to specify a network disk as a scan target for scheduled tasks. Doing so will result in an “Invalid Path” error. You may use UNC notation to specify scan targets for operations you run directly with the VirusScan application.

- b. Select the **Include subfolders** checkbox to have the VirusScan application look for viruses in any folders inside your scan target.

NOTE: Choosing **Include subfolders** 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, clear the **Include subfolders** checkbox.

- c. Click **OK** to close the dialog box.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Item to Scan dialog box (Figure 6-10).

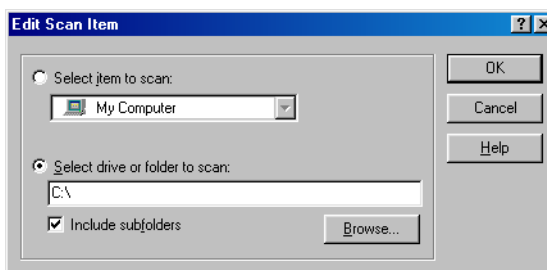


Figure 6-10. Edit Scan Item dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

2. Specify the types of files you want the VirusScan application to examine. You can:

- **Scan compressed files.** Select the **Compressed files** checkbox to have the VirusScan application look for viruses in compressed files and file archives. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

To see a list of the types of files and archives that the application scans, see [“Current list of compressed files scanned” on page 296](#).

- **Scan all files.** Select the **All Files** checkbox to have the application scan all of the files on the target you specified, whatever their extensions.

NOTE: McAfee recommends that you choose this option for your first scan operation, or periodically thereafter, to ensure that your system is virus-free. You can then limit the scope of later scan operations.

- **Choose file types.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection. To do so, click the **Program files only** button.

To see or designate the file name extensions the application will examine, click **Extensions**. This opens the Program File Extensions dialog box. To learn about how to change the files listed there, see [“Adding file name extensions for scanning” on page 291](#).

3. Turn on heuristic scanning. Click **Advanced** to open the Advanced Scan Settings dialog box ([Figure 6-11](#)).

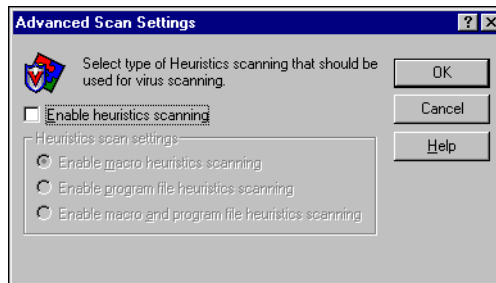


Figure 6-11. Advanced Scan Settings dialog box

Heuristic scanning technology enables the VirusScan application to recognize new viruses based on their resemblance to similar viruses that the module already knows. To do this, the application looks for certain “virus-like” characteristics in the files you’ve asked it to scan. The presence of a sufficient number of these characteristics in a file leads the application to identify the file as potentially infected with a new or previously unidentified virus.

Because the application looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat “potential” infections with the same caution you would confirmed infections.

The VirusScan application starts out without any heuristic scan options active. To activate heuristic scanning, follow these substeps:

- a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.
- b. Select the types of heuristics scanning you want the VirusScan application to use. Your choices are:
 - **Enable macro heuristics scanning.** Choose this option to have the application identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that contain embedded macros, then compare the macro code to its virus definitions database. The application will identify exact matches with the virus name; code signatures that resemble existing viruses cause it to tell you it has found a potential macro virus.
 - **Enable program file heuristics scanning.** Choose this option to have the VirusScan application locate new viruses in program files by examining file characteristics and comparing them against a list of known virus characteristics. The application will identify files with a sufficient number of these characteristics as potential viruses.
 - **Enable macro and program file heuristics scanning.** Choose this option to have the application use both types of heuristics scanning. McAfee recommends that you use this option for complete anti-virus protection.

NOTE: The application will use heuristic scanning techniques only on the file types you designate in the Program File Extensions dialog box. If you choose to scan **All files**, it will use heuristic scanning for all file types.

- c. Click **OK** to save your settings and return to the VirusScan Properties dialog box.

4. Choose special scanning options.

Boot-sector viruses load themselves into your computer's memory and conceal themselves in the boot blocks or master boot record on your hard drive. To use this scan task to detect those types of viruses, select the **Scan Memory** and **Scan boot sectors** checkboxes.

5. If you have scheduled scan operations that you want to run in your absence, select the **Start automatically** checkbox to tell the VirusScan application to begin scanning as soon as it launches.

If you do not select this checkbox, the Console will start VirusScan software, but the VirusScan application will wait for you to click **Scan Now** to start scanning. Leaving the checkbox clear gives you a chance to cancel the scan operation if it will interfere with your work.


6. Click the Action tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Console window, click **OK**. To return to the Console window without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When the VirusScan application detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want VirusScan software to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. To start from the Console window, select the task you created in the task list, then click  in the Console toolbar.
2. The VirusScan Properties dialog box appears (see [Figure 6-8 on page 210](#)). Click the Action tab to display the correct property page (see [Figure 6-12 on page 216](#)).

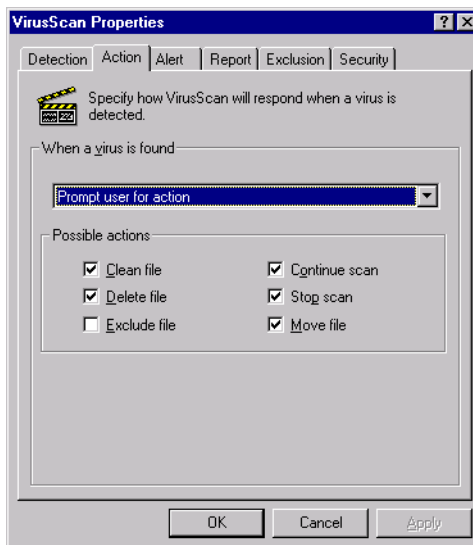


Figure 6-12. VirusScan Properties dialog box - Action page

3. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each response. Your choices are:
 - **Prompt user for action.** Choose this response if you expect to be at your computer when the VirusScan application examines your disk—the program will display an alert message when it finds a virus and offer you a range of possible responses.

Each of the checkboxes you select in the Action page causes an option button to appear in an alert message that the application displays when it finds a virus. Selecting **Delete file**, here, for example, causes a **Delete** button to appear in the alert message. To learn how to respond to these messages, see [“Responding when the VirusScan application detects a virus” on page 72](#).

You can choose from these options:

- **Clean file.** This option tells the application to try to remove the virus code from the infected file. If you have its reporting function enabled, it will record a log event each time it successfully cleans, or fails to clean, an infected file.
- **Delete file.** This option tells the application to delete the infected file immediately.
- **Exclude file.** This option tells the application to skip the file during later scan operations. This is the only option not selected by default.

- **Continue scan.** This option tells the application to continue with its scan operation, but not take any other actions. If you have its reporting options enabled, the application records the incident in its log file.
 - **Stop scan.** This option tells the application to stop the scan operation immediately. To continue, you must click **Scan Now** to restart the operation.
 - **Move file.** This option tells the application to move the infected file to a quarantine folder. The alert message will display a **Move file to** button that you can use to locate a quarantine folder.
- **Move infected files automatically.** Choose this response to have the application move infected files to a quarantine folder.


By default, the application moves these files to a folder named \Infected located in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on your hard disk.
 - **Clean infected files automatically.** Choose this response to tell the application to remove the virus code from the infected file as soon as it finds it. If the application cannot remove the virus, it will note the incident in its log file.
 - **Delete infected files automatically.** Choose this option to have the application delete every infected file it finds immediately. Be sure to enable the reporting feature so that you have a record of which files the application deleted. You will need to restore deleted files from backup copies. If the application cannot delete an infected file, it will note the incident in its log file.
 - **Continue scanning.** Use this option only if you plan to leave your computer unattended while the application checks for viruses. If you also activate the reporting feature, the application will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.
4. Click the Alert tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Console window, click **OK**. To return to the Console window without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let the VirusScan application look for and remove viruses from your system automatically, as it finds them, with almost no further intervention. To have the application tell you immediately when it finds a virus so that you can take appropriate action, however, configure it to send an alert message to you.

Follow these steps:

1. To start from the Console window, select the task you created in the task list, then click  in the Console toolbar.
2. The VirusScan Properties dialog box appears (see [Figure 6-8 on page 210](#)). Click the Alert tab to display the correct property page ([Figure 6-13](#)).

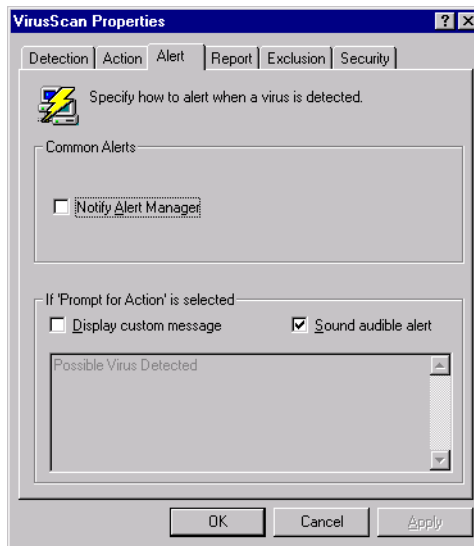


Figure 6-13. VirusScan Properties dialog box - Alert page

3. Select the **Notify Alert Manager** checkbox to have the VirusScan application send alert messages to Alert Manager for distribution.

Alert Manager is a separate McAfee software component that collects alert messages and uses a variety of methods to send them to recipients that you specify. To have the VirusScan application send these alert messages successfully, you must also set up the Alert Manager Client Configuration utility. See [“Using the Alert Manager Client Configuration utility” on page 285](#) for details.

You can pass alert messages directly to an Alert Manager server, or you can send alert messages as text (.ALR) files to a Centralized Alerting directory that the Alert Manager server checks periodically.

NOTE: Clearing this checkbox tells the VirusScan application not to send an alert message via Alert Manager, but does not affect other alert messages that you configure in this property page.

4. Select the **Sound audible alert** checkbox to have the application beep when it finds an infected file.

You can change the setting for this option only if you select **Prompt for user action** in the Action property page. Otherwise, the checkbox will display and use the setting it had when you last chose the **Prompt for user action** item. The application will sound the standard system warning beep or .WAV file you have your computer set to play.

5. Select the **Display custom message** checkbox to have the application add a custom message to the alert box it displays when it finds an infected file.

As with the audible alert, you can change the setting for this option only if you choose **Prompt for user action** in the Action property page. If you do not choose that item in the Action page, no alert box will appear and you will not see a custom message even if you select this checkbox.

6. Enter the message you want the application to display in the text box provided. You can enter a maximum of 250 characters here.
7. Click the Report tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Console window, click **OK**. To return to the Console window without saving your changes, click **Cancel**.


NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

The VirusScan application lists its current settings and summarizes all of the actions it takes during its scan operations in a log file called VSCLOG.TXT. You can have the application write its log to this file, or you can use any text editor to create a text file for the application to use. You can then open and print the log file for later review from within the application or from a text editor.

The VSCLOG.TXT file can serve as an important management tool for you to track virus activity on your system and to note which settings you used to detect and respond to the infections the VirusScan application found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your computer. Use the Reports property page to determine which information VirusScan software will include in its log file.

To decide what data the application will record and how large the log file can get, follow these steps:

1. To start from the Console window, select the task you created in the task list, then click  in the Console toolbar.
2. The VirusScan Properties dialog box appears (see [Figure 6-8 on page 210](#)). Click the Report tab to display the correct property page ([Figure 6-14](#)).

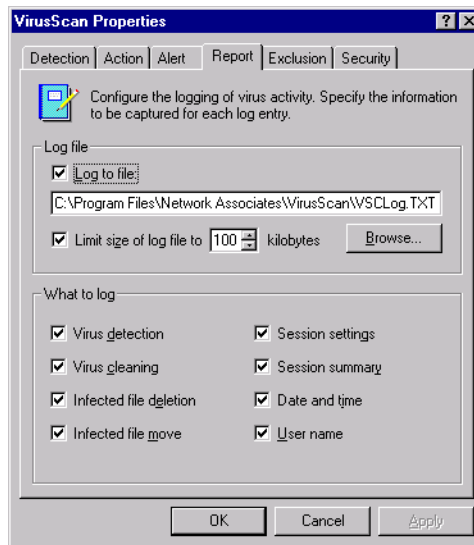


Figure 6-14. VirusScan Properties - Report page

3. Select the **Log to file** checkbox.

By default, the VirusScan application writes log information to the file VSCLOG.TXT in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network. You may use a different file, but the text file must already exist. The application will not create a new file.

4. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided. If you do not select this checkbox, the log file can grow to as large a size as your disk space permits.

Enter a value between 10KB and 999KB. By default, the application limits the file size to 100KB. If the data in the log exceeds the file size you set, the application erases the existing log and begins again from the point at which it left off.

5. Select the checkboxes that correspond to the information you want the application to record in its log file. Each checkbox you select here causes the application to record this information, usually when the scan operation ends, or when you shut your system down:
 - **Virus detection.** Select this checkbox to have the log file record how many viruses the application finds during each scan operation. Clear the checkbox to leave this information out of the log file.
 - **Virus cleaning.** Select this checkbox to have the log file record how many infected files the application cleans—or tries to clean—during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Infected file deletion.** Select this checkbox to have the log file record how many viruses the application deletes during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Infected file move.** Select this checkbox to have the log file record how many viruses the application moves to a quarantine folder during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Session settings.** Select this checkbox to have the log file record the configuration settings you used for the application during each scan operation. Clear this checkbox to leave this information out of the log file.
 - **Session summary.** Select this checkbox to have the log file summarize the actions that the application took during each scan operation. The log will record:
 - How many files the application examined.
 - How many infected files the application cleaned.
 - How many infected files the application deleted.
 - How many infected files the application moved to a quarantine folder.
 - Your application settings.

Clear the checkbox to leave this information out of the log file.

- **Date and time.** Select this checkbox to have the log file record the date and time at which the software starts each scan operation. Clear this checkbox to leave this information out of the log file.
- **User name.** Select this checkbox to have the log file record the name of the user logged into the workstation as the software starts each scan operation. Clear this checkbox to leave this information out of the log file.

To see the contents of the log file from VirusScan Console, select the task you created in the task list, then choose **View Activity Log** from the **Task** menu. You can also start the VirusScan application itself, then choose **View Activity Log** from the **File** menu.

6. Click the Exclusion tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Console window, click **OK**. To return to the Console window without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Exclusion options

Many of the files stored on your computer are not vulnerable to virus infection. Scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling the VirusScan application to look only at susceptible file types (see [“Choosing Detection options” on page 211](#) for details), or you can tell the application to ignore entire files or folders that you know cannot become infected.


Once you scan your system thoroughly, you can exclude the files and folders that do not change or that are not normally vulnerable to virus infection. You can also rely on the VShield scanner to provide you with protection between scheduled scan operations. Regular scan operations that examine all areas of your computer, however, provide you with the best virus defense.

To prevent the application from scanning files that do not get infected, you can identify which disks, folders, or individual files you want to exclude from scan operations in an exclusion list. By default, the VirusScan application does not scan the Recycle Bin because Windows will not run items stored there. This item, therefore, will appear in the exclusion list when you first open the window.

Each entry in the exclusion list displays the path to the item, notes whether the application will also exclude any nested folders within the target, and explains whether the application will exclude the item when it scans files, when it scans your hard disk boot sector, or both.

By default, you can exclude up to 100 unique scan targets. To change this number, open the VirusScan control panel, click the Components tab, then enter a new figure in the **Maximum number of exclude items** text box. To learn more about how to use the VirusScan control panel, see [“Understanding the VirusScan control panel” on page 281](#).

To exclude files or folders from scan operations, follow these steps:

1. To start from the Console window, select the task you created in the task list, then click  in the Console toolbar.
2. The VirusScan Properties dialog box appears (see [Figure 6-8 on page 210](#)). Click the Exclusion tab to display the correct property page. ([Figure 6-15](#)).

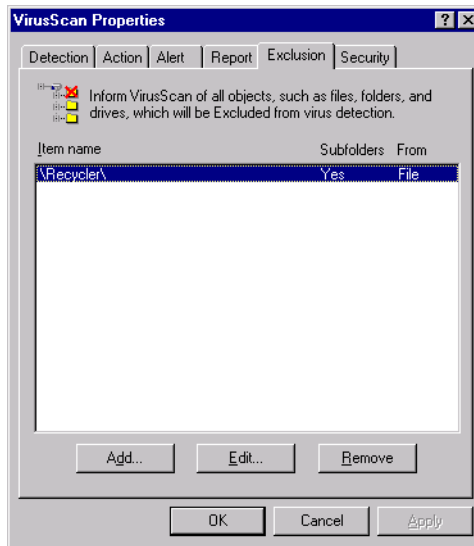


Figure 6-15. VirusScan Properties dialog box - Exclusion page

3. Specify the items you want to exclude. You can
 - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclude Item dialog box ([Figure 6-16](#)).

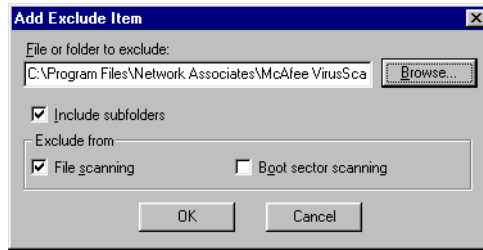


Figure 6-16. Add Exclude Item dialog box

Next, follow these substeps to add items to the list:

- a. Enter a path to a folder or a file name in the text box provided, or click **Browse** to locate the item you want the application to exclude.

