MCAFEE

Total Protection For Your PC

McAfee VirusScan

Administrator’s Guide

Version 5.1

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES, INC. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, McAfee hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

Table of Contents

Preface

Anti-virus protection as information security

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

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

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

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

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

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

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

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

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

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

- W32 / ExploreZip.worm and its variants, which used some of Melissa's techniques to spread, initially through e-mail. After it successfully infected a host machine, ExploreZip searched for unsecured network shares and quietly copied itself throughout a network. It carried a destructive payload that erased various Windows system files and Microsoft Office documents, replacing them with an unrecoverable zero-byte-length files.

- W32 / Pretty.worm, which did Melissa one better by sending itself to *every* entry in the infected computer's MAPI address book. It also connected to an Internet Relay Chat (IRC) server, joined a particular IRC channel, then opened a path to receive commands via the IRC connection. This potentially allowed those on the channel to siphon information from the infected computer, including the computer name and owner's name, his or her dial-up networking user name and password, and the path to the system root directory.

- W32 / FunLove.4099, which infected ActiveX .OCX files, among others. This meant that it could lurk on web pages with ActiveX content, and infect systems with low or nonexistent browser security settings as they downloaded pages to their hard disks. If a Windows NT computer user had logged into a system with administrative rights, the infecting virus would patch two critical system files that gave *all* users on the network —*including* the virus—administrative rights to all files on the target computer. It spread further within the network by attaching itself to files with the extensions .SCR, .OCX, and .EXE.

- VBS / Bubbleboy, a proof-of-concept demonstration that showed that a virus could infect target computers directly from e-mail messages themselves, without needing to propagate through message attachments. It effectively circumvented desktop anti-virus protection altogether, at least initially. Its combination of HTML and VBScript exploited existing vulnerabilities in Internet-enabled mail systems; its author played upon the same end-user psychology that made Melissa successful.

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

Information security as a business necessity

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

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

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

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

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

Active Virus Defense security perimeters

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

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

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

At the desktop: VirusScan software

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

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

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

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

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

- Alert Manager client configuration. VirusScan software includes a client configuration utility you can use to have it pass alert messages directly to Alert Manager servers on your network, to a Centralized Alerting share, or to a Desktop Management Interface administrative application. Other alert methods include local custom messages and beeps, detection alerts and response options, and e-mail alert messages.
- Integration with McAfee VirusScan’s ePolicy Orchestrator management software. Centralized anti-virus management takes a quantum leap forward with this highly scalable management tool. VirusScan software ships with a plug-in library file that works with the ePolicy Orchestrator server to enforce enterprise-wide network security policies.

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

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

McAfee VirusScan's anti-virus research

Even the best anti-virus software is only as good as its latest update. Because as many as 200 to 300 viruses and variants appear each month, the .DAT files that enable McAfee VirusScan's 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 VirusScan's has, however, assembled the world's largest and most experienced anti-virus research staff in its Anti-Virus Emergency Response Team (AVERT)*. This premier anti-virus research organization has a worldwide reach and a "follow the sun" coverage policy, that ensures that you get the files you need to combat new viruses as soon as—and often before—you need them. You can take advantage of many of the direct products of this research by visiting the AVERT research site on the Network Associates website:

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

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

http://www.mcafeeb2b.com/

About VirusScan Software 1

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 VirusScan's 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 VirusScan's 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 Network Associates 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 24.

The new release also adds multiplatform support for Windows 95, Windows 98, Windows ME, 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 VirusScan's 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 VirusScan 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 thatMcAfee VirusScan researchers developed independently for more than a decade.

Fast, accurate virus detection

The foundation for that combination is the unique development environment that McAfee VirusScan 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 VirusScan 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 VirusScan 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.

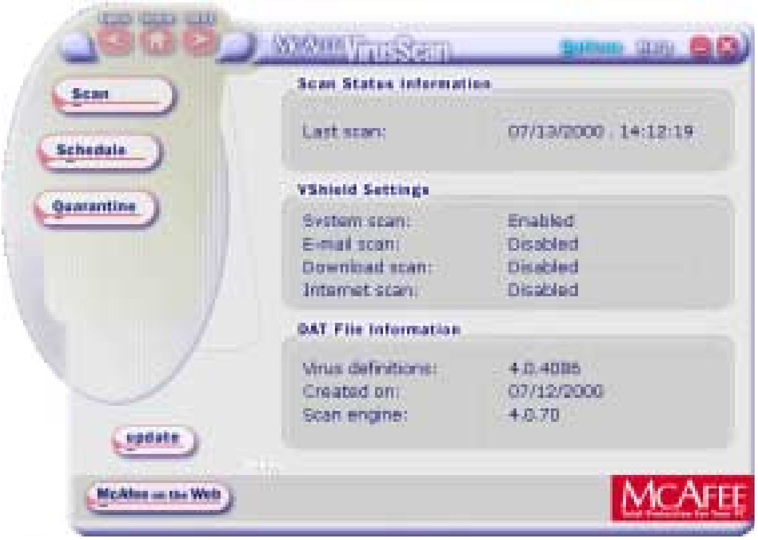
The latest VirusScan software releases, as a consequence, do not simply wait for viruses to appear on your system, they scan proactively at the source or work to deflect hostile agents away from your system. The VShield scanner that comes with VirusScan software has three modules that concentrate on 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 Central.** This is your main entry point in using all of the available components of McAfee VirusScan. This home screen (see Figure 1-2) provides relevant information such as the last time a virus scan was performed on your computer; what VShield settings are enabled or disabled and available DAT information and when it was created.



Scan Status information

Last scan: 07/13/2000 , 14:12:19

VShield Settings

System scan: Enabled
E-mail scan: Disabled
Download scan: Disabled
Internet scan: Disabled

DAT File information

Virus definitions: 4.0.4085
Created on: 07/12/2000
Scan engine: 4.0.70

Figure 1-1. McAfee VirusScan Central screen

- **The VirusScan Console**. This component allows you to create, configure and run VirusScan tasks at times you specify. A “task” can include anything from running a scan operation on a set of disks at a specific time or interval, to running an update or upgrade operation. You can also enable or disable the VShield scanner from the Console window.

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

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

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

- **Safe & Sound**. This component allows you to create backup sets in protected volume files, which is the safest and preferred type of backup. A *protected volume file* is a sectioned-off area of the drive, sometimes called a logical drive.

NOTE: Safe & Sound is only available for Windows 95, 98 and Windows ME. For more information, access the PDF formatted file of the User's Guide (i.e., vscan51_userguide.pdf) included in the McAfee VirusScan CD-ROM and read "About Safe & Sound".

- **Quarantine**. This component allows you to move infected files to a quarantine folder. This moves infected files from areas where they can be accessed and enables you to clean or delete them at your convenience.

NOTE: For more information, access the PDF formatted file of the User's Guide (i.e., vscan51_userguide.pdf) included in the McAfee VirusScan CD-ROM and read "About Quarantine".

- **The E-Mail Scan extension**. This component allows you to scan your Microsoft Exchange or Outlook mailbox, or public folders to which you have access, directly on the server. This invaluable "x-ray" peek into your mailbox means that VirusScan software can find potential infections before they make their way to your desktop, which can stop a Melissa-like virus in its tracks.
- **A cc:Mail scanner**. This component includes technology optimized for scanning Lotus cc:Mail mailboxes that do not use the MAPI standard. Install and use this component if your workgroup or network uses cc:Mail v7.x or earlier.

- **The Alert Manager Client configuration utility**. This component lets you choose a destination for Alert Manager "events" that VirusScan software generates when it detects a virus or takes other noteworthy actions. You can also specify a destination directory for older-style Centralized Alerting messages, or supplement either method with Desktop Management Interface (DMI) alerts sent via your DMI client software.

- **The ScreenScan utility**. This optional component scans your computer as your screen saver runs during idle periods.

- **The SendVirus utility**. This component gives you an easy and painless way to submit files that you believe are infected directly to McAfee VirusScan's anti-virus researchers. A simple wizard guides you as you choose files to submit, include contact details and, if you prefer, strip out any personal or confidential data from document files.

- **The Emergency Disk creation utility**. This essential utility helps you to create a floppy disk that you can use to boot your computer into a virus-free environment, then scan essential system areas to remove any viruses that could load at startup.

- **Command-line scanners**. This component consists of a set of full-featured scanners you can use to run targeted scan operations from the MS-DOS Prompt or Command Prompt windows, or from protected MS-DOS mode. The set includes:

  - SCAN.EXE, a scanner for 32-bit environments only. This is the primary command-line interface. When you run this file, it first checks its environment to see whether it can run by itself. If your computer is running in 16-bit or protected mode, it will transfer control to one of the other scanners.

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

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

  - BOOTSCAN.EXE, a smaller, specialized scanner for use primarily with the Emergency Disk utility. This scanner ordinarily runs from a floppy disk you create to provide you with a virus-free boot environment.

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

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

- **Documentation.** VirusScan software documentation includes:
  - A printed *Getting Started Guide*, which introduces the product, provides installation instructions, outlines how to respond if you suspect your computer has a virus, and provides a brief product overview. The printed *Getting Started Guide* comes with the VirusScan software copies distributed on CD-ROM discs—you can also download it as vs51_getstart.PDF from Network Associates website or from other electronic services.
  - A 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 a vscan51_userguide.PDF file 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.
  - This 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 vs51_admin.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 17, 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 VirusScan's 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 Network Associates 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*.

Interface enhancements

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

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

- New VShield system tray icon states tell you more about which VShield modules are active. These states are:
  - All VShield modules are active
  - The System Scan module is active, but one or more of the other VShield modules is inactive
  - The System Scan module is inactive, but one or more of the other VShield modules is active
  - All VShield modules are inactive
- New interface settings for task configuration allow you to tell the VirusScan application how you want it to appear as your scheduled task runs and what you want it to do when it finishes. You can also set a password to protect individual task settings from changes, or to protect an entire task configuration at once.

- An updated randomization feature for scheduled tasks allows you to set a time for the task to run, then set a randomization “window.” The VirusScan Console then picks a random time within the window to actually start the task.
- System Scan module action options now include a new Prompt Type configuration option for Windows 95 and Windows 98 systems. This option lets you determine how the **Prompt for user action** alert appears.

Changes in product functionality

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

New update options for your VirusScan software

Even with the majority of the virus definitions it requires now incorporated directly into its engine in generic routines, VirusScan software still requires regular .DAT file updates to keep pace with the 200 to 300 new viruses that appear each month. To meet this need, McAfee VirusScan 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.

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.

NOTE: For more information, access the PDF formatted file of the User’s Guide (i.e., vscan51_userguide.pdf) included in the McAfee VirusScan CD-ROM and read “Using the SecureCast Service to Get New Data Files.”

Installing VirusScan Software 2

Before you begin

McAfee VirusScan Software distributes VirusScan software in two ways: 1) as an archived file that you can download from the McAfee Web site; 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 to verify that VirusScan software will run on your system.

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 VirusScan Software 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 VirusScan Software recommends 75MB.
- At least 16MB of free random-access memory (RAM). McAfee VirusScan Software recommends at least 20MB.
- Microsoft Windows 95, Windows 98, Windows ME, Windows NT Workstation v4.0 with Service Pack 4 or later, or Windows 2000 Professional. McAfee VirusScan Software 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 via a high-speed modem and an Internet service provider.

Preparing to install VirusScan software

After inserting the McAfee VirusScan on your CD-ROM drive , you should see a VirusScan welcome image appear automatically. To install VirusScan software immediately, click **Install VirusScan**, then skip to Step 4 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.

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.

Installation steps

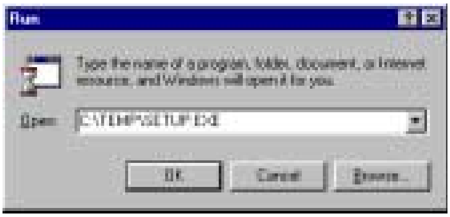
McAfee VirusScan Software recommends that you first quit all other applications you have running on your system before you start Setup. Doing so reduces the possibility that software conflicts will interfere with your installation.

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).



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: C:\TEMP\SETUP.EXE

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**.