NOTE: If you have chosen to move infected files to a quarantine folder automatically, the application excludes that folder from scan operations.

- b. Select the **Include subfolders** checkbox to tell the application to ignore files stored in any subfolders within the folder you specified in [Step a](#).

NOTE: Choosing **Include subfolders** causes the application to ignore only those files stored in the subfolders themselves. The application will still scan files stored at the root level of the folder you designate. To exclude the files at the folder root level, clear the **Include subfolders** checkbox.

- c. Select the **File scanning** checkbox to exclude the item you specified in the first step from scan operations in which the application looks for file-infecting viruses. These viruses usually appear in files in the visible portions of your hard disk.
- d. Select the **Boot sector scanning** checkbox to exclude the item you specified in the first step from scan operations in which the application looks for boot-sector viruses.

These viruses usually appear in memory or in files that reside in your hard disk's boot sector or master boot record. Use this option to exclude system files, such as COMMAND.COM, from scan operations.

 **WARNING:** McAfee recommends that you do *not* exclude your system files from scan operations.

- e. Repeat [Step a.](#) through [Step d.](#) until you have listed all of the files and folders you do not want scanned.
 - **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclude Item dialog box. Make the changes you need, then click **OK** to close the dialog box.
 - **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. This means that the VirusScan application *will* scan this file or folder during its next scan operation.
4. Click the Security tab to choose additional VirusScan options. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Console window, click **OK**. To return to the Console window without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.


Choosing security options

VirusScan software lets you set a password to protect the settings you choose in each property page from unauthorized changes. This feature is particularly useful for system administrators who need to keep users from tampering with their security measures by changing VirusScan settings. Use the Security property page to lock your settings.

You can also protect all of the settings for this task at once, without choosing individual pages. To do so, select the task in the Console window, then choose **Password Protect Task** from the **Task** menu.

You can also double-click the task to open the Task Properties dialog box. There, you can select the **Password protect this task** checkbox, then click **Password** to assign a password. Enter the password you want to use, then select the **Protect all options checkbox** to protect all VirusScan application property pages at once.

To protect individual task settings, follow these steps:

1. To start from the Console window, select the task you created in the task list, then click  in the Console toolbar.
2. The VirusScan Properties dialog box appears (see [Figure 6-8 on page 210](#)). Click the Security tab to display the correct property page. (see [Figure 6-17 on page 226](#)).

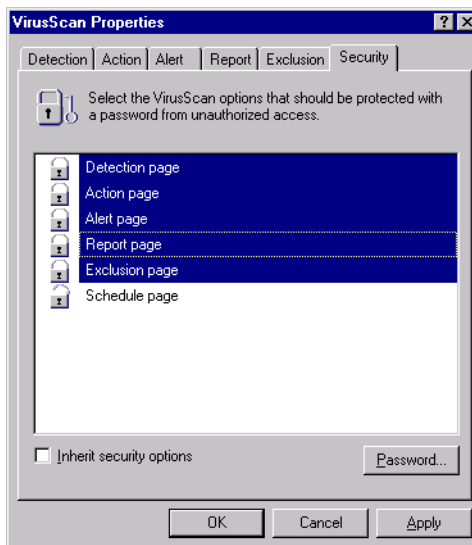




Figure 6-17. VirusScan Properties dialog box - Security page

3. Select the settings you want to protect in the list shown.

You may protect any or all VirusScan property pages. Protected property pages display a locked padlock icon  in the security list shown in [Figure 6-17](#). To remove protection from a property page, click the locked padlock icon to unlock it .

4. Click **Password** to open the Specify Password dialog box ([Figure 6-18](#)).

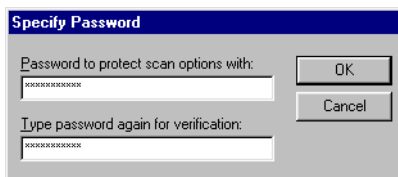


Figure 6-18. Specify Password dialog box

- a. Enter a password in the first text box shown, then enter the same password again in the text box below to confirm your choice.
 - b. Click **OK** to close the Specify Password dialog box.
5. To ensure that your security settings will appear by default in any task you create by copying this task (see [“Using the Console window” on page 196](#) for details), select the **Inherit security options** checkbox.

6. Click a different tab to change any of your VirusScan settings. To save your changes without closing the VirusScan Properties dialog box, click **Apply**. To save your changes and return to the Console window, click **OK**. To return to the Console window without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

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 D, “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 C, “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 232](#) and [“Understanding the AutoUpgrade utility” on page 242](#).
- **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 D, “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 252.](#)

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 254.](#)

- **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.mcafeeb2b.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 49](#). To learn how to use the Emergency Disk to scan your system, see [“If you suspect you have a virus...” on page 61](#).

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 C, “Using the SecureCast Service to Get New Data Files”](#) or visit the McAfee website at:

http://www.mcafeeb2b.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 206](#).

- 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 201](#)).

To learn how to set a password for this task, see [“Working with the AutoUpgrade and AutoUpdate tasks” on page 201](#). To learn how to set a schedule for the task, see [“Enabling tasks” on page 206](#).

2. Click **Configure**.

The Automatic Update dialog box appears with the Update Sites property page selected (see [Figure 7-1 on page 234](#)).

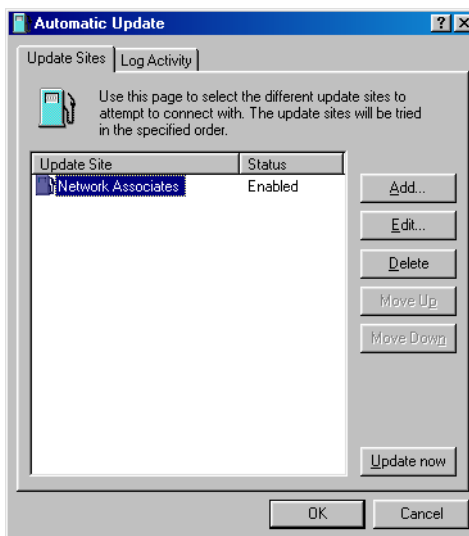


Figure 7-1. Automatic Update dialog box - Update Sites page

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 7-2 on page 235). To learn how to specify options for your new site, see “Configuring update options” on page 237.

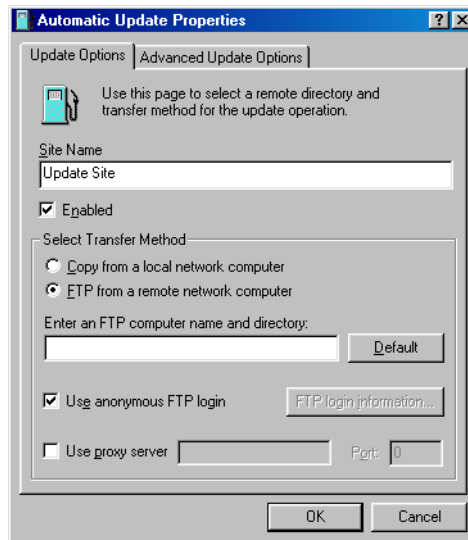


Figure 7-2. Automatic Update Properties dialog box - Update Options page

- 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 7-2). 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 237.
- 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 237](#) 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 239](#) for more details.

4. Click the Log Activity tab to display the next property page ([Figure 7-3](#)).

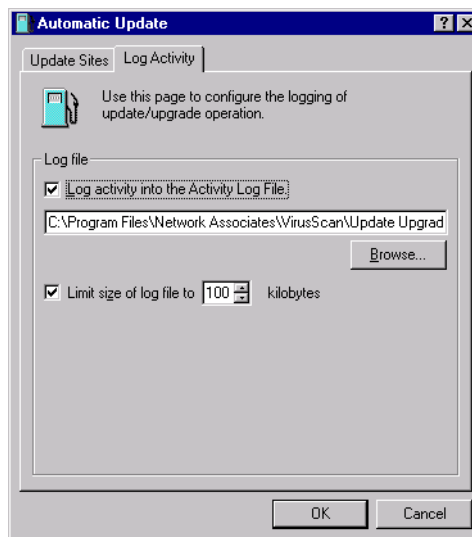



Figure 7-3. Automatic Update dialog box - Log Activity page

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.

- 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.

- 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 7-1 on page 234](#)), or select a listed site, then click **Edit**. Either action will open the Automatic Update Properties dialog box ([Figure 7-4](#)).

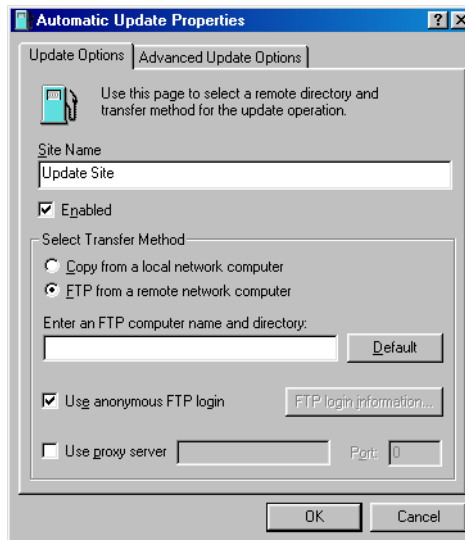


Figure 7-4. Automatic Update Properties dialog box - Update Options page

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 7-5 on page 240](#).

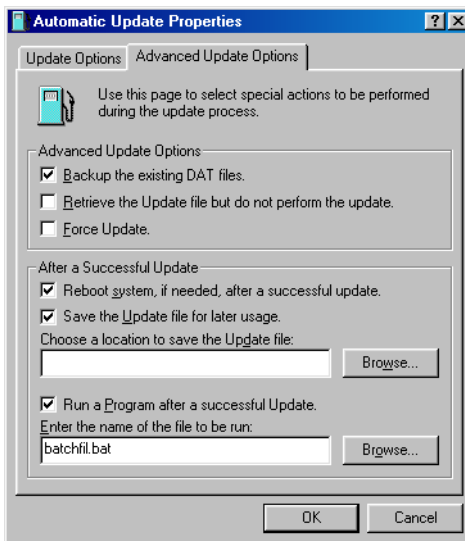


Figure 7-5. Automatic Update Properties dialog box - Advanced Update Options page

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 252](#).

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 C, “Using the SecureCast Service to Get New Data Files”](#) or visit the Network Associates website at:

http://www.mcafeeb2b.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 206](#).

- 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 7-6).

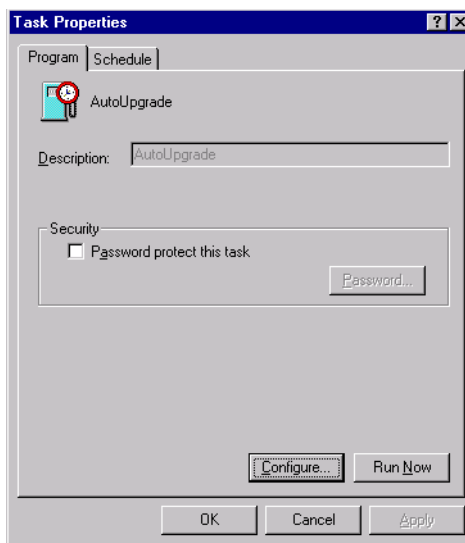


Figure 7-6. AutoUpgrade Task Properties dialog box

To learn how to set a password for this task, see [“Working with the AutoUpgrade and AutoUpdate tasks”](#) on page 201. To learn how to set a schedule for the task, see [“Enabling tasks”](#) on page 206.

2. Click **Configure**.

The Automatic Upgrade dialog box appears with the Upgrade Sites property page selected (see [Figure 7-7](#) on page 245).

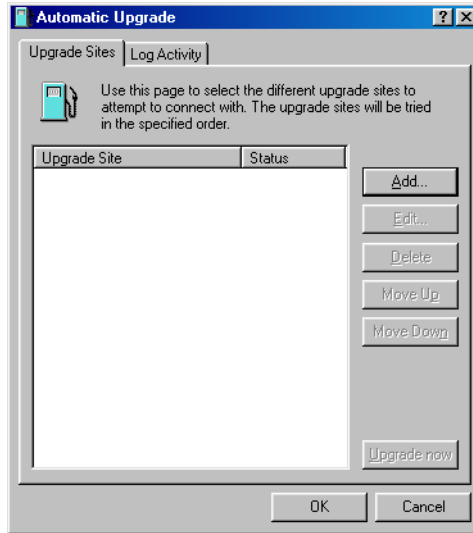


Figure 7-7. Automatic Upgrade dialog box - Upgrade Sites page

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 7-2 on page 235). To learn how to specify options for your new site, see “Configuring upgrade options” on page 248.

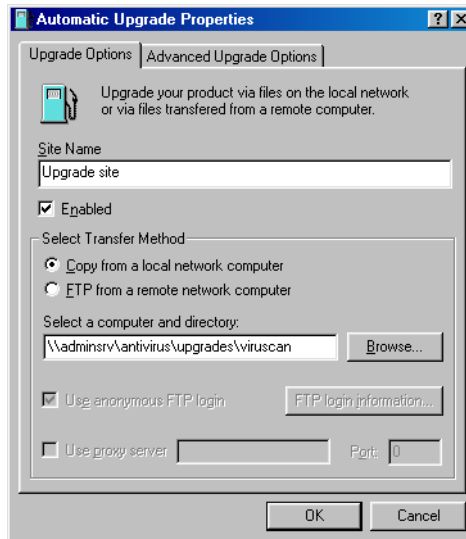


Figure 7-8. Automatic Upgrade Properties dialog box - Upgrade Options page

- 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 7-8). 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 248.
- 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 248 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 7-9](#)).

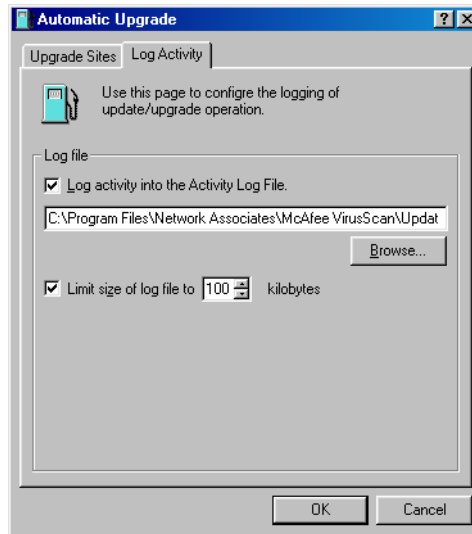



Figure 7-9. Automatic Upgrade dialog box - Log Activity page

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 7-7 on page 245](#)), or select a listed site, then click **Edit**. Either action will open the Automatic Upgrade Properties dialog box ([Figure 7-10](#)).

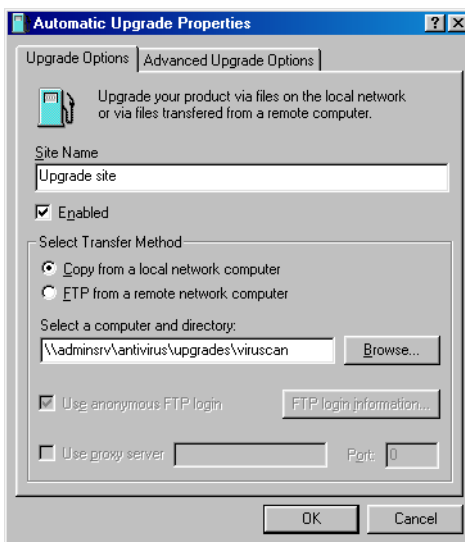


Figure 7-10. Automatic Upgrade Properties dialog box - Upgrade Options page

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 7-5 on page 240](#).

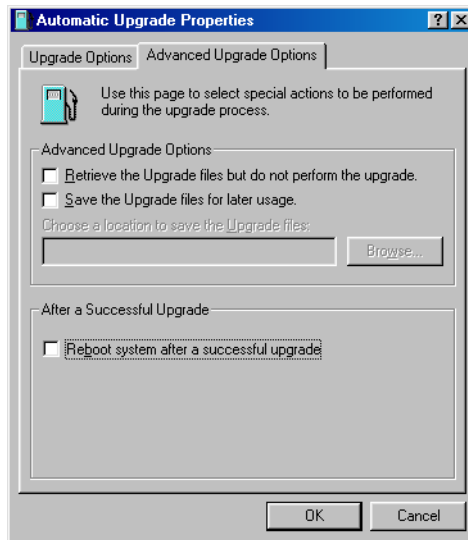


Figure 7-11. Automatic Update Properties dialog box - Advanced Update Options page

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 C, “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

Scanning Microsoft Exchange and Outlook mail

VirusScan software provides you with two complementary methods to protect your Microsoft Exchange or Outlook e-mail system:

- The VShield scanner includes an E-Mail Scan module that runs continuous background scan operations on e-mail as it arrives on your server.
- The E-Mail Scan extension allows you to scan your mailbox on the Exchange server at your own initiative, and at times convenient for you.

An unobtrusive plug-in architecture gives you access to the E-Mail Scan extension from directly within your Exchange or Outlook client application.

When and why you should use the E-Mail Scan extension

Most of the fastest-spreading viruses, worms, and other hostile agents that have emerged in the last few years have proliferated via e-mail. E-mail offers a fast and omnipresent medium that virus writers can use to distribute infected attachments, which they often trick users into opening and activating. Newer viruses, as VBS/BUBBLEBOY demonstrated, might even be able to work without users having to open or read even the e-mail message itself.

The Microsoft Exchange and Outlook e-mail clients are particularly vulnerable to infections of this sort because of their powerful macro and script interpretation capabilities. As with the rest of the Microsoft Office application suite, the Exchange client software makes extensive use of macros, marked-up text, script commands, and similar capabilities that lend themselves to virus attack.

Use the VShield E-Mail Scan module to run background scan operations on your e-mail system and to maintain a constant level of vigilance between the scan operations you run with the E-Mail Scan extension. Under most circumstances, this should protect your system's integrity.

If you have a large backlog of mail on your server that you have not yet scanned, if you log off from your Exchange server, or if you stop the E-Mail Scan module at any point, you should use the E-Mail Scan extension to scan your mailbox to ensure system integrity. Viruses could easily remain in old e-mail messages stored on your server or in e-mail messages that arrive during periods you are logged off from your e-mail system.


Good anti-virus security measures incorporate complete, regular scan operations on your mailbox because:

- **Good security is redundant security.** The VShield E-Mail Scan module looks for virus code as your e-mail arrives on your server, or as executable attachments run after they've downloaded to your system. The E-Mail Scan extension, however, can scan old e-mail stored on the server that the E-Mail Scan module will not see, look for viruses in e-mail that arrives in between times you log in to your Exchange server, or can scan your mailbox if you've temporarily disabled the VShield E-Mail Scan module.
- **Preventative maintenance means safety.** With fast e-mail connections between powerful, web-enabled, scripted client software, it takes only a moment to get infected, sometimes even before you open your mail. Regular scan operations can often catch infections before they spread or do any harm.

Using the E-Mail Scan extension

To use the E-Mail Scan Extension, you must install VirusScan software with a Custom installation and choose the E-Mail Scan component for installation (see “[Installation steps](#)” on page 37 for details). To use the E-Mail Scan extension with its default settings, first start your Microsoft Exchange or Microsoft Outlook client software.




Next, follow these steps:

1. Log on to your mail server as you would normally.
2. Choose **Scan for Viruses** from the **Tools** menu, or click  in the Exchange or Outlook toolbar.

-
- **NOTE:** If you use Microsoft Exchange 5.0, a limitation in the way the program updates its toolbar prevents the E-Mail Scan extension buttons from appearing immediately. To add the Scan for Viruses button to the toolbar, choose **Customize Toolbar** from the **Tools** menu, then add the E-mail Scan extension buttons from the list of available buttons in the Customize Toolbar dialog box.
-

Once you've started it, the E-Mail Scan extension will immediately begin to scan your Exchange or Outlook mailbox for viruses (see [Figure 8-1 on page 259](#)).

By default, the E-Mail Scan extension examines *all* of the mail messages stored in your mailbox on the Exchange mail server, looking for messages and attachments susceptible to virus infection. If you have a large number of messages stored there that you have not yet downloaded, this scan operation can take a long time.

To pause the operation, click . To stop it altogether, click . To resume the operation, click .

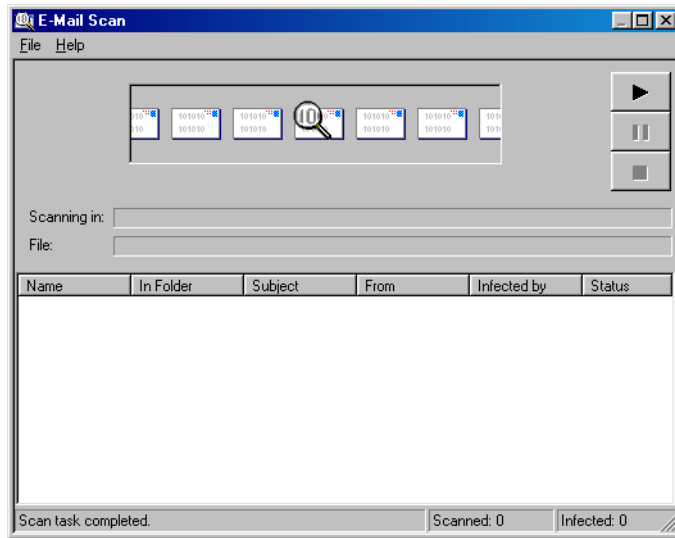


Figure 8-1. E-Mail Scan extension at work

If it finds an infected file, the E-Mail Scan extension will ask you how to respond to the virus. See [“Responding when the E-Mail Scan extension detects a virus”](#) on page 74 for details.

Configuring the E-Mail Scan extension

The E-Mail Scan extension comes set to protect your system in most situations and against most likely hostile agents that arrive via e-mail. You can change the configuration options for the extension so that they better suit your own work environment, however. To change your settings, you must tell the E-Mail Scan extension:

- what you want it to scan
- what you want it to do if it finds a virus
- how it should let you know when it finds a virus
- whether you want it to keep track of its actions

A series of property pages in the E-Mail Scan Properties dialog box controls the options for each scan operation you run. You can click each tab in turn to choose options for the extension to use to scan your e-mail.

To display this dialog box, follow these steps:

1. Start your Microsoft Exchange or Outlook client and log in to your e-mail server.

NOTE: If you have already logged into the network domain that hosts your e-mail server, you might not need to log into to your e-mail server directly-instead, you can simply start Exchange or Outlook. See your network administrator to learn the login requirements for your server.

2. Choose **E-Mail Scan Properties** from the **Tools** menu, or click  in the client application toolbar.

The E-Mail Scan Properties dialog box will appear (Figure 8-2).

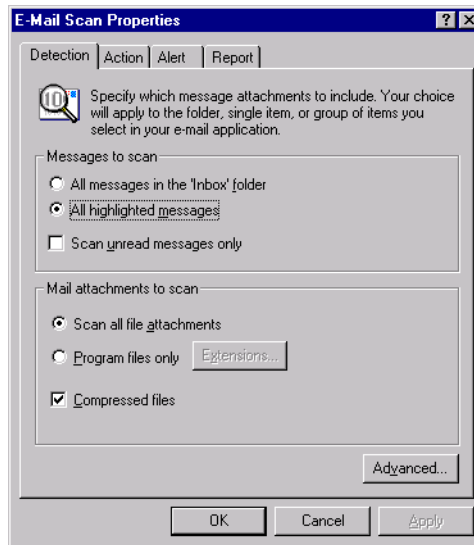


Figure 8-2. E-Mail Scan Properties dialog box - Detection page

Choosing Detection options

When you first open the E-Mail Scan Properties dialog box to configure a scan operation, the E-Mail Scan extension assumes that you want it to scan all of the messages in your Inbox, to scan all message file attachments, to scan compressed files, and to scan only those files susceptible to virus infection.

The E-Mail Scan extension does in fact scan the e-mail messages themselves, as Microsoft Exchange files can carry embedded macros, Hyper Text Markup Language (HTML) tags, and VBScript applets, all of which can in turn harbor specialized viruses, worms, or Trojan horse programs.

-
- NOTE:** The E-Mail Scan extension connects directly to your mailbox on your Microsoft Exchange mail server to run its scan operations. You can also scan any public folders to which you have access, but the extension does not scan messages stored in Microsoft Outlook personal folders (.PST files) or archived items. Other VirusScan components, however, will scan .PST files during their own regular scan operations unless you specifically exclude them.
-

To change these settings, follow these steps:

1. Choose which e-mail messages you want the E-Mail Scan extension to examine for viruses. You can scan:
 - **All messages in the 'Inbox' folder.** Click this button to have the extension look for viruses in all e-mail messages stored in your Microsoft Exchange or Microsoft Outlook Inbox, whether you have read them or not.

If you have a large volume of messages stored in your Inbox, such a scan operation can take considerable time. If, however, you installed the E-Mail Scan extension after you have installed and used your mail system for some time, McAfee recommends that you perform at least one such scan operation to ensure that your older mail messages do not contain viruses.

-
- NOTE:** Once you download mail to your computer, VirusScan software treats your personal folder or archive file as it would any other file, unless you specifically exclude it from scan operations. This gives you an added layer of anti-virus security.
-

- **All highlighted messages.** Click this button to have the extension look for viruses in only those e-mail messages you select from those stored in your Microsoft Exchange or Microsoft Outlook Inbox.

2. To restrict this scan operation so that it examines only unread messages, select the **Scan unread messages only** checkbox. Depending on which option you select in [Step 1](#), this means that the extension will scan all unread messages in your mailbox or in accessible public folders, or all unread messages within the range you've selected.
3. Specify the file types you want the extension to examine. You can:

- **Scan compressed files.** Select the **Compressed files** checkbox to have the E-Mail Scan extension look for viruses in compressed files and file archives. Although it does give you better protection, scanning compressed files can lengthen a scan operation.

The extension scans the same types of compressed files and archives that the VirusScan application does. To see a list of those files and archives, see [“Current list of compressed files scanned” on page 296](#).

- **Scan all files.** Select the **All Files** checkbox to have the E-Mail Scan extension scan all file types in your mailbox, whatever their file name extensions.

NOTE: McAfee recommends that you choose this option for your first scan operation, or periodically thereafter, to ensure that your mailbox is virus-free. You can then limit the scope of later scan operations.

- **Choose file types.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection. To do so, click the **Program files only** button.

To see or designate the file types that the E-Mail Scan extension will examine, click **Extensions**. This opens the Program File Extensions dialog box. To learn about how to change the files listed there, see [“Adding file name extensions for scanning” on page 291](#).

4. Turn on heuristic scanning. Click **Advanced** to open the Advanced Scan Settings dialog box ([Figure 8-3](#)).

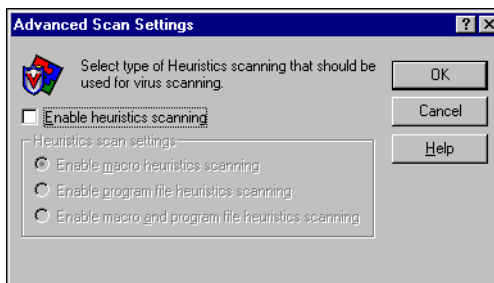


Figure 8-3. Advanced Scan Settings dialog box

Heuristic scanning technology enables the E-Mail Scan extension to recognize new viruses based on their resemblance to similar viruses that the module already knows. To do this, the extension looks for certain “virus-like” characteristics in the files you’ve asked it to scan. The presence of a sufficient number of these characteristics in a file leads the extension to identify the file as potentially infected with a new or previously unidentified virus.

Because the extension looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat “potential” infections with the same caution you would confirmed infections.

The E-Mail Scan extension starts out without any heuristic scan options active. To activate heuristic scanning, follow these substeps:

- a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.
- b. Select the types of heuristics scanning you want the E-Mail Scan extension to use. Your choices are:
 - **Enable macro heuristics scanning.** Choose this option to have the extension identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that contain embedded macros, then compare the macro code to its virus definitions database. The extension will identify exact matches with the virus name; code signatures that resemble existing viruses cause it to tell you it has found a potential macro virus.
 - **Enable program file heuristics scanning.** Choose this option to have the E-Mail Scan extension locate new viruses in program files by examining file characteristics and comparing them against a list of known virus characteristics. The extension will identify files with a sufficient number of these characteristics as potential viruses.
 - **Enable macro and program file heuristics scanning.** Choose this option to have the extension use both types of heuristics scanning. McAfee recommends that you use this option for complete anti-virus protection.

NOTE: The extension will use heuristic scanning techniques only on the file types you designate in the Program File Extensions dialog box. If you choose to scan **All files**, it will use heuristic scanning for all file types.

- c. Click **OK** to save your settings and return to the E-Mail Scan Properties dialog box.

5. Click the Action tab to choose additional E-Mail Scan extension options. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Action options

When the E-Mail Scan extension detects a virus, it can respond either by asking you what it should do with the infected file, or by automatically taking an action that you determine ahead of time. Use the Action property page to specify which response options you want the extension to give you when it finds a virus, or which actions you want it to take on its own.

Follow these steps:

1. Click the Action tab in the E-Mail Scan Properties dialog box to display the correct property page (Figure 8-4).

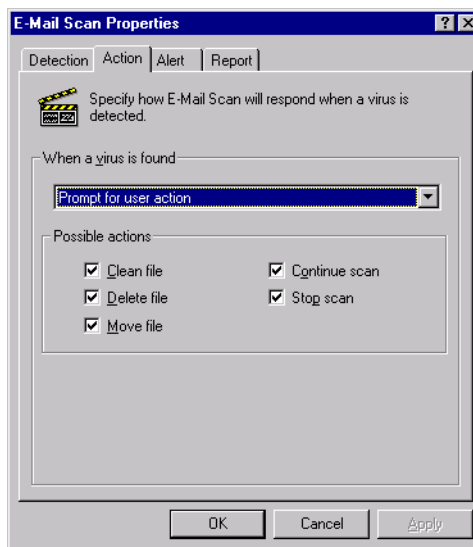


Figure 8-4. E-Mail Scan Properties dialog box - Action page


2. Choose a response from the **When a virus is found** list. The area immediately beneath the list will change to show you additional options for each response.

Your choices are:


- **Prompt for user action.** Choose this response if you expect to be at your computer when the E-Mail Scan extension examines your mailbox—the program will display an alert message when it finds a virus and offer you a range of possible responses.

Each of the checkboxes you select in the Action page causes an option button to appear in an alert message that the extension displays when it finds a virus. Selecting **Delete file**, here, for example, causes a **Delete** button to appear in the alert message.


You can choose from these options:

- **Clean file.** This option tells the extension to try to remove the virus code from the infected file. If you have its reporting function enabled, it will record a log event each time it successfully cleans, or fails to clean, an infected file.
 - **Delete file.** This option tells the extension to delete the infected file immediately.
 - **Move file.** This option tells the extension to move the infected file to a quarantine folder. The alert message will display a **Move file to** button that allows you to send the infected item to a quarantine folder on your Microsoft Exchange server. You can move infected items to any other folder you've created in your Exchange or Outlook mailbox, or to any public folder on the Exchange server to which you have access. The item will remain on the Exchange server until you dispose of it—it will not get downloaded to your computer.
 - **Continue scan.** This option tells the extension to continue with its scan operation, but not take any other actions. If you have its reporting options enabled, the extension records the incident in its log file.
 - **Stop scan.** This option tells the extension to stop the scan operation immediately. To continue, you must click  in the Exchange or Outlook toolbar again, or you must choose **Scan for Viruses** from the **Tools** menu to restart the operation.
- **Move infected files automatically.** Choose this response to have the extension move infected files to a quarantine folder on your Microsoft Exchange server as soon as it finds them. The extension moves these files to a folder named **Infected**, which is located on your Microsoft Exchange server.

- **Clean infected files automatically.** Choose this response to tell the extension to remove the virus code from the infected attachment as soon as it finds it. If the extension cannot remove the virus, it will note the incident in its log file.
- **Delete infected files automatically.** Choose this option to have the extension delete every infected e-mail attachment it finds immediately. Be sure to enable the reporting feature so that you have a record of which files the extension deleted. If the extension cannot delete an infected file, it will note the incident in its log file.
- **Continue scanning.** Use this option only if you plan to leave your computer unattended while the application checks for viruses. If you also activate the reporting feature, the application will record the names of any viruses it finds and the names of infected files so that you can delete them at your next opportunity.

 **WARNING:** The E-mail Scan extension will *not* try to break any encrypted messages to scan them. If an infected attachment includes a digital signature, the extension will *remove* the digital signature in order to clean or delete the infected file.

3. Click the Alert tab to choose additional E-Mail Scan extension options. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

 **NOTE:** Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Alert options

Once you configure it with the response options you want, you can let the E-Mail Scan extension look for and remove viruses from your Exchange mailbox automatically, as it finds them, with almost no further intervention. To have the extension tell you immediately when it finds a virus so that you can take appropriate action, however, configure it to send an alert message to you.

Follow these steps:

1. Click the Alert tab in the E-Mail Scan Properties dialog box to display the correct property page (Figure 8-5).

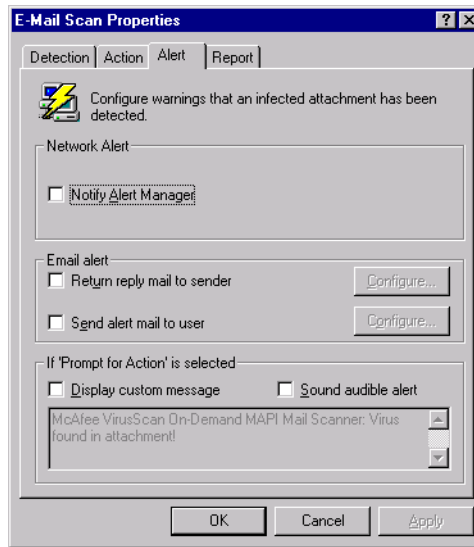


Figure 8-5. E-Mail Scan Properties dialog box - Alert page

2. Select the **Notify Alert Manager** checkbox to have the E-Mail Scan extension send alert messages to Alert Manager for distribution.

Alert Manager is a separate McAfee software component that collects alert messages and uses a variety of methods to send them to recipients that you specify. To have the extension send these alert messages successfully, you must also set up the Alert Manager Client Configuration utility. See [“Using the Alert Manager Client Configuration utility” on page 285](#) for details.

You can pass alert messages directly to an Alert Manager server, or you can send alert messages as text (.ALR) files to a Centralized Alerting directory that the Alert Manager server checks periodically.

-
- NOTE:** Clearing this checkbox tells the E-Mail Scan extension not to send an alert message via Alert Manager, but does not affect other alert messages that you configure in this property page.
-

As part of your anti-virus warning system, the E-Mail Scan extension can reply directly with an alert message to anybody who sends you an infected message or attachment. You can copy that message to any other recipient in your organization, or any number of other recipients.