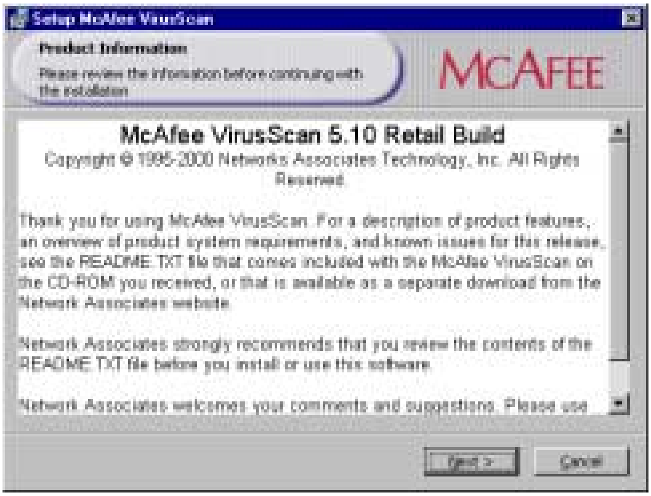
   ❑ **NOTE:** If your VirusScan software copy came on an Active Virus Defense or a Total Virus Defense CD-ROM, you must also specify which folder contains the VirusScan software.

   Before it continues with the installation, Setup first 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, this 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. In either of these cases, Setup will display its first wizard panel immediately. Skip to Step 4 to continue.

   If Setup does not find MSI v1.1 on your computer, it installs files it needs to continue the installation, then prompts you to restart your computer. Click **Restart System**.

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



Product Information

Please review the information before continuing with the installation

McAfee VirusScan 5.10 Retail Build

Copyright © 1995-2000 Networks Associates Technology, Inc. All Rights Reserved.

Thank you for using McAfee VirusScan. For a description of product features, an overview of product system requirements, and known issues for this release, see the README.TXT file that comes included with the McAfee VirusScan on the CD-ROM you received, or that is available as a separate download from the Network Associates website.

Network Associates strongly recommends that you review the contents of the README.TXT file before you install or use this software.

Network Associates welcomes your comments and suggestions. Please use

Figure 2-2. Setup welcome panel

4. 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.

5. 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 previous VirusScan versions or incompatible software exists on your computer. If you have no other anti-virus software or any previous VirusScan versions on your system, it will display the Security Type or the Setup Type panel. Skip to Step 8 to continue.

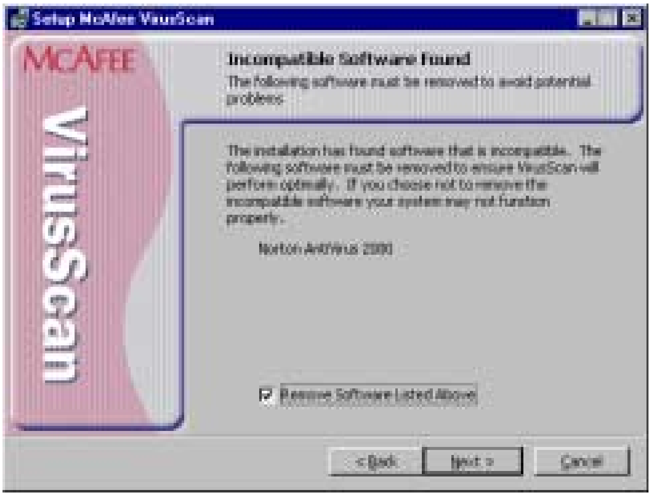
   If Setup discovers an earlier VirusScan version on your system, it will tell you that it must remove that earlier version. If your computer runs Windows 95 or Windows 98, Setup also gives you the option to preserve the VShield configuration settings you chose for the earlier version.

   If your computer runs Windows NT Workstation v4.0 or Windows 2000 Professional, Setup will remove the previous VirusScan version, but will *not* preserve any previous VShield scanner settings.

6. 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.

   If you have no incompatible software on your system and your computer runs Windows 95 or Windows 98, skip to Step 9 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 8 to continue. Otherwise, continue with Step 7.



The following software must be removed to avoid potential problems.

The installation has found software that is incompatible. The following software must be removed to ensure VirusScan will perform optimally. If you choose not to remove the incompatible software your system may not function properly.

Norton AntiVirus 2000

☑ Remove Software Listed Above

Figure 2-3. Incompatible software panel

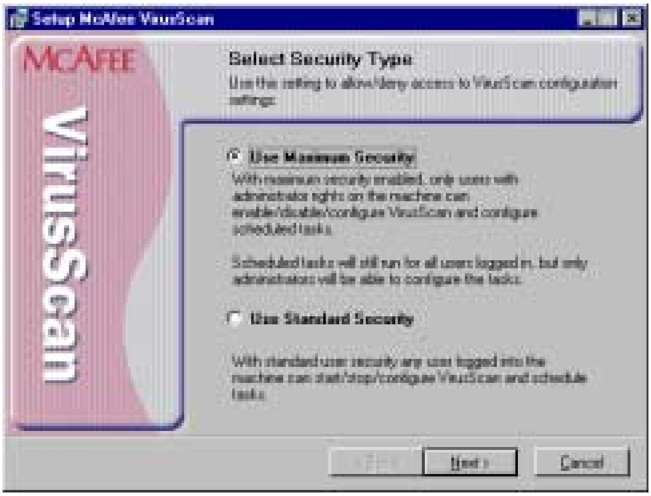
7. Select the checkbox shown, then click **Next>**. Setup will start the uninstallation utility that the conflicting software normally uses, and allow it to remove the software. The uninstallation utility might tell you that you need to restart your computer to completely remove the other software. You 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 VirusScan Software 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.

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.



Select Security Type

Use this setting to allow/deny access to VirusScan configuration settings.

● Use Maximum Security

With maximum security enabled, only users with administrator rights on the machine can enable/disable/configure VirusScan and configure scheduled tasks.

Scheduled tasks will still run for all users logged in, but only administrators will be able to configure the tasks.

○ Use Standard Security

With standard user security any user logged into the machine can start/stop/configure VirusScan and schedule tasks.

Figure 2-4. Security Type panel

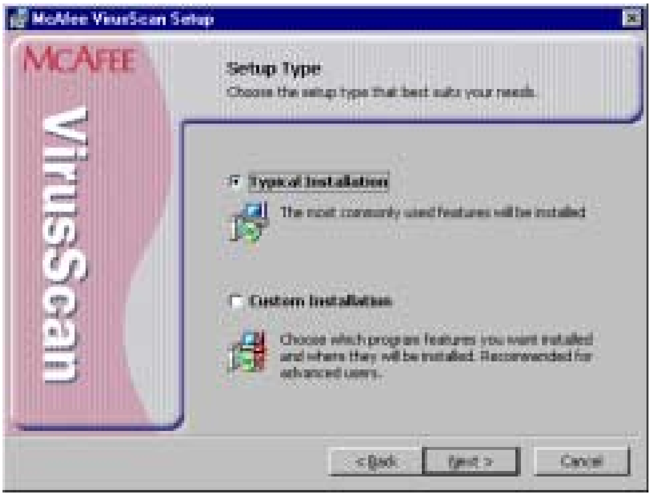
8. Select the security mode you prefer. Your choices are:

   - **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.

- **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 2-4).



McAfee VirusScan Setup

Setup Type

Choose the setup type that best suits your needs.

● Typical Installation

The most commonly used features will be installed

○ Custom Installation

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

Figure 2-5. Setup Type panel

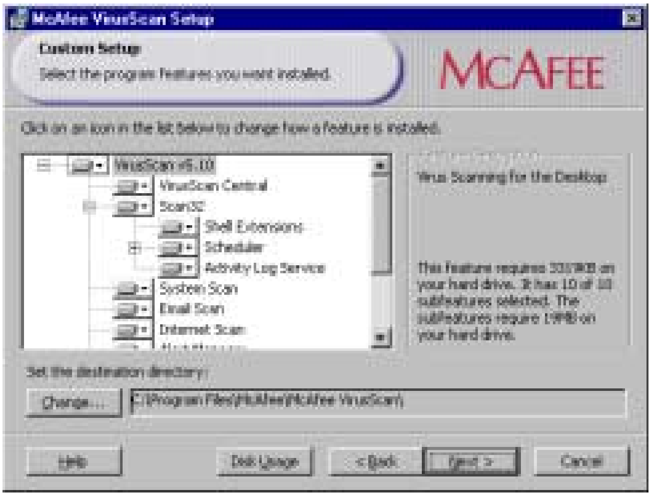
9. Choose the Setup Type you prefer. Your choices are:

   - **Typical Installation**. This option installs all available features contained in the McAfee VirusScan product.

   - **Custom Installation**. This option allows you to customized McAfee VirusScan by only selecting specific features of the product to be installed on your computer.

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

    If you chose **Custom Setup**, you'll see the panel shown in Figure 2-5. Otherwise, skip to Step 13 to continue with your installation.



McAfee VirusScan Setup

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- VirusScan v5.10
  - VirusScan Central
  - Scan32
    - Shell Extensions
    - Scheduler
    - Activity Log Service
  - System Scan
  - Email Scan
  - Internet Scan

Virus Scanning for the Desktop

This feature requires 3319KB on your hard drive. It has 10 of 10 subfeatures selected. The subfeatures require 19MB on your hard drive.

Set the destination directory:

C:\Program Files\McAfee\McAfee VirusScan\

Figure 2-6. Custom Setup panel

11. 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.

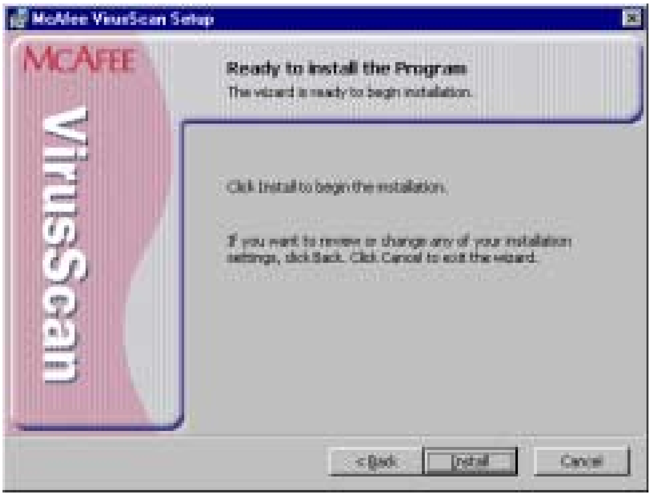
    - Remove a component from the installation. Click ▭ ▾ beside a component name, then choose ✕ **This feature will not be available** from the menu that appears.

    ❒ **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.

12. 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 2-6).



McAfee VirusScan Setup

Ready to Install the Program

The wizard is ready to begin installation.

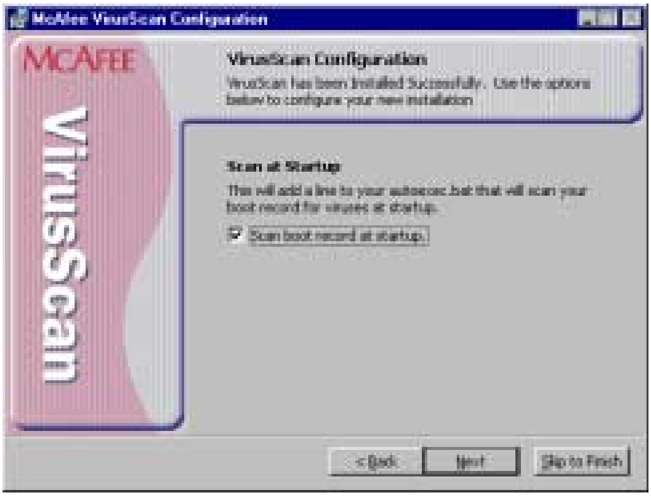
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Figure 2-7. Ready to Install panel

13. 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 previous VirusScan versions or incompatible software from your system, 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 2-8).



McAfee VirusScan Configuration

VirusScan Configuration

VirusScan has been Installed Successfully. Use the options below to configure your new installation

Scan at Startup

This will add a line to your autoexec.bat that will scan your boot record for viruses at startup.

☑ Scan boot record at startup.

Figure 2-8. VirusScan Configuration panel

14. From the VirusScan Configuration panel (Figure 2-8), you can skip configuration to finish installation, or you can select to configure the available options displayed.

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

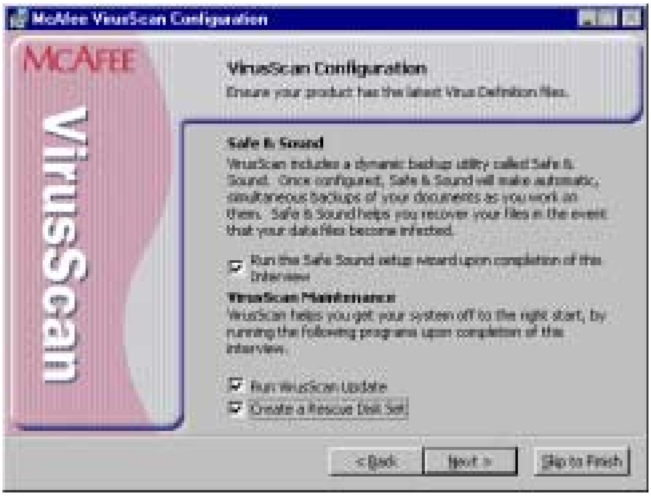
      ```
      C:\PROGRA~1\COMMON~1\NETWOR~1\VIRUSS~1\40~1.XX\SCAN
      .EXE C:\
      @IF ERRORLEVEL 1 PAUSE
      ```

      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.