If you prefer not to send a reply, you can simply have the extension send an e-mail notification, perhaps to a system administrator, whenever it detects a virus.

Sending reply messages can aid your ability to track virus sources and pinpoint where infectious agents enter your network; copies of these messages sent to system administrators can help them track how infections spread.

You can also choose to send a messages to any recipient without replying to the source of the infected attachment. The E-Mail Scan extension can draw recipients directly from your Microsoft Exchange, Microsoft Outlook, or other MAPI-compliant address book, or from an equivalent Lotus cc:Mail directory. You can also enter recipient addresses directly.

The message you create for a response is a template—the E-Mail Scan extension will send the message you compose automatically to each recipient you designate, so McAfee recommends that you enter a message that all recipients can read and understand. Apart from the steps you take to compose this template message, the extension will not give you an opportunity to edit the message before it sends it.

You may send one message to reply to the source of the infected message and a different message to other recipients, but you cannot tailor the same message for different recipients.

3. To compose your template messages, follow these substeps:

- a. Select the **Return reply mail to sender** checkbox in the Alert property page, then click **Configure** to open a standard mail message form.

Because the E-Mail Scan extension will send this message directly back to the source of the infected e-mail message, the **To:** button and text box are unavailable.

- b. To send a copy of this message to someone else, enter an e-mail address in the text box labeled Cc; or click **Cc:** to choose a recipient from your mail system's user directory or address book.

NOTE: To find an e-mail address in your mail system's user directory, you must store address information in a MAPI-compliant user directory, database, or address book, or in an equivalent Lotus cc:Mail directory. If you have not yet logged onto your e-mail system, the E-Mail Scan extension tries to use your default MAPI profile to log onto MAPI-compliant mail systems, or asks you to supply a user name, password and path to your Lotus cc:Mail mailbox. Enter the information the extension requires, then click **OK** to continue.

- c. Enter a subject for the message that conveys its urgency, then add any comments you want to make in the body of the message, below a standard infection notice that the extension itself will supply. You may add up to 1024 characters of text.
- d. Click **OK** to save the message.

Whenever it detects a virus, the extension will send a copy of this message to each person who sends you e-mail with an infected attachment. It fills in the recipient's address with information found in the original message header, and identifies the virus and the affected file in the area immediately below the subject line. If you have activated its report feature, the extension also logs each instance when it sends an alert message.

- e. To send an e-mail message to warn others—a network administrator, for example—about an infected attachment, select the **Send alert mail to user** checkbox in the Alert property page. You can then compose a standard reply in the same way you did in [Step a](#) through [Step d](#) above. In this case, however, you can fill out both the To: and the Cc: text boxes.

Whenever it detects a virus, the E-Mail Scan extension sends a copy of this message to all of the addresses that you entered for this message.

4. Select the **Sound audible alert** checkbox to have the extension beep when it finds an infected file.

You can change the setting for this option only if you select **Prompt for user action** in the Action property page. Otherwise, the checkbox will display and use the setting it had when you last chose the **Prompt for user action** item.

The extension will sound the standard system warning beep or .WAV file you have your computer set to play.

5. Select the **Display custom message** checkbox to have the extension add a custom message to the alert box it displays when it finds an infected file.

As with the audible alert, you can change the setting for this option only if you choose **Prompt for user action** in the Action property page. If you do not choose that item in the Action page, no alert box will appear and you will not see a custom message even if you select this checkbox.

6. Enter the message you want the extension to display in the text box provided. You can enter a maximum of 250 characters here.

7. Click the Report tab to choose additional E-Mail Scan extension options. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Choosing Report options

E-Mail Scan lists its current settings and summarizes all of the actions it takes during its scanning operations in a log file called MAILSCAN.TXT. You can have E-Mail Scan write its log to this file, or you can use any text editor to create a text file for E-Mail Scan to use. You can then open and print the log file for later review from within E-Mail Scan or from a text editor.

You can use the MAILSCAN.TXT file to track virus activity on your system and to note which settings the extension used to detect and respond to infections it found. You can also use the incident reports recorded in the file to determine which files you need to examine in quarantine, or delete from your computer.

To set E-Mail Scan to record its actions in a log file, follow these steps:

1. Click the Report tab in the E-Mail Scan Properties dialog box to display the correct property page (Figure 8-6).

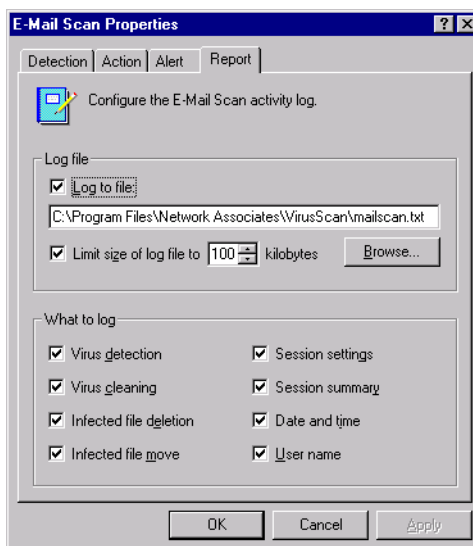


Figure 8-6. E-Mail Scan Properties dialog box - Report page

2. Select the **Log to file** checkbox.

By default, the E-Mail Scan extension writes log information to the file MAILSCAN.TXT in the VirusScan program directory. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your hard disk or on your network. You may use a different file, but the text file must already exist. The extension will not create a new file.

-
- NOTE:** If you choose a different location for your log file on a Windows NT Workstation v4.0 or Windows 2000 Professional system, verify that you choose a location to which you have user-level access. Because the E-Mail Scan extension runs with the same access rights that your e-mail client program does, it cannot write to this log file correctly if the file exists in a location that requires Administrator access rights, and you have logged in as a user to run your e-mail client program. Instead, the E-Mail Scan extension will give you an “Activity Log Access Error” message when it detects a virus.
-

3. To minimize the log file size, select the **Limit size of log file to** checkbox, then enter a value for the file size, in kilobytes, in the text box provided. If you do not select this checkbox, the log file can grow to as large a size as your disk space permits.

Enter a value between 10KB and 999KB. By default, the extension limits the file size to 100KB. If the data in the log exceeds the file size you set, the extension erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want the extension to record in its log file. Each checkbox you select here causes the extension to record this information, usually when the scan operation ends, or when you shut your system down:
 - **Virus detection.** Select this checkbox to have the log file record how many viruses the extension finds during each scan operation. Clear the checkbox to leave this information out of the log file.
 - **Virus cleaning.** Select this checkbox to have the log file record how many infected files the extension cleans—or tries to clean—during each scan operation. Clear this checkbox to leave this information out of the log file.

- **Infected file deletion.** Select this checkbox to have the log file record how many viruses the extension deletes during each scan operation. Clear this checkbox to leave this information out of the log file.
- **Infected file move.** Select this checkbox to have the log file record how many viruses the extension moves to a quarantine folder during each scan operation. Clear this checkbox to leave this information out of the log file.
- **Session settings.** Select this checkbox to have the log file record the configuration settings you used for the extension during each scan operation. Clear this checkbox to leave this information out of the log file.
- **Session summary.** Select this checkbox to have the log file summarize the actions that the extension took during each scan operation. The log will record:
 - How many files the extension examined.
 - How many infected files the extension cleaned.
 - How many infected files the extension deleted.
 - How many infected files the extension moved to a quarantine folder.
 - Your extension settings.

Clear the checkbox to leave this information out of the log file.

- **Date and time.** Select this checkbox to have the log file record the date and time at which the extension starts your scan operation. Clear this checkbox to leave this information out of the log file.
 - **User name.** Select this checkbox to have the log file record the name of the user logged into the workstation as the extension starts each scan operation. Clear this checkbox to leave this information out of the log file.
5. Click a different tab to change any of your E-Mail Scan extension settings. To save your changes without closing the E-Mail Scan Properties dialog box, click **Apply**. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

Scanning cc:Mail

VirusScan software includes native support for Microsoft Exchange and Outlook clients, and for Lotus cc:Mail v6.0, v7.0, and v8.0. The cc:Mail clients use a proprietary e-mail system that the E-Mail Scan extension does not support directly. Instead, VirusScan software includes a specialized cc:Mail extensions that plugs into VShield software, logs on to your cc:Mail system, then operates unobtrusively in the background, polling your cc:Mail Inbox to check for new mail. When new mail arrives, the cc:Mail scanner examines it for any infected attachments before your client software downloads it to your computer.

The only real interaction you will have with cc:Mail Scan is when you choose which corporate e-mail system you want the VShield scanner to examine for viruses. To learn how to specify cc:Mail as your corporate e-mail system, see [“Choosing Detection options” on page 118](#).

If you have not yet logged in to your cc:Mail server, the cc:Mail scanner might also ask you to enter your user name and password into a login screen so that it can get access to your cc:Mail server and scan your Inbox. Enter your cc:Mail user name and password, just as if you were logging directly into cc:Mail, then click **OK** to continue. Next, start your cc:Mail client application, then set the interval for the client to poll your cc:Mail server to a period longer than five minutes. This gives VShield software a chance to examine your mail before your client software retrieves it.

The cc:Mail component logs off from your e-mail server when you quit your client software.

Using the ScreenScan utility

The ScreenScan utility scans your system in the background as your screen saver runs. With it, you can turn otherwise idle computer time to productive use by allowing your machine to check itself for virus infections. ScreenScan will not take any action against viruses it detects, but it will record the results of its scan operations in a log file that you can review at your leisure.

-
- ❑ **NOTE:** To use ScreenScan, you must choose the Custom installation option during Setup—the Setup utility does not install this component by default. See [“Installation steps” on page 37](#) for details.
-

Once installed, ScreenScan displays a property page in the Windows Display Properties dialog box. Here you can choose the detection and report options that you want ScreenScan to use.

Provided that you have configured and enabled it, the utility will start whenever your computer's screen saver starts, and it will stop whenever you move your mouse, press a key on your keyboard, or take any other action that interrupts your screen saver.

To configure ScreenScan, follow these steps:

1. Click **Start** in the Windows taskbar, point to **Settings**, then choose **Control Panel**.
2. Locate and double-click the Display control panel in the window that appears in order to open the Display Properties dialog box. Next, click the ScreenScan tab (Figure 8-7).

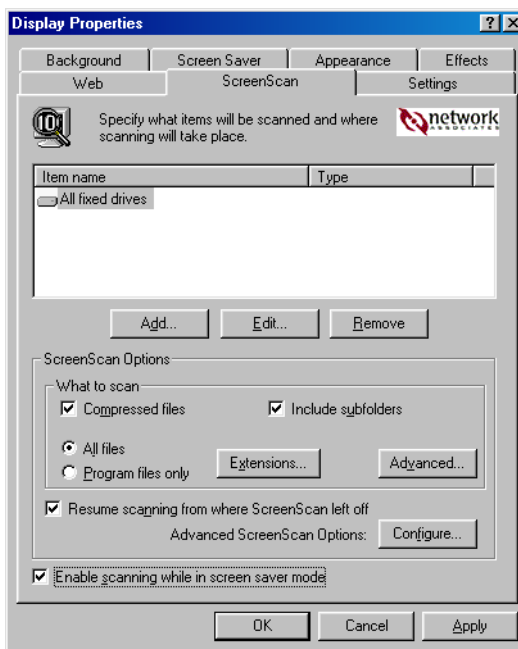


Figure 8-7. Display Properties dialog box - ScreenScan page

3. Select the **Enable scanning while in screen saver mode** checkbox to activate the options in the rest of the property page.
4. Choose which parts of your system you want the ScreenScan utility to examine for viruses. You can
 - **Add scan targets.** Click **Add** to open the Add Scan Item dialog box (see Figure 8-8 on page 275).

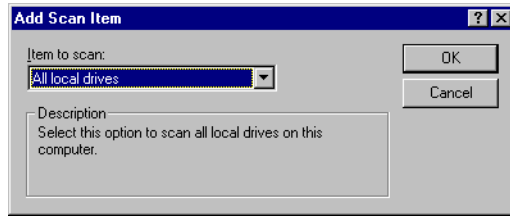


Figure 8-8. The Add Scan Item dialog box

Next, choose the scan target from the list provided. Your choices are:

- **All local drives.** This tells the utility to scan all drives physically attached to your computer, including removable media drives.
- **Drive or folder.** This tells the utility to scan particular files or folders on your system. Type in the text box provided the drive letter or the path to the folder you want scanned, or click **Browse** to locate the scan target on your computer.
- **All fixed drives.** This tells the utility to scan hard disks physically connected to your computer.

When you've chosen your target, click **OK** to close the dialog box.

- **Change scan targets.** Select one of the listed scan targets, then click **Edit** to open the Edit Scan Item dialog box (Figure 8-9).

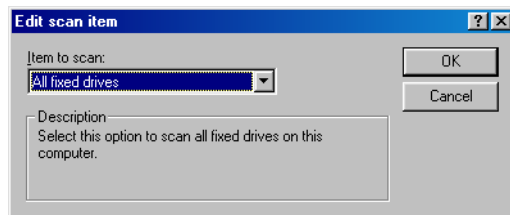


Figure 8-9. The Edit Scan Item dialog box

The dialog box appears with the existing scan target specified. Choose or enter a new scan target, then click **OK** to close the dialog box.

- **Remove scan targets.** Select one of the listed scan targets, then click **Remove** to delete it.

5. Specify the types of files you want the ScreenScan utility to examine. You can

- **Scan compressed files.** Select the **Compressed files** checkbox to have the utility look for viruses in compressed files or file archives. To see a list of the types of files and archives that the application scans, see [“Current list of compressed files scanned” on page 296](#).
- **Scan subfolders within the designated target.** Select the **Include subfolders** checkbox to have the utility look for viruses in any folders inside your scan target.

NOTE: Choosing **Include subfolders** causes the utility to scan only those files stored in the subfolders themselves. The utility will not scan files stored at the root level of the folder you designate. To scan those files, clear the **Include subfolders** checkbox.

- **Scan all files.** Select the **All Files** checkbox to have the utility scan all of the files in the mailbox or public folder you specified, whatever their extensions.

NOTE: McAfee recommends that you choose this option for your first scan operation, or periodically thereafter, to ensure that your system is virus-free. You can then limit the scope of later scan operations.

- **Choose file types.** Viruses cannot infect files that contain no executable code, whether script, macro, or binary code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection. To do so, click the **Program files only** button.

To see or designate the file name extensions the ScreenScan utility will examine, click **Extensions**. This opens the Program File Extensions dialog box. To learn about how to change the files listed there, see [“Adding file name extensions for scanning” on page 291](#).

6. Turn on heuristic scanning. Click **Advanced** to open the Advanced Scan Settings dialog box (see [Figure 8-10 on page 277](#)).

Heuristic scanning technology enables the ScreenScan utility to recognize new viruses based on their resemblance to similar viruses that the module already knows. To do this, the utility looks for certain “virus-like” characteristics in the files you’ve asked it to scan.

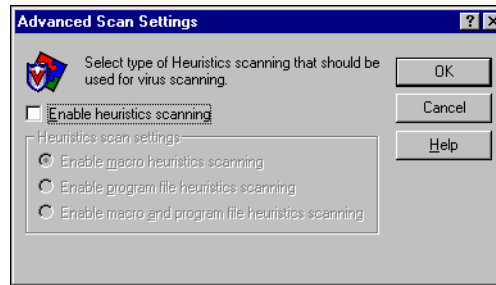


Figure 8-10. Advanced Scan Settings dialog box

The presence of a sufficient number of these characteristics in a file leads the utility to identify the file as potentially infected with a new or previously unidentified virus.

Because the utility looks simultaneously for file characteristics that rule out the possibility of virus infection, it will rarely give you a false indication of a virus infection. Therefore, unless you know that the file does *not* contain a virus, you should treat “potential” infections with the same caution you would confirmed infections.

The ScreenScan utility starts out without any heuristic scan options active. To activate heuristic scanning, follow these substeps:

- a. Select the **Enable heuristics scanning** checkbox. The remaining options in the dialog box activate.
- b. Select the types of heuristics scanning you want the ScreenScan utility to use. Your choices are:
 - **Enable macro heuristics scanning.** Choose this option to have the utility identify all Microsoft Word, Microsoft Excel, and other Microsoft Office files that contain embedded macros, then compare the macro code to its virus definitions database. The utility will identify exact matches with the virus name; code signatures that resemble existing viruses cause it to tell you it has found a potential macro virus.
 - **Enable program file heuristics scanning.** Choose this option to have the ScreenScan utility locate new viruses in program files by examining file characteristics and comparing them against a list of known virus characteristics. The utility will identify files with a sufficient number of these characteristics as potential viruses.

- **Enable macro and program file heuristics scanning.**
Choose this option to have the utility use both types of heuristics scanning. McAfee recommends that you use this option for complete anti-virus protection.

NOTE: The utility will use heuristic scanning techniques only on the file types you designate in the Program File Extensions dialog box. If you choose to scan **All files**, it will use heuristic scanning for all file types.

7. Set the ScreenScan utility to resume any scan operations that got interrupted from the point at which it left off. Select **Resume scanning from where ScreenScan left off**.

If you do not select this checkbox, the utility will begin its scan operation again from the root level of the first drive you specified as a scan target each time your screen saver starts to run. This could mean that the utility will scan some parts of your system repeatedly but will miss other parts completely.