      If your computer runs Windows NT Workstation v4.0, Windows ME 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, Windows ME, 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.

15. The next set of screens will display options that will allow you to run other components of McAfee VirusScan such as running the Safe & Sound utility, the VirusScan update, and the Rescue Disk (Figure 2-9).

NOTE: Safe & Sound utility will not be available when installing in Windows NT or Windows 2000.



VirusScan Configuration

Ensure your product has the latest Virus Definition files.

Safe & Sound

VirusScan includes a dynamic backup utility called Safe & Sound. Once configured, Safe & Sound will make automatic, simultaneous backups of your documents as you work on them. Safe & Sound helps you recover your files in the event that your data files become infected.

☑ Run the Safe Sound setup wizard upon completion of this Interview

VirusScan Maintenance

VirusScan helps you get your system off to the right start, by running the following programs upon completion of this interview.

☑ Run VirusScan Update

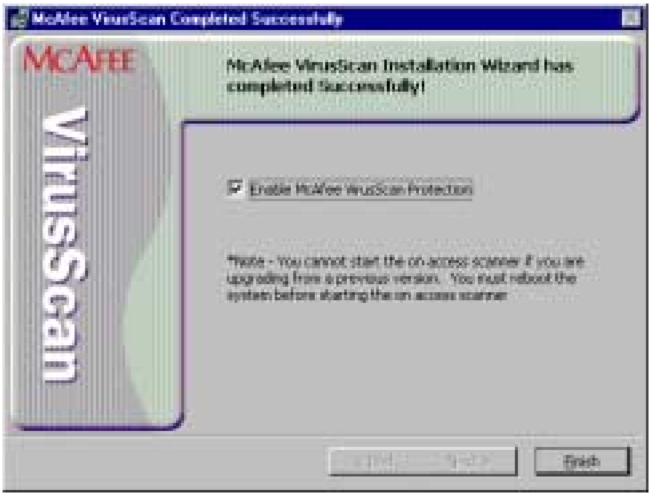
☑ Create a Rescue Disk Set

Figure 2-9. Configuration panel

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.

NOTE: For more information on any of these options, you can refer to the online Help of McAfee VirusScan.

16. In the next screen (Figure 2-10), select the **Enable McAfee VirusScan Protection** 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.



McAfee VirusScan Completed Successfully

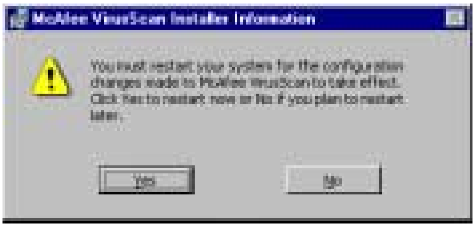
McAfee VirusScan Installation Wizard has completed Successfully!

☑ Enable McAfee VirusScan Protection

*Note - You cannot start the on-access scanner if you are upgrading from a previous version. You must reboot the system before starting the on access scanner

Figure 2-10. Successful Installation panel

17. After you click Finish, the McAfee VirusScan Installer Information dialog box is displayed where you will be prompted to restart your computer (Figure 2-11).



McAfee VirusScan Installer Information

You must restart your system for the configuration changes made to McAfee VirusScan to take effect. Click Yes to restart now or No if you plan to restart later.

Figure 2-11. McAfee VirusScan Installer Information dialog box

NOTE: If you had a previous VirusScan version installed on your computer, you must restart your system in order to start the VShield scanner. Click Yes to restart your computer.

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. You can also start the Emergency Disk wizard at any point after you install VirusScan software.

NOTE: McAfee VirusScan 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\McAfee VirusScan\VirusScan Engine\4.0.xx

The special .DAT files have these names:

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

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

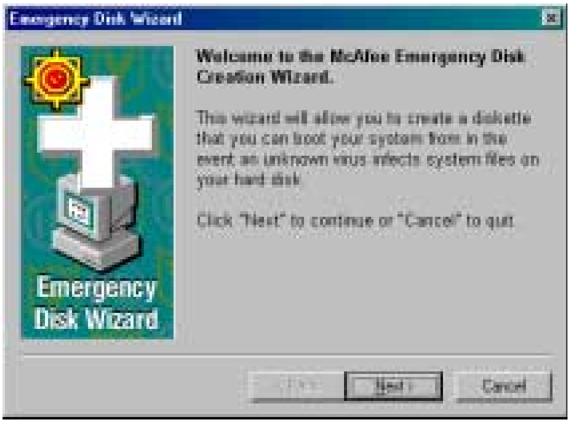
http://www.nai.com/asp_set/anti_virus/avert/tools.asp

NOTE: McAfee VirusScan Software 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 after installation, click **Start** in the Windows taskbar, point to **Programs**, then to **McAfee VirusScan**. Next, choose **Create Emergency Disk**.

The Emergency Disk wizard welcome panel will appear (Figure 2-9).



Welcome to the McAfee Emergency Disk Creation Wizard.

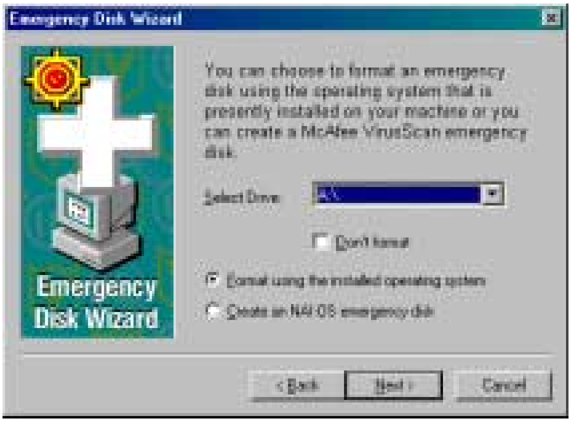
This wizard will allow you to create a diskette that you can boot your system from in the event an unknown virus infects system files on your hard disk.

Click "Next" to continue or "Cancel" to quit.

Figure 2-12. Emergency Disk welcome panel

1. Click **Next>** to continue.

   The next wizard panel appears (Figure 2-10).



You can choose to format an emergency disk using the operating system that is presently installed on your machine or you can create a McAfee VirusScan emergency disk.

Select Drive: A:\

□ Don't format

● Format using the installed operating system

○ Create an NAI OS emergency disk

Figure 2-13. 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 proprietary 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 single 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:

   - If you chose to format your disk with the NAI-OS, the wizard displays an informational panel.

     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 *VirusScan 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.

     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 to continue.

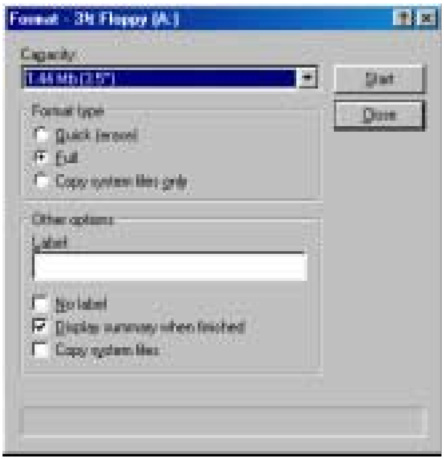
   - If you do *not* have a virus-free floppy disk formatted with DOS or Windows system files, you must create one in order to use the Emergency Disk to start your computer. Follow these substeps:

a. Insert an unlocked and unformatted floppy disk into your floppy drive. McAfee VirusScan Software 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 2-11).



Format - 3½ Floppy (A:)

Capacity: 1.44 Mb (3.5")

Format type

○ Quick (erase)
● Full
○ Copy system files only

Other options

Label:

□ No label
☑ Display summary when finished
□ Copy system files

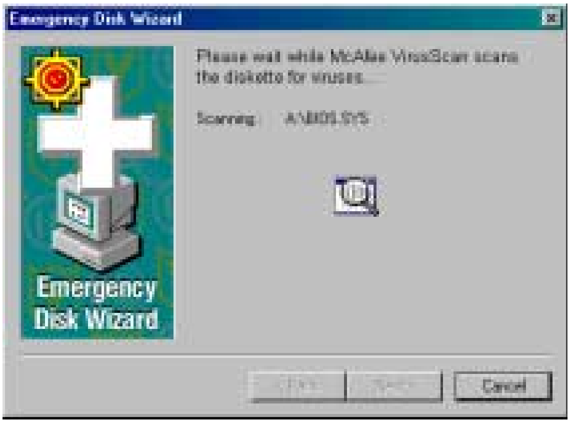
Figure 2-14. Windows Format dialog box

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 2-12).



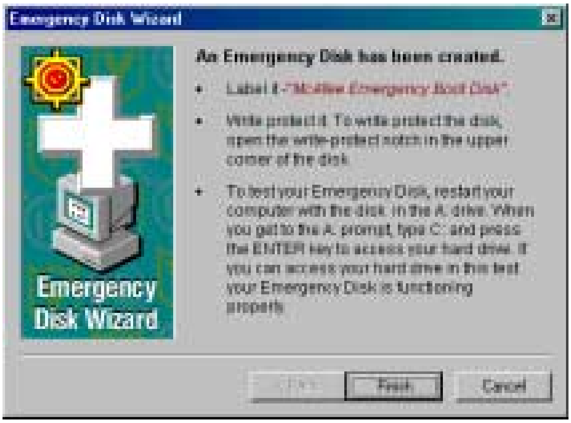
Please wait while McAfee VirusScan scans the diskette for viruses...

Scanning: A:\BIOS.SYS

Figure 2-15. 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.

4. When the wizard finishes copying the Emergency Disk files, it displays the final wizard panel (Figure 2-13).



An Emergency Disk has been created.

- Label it "McAfee Emergency Boot Disk"
- Write protect it. To write protect the disk, open the write-protect notch in the upper corner of the disk.
- To test your Emergency Disk, restart your computer with the disk in the A: drive. When you get to the A: prompt, type C: and press the ENTER key to access your hard drive. If you can access your hard drive in this test your Emergency Disk is functioning properly.

Figure 2-16. Final Emergency Disk panel

5. Click **Finish** to quit the wizard. Next, remove the new Emergency Disk from your floppy drive, label it, 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 VirusScan Software 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 which circumstances require you to 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 VirusScan 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 v5.1** in the list, then click **Add/Remove**.

Setup will start and display the first Maintenance wizard panel.

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

   Setup displays the Program Maintenance wizard panel. 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. Start with Step 11 to choose the components you want to add or remove.

     ❐ **NOTE:** This particular panel 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. 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.

If the VirusScan application detects a virus during Setup, you’ll need to remove it from your system before you install the program.

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.

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 VirusScan Software 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

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 VirusScan 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.

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 McAfee 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 McAfee 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. Because each module detects different objects or scans different virus entry points, each has a different set of default responses.

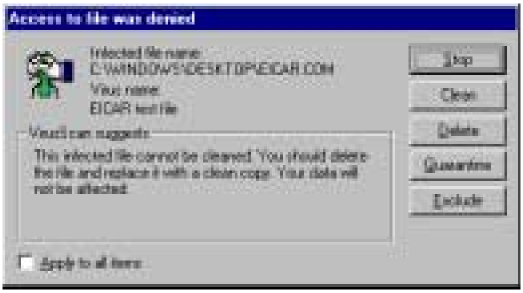
Responding when the System Scan module detects a virus

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

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

Because it scans files this way, the System Scan module can serve as a backup in case any of the other VShield modules does not detect a virus when it first enters your system. In its initial configuration, the module will deny access to any infected file it finds, whichever Windows version your computer runs. It will also display an alert message that asks you what you want to do about the virus (see Figure 3-11). 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.



Access to file was denied

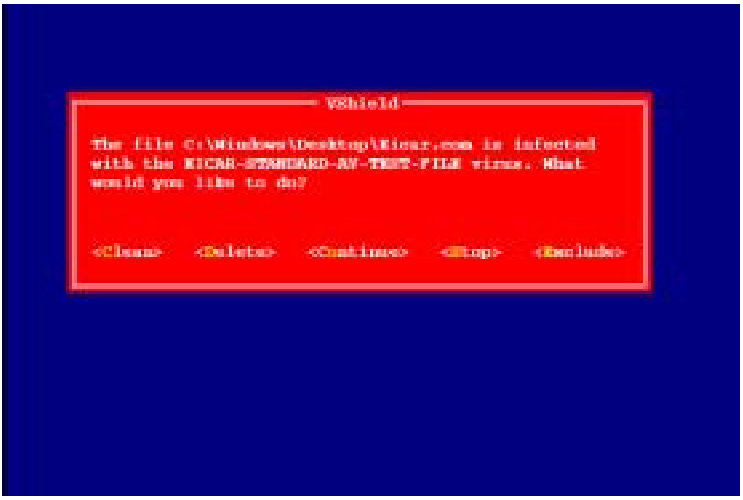
Infected file name:
C:\WINDOWS\DESKTOP\EICAR.COM
Virus name:
EICAR test file

VirusScan suggests:
This infected file cannot be cleaned. You should delete the file and replace it with a clean copy. Your data will not be affected.

□ Apply to all items

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.



VShield

The file C:\Windows\Desktop\Eicar.com is infected with the EICAR-STANDARD-AV-TEST-FILE virus. What would you like to do?

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.

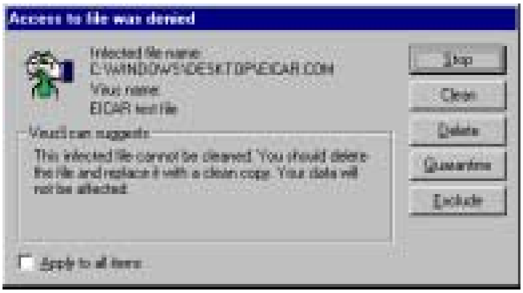
- **Stop the scan operation.** Click **Stop** in the dialog box, or type S when you see the full-screen warning, to tell the System Scan module to deny any access to the file but not to take any other action. Denying access to the file prevents anyone from opening, saving, copying or renaming it. To 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

NOTE: This feature only applies to exchange server e-mails.

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.



Access to file was denied

Infected file name:
C:\WINDOWS\DESKTOP\EICAR.COM
Virus name:
EICAR test file

VirusScan suggests:
This infected file cannot be cleaned. You should delete the file and replace it with a clean copy. Your data will not be affected.

□ Apply to all items

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.

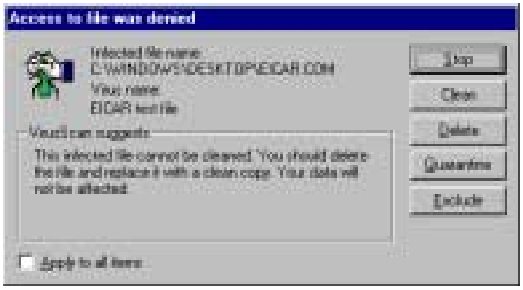
- **Exclude**. Click this button to prevent the E-Mail Scan module from flagging this file as a virus in future scan operations. If you copy this file to your hard disk, this also prevents the System Scan module from detecting the file as a virus.

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. A fourth option provides you with additional information.



Access to file was denied

Infected file name:
C:\WINDOWS\DESKTOP\EICAR.COM
Virus name:
EICAR test file

VirusScan suggests:
This infected file cannot be cleaned. You should delete the file and replace it with a clean copy. Your data will not be affected.

☐ Apply to all items

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.

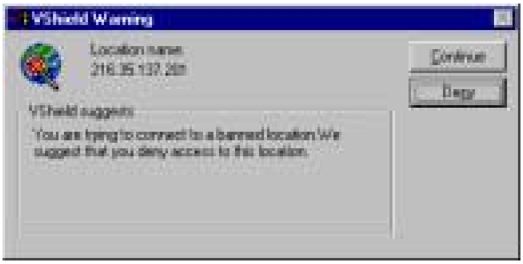
- **Delete**. Click this to tell the Download Scan module to delete the infected file or e-mail attachment you received. By default, the module notes the name of the infected file in its log file.

- **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.



Location name:
216.35.137.201

VShield suggests:

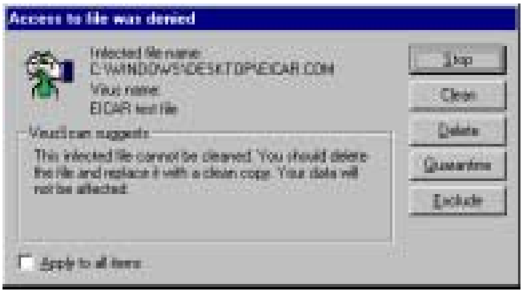
You are trying to connect to a banned location. We suggest that you deny access to this location.

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.


Access to file was denied

Infected file name:
C:\WINDOWS\DESKTOP\EICAR.COM
Virus name:
EICAR test file

VirusScan suggests:
This infected file cannot be cleaned. You should delete the file and replace it with a clean copy. Your data will not be affected.

☐ Apply to all items

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, 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.

Access to file was denied

Infected file name:
C:\WINDOWS\DESKTOP\EICAR.COM
Virus name:
EICAR test file

VirusScan suggests:
This infected file cannot be cleaned. You should delete the file and replace it with a clean copy. Your data will not be affected.

☐ Apply to all items

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 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.

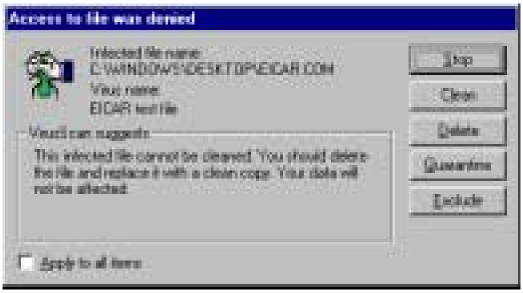
- **Clean.** Click this button to have the VirusScan application try to remove the virus code from the infected file. If it cannot clean the file—either because it has no remover or because the virus has damaged the file beyond repair—it will record the incident in its log file and suggest alternative responses.

  In the example shown in Figure 3-6, 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 McAfee Virus Information Library. This choice does not take any action against the virus that the application detected.

Responding when the E-Mail Scan extension detects a virus

NOTE: This feature only applies to exchange server e-mails.

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.



Access to file was denied

Infected file name:
C:\WINDOWS\DESKTOP\EICAR.COM
Virus name:
EICAR test file

VirusScan suggests:
This infected file cannot be cleaned. You should delete the file and replace it with a clean copy. Your data will not be affected.

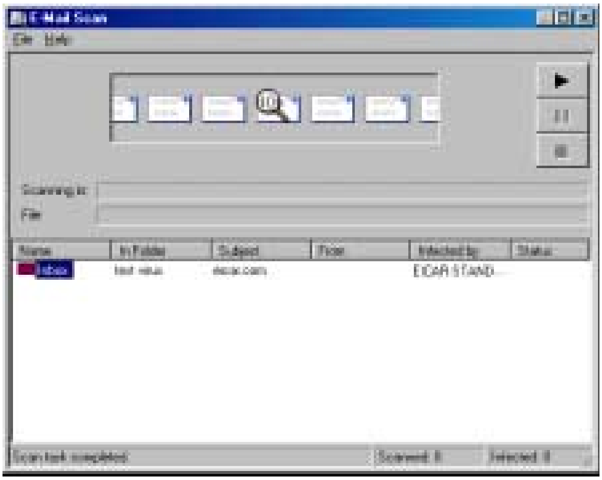
□ Apply to all items

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, 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 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.



Name	In Folder	Subject	From	Infected by	Status
Inbox	test virus	eicar.com		EICAR STAND...	

Scan task completed | Scanned: 8 | Infected: 8

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, **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 McAfee Virus Information Library. This choice does not cause the E-Mail Scan extension to take any action against the virus it detected.

Viewing virus information

Clicking **Info** in any of the virus response dialog boxes will connect you to the McAfee online Virus Information Library, provided you have an Internet connection and web browsing software available on your computer.

Figure 3-10. McAfee 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.

The Library is part of the 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.

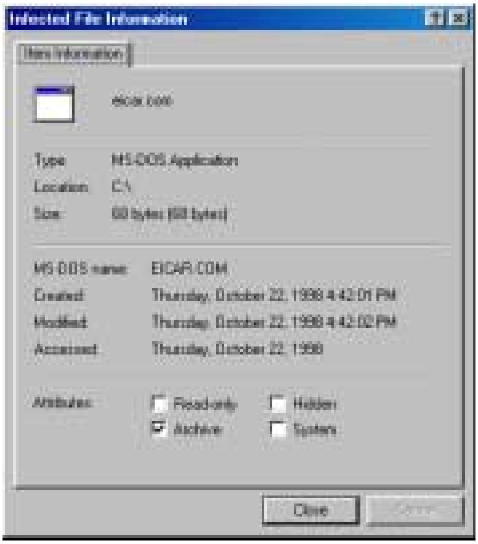
Examples include:

- Current information and risk assessments on emerging and active virus threats
- Software tools you can use to extend or supplement your McAfee VirusScan's 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), 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.



eicar.com

Type: MS-DOS Application
Location: C:\
Size: 68 bytes (68 bytes)

MS-DOS name: EICAR.COM
Created: Thursday, October 22, 1998 4:42:01 PM
Modified: Thursday, October 22, 1998 4:42:02 PM
Accessed: Thursday, October 22, 1998

Attributes: □ Read-only □ Hidden ☑ Archive □ System

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 VirusScan Software 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.

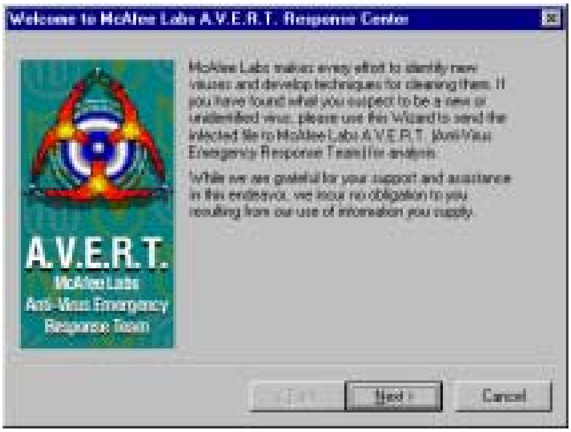
Using the SendVirus utility to submit a file sample

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 VirusScan 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\McAfee\VirusScan
3. Double-click the file to display the first AVERT Labs Response Center wizard panel.



Welcome to McAfee Labs A.V.E.R.T. Response Center

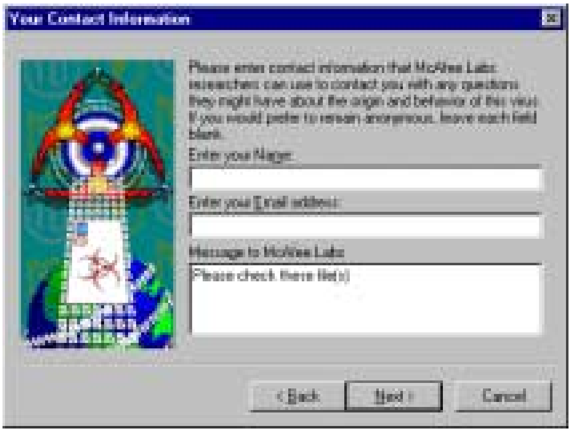
McAfee Labs makes every effort to identify new viruses and develop techniques for cleaning them. If you have found what you suspect to be a new or unidentified virus, please use this Wizard to send the infected file to McAfee Labs A.V.E.R.T. (Anti-Virus Emergency Response Team) for analysis.

While we are grateful for your support and assistance in this endeavor, we incur no obligation to you resulting from our use of information you supply.

Figure 3-12. First SENDVIR.EXE panel

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

   The Contact Information wizard panel appears.



Your Contact Information

Please enter contact information that McAfee Labs researchers can use to contact you with any questions they might have about the origin and behavior of this virus. If you would prefer to remain anonymous, leave each field blank.

Enter your Name:

Enter your Email address:

Message to McAfee Labs:

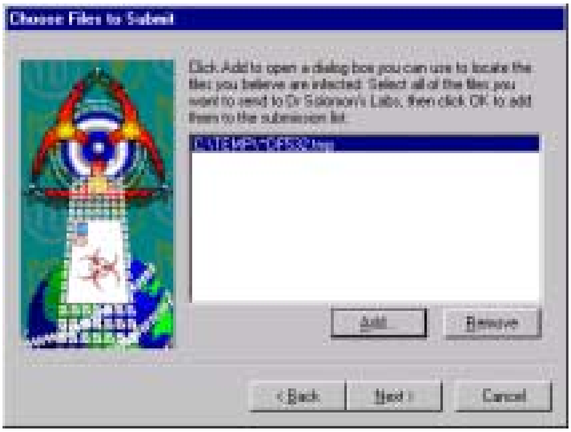
Please check these file(s)

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.