8. Set Advanced ScreenScan options. Click **Configure** to open the Advanced Scanner Settings dialog box (Figure 8-11).

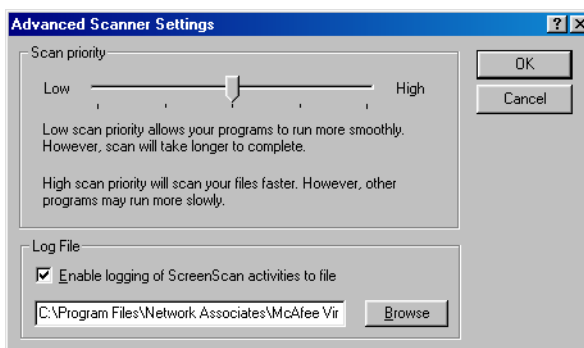


Figure 8-11. Advanced Scanner Settings dialog box

Your choices are:

- **Set an execution priority for ScreenScan tasks.** Slide the scan priority control toward **High** to give a higher priority for system resources and time to the ScreenScan utility than to other background activities, such as disk defragmentation operations, that operate during otherwise idle periods on your computer. This causes the other activities to run more slowly.

Slide the control toward **Low** to give the other background tasks higher priority than you do to the ScreenScan utility. This causes the ScreenScan utility to run more slowly.

- **Tell the utility to log its actions.** Select the **Enable logging of ScreenScan activities to file** checkbox to have the ScreenScan utility summarize the actions it took as it ran in the file SCREENSCAN ACTIVITY LOG.TXT.

The utility will record its actions 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 ScreenScan utility will not generate a text file—it will write only to an existing file.

9. Click **Apply** to save your changes without closing the Display Properties dialog box. To save your changes and close the dialog box, click **OK**. To close the dialog box without saving your changes, click **Cancel**.

NOTE: Clicking **Cancel** will not undo any changes you already saved by clicking **Apply**.

The ScreenScan utility will run the next time your current screen saver does. If you change screen savers, you should reconfigure your ScreenScan utility options also.

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 (see [Figure 9-1 on page 282](#)).

If you have assigned a password to protect your VShield settings, the control panel will ask for that password in order to give you access. Enter the correct password in the text box that appears. To learn more about setting a password to protect the control panel, see “[Enabling password protection](#)” on page 152.

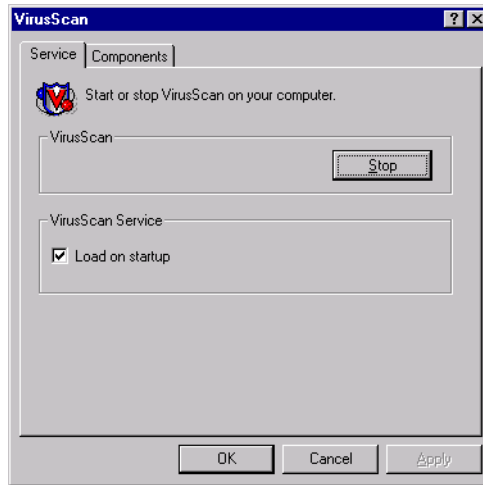


Figure 9-1. VirusScan control panel - Service page

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 9-2).

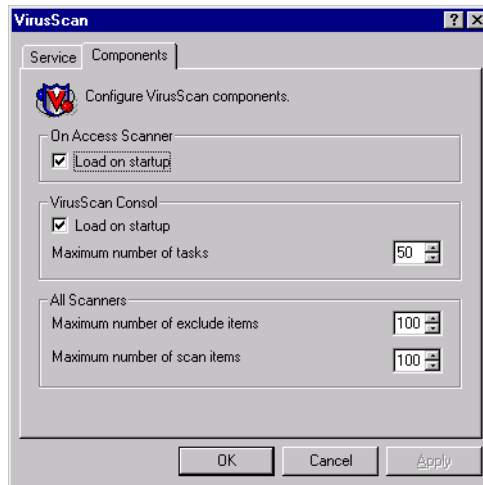




Figure 9-2. VirusScan control panel - Components page

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.

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 virus statistics 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 9-3).



Figure 9-3. 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 9-4).



Figure 9-4. 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 9-5).

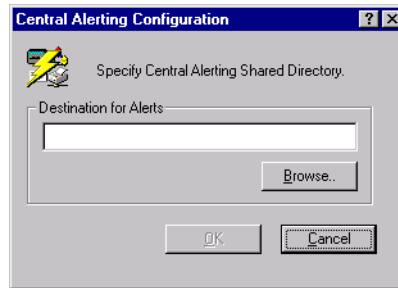


Figure 9-5. Central Alerting Configuration dialog box

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 9-6).

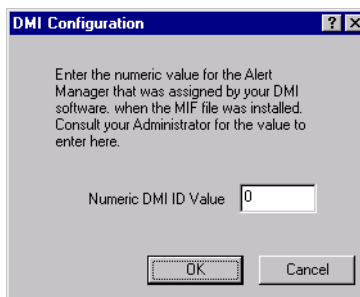


Figure 9-6. DMI Configuration dialog box

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.

Default Vulnerable and Compressed File Extensions

A

Adding file name extensions for scanning

Because viruses ordinarily cannot infect files that contain no executable code, VirusScan software initially looks for viruses only in files that are susceptible to infection. The software uses a list of file name extensions to keep track of vulnerable files. This list appears in the Program Extensions dialog box, and is something you can edit to suit your own needs.

To change the extensions shown in the Program Extensions dialog box, follow these steps:

1. Click **Extensions** in the Detection property page for whichever VirusScan component you are configuring.
2. The Program File Extensions dialog box will appear.

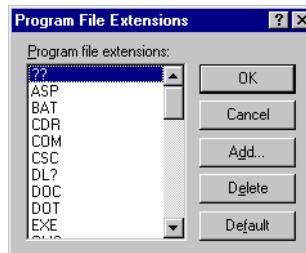


Figure A-1. Program File Extensions dialog box

3. You can:
 - Click **Add** to include a new extension.

This opens the Add Program File Extension dialog box. Type the three-character extension you want to add in the text box provided. Do not include the dot that normally precedes a file name extension. If you want the software to look for viruses in files without extensions, don't type anything in the text box—leave it blank.

Next, click **OK** to return to the Program File Extensions dialog box. If you left the text box blank, the software will ask you whether you want to scan files with no extension. Click **OK** to continue.

You can add as many unique extensions as you want.

- Select one of the extensions shown, then click **Edit** to change its definition.
 - Select one of the extensions shown, then click **Remove** to delete it from the list.
 - Click **Default** to restore the original extension entries. This removes any extensions you have added to the list.
4. When you have finished changing the list, click OK to save your changes and close the dialog box. Click Cancel to close the dialog box without saving your changes.

Current list of vulnerable file name extensions

In this list, ? symbols represent wildcards—VirusScan software substitutes any character for the ? so that it scans more than one file type with similar extensions. For example, the software will use the .XL? wildcard to look for viruses in Microsoft Excel spreadsheet (.XLS) and template (.XLT) files.

-
- NOTE:** McAfee recommends that you scan your system thoroughly during your first scan operation, or periodically thereafter, without limiting the scope of the scan operation to these file types. This ensures that your system starts in a virus-free condition. You can then use this list of extensions to limit the scope of later scan operations.
-

Table 9-1. Vulnerable file name extensions

Extension	File Type	File Description
(NoExtension)	Any	Files with no extension.
.??_	Compressed	Windows compressed files.
.ARC	Macro/script	LH ARC files, older version
.ARJ	Archive	Robert Jung .ARJ compressed archive files.
.ASP	Macro/script	Microsoft Active Server Pages files. These files contain script commands for use with Microsoft Internet Information Server.
.BAT	Program	DOS batch files.
.CAB	Compressed	Windows Compressed Application Binary or "cabinet" files.
.CDR	Macro	Corel Draw document file. Later versions of Corel Draw include a scripting language that can generate macro viruses.

Table 9-1. Vulnerable file name extensions

Extension	File Type	File Description
.CLA	Program	Java class files (truncated from .CLASS)
.COM	Program	Command/binary image files. These common files run as infectable executable programs. DOS and Windows system files frequently make use of this extension.
.CSC	Script/macro	Corel script files. Script files can include viruses or generate macro viruses.
.DL?	Program	Dynamic Link Library file; C++ dialog script files. Dynamic Link Library files are resource files linked to executable program files. Executable files can load viruses stored in them and run them as part of their native code.
.DOC	Macro	Microsoft Word document files. These files can contain Word Basic macros and, therefore, macro viruses
.DOT	Macro	Microsoft Word document template files. These files can contain Word Basic macros and macro viruses
.EXE	Program	Executable files. Most software uses this extension to identify files that start its command shell or program kernel.
.GMS	Macro	Corel Global Macro Storage files.
.GZ?	Compressed	UNIX GNU Gzip compressed files.
.HLP	Macro	Windows Help files. These files can contain executable Word Basic or other macro code.
.HT?	Script/macro	Hyper Text Markup Language and related files; Microsoft Hyper Text template files. Although they are nominally plain text, these files can contain powerful scripting functions that act through browser software
.ICE	Compressed	ICE compressed files.
.IM?	Program	Image files for creating disk images.
.INI	Program	Windows initialization files. Although these are generally text files, infected .INI files can cause mIRC clients to perform unwanted actions.

Table 9-1. Vulnerable file name extensions

Extension	File Type	File Description
.JS?	Script	JavaScript source files. JavaScript files can contain virus code that acts directly on web browsers.
.LZH	Compressed	LHARC compressed files
.MD?	Macro	Microsoft Access database, add-in, and related files. These files can contain infectable Visual Basic for Applications macros.
.MPP	Macro	Microsoft Project files. These files can contain infectable Visual Basic for Applications macros.
.MPT	Macro	Microsoft Project template files. These files can contain infectable Visual Basic for Applications macros.
.MSG	Macro	Microsoft Mail, Exchange and Outlook message files. These files can contain script commands that can introduce virus infections.
.MSO	Macro	Microsoft Office 2000 files.
.OCX	Program	Microsoft Object Linking and Embedding custom controls. These files are similar to ActiveX controls and can function as harmful software in their own right.
.OLE	Program	Microsoft Object Linking and Embedding object files. These files are similar to ActiveX controls. They are files created in one application to be embedded in another application.
.OV?	Program	Overlay files.
.POT	Macro	Microsoft PowerPoint template files. These files can contain infectable Visual Basic for Applications macros.
.PP?	Macro	Microsoft PowerPoint document and slide show files. These files can contain infectable Visual Basic for Applications macros.
.RAR	Archive	RAR compressed archives.
.RTF	Macro	Rich Text Format files. These files serve as a common text file format for many document files.

Table 9-1. Vulnerable file name extensions

Extension	File Type	File Description
.SCR	Program	Windows screen saver files.
.SHS	Program	Windows shell script (scrap object) files. These files can introduce commands that cause unwanted behavior on the host computer.
.SMM	Macro	Lotus AmiPro spreadsheet files. These files include macro capabilities.
.SYS	Program	DOS or Windows system files and device drivers. These executable files frequently start along with or as part of program execution.
.TAR	Archive	UNIX tape archive files.
.VBS	Script	Visual Basic script files and VBScript files. VBScript is an implementation of the Microsoft Visual Basic programming language. It powers special features on many web pages, and can directly manipulate many functions inside Microsoft Outlook and other software.
.VS?	Macro	Visio drawing and related files. Later Visio versions include infectable scripting extensions.
.VXD	Program	Windows virtual device drivers. These are executable files that often reside in memory.
.WBK	Macro	Microsoft Word backup files
.WPD	Macro	Corel WordPerfect document files.
.XL?	Macro	Microsoft Excel worksheet, add-in, toolbar, chart, dialog box, backup, macro, workspace, Visual Basic module, and template files. These files can contain infectable Visual Basic for Applications macros.
.XML	Script/macro	Extensible Markup Language files. Although they are nominally plain text, these files can contain powerful scripting functions that act through browser software.
.ZIP	Archive	WinZip and PKZip compressed archive files.

Current list of compressed files scanned

The VirusScan application and the VShield scanner look for viruses in a range of compressed and archived file formats. Each component uses slightly different technologies for this purpose, however, and therefore treats each file type differently.

For the purpose of this discussion, a “compressed” file means a single file. Compression utilities such as PKLite, LZEXE, and others combine or discard redundant data within these files to reduce their size. An “archived” file means a file that acts as a “wrapper” or an envelope that contains other files within itself. The files within the wrapper can be compressed or not compressed. Examples of such files include WinZip files, .TAR files, and .ARC files. Most WinZip files compress other files and wrap them in a single archive.

This table summarizes how each VirusScan component treats each file type:

Table 9-1. Compressed file and archive scanning treatment

VirusScan component	Archived file	Compressed file
VirusScan application	<ul style="list-style-type: none"> Select the Compressed files checkbox to enable. Opens archives and scans the files within. Specify All Files as your scan target or add the archive's file name extension to the Program Extensions dialog box to have the application scan the archive as a file. 	<ul style="list-style-type: none"> Select the Compressed Files checkbox to enable. Scans the compressed file if you specify All Files as your scan target or add the compressed file's extension to the Program Extensions dialog box.
VShield scanner	<ul style="list-style-type: none"> The scanner will not open the archive to scan the files within. Specify All Files as your scan target or add the archive's file name extension to the Program Extensions dialog box, to have the scanner examine the archive as a file. 	<ul style="list-style-type: none"> Select the Compressed Files checkbox to enable. Specify All Files as your scan target, or add the compressed file's extension to the Program Extensions dialog box, to have the scanner look for viruses in the compressed file.

Both VirusScan components include built-in support for a number of compressed and archived file formats. The table below lists each format and describes how each component scans it when you select the Compressed Files checkbox. You may not edit or add items to this list.

Table 9-1. How VirusScan software treats each file type

Format	Description	VirusScan application support?	VShield scanner support?
.??_	Windows compressed file	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box 	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box
.GZ?	UNIX GNU Gzip compressed file	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box 	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box
.TD0	Teledisk compressed file	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box 	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box
.ARC	LH ARC file, older version	<ul style="list-style-type: none"> Scans archive Scans files within archive 	<ul style="list-style-type: none"> Scans archive as a file if listed in the Program Extensions dialog box Will not scan files within archive
.ARJ	Robert Jung ARJ compressed file	<ul style="list-style-type: none"> Scans archive Scans compressed files within archive 	<ul style="list-style-type: none"> Scans archive as a file if listed in the Program Extensions dialog box Will not scan compressed files within archive
.CAB	Windows Compressed Application Binary or "cabinet" file	<ul style="list-style-type: none"> Scans archive Scans compressed files within archive 	<ul style="list-style-type: none"> Scans archive as a file if listed in the Program Extensions dialog box Will not scan compressed files within archive

Table 9-1. How VirusScan software treats each file type

Format	Description	VirusScan application support?	VShield scanner support?
.ICE	ICE compressed file	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box 	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box
.LZH	LHARC compressed file	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box 	<ul style="list-style-type: none"> Scans compressed file if listed in Program Extensions dialog box
.RAR	RAR compressed archive	<ul style="list-style-type: none"> Scans archive Scans files within archive 	<ul style="list-style-type: none"> Scans archive as a file if listed in the Program Extensions dialog box Will not scan files within archive
.TAR	UNIX tape archive file	<ul style="list-style-type: none"> Scans archive Scans files within archive 	<ul style="list-style-type: none"> Scans archive as a file if listed in the Program Extensions dialog box Will not scan files within archive
.ZIP	PKZip or WinZip file	<ul style="list-style-type: none"> Scans archive Scans compressed files within archive 	<ul style="list-style-type: none"> Scans archive as a file if listed in the Program Extensions dialog box Will not scan compressed files within archive

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 B-1. Corporate PrimeSupport Plans at a Glance

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

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

PrimeSupport options for home users

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

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

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

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

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

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

To contact Network Associates electronic services

- Call the automated voice and fax system at (408) 346-3414
- Visit the Network Associates website at <http://support.nai.com>
- Visit the Network Associates CompuServe forum at GO NAI
- Visit Network Associates on America Online: keyword MCAFEE
- Free access to the PrimeSupport KnowledgeBase: online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes. Visit the KnowledgeBase at:

http://www.nai.com/asp_set/support/technical/intro.asp

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

(972) 855-7044

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

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

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

All McAfee products

(800) 950-1165

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

All products except PGP encryption
software

(900) 225-5624

- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via Network Associates online or electronic services.
- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot obtain product upgrades online. This service is available for McAfee VirusScan and NetShield software only.

How to reach international home user support

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

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

* long distance charges might apply

Ordering a PrimeSupport plan for home users

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

- In North America, call Network Associates Customer Service at (972) 855-7044
- In international locations, contact the Network Associates retail technical support center closest to your location for more information. Some support options may not be available in some locations.

Network Associates consulting and training

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

Professional Services

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

Jumpstart Services

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

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

Network consulting

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

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

To learn more about the options available:

- Contact your regional sales representative.
- In North America, call 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/services/education/>

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 C-1 on page 312](#)).



Figure C-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 C-2).