Choose Files to Submit

Click Add to open a dialog box you can use to locate the files you believe are infected. Select all of the files you want to send to Dr Solomon's Labs, then click OK to add them to the submission list.

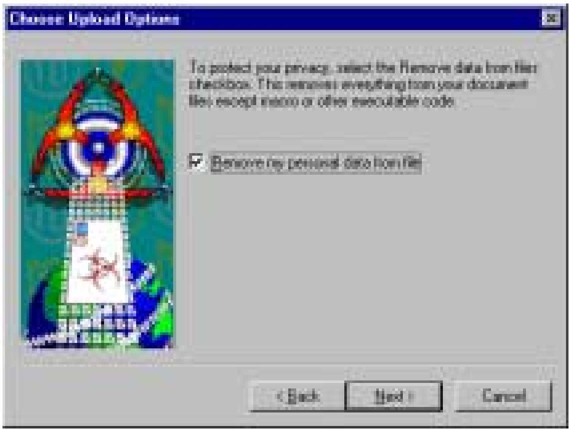
C:\TEMP\~DF532.tmp

Figure 3-14. Choose Files to Submit panel

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

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

The Choose Upload Options panel appears.



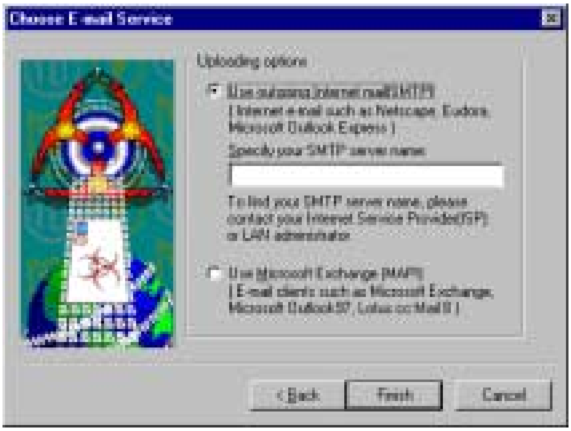
To protect your privacy, select the Remove data from files checkbox. This removes everything from your document files except macro or other executable code.

☑ Remove my personal data from file

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.



Uploading options

● Use outgoing Internet mail(SMTP)
(Internet e-mail such as Netscape, Eudora, Microsoft Outlook Express)

Specify your SMTP server name

To find your SMTP server name, please contact your Internet Service Provider(ISP) or LAN administrator

○ Use Microsoft Exchange (MAPI)
(E-mail clients such as Microsoft Exchange, Microsoft Outlook97, Lotus ccMail8)

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 VirusScan 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-infecting, 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 VirusScan's anti-virus researchers. The researchers would also benefit from having samples of your 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-infecting or macro viruses

If you suspect you have a file-infecting virus or a macro virus that has infected any of your Microsoft Word, Excel, or PowerPoint files, send these files to McAfee VirusScan’s 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 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 VirusScan’s 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 VirusScan's 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 VirusScan researchers at one of these e-mail addresses:

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

In your message, include this information:

- Which symptoms cause you to suspect that your machine is infected
- Which product and version number detected the virus, if any did, and what the results were
- Your VirusScan and .DAT file version numbers

- Details about your system that might help to reproduce the environment in which you detected the virus
- Your name, company name, phone number, and e-mail address, if possible
- A list of all items contained in the package you are sending

Mailing infected floppy disks

You can also mail the actual disks you created directly to McAfee VirusScan anti-virus researchers. McAfee VirusScan Software 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 Toranomon Mori-bldg. 33
3-8-21 Toranomon, 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: AVERT Labs does keep all submitted samples, but once you submit a sample, AVERT cannot return it to you. AVERT does not accept or process Iomega Ditto or Jazz cartridges, Iomega Zip disks, or other types of removable media.

Using VirusScan Software 4

Using the VShield scanner

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

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

To learn how to configure VShield properties and how to start and stop the VShield scanner, see the Using the VShield Scanner sectiion in the McAfee VirusScan User’s Guide.

Using the VirusScan application

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

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

To learn how to configure VirusScan properties and how to start and stop VirusScan software, see the Using the VirusScan application section in the McAfee VirusScan User’s Guide.

Scheduling scan tasks

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

To learn how to configure VirusScan Console properties, see the Creating and Configuring Scheduled Tasks section in the McAfee VirusScan User's Guide.

Using specialized scanning tools

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

To learn how to configure the E-Mail Scan extension and other specialized scanners, see the Using Specialized Scanning Tools section in the McAfee VirusScan User's Guide.

Sending Alert Messages 5

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 v5.1 anti-virus product series, the Alert Manager server now comes as an independent package bundled with McAfee NetShield anti-virus software. You can install this new Alert Manager server together with NetShield software, or by itself on a computer that you want to use as an alert collection point.

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

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

VirusScan software as an Alert Manager Client

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

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

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

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

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

Configuring the Alert Manager Client utility

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

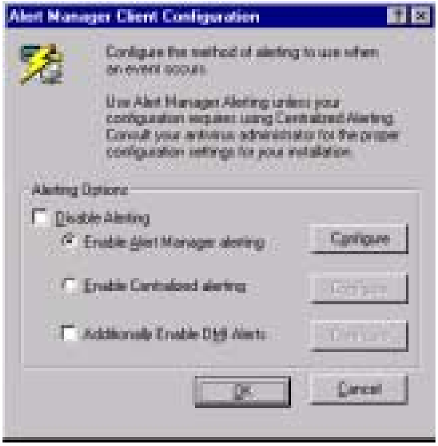
Setting up a complete alert system is a two-part process: First, you must enable the Alert Manager Client Configuration utility and point it to the correct Alert Manager server or Centralized Alerting location. Next, you must verify that you have selected the **Notify Alert Manager** checkbox in the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

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

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

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

   The Alert Manager Client Configuration page appears.



Alert Manager Client Configuration

Configure the method of alerting to use when an event occurs.

Use Alert Manager Alerting unless your configuration requires using Centralized Alerting. Consult your antivirus administrator for the proper configuration settings for your installation.

Alerting Options

□ Disable Alerting

● Enable Alert Manager alerting

○ Enable Centralized alerting

□ Additionally Enable DMI Alerts

Figure 5-1. Alert Manager Client Configuration dialog box

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

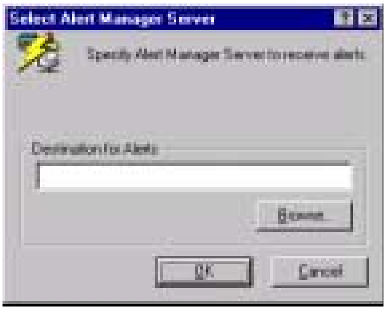
   Select this checkbox only if you want the Alert Manager Client Configuration utility *not* to pass alert messages from your anti-virus software to the Alert Manager server or to your Desktop Management Interface (DMI) administrative software. By default, this checkbox is clear. McAfee recommends that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

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

3. Select the alerting method you want to use. Your choices are:

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

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



Select Alert Manager Server

Specify Alert Manager Server to receive alerts.

Figure 5-2. Select Alert Manager Server dialog box

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

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

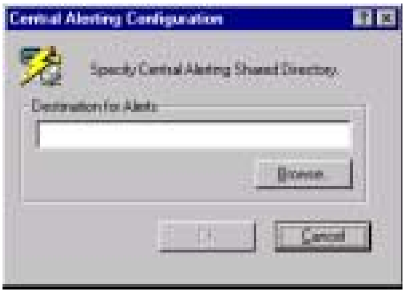
If you have Active Directory Services installed on your computer, clicking Browse displays a list of logical Alert Manager server names. If you do not have Active Directory installed, the display will show your entire directory tree. In that case, consult your system administrator to learn which computer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

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

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

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

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



Specify Central Alerting Shared Directory.

Figure 5-3. Central Alerting Configuration dialog box

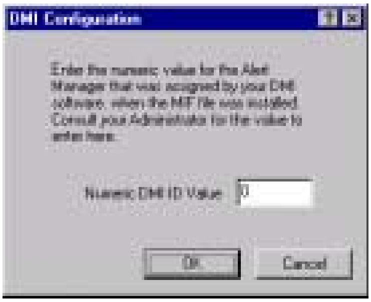
Next, enter the path to the Centralized Alerting directory you want to use, or click **Browse** to locate the directory on your network. When you've chosen a destination, click **OK** to close the dialog box.

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

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

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

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



Enter the numeric value for the Alert Manager that was assigned by your DMI software, when the MIF file was installed. Consult your Administrator for the value to enter here.

Numeric DMI ID Value: 0

Figure 5-4. DMI Configuration dialog box

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

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

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

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

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

Using VirusScan Administrative Utilities

A

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 VirusScan Software 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.

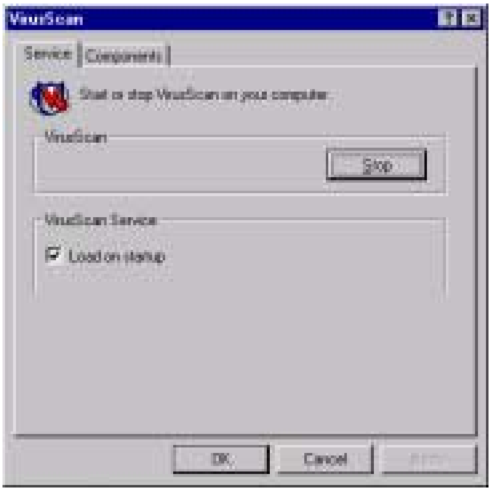
Opening the VirusScan control panel

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.



Start or stop VirusScan on your computer.

☑ Load on startup

Figure A-1. VirusScan control panel - Service page

Choosing VirusScan control panel options

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

To choose your options, follow these steps:

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

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

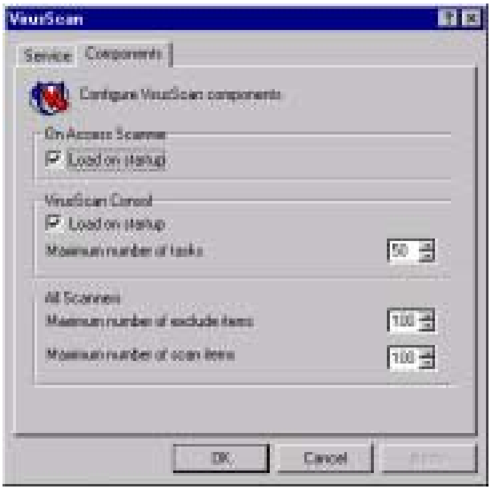
   You can also restart the VirusScan application and the Console individually from the Windows **Start** menu.
3. Select the **Load on startup** checkbox in the VirusScan Service area to start the VirusScan management service (AVSYNMGR.EXE) as soon as you start your computer.

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

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

□ **NOTE:** McAfee VirusScan Software 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.



Configure VirusScan components

On Access Scanner

☑ Load on startup

VirusScan Consol

☑ Load on startup

Maximum number of tasks 50

All Scanners

Maximum number of exclude items 100

Maximum number of scan items 100

Figure A-2. VirusScan control panel - Components page

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

□ **NOTE:** McAfee VirusScan Software 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. 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.

Installed Files B

What’s in this appendix?

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

VShield scanner

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

Program files

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

Table B-1. VShield scanner program files

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

Table B-1. VShield scanner program files

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

Table B-1. VShield scanner program files

NTCLIENT.DLL	Support file for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Network Associates\VirusScan
SCANSERV.DLL	Support file for System Scan module. Runs only on Windows NT and Windows 2000 systems	C:\Program Files\Common Files\Network Associates\McShield
VSHIELD.VXD	VShield System Scan module. Runs as a Windows virtual device driver only on Windows 95 and Windows 98 systems	C:\Windows\System
VSHINIT.VXD	VShield support file. Initializes services for DOS protected-mode interface. Runs only on Windows 95 and Windows 98 systems	C:\Windows\System
MCUTIL.VXD	Support file for System Scan module. Runs only on Windows 95 and Windows 98 systems	C:\Windows\System
MCKRNL.VXD	Support file for System Scan module. Runs only on Windows 95 and Windows 98 systems	C:\Windows\System
EMALSCAN.DLL	Scans e-mail you receive from the Internet or from your network via Messaging Application Programming Interface (MAPI) e-mail systems	C:\Program Files\Network Associates\VirusScan

Table B-1. VShield scanner program files

CCM_SCAN.EXE	Scans e-mail you receive via Lotus cc:Mail v7.x and earlier cc:Mail systems	C:\Program Files\Network Associates\VirusScan
WEBSCANX.EXE	Provides functionality for VShield Download Scan and Internet Filter modules. Initializes WBHOOK32.DLL	C:\Program Files\Network Associates\VirusScan
WBHOOK32.DLL	Provides functionality for VShield Download Scan, and Internet Filter modules. Intercepts files downloaded through web browsers for scan engine to examine	C:\Program Files\Network Associates\VirusScan

Dependent files

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

Table B-2. VShield scanner dependent files

File	Function	Location
AVSYNMGR.EXE	VirusScan management service. Initializes, starts and stops all VirusScan services and components. Must run to enable all VirusScan components.	C:\Program Files\Network Associates\VirusScan
AVSYNCH.DLL	Handles inter-component communication through shared memory	C:\Program Files\Network Associates\VirusScan

Table B-2. VShield scanner dependent files

SYNCUTIL.DLL	Stores data shared between components	C:\Program Files\Network Associates\VirusScan
VSUTIL.DLL	Provides common utilities for components	C:\Program Files\Network Associates\VirusScan
AVSMCPA.CPL	VirusScan control panel applet	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	Resource file for all components	C:\Program Files\Common Files\Network Associates\McPal
MCSCAN32.DLL	McAfee VirusScan’s Scan engine file	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS16.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS32.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates \VirusScan Engine\4.0.xx
MESSAGES.DAT	Support file for scan engine. Provides virus detection messages to engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

Temporary files

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

Table B-3. VShield scanner temporary files

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

Table B-3. VShield scanner temporary files

DAV_SCAN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DEXCLDEF.MFF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DSCANDEF.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DVS_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANGEN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANOAS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANODS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan

Dependent and related files for the VirusScan application

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

Program files

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

Table B-4. VirusScan application program file

File	Function	Location
ADVGUI.DLL	VirusScan application library file. Provides user interface elements for the VirusScan Advanced interface	C:\Program Files\Network Associates\VirusScan

Dependent files

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

Table B-5. VirusScan application dependent files

File	Function	Location
AVSYNMGR.EXE	VirusScan management service. Initializes, starts and stops all VirusScan services and components. Must run to enable all VirusScan components.	C:\Program Files\Network Associates\VirusScan

Table B-5. VirusScan application dependent files

AVSYNCH.DLL	Handles inter-component communication through shared memory	C:\Program Files\Network Associates\VirusScan
SYNCUTIL.DLL	Stores data shared between components	C:\Program Files\Network Associates\VirusScan
VSUTIL.DLL	Provides common utilities for components	C:\Program Files\Network Associates\VirusScan
AVSMCPA.CPL	VirusScan control panel applet	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	Resource file for all VirusScan components	C:\Program Files\Common Files\Network Associates\McPal
RWABS16.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS32.DLL	Support file for scan engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
MESSAGES.DAT	Support file for scan engine. Provides virus detection messages to engine	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
S95EXT.DLL	Shell extension file. Allows you to right-click .VSC settings files you saved and start scan operations or view scan task properties.	C:\Program Files\Network Associates\VirusScan

Temporary files

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

Table B-6. VirusScan application temporary files

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

Alert Manager

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

Table B-7. Alert Manager files

File	Function	Location
ADSLOOKUP.DLL	Library file. Allows client utility to locate Alert Manager server through Microsoft Active Directory services	C:\Program Files\Common Files\Network Associates\McPal
AMG.MIF	Management Information File for use with Desktop Management Interface client application software	C:\Program Files\Common Files\Network Associates\McPal
NAARCHIV.DLL	Library file for VirusScan data compression routines	C:\Program Files\Common Files\Network Associates\McPal
NAEVENT.DLL	Library file. Handles event processing from desktop client anti-virus software to Alert Manager utility and ePolicy Orchestrator software	C:\Program Files\Common Files\Network Associates\McPal
NAGUI32.DLL	Graphical library file for various VirusScan utilities	C:\Program Files\Common Files\Network Associates\McPal
NAKRNL32.DLL	Library file for various VirusScan utilities	C:\Program Files\Common Files\Network Associates\McPal
NAUTIL32.DLL	Library file for various VirusScan utilities	C:\Program Files\Common Files\Network Associates\McPal

VirusScan control panel files

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

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

Table B-8. VirusScan control panel files

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

Temporary files

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

Table B-9. VirusScan control panel temporary files

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

Table B-9. VirusScan control panel temporary files

DEXCLDEF.MFF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DSCANDEF.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
DVS_EXCL.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANGEN.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANOAS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan
VSCANODS.MMF	Memory map file for SYNCUTIL.DLL	C:\Program Files\Network Associates\VirusScan

ScreenScan

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

Program files

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

Table B-10. ScreenScan program files

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

Dependent files

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

Table B-11. ScreenScan dependent files

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

VirusScan Emergency Disk files

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

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

Table B-12. VirusScan Emergency Disk files

File	Function	Location
AUTOEXEC.BAT	MS-DOS batch file. This file leads you through an immediate scan operation, as soon as the Emergency Disk finishes starting your computer	A:\
BIOS.SYS	System file	A:\
BOOTSCAN.EXE	McAfee VirusScan's command-line scanner. This file conducts the scan operation on your hard disk	A:\
CLEAN.DAT	McAfee VirusScan's virus definition file. This file is a smaller, specialized version of the CLEAN.DAT file that other VirusScan components use. You may *not* use a CLEAN.DAT file from the VirusScan program directory for the Emergency Disk.	A:\
COMMAND.COM	Command interpreter. This file is a command shell that responds to command-line input	A:\
GETREPLY.EXE	Application file. This file processes output from the scan operation	A:\
KERNEL.SYS	System file	A:\
LICENSE.DAT	McAfee VirusScan's License file. The command-line scanner uses this to track use eligibility for this product	A:\

Table B-12. VirusScan Emergency Disk files

MESSAGES.DAT	McAfee VirusScan's resource file. This file stores application messages for use during scan operations	A:\
NAMES.DAT	McAfee VirusScan's virus definition file. This file is a smaller, specialized version of the NAMES.DAT file that other VirusScan components use. You may not use a NAMES.DAT file from the VirusScan program directory for the Emergency Disk	A:\
SCAN.DAT	McAfee VirusScan's virus definition file. This file is a smaller, specialized version of the NAMES.DAT file that other VirusScan components use. You may not use a NAMES.DAT file from the VirusScan program directory for the Emergency Disk	A:\

Dependent and related files for the E-Mail Scan extension

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

Program files

Table B-13. E-Mail Scan program files

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

Dependent files

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

Table B-14. E-Mail Scan dependent files

File	Function	Location
AVSYNMGR.EXE	VirusScan management service. Initializes, starts and stops all VirusScan services and components. Must run to enable all VirusScan components.	C:\Program Files\Network Associates\VirusScan
AVSYNCH.DLL	Handles inter-component communication through shared memory.	C:\Program Files\Network Associates\VirusScan
SYNCUTIL.DLL	Stores data shared between components.	C:\Program Files\Network Associates\VirusScan

Table B-14. E-Mail Scan dependent files

VSUTIL.DLL	Provides common utilities for components.	C:\Program Files\Network Associates\VirusScan
AVSMCPA.CPL	VirusScan control panel applet.	C:\Windows\System or C:\Winnt\System 32
RESDLL.DLL	Resource file for all VirusScan components.	C:\Program Files\Common Files\Network Associates\McPal
RWABS16.DLL	Support file for scan engine.	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
RWABS32.DLL	Support file for scan engine.	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx
MESSAGES.DAT	Support file for scan engine. Provides virus detection messages to engine.	C:\Program Files\Common Files\Network Associates\VirusScan Engine\4.0.xx

Temporary files

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

Table B-15. E-Mail Scan temporary files

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

Table B-15. E-Mail Scan temporary files

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

Using VirusScan Command-line Options

C

Adding advanced VirusScan engine options

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

For additional information about adding advanced engine options:

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

Running the VirusScan Command Line program

A typical installation of VirusScan software includes the VirusScan Command Line program. You can run VirusScan Command Line either from a Windows MS-DOS Prompt window, or by restarting your computer in DOS mode. Network Associates recommends restarting in DOS mode for best results. To learn how to restart your computer in DOS mode, see your Microsoft Windows documentation. To run the program, change to the directory in which the file SCAN.EXE is located, and type `scan` followed by the scanning options you want to use (see Table C-1, "VirusScan command-line scanner options," on page 109 for details).

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

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

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

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

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

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

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

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

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

Table C-1. VirusScan command-line scanner options

Command-line Option	Limitations	Description
/? or /HELP	None	Displays a list of VirusScan command-line options, each with a brief description.
/ADL	On-demand scanning only	Scan all local drives—including compressed drives and PC cards, but not disks—in addition to any other drive specified on the command line. To scan both local and network drives, use the /ADL and /ADN commands together in the same command line. OS/2: /ADL includes the CD-ROM drive in the scan, when used with /NODDA.
/ADN	On-demand scanning only	Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command line. To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command line.
/ALERTPATH *<dir>*	On-demand scanning only	Designates the directory <dir> as a network path for Centralized Alerting alert messages.
/ALL	On-demand scanning only	Overrides the default scan setting by scanning all infectable files—regardless of extension. Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect that you have one.
/ANALYZE	On-demand scanning only Extended memory required.	Sets scanner to use its full heuristics, both program and macro. /MANALYZE targets macro viruses only. /PANALYZE targets program viruses only.
/ANYACCESS	On-access scanning only	Scans: • the boot sector whenever a disk is either read or written to • executables • any newly created files

Table C-1. VirusScan command-line scanner options

/APPEND	On-demand scanning only	Used with /REPORT to append report message text to the specified report file instead of overwriting it.
/BOOT	On-demand scanning only	Scan boot sector and master boot record only.
/BOOTACCESS	On-access scanning only	Scans a disk's boot sector for viruses whenever the disk is accessed (including read/write operations).
/CLEAN	On-demand scanning only	Clean viruses from all infected files and system areas.
/CLEANDOCALL	On-demand scanning only	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. This option deletes all macros, including macros not infected by a virus.
/CONTACT <*message*>	On-access scanning only	Displays specified message when a virus is detected. This message cannot exceed 255 characters.
/CONTACTFILE <*filename*>	None	Display the contents of <filename> when a virus is found. Use this to provide contact information and instructions to the user when the scanner finds a virus. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.
/DEL	On-demand scanning only	Deletes infected files permanently.
/EXCLUDE <*filename*>	On-demand scanning only	Do not scan or add validation codes to the files listed in <*filename*>. Use this option to exclude specific files from a scan operation. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?
/FILEACCESS	On-access scanning only	Scans executable files when you modify them in any way, including executing them. This scan operation will not check the boot sector.

Table C-1. VirusScan command-line scanner options

/FREQUENCY <*n* >	On-demand scanning only	Do not scan <n> hours after the previous scan operation. In environments where the risk of viral infection is very low, use this option to prevent unnecessary scan operations. Note that the greater the scan frequency, the greater your protection against infection.
/HELP or /?	None	Displays a list of VirusScan scanner command-line options, each with a brief description.
/IGNORE <*drive(s)*>	On-access scanning only	Does not check any files loaded from the specified drive(s).
/LOAD <*filename*>	On-demand scanning only	Load scanning options from the named file. Use this option to perform a scan you've already configured by loading custom settings saved in an ASCII-formatted file.
/LOCK	Not available in low-memory environments	With this /LOCK option enabled, VirusScan will halt and lock your system if it finds a virus. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. McAfee VirusScan recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system.
/MANALYZE	On-demand scanning only Extended memory required	Sets the scanner's heuristic scanning features to target macro viruses only. /PANALYZE targets program viruses only. /ANALYZE targets both program and macro viruses.
/MANY	On-demand scanning only	Scans multiple disks consecutively in a single drive. The scanner will prompt you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run the scanner from a boot disk and you have only one floppy drive.
/MAXFILESIZE <*xxx.x*>	On-demand scanning only	Scan only files no larger than <xxx.x> megabytes.
/MEMEXCL	On-demand scanning only Not available for Windows	Excludes the memory address A0000:0000 from scanning.

Table C-1. VirusScan command-line scanner options

/MOVE <*dir*> or *.???	On-demand scanning only	/MOVE <directory>: Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files. /MOVE*.???: The scanner will change the extension of infected files, but not move them. For example, using the /MOVE*.BAD option will result in any infected files being simply renamed with the extension .BAD but not physically moved.
/NOBEEP	On-demand scanning only	Disables the tone that sounds whenever the scanner finds a virus.
/NOBREAK	On-demand scanning only	Disables CTRL-C and CTRL-BREAK during scans. Users will not be able to halt scans in progress with /NOBREAK in use. Use this option with /LOG to create a meaningful audit trail of regularly scheduled scans.
/NOCOMP	On-demand scanning only Extended memory required.	Skips checking of compressed executables created with the LZEXE or PkLite file compression programs. This reduces scanning time when you do not need to run a full operation. Otherwise, by default, the scanner checks inside executable, or self-decompressing, files by decompressing each file in memory and checking for virus signatures. The scanner will still check for modifications to compressed executables if they contain VirusScan validation codes.