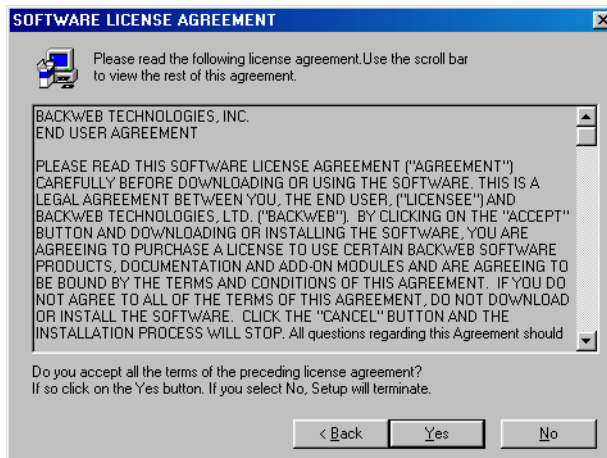


Figure C-2. BackWeb Software License Agreement panel

5. Click **Yes** to continue.
6. The Choose Destination Location panel appears (Figure C-3 on page 313).

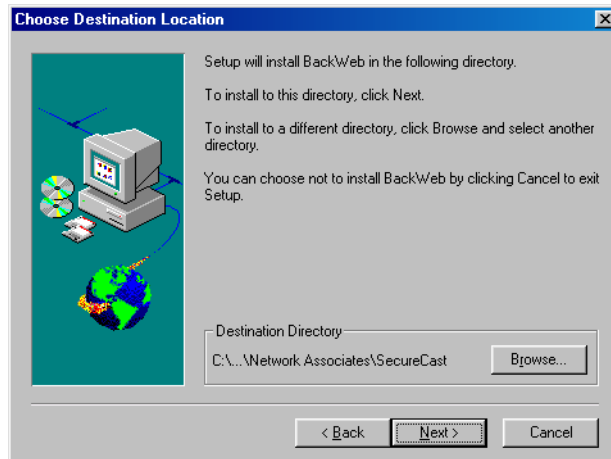


Figure C-3. Choose Destination Location panel

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 C-4).

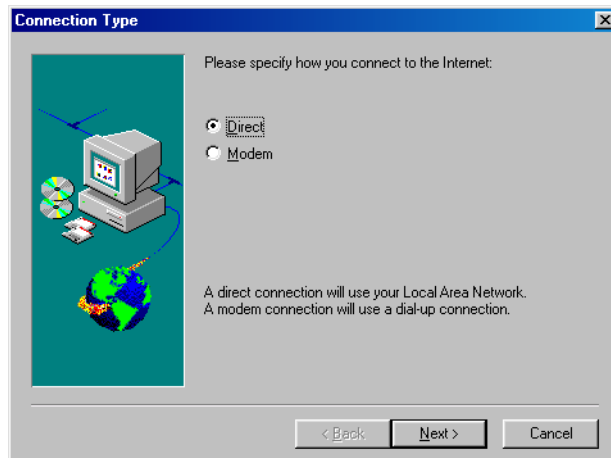


Figure C-4. Connection Type panel

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 C-5](#)).

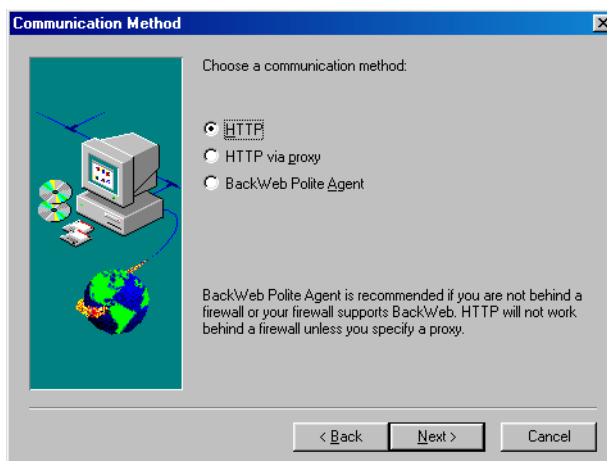


Figure C-5. Communication Method panel

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 C-6).

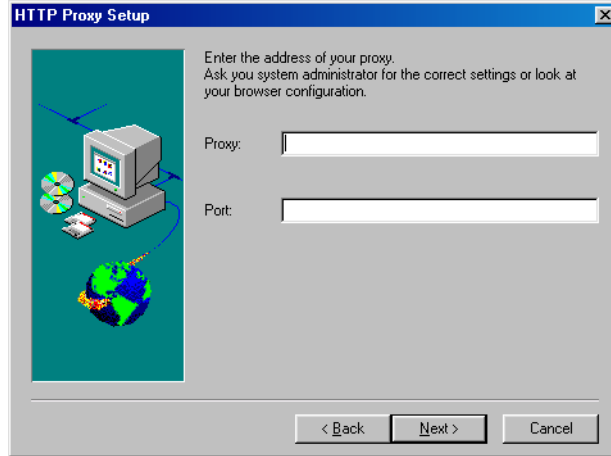


Figure C-6. HTTP Proxy Setup panel

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 C-7 on page 315).

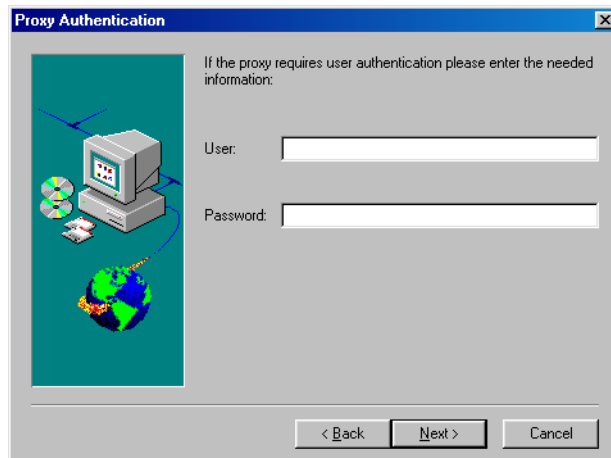


Figure C-7. Proxy Authentication panel

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 C-8).

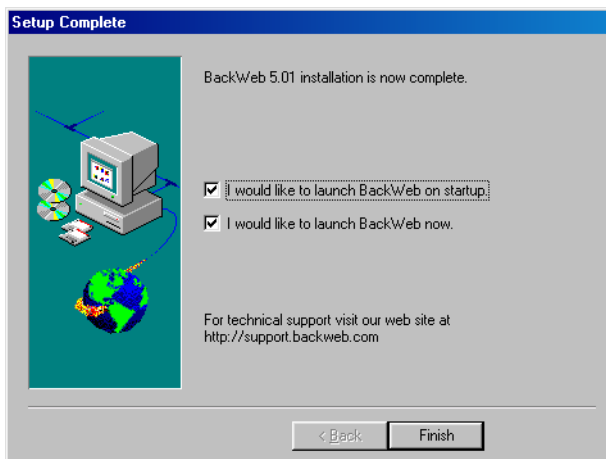


Figure C-8. Setup Complete panel

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 C-9).

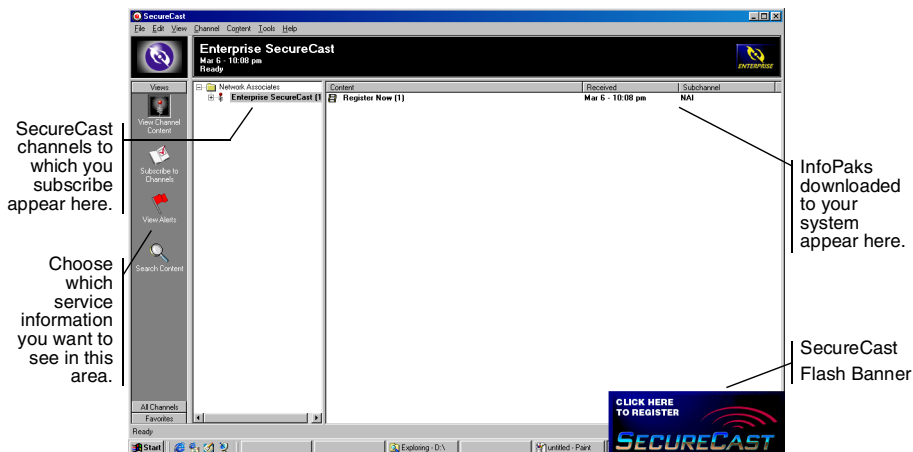



Figure C-9. The Enterprise SecureCast client window

The SecureCast service alerts you that an InfoPak has arrived with the Flash message shown at the bottom right corner of [Figure C-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 C-10](#)).



Figure C-10. SecureCast Flash banner

2. Click the banner. The Network Associates Welcome panel appears ([Figure C-11](#)).

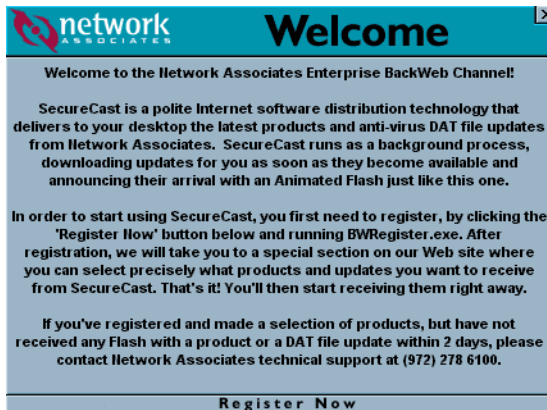


Figure C-11. Network Associates Welcome panel

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 C-12](#)).

Figure C-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 C-13 on page 319](#)). Skip to [Step 7 on page 319](#).
- If you have cleared the **Subsidiary of a Parent Company** checkbox, continue with [Step 6 on page 319](#).

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 C-13. SecureCast Parent Company Information form

- 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 C-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 C-14. SecureCast Proxy Communication Configuration

- 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.

- When you have finished, click **Next>**. The **Online Activity Status** panel appears displaying the progress of the registration process (Figure C-15 on page 320).

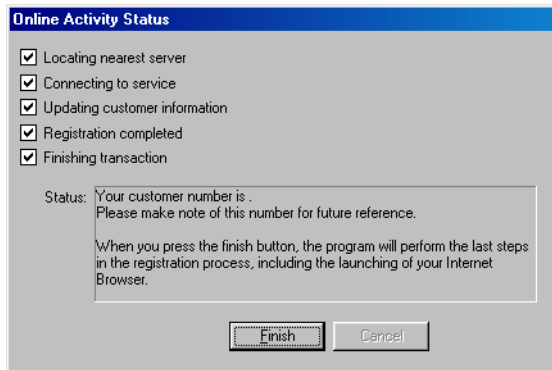


Figure C-15. SecureCast Online Activity Status panel

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 C-16](#):

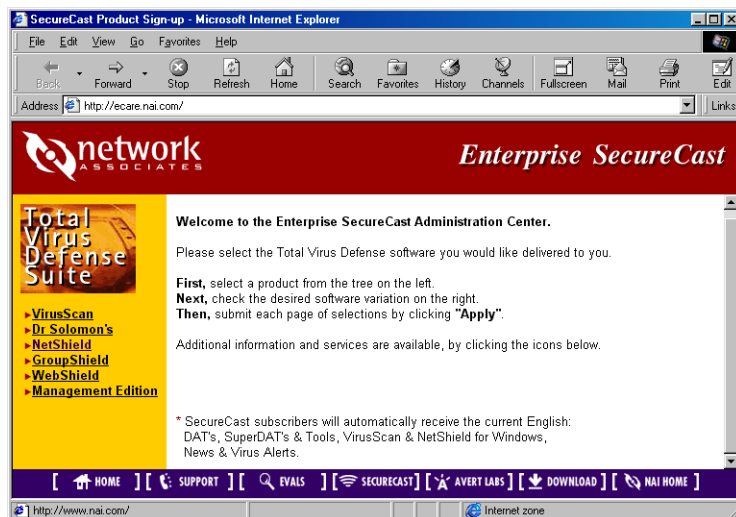


Figure C-16. SecureCast Electronic Corporate Customer Care


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 C-9 on page 316](#)), 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/>

Index

A

action options, choosing

- for VirusScan in Console, 215 to 217
- in Download Scan module, 136 to 138
- in E-mail Scan module, 123 to 125
- in Internet Filter module, 147 to 148
- in System Scan module, 107 to 110
- in the E-Mail Scan program component, 264 to 266
- in VirusScan Advanced, 182 to 184
- in VirusScan Classic, 173 to 175

Active Virus Defense

- VirusScan as component of, 24

ActiveX controls

- as malicious software, xiii to xiv
- detecting with VShield's Internet Filter module, 142 to 143
- distinction between viruses and, xiii

alarms, false, understanding, 66

Alert Manager

- using Centralized Alerting with, 289

Alert Manager Client Configuration utility

- configuring, 286 to 290
- understanding and using, 285 to 286

alert messages

- audible, sounding, 176

alert mode

- BIOS, 108

alert options, choosing

- for VirusScan in Console, 218 to 219
- in Download Scan module, 138 to 139
- in E-mail Scan module, 126 to 129
- in Internet Filter module, 148 to 149
- in System Scan module, 110 to 111
- in the E-Mail Scan program component, 266 to 270
- in VirusScan Advanced, 184 to 188

.ALR files, use of for Centralized Alerting messages, 286

America Online

- mail client, supported in VShield, 90
- technical support via, xvii

America Online, technical support via, 304

anonymous FTP, use of to log on to update and upgrade sites, 239, 250

anti-virus software

- code signatures, use of for virus detection, xi
- consequences of running multiple vendor versions, 66
- reporting new viruses not detected by to McAfee, xix

audible alert messages, sounding, 111, 128, 139, 149, 176, 185, 219

automatic start, setting for scan task, 215

- AutoUpdate
 - advanced options for, configuring, [239](#) to [242](#)
 - Force Update, use of to replace corrupted .DAT files, [241](#)
 - number of connection attempts made for update sites, [238](#)
 - options for, configuring, [232](#) to [252](#)
 - use of in conjunction with SecureCast, [232](#), [243](#)
- AutoUpgrade
 - advanced options for, configuring, [250](#) to [252](#)
 - number of connection attempts made for update sites, [249](#)
 - options for, configuring, [242](#) to [252](#)
 - use of with SuperDAT utility, [252](#) to [254](#)
- B**
- background scan tasks, configuring
 - in configuration wizard, [96](#)
 - in ScreenScan, [273](#) to [279](#)
 - in System Scan Properties dialog box, [99](#) to [117](#)
- Basic, as macro virus programming language, [xii](#)
- batch files, running after successful updates, [242](#)
- BIOS
 - as alert mode in VShield scanner on Windows 95 and Windows 98 systems, [108](#)
 - possible VirusScan conflicts with anti-virus features of, [66](#)
- boot blocks
 - scanning, [215](#)
- BOOTSCAN.EXE
 - use of on Emergency Disk, [62](#)
- boot-sector viruses, definition and behavior of, [ix](#) to [x](#)
- "Brain" virus, [ix](#)
- browsers supported in VShield, [89](#)
- C**
- cc:Mail
 - as e-mail client supported in VShield, [90](#)
 - choosing correct options for
 - in configuration wizard, [97](#)
 - in E-mail Scan Properties dialog box, [119](#)
 - logging on to and scanning v6.0, v7.0 and v8.0 mailboxes, [273](#)
- CENTALRT.TXT file
 - necessity for in Centralized Alerting, [289](#)
- Centralized Alerting
 - enabling for use with Alert Manager, [289](#)
 - need for CENTALRT.TXT file, [289](#)
 - use of .ALR messages for, [286](#)
- Centralized Alerting, versus sending alert messages to Alert Manager server, [286](#)
- client for Alert Manager
 - configuring, [286](#) to [290](#)
 - understanding and using in VirusScan software, [285](#) to [286](#)
- code signatures
 - use of by viruses, [xi](#)
- COMMAND.COM files, virus infections in, [x](#)
- components, included with VirusScan, [27](#) to [31](#)
- CompuServe, technical support via, [xvii](#), [304](#)
- computer problems, attributing to viruses, [61](#)
- Concept virus, introduction of, [xii](#)

- configuration
 - choosing options for VirusScan in Console, 210 to 227
 - of E-Mail program
 - component, 259 to 272
 - of ScreenScan, 273 to 279
 - of VirusScan Advanced, 176 to 191
 - of VirusScan Classic, 171 to 176
 - of VShield
 - in Download Scan module, 132 to 142
 - in E-mail Scan module, 117 to 131
 - in Internet Filter module, 142 to 151
 - in Security module, 151 to 154
 - in System Scan module, 100 to 117
 - using wizard, 90, 95 to 99
- configuration wizard
 - Download Scan module options, choosing with, 98
 - E-mail Scan module options, choosing with, 97
 - Internet Filter module options, choosing with, 99
 - starting, 95
 - System Scan module options, choosing with, 96
 - using, 90, 95 to 99
- Console
 - action options for VirusScan, configuring from, 215 to 217
 - alert options for VirusScan, configuring from, 218 to 219
 - commands available in, 196 to 197
 - configuring tasks in, 196, 210 to 227
 - copying and pasting tasks in, 196
 - creating new tasks in, 196, 202, 206
 - default scan tasks included with, 198
 - definition of scan task in, 195
 - deleting tasks from, 196
 - detection options for VirusScan, configuring from, 211 to 215
 - disabling and enabling tasks from, 197
 - exclusion options for VirusScan, configuring from, 222 to 225
 - necessity to have running to start scan tasks, 208
 - overview of, 196 to 197
 - possible applications for, 193
 - purpose of, 193
 - report options for VirusScan, configuring from, 219 to 222
 - scheduling and enabling tasks in, 196, 206 to 208
 - security options for VirusScan, configuring from, 225 to 227
 - starting, 194
 - starting tasks from, 197
 - status bar in, hiding and displaying, 196
 - stopping tasks from, 197
 - title bar in, hiding and displaying, 196
 - toolbar in, hiding and displaying, 195
 - window, elements of, 195
- consulting services, 307
- contents of log file, 113, 130, 141, 187, 221, 271
- context menus
 - use of in VirusScan Console window, 196
- control panel, VirusScan
 - choosing options for, 282 to 284
 - opening, 281 to 282
 - understanding, 281
- Copy**
 - in **Edit** menu, 196

corporate e-mail systems, choosing
 in configuration wizard, 97
 in E-Mail Scan Properties dialog box, 119
costs from virus damage, vii to viii
crashes, when not attributable to viruses, 65
CTRL+ALT+DEL, ineffective use of to clear
 viruses, xi
Customer Service
 contacting, xvi

D

damage from viruses, vii
 payloads, ix
.DAT file updates
 what they are, 229
 definition of and numbering convention
 for, 231
 reporting new items for, xix
data files
 common, delivered via SecureCast, 310
date and time, recorded in log file, 113, 130,
 141
defaults
 scan targets, 292
definitions
 task, 195
 virus, vii
Delete
 in **Task** menu, 196
descriptions, of VirusScan program
 components, 27 to 31
Desktop Management Interface (DMI) alerts,
 use of with Alert Manager server, 290
detection
 options
 adding scan targets, 172, 178 to 180,
 211 to 276
 adding scan targets in
 ScreenScan, 274 to 275
 choosing for VirusScan in
 Console, 211
 choosing in the E-Mail Scan program
 component, 261 to 264
 choosing in VirusScan
 Advanced, 177 to 182
 configuring for Download Scan
 module, 132 to 135
 configuring for E-mail Scan
 module, 118 to 123
 configuring for Internet Filter
 module, 143 to 147
 configuring for System Scan
 module, 101 to 106
 removing scan targets, 179, 212, 275
Detection page
 for VirusScan in the Console, 211 to 215
 in Download Scan module, 132 to 135
 in E-mail Scan module, 118 to 123
 in Internet Filter module, 143 to 147
 in System Scan module, 101 to 106
 in the E-Mail Scan program
 component, 261 to 264
 in VirusScan Advanced, 177 to 182
detections, false, understanding, 66
Disable
 in **Task** menu, 197
disguising virus infections, xi

- disks
 - choosing as scan targets, [172](#), [178 to 180](#), [211 to 262](#), [274 to 276](#)
 - floppy
 - as medium for virus transmission, [ix to x](#)
 - distribution
 - of update files, recommended methods for, [232 to 243](#)
 - distribution of VirusScan
 - electronically and on CD-ROM disc, [35](#)
 - DMI alerts, use of with Alert Manager server, [290](#)
 - document files, as agents for virus transmission, [xii](#)
 - double heuristics analysis, [26](#)
 - Download Scan module
 - configuring, [132 to 142](#)
 - default response options for, [71 to 72](#)
 - set up
 - using configuration wizard, [98](#)
 - using VShield Properties dialog box, [132 to 142](#)
- ## E
- Edit** menu
 - Copy**, [196](#)
 - Paste**, [196](#)
 - educational services, description of, [308](#)
 - EICAR "virus," use of to test installation, [56](#)
 - electronic services, contacting for technical support, [304](#)
 - e-mail
 - addresses for reporting new viruses to McAfee, [xix](#)
 - as agent for virus transmission, [xii](#)
 - client software
 - choosing in configuration wizard, [97](#)
 - choosing in E-Mail Scan Properties dialog box, [118 to 123](#)
 - supported in VShield, [89](#)
 - E-mail Scan module
 - configuring, [117 to 131](#)
 - set up
 - using configuration wizard, [97](#)
 - using VShield Properties dialog box, [117 to 131](#)
 - E-Mail Scan program component, default responses when virus found, [74 to 75](#)
 - Emergency .DAT files, location and use of, [232](#)
 - Emergency Disk
 - creating
 - on uninfected computer, [62](#)
 - use of BOOTSCAN.EXE on, [62](#)
 - use of to reboot system, [62](#)
 - Enable**
 - in **Task** menu, [197](#)
 - encrypted viruses, [xi](#)
 - Enterprise SecureCast, [309](#)
 - features of, [310](#)
 - setting up, [321](#)
 - support resources for, [321](#)
 - system requirements for, [311](#)
 - troubleshooting, [321](#)
 - unsubscribing from, [321](#)

- Eudora and Eudora Pro
 - as e-mail clients supported in VShield, 90
- Excel files, as agents for virus transmission, xii
- Exchange
 - as e-mail client supported in VShield, 90
- exclusion options, choosing
 - for System Scan module, 114 to 117
 - for VirusScan Advanced, 188 to 190
 - for VirusScan in Console, 222 to 225
- executable programs
 - as agents for virus transmission, x
- extensions, use of to identify scan targets, 292
- EXTRA.DAT files, location, use, and description of, 231
- F**
- false detections, understanding, 66
- file information, viewing, 76 to 77
- File menu
 - View Activity Log**, 186, 222
- file name extensions
 - use of to identify vulnerable files, 292
- File Transfer Protocol (FTP)
 - use of to obtain VirusScan upgrades, 250
- file-infecting viruses
 - definition and behavior of, x
 - setting heuristic scanning options for, 105 to 106, 121, 134 to 135, 180 to 182, 213, 262, 276
- files
 - choosing as scan targets, 172, 178 to 180, 211 to 213, 262 to 264, 274 to 276
 - infected
 - cleaning, 107 to 110, 124 to 125, 136, 138, 174 to 175, 182 to 184, 216 to 217, 264 to 266
 - cleaning by yourself when VirusScan cannot, 63
 - deleting, 107 to 110, 124 to 125, 136, 138, 174 to 175, 182 to 184, 216 to 217, 264 to 266
 - moving, 107 to 110, 124 to 125, 136, 138, 174 to 175, 182 to 184, 216 to 217, 264 to 266
 - MAILSCAN.TXT, as E-Mail program component log, 270
 - SCREENSCAN ACTIVITY LOG.TXT, as ScreenScan log, 279
 - VSCLOG.TXT, as VirusScan log, 175 to 176, 185 to 186, 219 to 271
 - VSHLOG.TXT, as VShield log, 112 to 113
 - WEBEMAIL.TXT, as VShield log, 129
 - WEBFLTR.TXT, as VShield log, 150 to 151
 - WEBINET.TXT, as VirusScan log, 140
- floppy disks
 - role in spreading viruses, ix to x
- folders
 - choosing as scan targets, 172, 178 to 180, 211 to 262, 274 to 276
- Force Update, use of to replace corrupted .DAT files, 241
- FTP (File Transfer Protocol)
 - use of to obtain VirusScan upgrades, 250

H

Help

- opening from the Console, [197](#)
- opening from VirusScan Classic and VirusScan Advanced, [167](#)

Help Topics

- in **Help** menu, [167, 197](#)

heuristic scanning

- definition of, [26, 105 to 106, 121, 134 to 135, 180 to 182, 213, 262, 276](#)

history of viruses, [vii to xiv](#)

hostile objects

- distinction between viruses and, [xiii](#)
- Java classes and ActiveX controls as, [xiii to xiv](#)

I

incremental .DAT (iDAT) files

- what they are, [229](#)

infected files

- cleaning by yourself when VirusScan cannot, [63](#)
- deleting
 - recorded in log file, [113, 130, 141](#)
- moving, [109, 124, 137](#)
 - recorded in log file, [113, 130, 141](#)
- removing viruses from, [61 to 75](#)
- use of quarantine folder to isolate, [109, 124, 137](#)

installation

- aborting if virus detected during, [61](#)
- testing effectiveness of, [56](#)

Internet

- e-mail clients, choosing
 - in configuration wizard, [97](#)
 - in E-mail Scan Properties dialog box, [119](#)
- spread of viruses via, [xii](#)

Internet Explorer

- as browser supported in VShield, [89](#)

Internet Filter module

- configuring, [142 to 151](#)
- default response options for, [72](#)
- set up
 - using configuration wizard, [99](#)
 - using VShield Properties dialog box, [142 to 151](#)

Internet Relay Chat

- as agent for virus transmission, [xiv](#)

J

Java classes

- as malicious software, [xiii to xiv](#)
- distinction between viruses and, [xiii](#)

L

log file

- creating with text editor, [112 to 113, 129, 140, 150 to 151, 175 to 176, 185 to 186, 219 to 221, 270 to 271, 279](#)
- information recorded in, [113, 130, 141, 187, 221, 271](#)
- limiting size of, [113, 130, 141, 151, 176, 186, 221, 237, 247, 271](#)
- MAILSCAN.TXT as, [270](#)
- SCREENSCAN ACTIVITY LOG.TXT as, [279](#)
- UPDATE UPGRADE ACTIVITY.TXT as, [236, 247](#)

- VSCLOG.TXT as, 175 to 176, 185 to 186, 219 to 271
- VSHLOG.TXT as, 112 to 113
- WEBEMAIL.TXT as, 129
- WEBFLTR.TXT as, 150 to 151
- WEBINET.TXT as, 140
- logging options. *See* report options
- Lotus cc:Mail
- as e-mail client supported in VShield, 90
 - choosing correct options for
 - in configuration wizard, 97
 - in E-mail Scan Properties dialog box, 119
 - logging on to and scanning v6.0, v7.0, and v8.0 mailboxes, 273
- M**
- macro viruses
- Concept virus, xii
 - definition and behavior of, xii
 - setting heuristic scanning options for, 105 to 106, 121, 134 to 135, 180 to 182, 213, 262, 276
- MAILSCAN.TXT, as E-Mail Scan program component report file, 270
- malicious software
- ActiveX controls as, xiii to xiv
 - distinction between hostile objects and viruses, xiii
 - Java classes as, xiii to xiv
 - payload, ix
 - script viruses as, xiv
 - spread via World Wide Web, xii to xiv
 - types
 - Trojan horses, ix
 - worms, viii
- MAPI (Messaging Application Programming Interface) e-mail clients
- choosing in configuration wizard, 97
 - choosing in E-mail Scan Properties dialog box, 119
- master boot record (MBR), susceptibility to virus infection, x
- McAfee
- contacting
 - via America Online, xvii
 - via CompuServe, xvii
 - within the United States, xvii
- memory
- scanning as part of scan task, 215
 - virus infections in, ix to x
- menus, shortcut
- use of from system tray
 - for VShield, 155
 - use of in VirusScan Console window, 196
- methods for updating and upgrading VirusScan software, 230 to 232
- Microsoft
- Exchange, Outlook and Outlook Express, as e-mail clients supported in VShield, 90
 - Internet Explorer
 - as browser supported in VShield, 89
 - Visual Basic, as macro virus programming language, xii
 - Word and Excel files, as agents for virus transmission, xii
- military time, using to schedule scan tasks, 208
- mIRC script virus, xiv
- mutating viruses, definition of, xi

N

Netscape Navigator and Netscape Mail

as browser and e-mail client supported in
VShield, 89

Network Associates

consulting services from, 307

contacting

Customer Service, xvi

outside the United States, xx

educational services, 308

support services, 299

training, xviii, 307

website address for software updates and
upgrades, 304

new scan task, creating, 196, 202 to 206

New Task

in **Task** menu, 196, 203

new viruses, reporting to McAfee, xix

numbering conventions for .DAT files, 231

O

objects, Java and ActiveX

as malicious software, xiii to xiv

Office, Microsoft, files as agents for virus
transmission, xii

Olympus scan engine

what it is, 229

online help

opening from the Console, 197

opening from VirusScan Classic and
VirusScan Advanced, 167

options

Download Scan module,
configuring, 132 to 142

E-mail Scan module,
configuring, 117 to 131

E-Mail Scan program component

Action, 264 to 266

Alert, 266 to 270

configuring, 259 to 272

Detection, 261 to 264

Report, 270 to 272

Internet Filter module,

configuring, 142 to 151

ScreenScan, configuring, 273 to 279

Security module, configuring, 151 to 154

System Scan module,
configuring, 100 to 117

VirusScan

Action, 215 to 217

Alert, 218 to 219

configuring, 210 to 227

Detection, 211

Exclusion, 222 to 225

Report, 219 to 222

Security, 225 to 227

VirusScan Advanced

Action, 182 to 184

Alert, 184 to 188

Detection, 177 to 182

Exclusion, 188 to 190

Report, 185 to 188

Security, 191

VirusScan Classic

Action, 173 to 175

Report, 175 to 176

Where & What, 171 to 173

origin of viruses, [vii to xiv](#)
Outlook and Outlook Express
 as e-mail clients supported in
 VShield, [90](#)
 distinguishing between, [97](#)
overview, of VirusScan Console, [196 to 197](#)

P

panic, avoiding when your system is
 infected, [61](#)
password, choosing
 for VirusScan in Console, [226](#)
 in VirusScan Advanced, [191](#)
 in VShield Security module, [153](#)

Paste

 in **Edit** menu, [196](#)

payload, definition of, [ix](#)

PC viruses, origins of, [ix](#)

PKGDESC.INI file, use of for SuperDAT
 utility upgrades, [254](#)

plain text, use of to transmit viruses, [xiv](#)

polymorphic viruses, definition of, [xi](#)

POP-3 e-mail clients, choosing options for
 in configuration wizard, [97](#)
 in E-mail Scan dialog box, [119](#)

pranks, as virus payloads, [ix](#)

PrimeSupport

 corporate

 at a glance, [303](#)

 KnowledgeCenter, [299](#)

 ordering, [302](#)

 PrimeSupport Connect, [300](#)

 PrimeSupport Enterprise, [301](#)

 PrimeSupport Priority, [301](#)

 for home users

 Online Upgrades plan, [305](#)

 ordering, [306](#)

 Pay-Per-Minute plan, [305](#)

 Quarterly Disk/CD plan, [305](#)

 Small Office/Home Office Annual
 Plan, [305](#)

Professional Consulting Services

 description of, [307](#)

program components, included with
 VirusScan, [27 to 31](#)

program extensions, designating as scan
 targets, [292](#)

programs

 running after successful updates, [242](#)

Properties

 configuring for VirusScan, [210 to 227](#)

 Download Scan module, configuring
 for, [132 to 142](#)

 E-mail Scan module, configuring
 for, [117 to 131](#)

 Internet Filter module, configuring
 for, [142 to 151](#)

 Security module, configuring
 for, [151 to 154](#)

 System Scan module, configuring
 for, [100 to 117](#)

VShield

 setting with configuration
 wizard, [90, 95 to 99](#)

Properties

 in **Task** menu, [196](#)

property pages

 locking and unlocking, [154, 191, 226](#)

proxy servers, working through to obtain
 updates and upgrades, [239, 250](#)

Q

- Qualcomm Eudora and Eudora Pro
 - as e-mail clients supported in VShield, 90
- quarantine folder, use of to isolate infected files, 109, 124, 137
- quick start for VShield configuration, 90, 95 to 99
- quitting VShield, 155 to 160

R

- RAM
 - scanning as part of scan task, 215
 - virus infections in, ix to x
- reasons to run VShield, 88
- rebooting, with the Emergency Disk, 62
- Recycle Bin, excluded from scheduled scan operations, 188, 222
- remover
 - actions available when VirusScan has none, 63
- report file
 - limiting size of, 113, 130, 141, 151, 176, 186, 221, 237, 247, 271
 - MAILSCAN.TXT as, 270
 - SCREENSCAN ACTIVITY LOG.TXT as, 279
 - UPDATE UPGRADE ACTIVITY.TXT as, 236, 247
 - VSCLOG.TXT as, 175 to 176, 185 to 186, 219 to 271
 - VSHLOG.TXT as, 112 to 113
 - WEBEMAIL.TXT as, 129
 - WEBFLTR.TXT as, 150 to 151
 - WEBINET.TXT as, 140

- report options, choosing
 - for VirusScan in Console, 219 to 222
 - in Download Scan module, 140 to 142
 - in E-mail Scan module, 129 to 131
 - in Internet Filter module, 150 to 151
 - in System Scan module, 112 to 114
 - in the E-Mail Scan program component, 270 to 272
 - in VirusScan Advanced, 185 to 188
 - in VirusScan Classic, 175 to 176
- reporting viruses not detected to McAfee, xix
- response options
 - choosing
 - when Download Scan module finds a virus, 71 to 72
 - when E-mail Scan module finds a virus, 70 to 71
 - when Internet Filter module finds harmful objects, 72
 - when System Scan module finds a virus, 67 to 69
 - when the E-Mail Scan program component detects a virus, 74 to 75
 - when VirusScan detects a virus, 72 to 74
 - setting
 - for Download Scan module, 136 to 138
 - for E-mail Scan module, 123 to 125
 - for Internet Filter module, 147
 - for System Scan module, 107 to 110
 - for VirusScan Advanced, 182 to 184
 - for VirusScan Classic, 173 to 175
 - for VirusScan in Console, 215 to 217
- responses, default, when infected by viruses, 61 to 75