Table C-1. VirusScan command-line scanner options

/NODDA	On-demand scanning only	No direct disk access. This prevents the scanner from examining the boot record. This feature has been added to allow the scanner to run under Windows NT. You might need to use this option on some device-driven drives. Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.
/NODISK	On-access scanning only	Does not scan boot sector while loading the VShield scanner.
/NODOC	On-demand scanning only	Does not scan Microsoft Office files.
/NOEMS	On-access scanning only	Keeps the VShield scanner from using extended memory (XMS).
/NOEXPIRE	On-demand scanning only	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMEM	None	Does not scan memory for viruses. This greatly reduces scan time. Use /NOMEM only when you are absolutely certain that your computer is virus-free.
/NOREMOVE	On-access scanning only	Prevents users from removing the VShield scanner from memory with the /REMOVE switch.
/NOWARMBOOT	On-access scanning only	Does not check the disk boot sector of the floppy disk in drive A: for viruses during warm boot (system reset or CTRL+ALT+DEL).
/NOXMS	On-access scanning only	Does not use extended memory (XMS).
/ONLY *<drive(s)>*	On-access scanning only	Checks only files loaded from the specified drive(s).
/PANALYZE	On-demand scanning only Extended memory required	Sets the VirusScan scanner to use program heuristics. /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.

Table C-1. VirusScan command-line scanner options

/PAUSE	On-demand scanning only	Enables screen pause. The `Press any key to continue` prompt will appear when the scanner fills a screen with messages. Otherwise, by default, the scanner fills and scrolls a screen continuously without stopping, which allows it to run on PCs with multiple drives or that have severe infections, without needing your input. McAfee VirusScan recommends omitting /PAUSE when using the report options (/REPORT, /RPTCOR, and /RPTERR)
/PLAD	On-demand scanning only	Preserves the last access dates on Novell NetWare drives. Normally, proprietary network drives update the last access date when the scanner opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning
/RECONNECT	On-access scanning only	Restores the VShield scanner after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	On-access scanning only	Unloads the VShield scanner from memory.
/REPORT *<filename>*	On-demand scanning only	Creates a report of infected files and system errors, and saves the data to <filename> in ASCII text file format. If <filename> already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: The scanner will instead add report information to the end of the file, instead of overwriting it. You can also use /RPTALL, /RPTCOR, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report. You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive. McAfee VirusScan recommends omitting /PAUSE when using any report option.

Table C-1. VirusScan command-line scanner options

/RPTALL	On-demand scanning only	Include all scanned files in the /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. McAfee VirusScan recommends omitting /PAUSE when using any report option.
/RPTERR	On-demand scanning only	Include errors in /REPORT file. When used with /REPORT, this option adds a list of system errors to the report file. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems. McAfee VirusScan recommends omitting /PAUSE when using any report option.
/SAVE	On-access scanning only	Saves the command-line options to the VSHIELD.INI file.
/SUB	On-demand scanning only	Scans subdirectories inside a directory. • By default, when you specify a directory to scan rather than a drive, the scanner will examine only the files it contains, not its subdirectories. • Use /SUB to scan all subdirectories within any directories you have specified. • It is not necessary to use /SUB if you are scanning an entire drive.
/UNZIP	On-demand scanning only Extended memory required	Scan inside compressed files.

Table C-1. VirusScan command-line scanner options

/VIRLIST	On-demand scanning only	Displays the name and a brief description of each virus that the scanner detects. You may use the /PAUSE option on the same command line as /VIRLIST to read the virus list one screen at a time. To redirect the /VIRLIST output to a text file: At the command prompt, type scan /VIRLIST <*filename*>.txt Because the scanner can detect many viruses, this file will be over 250 pages long. This is too large for the MS-DOS Edit program to open; McAfee VirusScan recommends using Notepad or another text editor to open the virus list.
/XMSDATA	On-access scanning only	Loads VShield data files into XMS memory.

Using the SecureCast Service to Get New Data Files D

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 VirusScan's Software 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**. AVERT researchers publish virus alert messages to warn customers about potential high-risk virus threats. These messages connect you directly with the AVERT website, where you can download EXTRA.DAT files, if available, to counter the threat, and learn about the characteristics of the new virus.

Installing the BackWeb client and SecureCast service

Setting up SecureCast service and the BackWeb client is a two-phase process:

1. Download and install the BackWeb client
2. Register to receive SecureCast service InfoPaks

To get started with the SecureCast service, review the system requirements shown below, then follow the steps outlined in each section.

System requirements

The BackWeb client software will install and run on any personal computer equipped with:

- An Intel processor or a compatible processor
- Windows 95, Windows 98, Windows NT or Windows 2000
- At least 10MB free hard disk space, plus sufficient space for product and other downloads
- An active Internet connection—direct or dial-up—for a minimum of one hour per week.

Phase 1: Download and install BackWeb

1. To download the BackWeb client software, connect to the Network Associates website at:

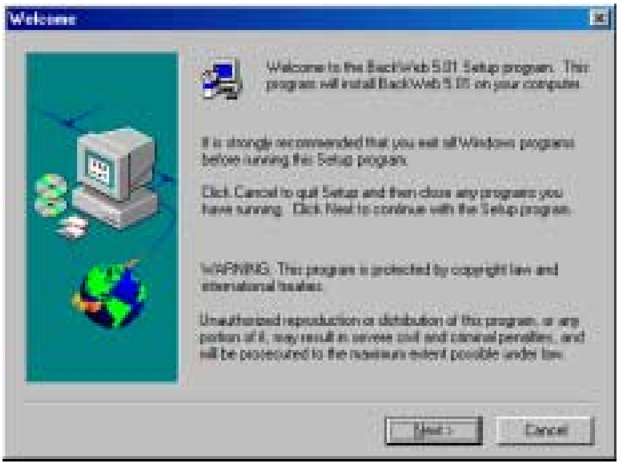
   http://www.nai.com/asp_set/anti_virus/alerts/register.asp

   Next, download the file ESC_501.EXE to a temporary directory on your hard disk.

   If your product came on CD-ROM, select the SecureCast service from the choices on the installation CD-ROM, or locate the file ESC_501.EXE on your CD-ROM.

2. Double-click the program icon to start.

   As soon as Setup has extracted the necessary installation files, the first BackWeb Setup panel appears (see Figure D-1 on page 120).



Welcome to the BackWeb 5.01 Setup program. This program will install BackWeb 5.01 on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

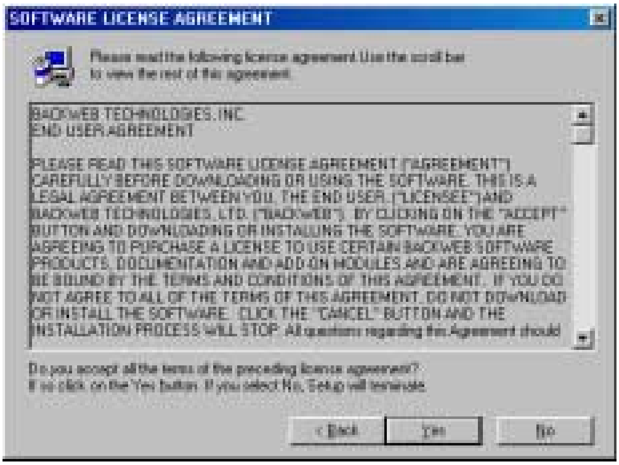
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure D-1. BackWeb client welcome panel

3. Read the instructions and warnings on this panel, then click **Next>** to continue.
4. The BackWeb license agreement appears (Figure D-2).



Please read the following license agreement. Use the scroll bar to view the rest of this agreement.

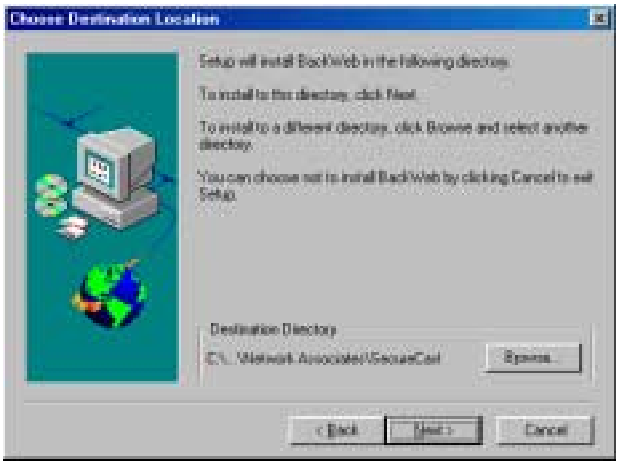
BACKWEB TECHNOLOGIES, INC.
END USER AGREEMENT

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE. THIS IS A LEGAL AGREEMENT BETWEEN YOU, THE END USER, ("LICENSEE") AND BACKWEB TECHNOLOGIES, LTD. ("BACKWEB"). BY CLICKING ON THE "ACCEPT" BUTTON AND DOWNLOADING OR INSTALLING THE SOFTWARE, YOU ARE AGREEING TO PURCHASE A LICENSE TO USE CERTAIN BACKWEB SOFTWARE PRODUCTS, DOCUMENTATION AND ADD ON MODULES AND ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT DOWNLOAD OR INSTALL THE SOFTWARE. CLICK THE "CANCEL" BUTTON AND THE INSTALLATION PROCESS WILL STOP. All questions regarding this Agreement should

Do you accept all the terms of the preceding license agreement? If so click on the Yes button. If you select No, Setup will terminate.

Figure D-2. BackWeb Software License Agreement panel

5. Click **Yes** to continue.
6. The Choose Destination Location panel appears (Figure D-3 on page 121).



Choose Destination Location

Setup will install BackWeb in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install BackWeb by clicking Cancel to exit Setup.

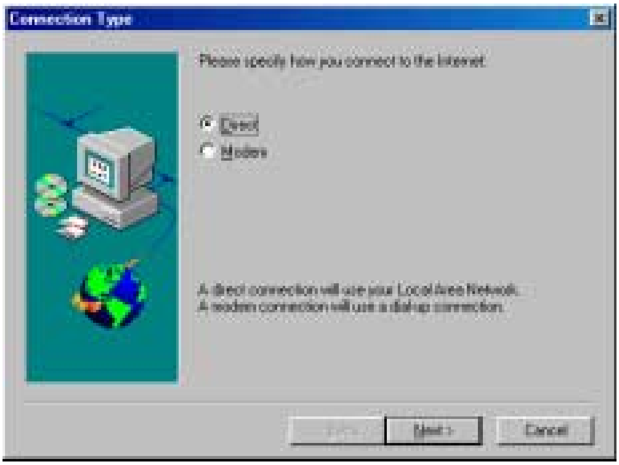
Destination Directory

C:\...\Network Associates\SecureCast

Figure D-3. Choose Destination Location panel

7. Enter a new location for Setup to install the client software, if you wish, or click **Browse** to locate a suitable folder. Click **Next>** to continue.

   Setup will begin to copy BackWeb program files to your computer. As it does so, it displays its progress. When it has finished, Setup displays the Connection Type panel (Figure D-4).



Connection Type

Please specify how you connect to the Internet.

● Direct
○ Modem

A direct connection will use your Local Area Network.
A modem connection will use a dial-up connection.

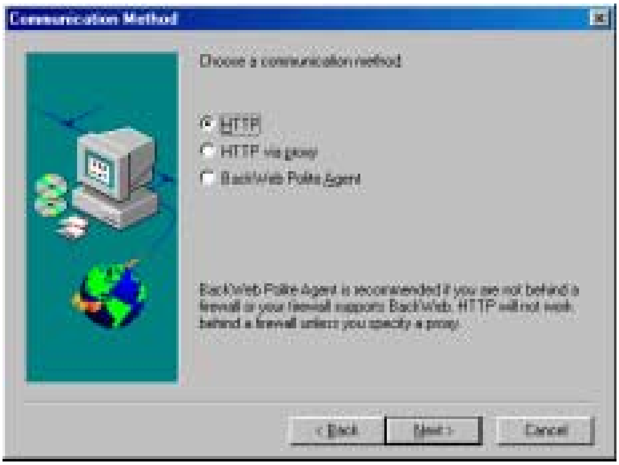
Figure D-4. Connection Type panel

8. Specify the type of connection your computer has to the Internet. Your choices are:

   - **Direct**. Choose this option if you connect to the Internet through a local-area network, a high-bandwidth connection such as a cable modem or digital subscriber line (DSL) connection. Continue with Step 9.