- restarting
 - with CTRL+ALT+DEL, ineffective use of to clear viruses, [xi](#)
 - with the Emergency Disk, [62](#)
- results
 - displayed in VShield Status dialog box, [161](#)
 - scan task status, [208](#) to [209](#)
- right-clicking
 - use of to display shortcut menus for VShield, [155](#)
 - use of to display shortcut menus in VirusScan Console, [196](#)
- S**
- scan engine
 - upgrading with AutoUpdate and the SuperDAT utility, [252](#) to [254](#)
 - what it is, [229](#)
- scan operations, deciding when to start, [64](#)
- scan task
 - action options, configuring, [173](#) to [175](#), [182](#) to [184](#), [215](#) to [217](#)
 - alert options, configuring, [184](#) to [188](#), [218](#) to [219](#)
 - boot blocks, examining as part of, [215](#)
 - configuring
 - options for in VirusScan Console, [210](#) to [227](#)
 - copying settings from one to another, [196](#)
 - defaults
 - included with VirusScan Console, [198](#)
 - definition of, [195](#)
 - deleting, [196](#)
 - detection options
 - choosing for VirusScan in Console, [211](#)
 - configuring in VirusScan Advanced, [177](#) to [182](#)
 - disabling, [197](#)
 - entering schedule times for, [208](#)
 - excluding items from, [222](#)
 - exclusion options, configuring
 - for VirusScan Advanced, [188](#) to [190](#)
 - for VirusScan in Console, [222](#) to [225](#)
 - logging options, configuring
 - for VirusScan in Console, [219](#) to [222](#)
 - in VirusScan Advanced, [185](#) to [188](#)
 - in VirusScan Classic, [175](#) to [176](#)
 - memory, scanning, [215](#)
 - naming, [203](#)
 - new, creating, [196](#), [202](#) to [206](#)
 - pasting settings from another, [196](#)
 - program to carry out, choosing, [203](#)
 - removing, [196](#)
 - report options, configuring
 - for VirusScan Advanced, [185](#) to [188](#)
 - for VirusScan Classic, [175](#) to [176](#)
 - for VirusScan in Console, [219](#) to [222](#)
 - schedule times and intervals available for, [207](#)
 - scheduling and enabling, [196](#), [206](#) to [208](#)
 - security options, configuring, [191](#), [225](#) to [227](#)
 - speeding up, [188](#)
 - starting, [197](#)
 - automatically, [215](#)
 - need for Console to be running, [208](#)
 - status, checking, [208](#) to [209](#)
 - stopping, [197](#)
 - targets for

- adding, [172](#), [178 to 180](#), [211 to 262](#),
[274 to 276](#)
- removing, [179](#), [212](#), [275](#)
- Where & What options,
configuring, [171 to 173](#)
- scan tasks
 - scheduling and enabling
 - as purpose of Console, [193](#)
 - possible applications for, [193](#)
 - speeding up, [222](#)
- scanning
 - excluding items from, [188 to 190](#)
 - speeding up scan times, [188 to 190](#)
- SCREENSCAN ACTIVITY LOG.TXT, as
ScreenScan report file, [279](#)
- script viruses, [xiv](#)
- SecureCast
 - common data files delivered via, [310](#)
 - Enterprise SecureCast, [309](#)
 - setting up, [321](#)
 - troubleshooting, [321](#)
 - unsubscribing from, [321](#)
 - features of, [310](#)
 - support resources for, [321](#)
 - system requirements, [311](#)
 - use of in conjunction with
AutoUpdate, [232](#), [243](#)
 - using to update your software, [309](#)
- security
 - password, choosing, [154](#), [191](#), [226](#)
- Security module
 - configuring, [151 to 154](#)
- security options
 - choosing for VirusScan Advanced, [191](#)
 - choosing for VirusScan in
Console, [225 to 227](#)
- Select, [196](#)
- session settings
 - recorded in log file, [113](#), [130](#), [141](#)
- session summary
 - recorded in log file, [113](#), [130](#), [141](#)
- settings
 - VShield, choosing with configuration
wizard, [90](#), [95 to 99](#)
- Setup
 - aborting if virus detected during, [61](#)
- SETUP.EXE, renaming SuperDAT packages
for use with AutoUpgrade, [254](#)
- SETUP.ISS file, use of for SuperDAT utility
upgrades, [254](#)
- shortcut menus
 - use of in VirusScan Console
window, [196](#)
 - use of with VShield, [155](#)
- signatures, use of for virus detection, [xi](#)
- SMTP e-mail clients
 - choosing options for
 - in configuration wizard, [97](#)
 - in E-mail Scan Properties dialog
box, [119](#)
- software conflicts, as potential cause for
computer problems, [65](#)
- software updates and upgrades, website
address for obtaining, [304](#)
- spreadsheet files, virus infections in, [xii](#)
- Start**
 - in **Task** menu, [197](#)
- statistics
 - displayed in VShield Status dialog
box, [161](#)
 - for scan task, [208 to 209](#)

- status
 - checking for scan operations, 208 to 209
 - checking for VShield, 161
 - Status Bar
 - in VirusScan Console, hiding and displaying, 196
 - Status Bar**
 - in **View** menu, 196
 - stealth viruses, definition of, xi
 - Stop**
 - in **Task** menu, 197
 - SuperDAT utility
 - use of for upgrade strategy, 230
 - use of in conjunction with the AutoUpgrade utility, 252 to 254
 - support
 - corporate
 - at a glance, 303
 - KnowledgeCenter, 299
 - ordering, 302
 - PrimeSupport Connect, 300
 - PrimeSupport Enterprise, 301
 - PrimeSupport Priority, 301
 - for home users, 304
 - Online Upgrades plan, 305
 - Pay-Per-Minute plan, 305
 - PrimeSupport
 - ordering, 306
 - Small Office/Home Office Annual Plan, 305
 - Quarterly Disk/CD plan, 305
 - hours of availability, 304
 - resources for SecureCast, 321
 - via electronic services, 304
 - system crashes, attributing to viruses, 61
 - system files, as agents for virus transmission, x
 - system requirements
 - for VirusScan, 35
 - SecureCast, 311
 - System Scan module
 - configuring, 100 to 117
 - default response options for, 67 to 69
 - set up
 - using configuration wizard, 96
 - using VShield Properties dialog box, 100 to 117
- ## T
- targets for scanning
 - adding, 172, 178 to 180, 211 to 262, 274 to 276
 - removing, 179, 212, 275
 - task
 - action options, configuring, 173 to 175, 182 to 184, 215 to 217
 - adding scan targets to, 172, 178 to 276
 - alert options, configuring, 184 to 188, 218 to 219
 - configuring options for in VirusScan Console, 210 to 227
 - copying settings from one to another, 196
 - defaults, included with VirusScan Console, 198
 - definition of, 195
 - deleting, 196
 - detection options
 - choosing for VirusScan in Console, 211 to 215
 - configuring in VirusScan Advanced, 177 to 182

- disabling and enabling, 197
- entering schedule times for, 208
- exclusion options, configuring
 - for VirusScan Advanced, 188 to 190
 - for VirusScan in Console, 222 to 225
- logging options, configuring
 - for VirusScan in Console, 219 to 222
 - in VirusScan Advanced, 185 to 188
 - in VirusScan Classic, 175 to 176
- memory, scanning as part of, 215
- naming, 203
- new, creating, 196, 202 to 206
- pasting settings from another, 196
- program to carry out, choosing, 203
- removing, 196
- removing scan targets, 179, 212, 275
- report options, configuring
 - for VirusScan Advanced, 185 to 188
 - for VirusScan Classic, 175 to 176
 - for VirusScan in Console, 219 to 222
- scan targets for
 - adding, 211, 274 to 275
- schedule times and intervals available for, 207
- scheduling and enabling, 196, 206 to 208
- security options, configuring, 191, 225 to 227
- starting, 197
 - automatically, 215
 - need for Console to be running, 208
- status, checking, 208 to 209
- stopping, 197
- Where & What options, configuring, 171 to 173
- task list
 - default tasks in, 195
- Task menu
 - View Activity Log**, 237, 248
- Task** menu
 - Delete**, 196
 - Disable**, 197
 - Enable**, 197
 - New Task**, 196, 203
 - Properties**, 196
 - Start**, 197
 - Stop**, 197
- technical support
 - corporate
 - at a glance, 303
 - KnowledgeCenter, 299
 - ordering, 302
 - PrimeSupport Connect, 300
 - PrimeSupport Enterprise, 301
 - PrimeSupport Priority, 301
 - e-mail address for, xvii
 - for home users
 - PrimeSupport
 - Online Upgrades plan, 305
 - Pay-Per-Minute plan, 305
 - Quarterly Disk/CD plan, 305
 - Small Office/Home Office Annual Plan, 305
 - hours of availability, 304
 - information needed from user, xviii
 - online, xvii
 - phone numbers for, xvii
 - PrimeSupport
 - for home users
 - ordering, 306

via electronic services, [304](#)

testing your installation, [56](#)

text

- editor, use of to create log file, [112](#) to [113](#), [129](#), [140](#), [150](#) to [151](#), [175](#) to [176](#), [185](#) to [186](#), [219](#) to [221](#), [270](#) to [271](#), [279](#)
- messages, use of to transmit viruses, [xiv](#)

Title Bar

- in VirusScan Console, hiding and displaying, [196](#)

Title Bar

- in **View** menu, [196](#)

Toolbar

- in VirusScan Console, hiding and displaying, [195](#)

Toolbar

- in **View** menu, [196](#)

Total Education Services

- description of, [307](#)

Total Service Solutions

- contacting, [307](#)

training for Network Associates products, [xviii](#), [307](#)

- scheduling, [xviii](#)

Trojan horse, definition of, [ix](#)

troubleshooting SecureCast

- firewall problems, [321](#)
- registration problems, [321](#)

24-hour clock, using to enter schedule times, [208](#)

U

uninfected computer, use of to create Emergency Disk, [62](#)

Universal Naming Convention (UNC) notation, use of to designate update and upgrade sites, [238](#), [249](#)

update and upgrade methods

- using with VirusScan software, [230](#) to [232](#)

UPDATE UPGRADE ACTIVITY.TXT

- as AutoUpdate and AutoUpgrade log file, [236](#), [247](#)

updates

- automatic, via AutoUpdate, [232](#) to [252](#)
- recommended method for downloading and distributing, [232](#) to [243](#)

updates and upgrades

- use of anonymous FTP to log into sites for, [239](#), [250](#)
- use of UNC notation to designate, [238](#), [249](#)

updates and upgrades, website address for obtaining, [304](#)

updating strategies for VirusScan software, [229](#)

upgrades

- automatic, via AutoUpgrade, [242](#) to [252](#)

user name, recorded in log file, [113](#), [130](#), [141](#)

V

View Activity Log

- in **File** menu, [186](#), [222](#)
- in **Task** menu, [222](#), [237](#), [248](#)

View menu

- Status Bar**, [196](#)
- Title Bar**, [196](#)
- Toolbar**, [196](#)
- Virus List**, [197](#)

Virus Information Library, connecting to from VirusScan, [76](#) to [77](#)

Virus List

- in **View** menu, [197](#)

- viruses
 - "Brain" virus, [ix](#)
 - boot-sector infectors, [ix to x](#)
 - cleaning, recorded in log file, [113, 130, 141](#)
 - code signatures, use of by, [xi](#)
 - Concept, [xii](#)
 - costs of, [vii to viii](#)
 - current numbers of, [vii](#)
 - deciding when to start scan operations for, [64](#)
 - default response to
 - when E-Mail Scan program component detects, [74 to 75](#)
 - when VirusScan detects, [72 to 74](#)
 - when VShield detects, [67 to 72](#)
 - definition of, [vii](#)
 - detecting, recorded in log file, [113, 130, 141](#)
 - disguising infections of, [xi](#)
 - distinction between hostile objects and, [xiii](#)
 - effects of, [vii, 61 to 75](#)
 - encrypted, definition of, [xi](#)
 - false detections of, understanding, [66](#)
 - file infectors, [x](#)
 - history of, [vii to xiv](#)
 - macro, [xii](#)
 - setting heuristic scanning options for, [105 to 106, 121, 134 to 135, 180 to 182, 213, 262, 276](#)
 - mutating, definition of, [xi](#)
 - origins of, [vii to xiv](#)
 - payload, [ix](#)
 - polymorphic, definition of, [xi](#)
 - programs similar to
 - Trojan horses, [ix](#)
 - worms, [viii](#)
 - recognizing when computer problems do not result from, [65](#)
 - removing
 - before installation, necessity of and steps for, [61](#)
 - from infected files, [61 to 75](#)
 - reporting new strains to McAfee, [xix](#)
 - role of PCs in spread of, [ix](#)
 - script language, [xiv](#)
 - spread of via e-mail and Internet, [xii](#)
 - stealth, definition of, [xi](#)
 - viewing information about, [76 to 77](#)
 - why worry?, [vii to viii](#)
- VirusScan
 - Action options
 - choosing for in Console, [215 to 217](#)
 - configuring in VirusScan Advanced, [182 to 184](#)
 - configuring in VirusScan Classic, [173 to 175](#)
 - Alert options
 - choosing in Console, [218 to 219](#)
 - configuring in Advanced mode, [184 to 185](#)
 - as component of Active Virus Defense suite, [24](#)
 - BIOS anti-virus features, potential conflicts with, [66](#)
 - components included with, [27 to 31](#)
 - configuring for scan operations, [210 to 227](#)
 - control panel
 - choosing options for, [282 to 284](#)
 - opening, [281 to 282](#)
 - understanding, [281](#)

- default responses to virus detection, [72 to 74](#)
 - description of program components, [27 to 31](#)
 - detection options
 - choosing in Console, [211](#)
 - configuring in VirusScan Advanced, [177 to 182](#)
 - distribution methods, [35](#)
 - exclusion options
 - choosing in Console, [222 to 225](#)
 - configuring in VirusScan Advanced, [188 to 190](#)
 - installation
 - as best protection against infection, [61](#)
 - what to do when virus found during, [61](#)
 - introducing, [23](#)
 - logging options, choosing in Console, [219 to 222](#)
 - main window
 - use of to select responses to infections, [73](#)
 - overview of features, [23](#)
 - password protection, configuring, [191](#)
 - property pages
 - Action, [173 to 175](#), [182 to 184](#), [215 to 217](#)
 - Alert, [184 to 188](#), [218 to 219](#)
 - Detection, [177 to 182](#), [211 to 215](#)
 - Exclusion, [188 to 190](#), [222 to 225](#)
 - Report, [185 to 188](#), [219 to 222](#)
 - Security, [225 to 227](#)
 - Where & What, [171 to 173](#)
 - report options
 - choosing in Console, [219 to 222](#)
 - configuring in VirusScan Advanced, [185 to 188](#)
 - security options, choosing in Console, [225 to 227](#)
 - updating via AutoUpdate, [232 to 252](#)
 - upgrading via AutoUpgrade, [242 to 252](#)
 - ways to use, [164](#)
 - what it does, [163](#)
- VirusScan Advanced
- Action options, choosing, [182 to 184](#)
 - Alert options, choosing, [184 to 188](#)
 - Detection options, choosing, [177 to 182](#)
 - Exclusion options, choosing, [188 to 190](#)
 - password protection, configuring, [191](#)
 - Report options, choosing, [185 to 188](#)
 - Security options, choosing, [191](#)
- VirusScan Classic
- Action options, choosing, [173 to 175](#)
 - Report options, choosing, [175 to 176](#)
 - Where & What options, choosing, [171 to 173](#)
- VirusScan Command Line
- use of when booting with Emergency Disk, [62](#)
- VirusScan Console, [196 to 197](#)
- action options for VirusScan, configuring from, [215 to 217](#)
 - alert options for VirusScan, configuring from, [218 to 219](#)
 - configuring tasks in, [196](#), [210 to 227](#)
 - copying and pasting tasks in, [196](#)
 - creating new tasks in, [196](#), [202](#), [206](#)
 - default scan tasks included with, [198](#)
 - deleting tasks from, [196](#)

- detection options for VirusScan,
 - configuring from, 211 to 215
 - disabling and enabling tasks from, 197
 - necessity to have running to start scan tasks, 208
 - overview of, 196 to 197
 - possible applications for, 193
 - purpose of, 193
 - scheduling and enabling tasks in, 196, 206 to 208
 - starting, 194
 - starting tasks from, 197
 - status bar in, hiding and displaying, 196
 - stopping tasks from, 197
 - title bar in, hiding and displaying, 196
 - toolbar in, hiding and displaying, 195
 - window, elements of, 195
- Visual Basic, as macro virus programming language, xii
- VSCLOG.TXT, as VirusScan report file, 175 to 176, 185 to 186, 219 to 271
- VShield
- browsers and e-mail clients supported in, 89
 - components included with VirusScan, 27 to 31
 - configuration wizard
 - starting, 95
 - using, 90, 95 to 99
 - default responses to virus detection, 67 to 72
 - disabling and enabling, 155 to 160
 - Download Scan module
 - configuring, 132 to 142
 - default response options for, 71 to 72
 - E-mail Scan module
 - configuring, 117 to 131
 - default response options for, 70 to 71
 - Internet Filter module
 - configuring, 142 to 151
 - default response options for, 72
 - Properties dialog box
 - Download Scan module, 132 to 142
 - E-mail Scan module, 117 to 131
 - Internet Filter module, 142 to 151
 - Security module, 151 to 154
 - System Scan module, 100 to 106
 - Wizard** button in, 95
 - reasons to run, 88
 - Security module
 - configuring, 151 to 154
 - stopping and unloading from memory, 155 to 160
 - System Scan module
 - configuring, 100 to 117
 - default response options for, 67 to 69
 - unloading from memory, 155 to 160
 - what it does, 87
- VSHLOG.TXT, as VShield report file, 112 to 113
- ## W
- warm boot, ineffective use of to clear viruses, xi
 - WEBEMAIL.TXT, as VShield logging file, 129
 - WEBFLTR.TXT, as VShield logging file, 150 to 151
 - WEBINET.TXT, as VirusScan logging file, 140

- website, Network Associates technical support via, [304](#)
- Where & What options
 - choosing in VirusScan Classic, [171](#) to [173](#)
- why worry about viruses?, [vii](#) to [viii](#)
- window elements, in VirusScan Console, [195](#)
- Wizard, button in VShield Properties dialog box, [95](#)
- Word files, as agents for virus transmission, [xii](#)
- World Wide Web, as source of malicious software, [xii](#) to [xiv](#)
- worms, definition of, [viii](#)