   - **Modem**. Choose this option if you dial up to connect to an Internet service provider, or into your corporate network. Skip to Step 13.

   The Communication Method panel appears (Figure D-5).



Choose a communication method

● HTTP
○ HTTP via proxy
○ BackWeb Polite Agent

BackWeb Polite Agent is recommended if you are not behind a firewall or your firewall supports BackWeb. HTTP will not work behind a firewall unless you specify a proxy.

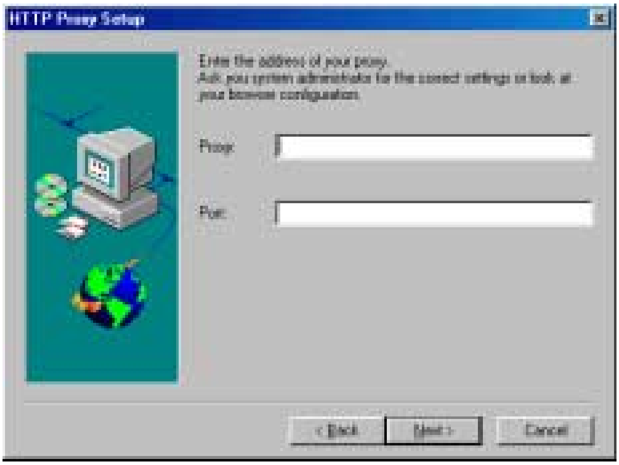
Figure D-5. Communication Method panel

9. Choose a communication method. Your choices are:

   - **HTTP**. Choose this option if you can connect directly to the Internet without going through a proxy server. Skip to Step 13.
   - **HTTP via proxy**. Choose this option if you connect to the Internet through a proxy server on your network. Continue with Step 10.
   - **BackWeb Polite Agent**. Choose this option to connect to the Internet through a Universal Datagram Protocol (UDP) connection. This allows you to control how the BackWeb client behaves with respect to other applications you might have running when SecureCast InfoPaks arrive at your desktop. For more information, see the BackWeb online help at http://www.backweb.com/.

     Next, skip to Step 13.

10. If you chose **HTTP via proxy** as your connection method, the HTTP Proxy Setup panel appears (Figure D-6).

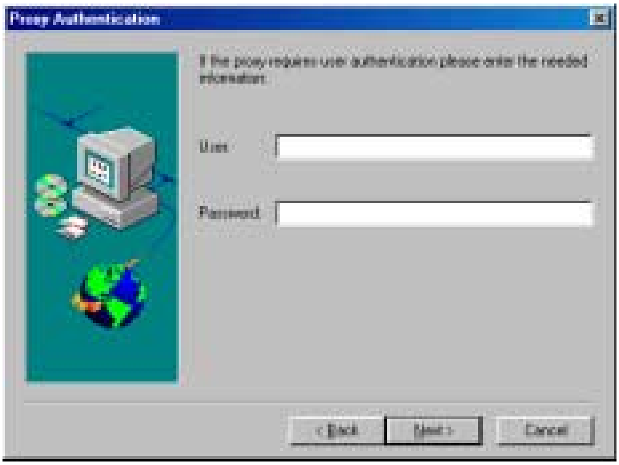


Enter the address of your proxy.
Ask your system administrator for the correct settings or look at your browser configuration.

Figure D-6. HTTP Proxy Setup panel

11. Enter the name of your proxy server in the Proxy text box, then enter the port the server uses for communication in the Port text box.

    When you have finished, click **Next>** to continue. The Proxy Authentication panel appears (Figure D-7 on page 123).

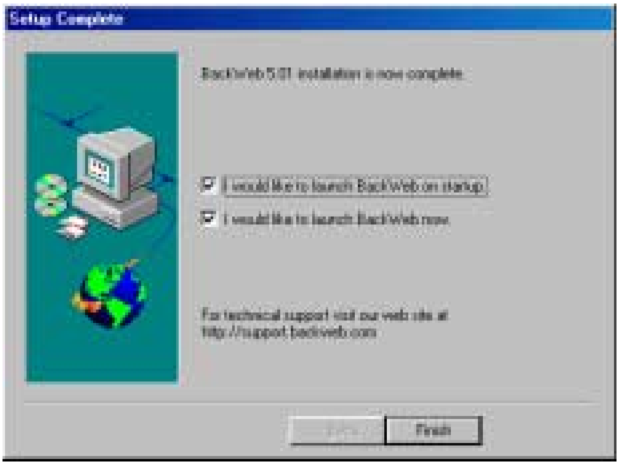


If the proxy requires user authentication please enter the needed information.

Figure D-7. Proxy Authentication panel

12. If the proxy server requires user authentication, enter in the text boxes provided a user name and password with sufficient rights to permit you to connect, then click **Next**> to continue.

The Setup Complete panel appears (Figure D-8).



BackWeb 5.01 installation is now complete.

☑ I would like to launch BackWeb on startup

☑ I would like to launch BackWeb now.

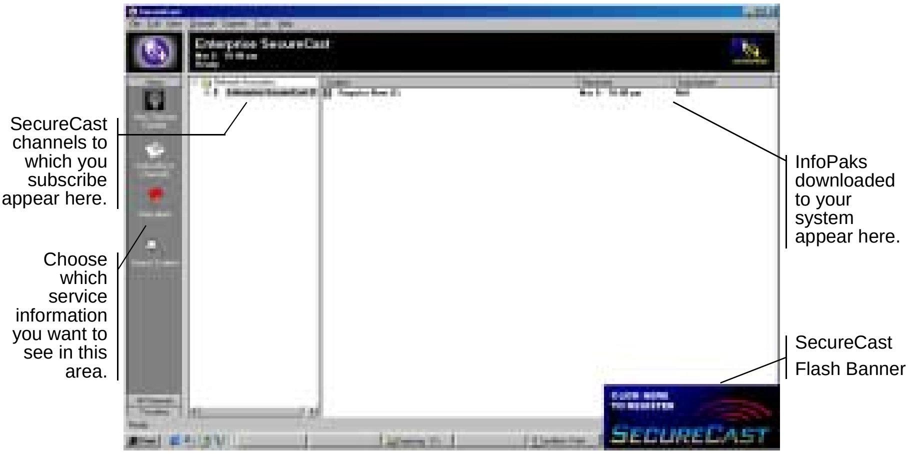
For technical support visit our web site at
http://support.backweb.com

Figure D-8. Setup Complete panel

13. To start immediately, leave both checkboxes selected in this panel, then click **Finish** to complete your installation.

Phase 2: Register with the Enterprise SecureCast service

After you install the BackWeb client and start it, the SecureCast service immediately opens the client application and sends its first InfoPak: the SecureCast registration forms (Figure D-9).



Enterprise SecureCast
SecureCast channels to which you subscribe appear here.
Choose which service information you want to see in this area.
InfoPaks downloaded to your system appear here.
SecureCast Flash Banner
CLICK HERE TO REGISTER
SECURECAST

Figure D-9. The Enterprise SecureCast client window

The SecureCast service alerts you that an InfoPak has arrived with the Flash message shown at the bottom right corner of Figure D-9.

🛎 **IMPORTANT:** If you are a corporate user and have a high-speed Internet connection, the window may list **Register Now** as an already received InfoPak. Continue with Step 1.

If you have a slower connection, or if there is unusually heavy traffic at the SecureCast service site or your site, the window might not list any InfoPaks. In that case, minimize or close the BackWeb window. After some time, you will receive a Flash message. Click the flashing message, then continue with Step 2.

To register for the Enterprise SecureCast channel, follow these steps:

1. If you see **Register Now** listed in the window, double-click it. The SecureCast service Flash banner appears (Figure D-10).

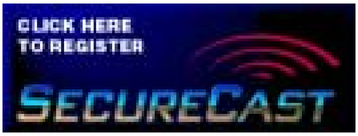
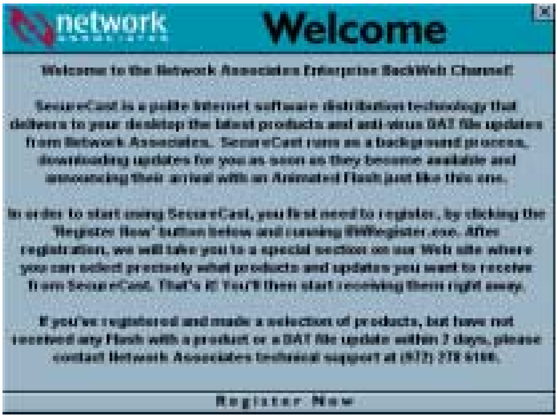


Figure D-10. SecureCast Flash banner

2. Click the banner. The Network Associates Welcome panel appears (Figure D-11).



Welcome to the Network Associates Enterprise BackWeb Channel!

SecureCast is a polite Internet software distribution technology that delivers to your desktop the latest products and anti-virus DAT file updates from Network Associates. SecureCast runs as a background process, downloading updates for you as soon as they become available and announcing their arrival with an Animated Flash just like this one.

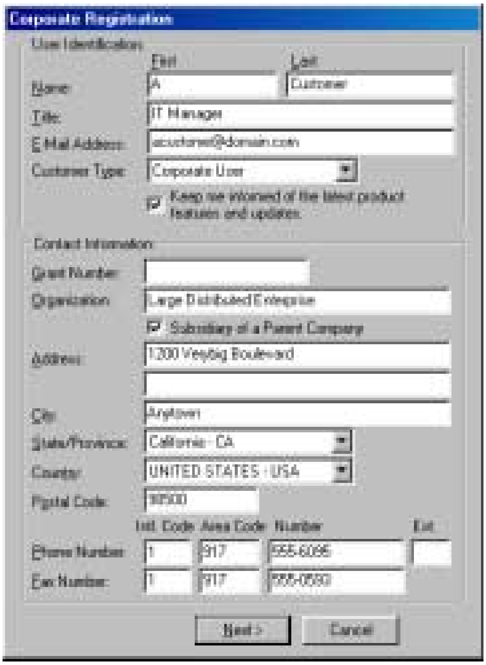
In order to start using SecureCast, you first need to register, by clicking the 'Register Now' button below and running BWRegister.exe. After registration, we will take you to a special section on our Web site where you can select precisely what products and updates you want to receive from SecureCast. That's it! You'll then start receiving them right away.

If you've registered and made a selection of products, but have not received any Flash with a product or a DAT file update within 7 days, please contact Network Associates technical support at (972) 278 6100.

Figure D-11. Network Associates Welcome panel

3. Review the information shown, then click **Register Now** at the bottom of the panel.

4. Double-click the **BW Register** icon in the window that opens next. A registration information form appears (Figure D-12).



Corporate Registration

User Identification

	First	Last
Name:	A	Customer
Title:	IT Manager	
E-Mail Address:	acustomer@domain.com	
Customer Type:	Corporate User	

☑ Keep me informed of the latest product features and updates.

Contact Information

Grant Number:				
Organization:	Large Distributed Enterprise			
	☑ Subsidiary of a Parent Company			
Address:	1200 Verybig Boulevard			
City:	Anytown			
State/Province:	California - CA			
Country:	UNITED STATES - USA			
Postal Code:	90500			
	Intl. Code	Area Code	Number	Ext.
Phone Number:	1	917	555-6096	
Fax Number:	1	917	555-0593	

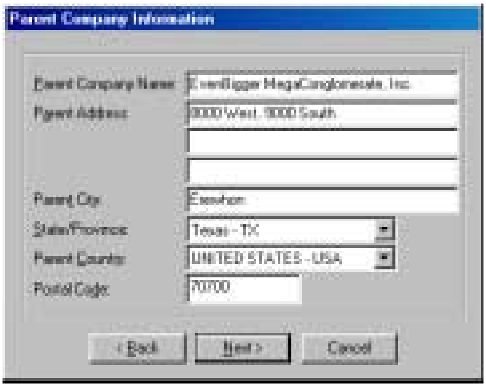
Figure D-12. SecureCast User Registration Information form

5. Enter your name, title and company contact information in the text boxes provided. Here you will also need to enter the grant number you received when you purchased your software, or that you received from Network Associates Customer Service.

> ❏ **NOTE:** If your company is not a subsidiary of another company, clear the **Subsidiary of a Parent Company** checkbox before you continue.

When you have entered your information, click **Next>** to continue.

- If you did not clear the **Subsidiary of a Parent Company** checkbox, the **Parent Company Information** dialog box appears (see Figure D-13 on page 127). Skip to Step 7 on page 127.
- If you have cleared the **Subsidiary of a Parent Company** checkbox, continue with Step 6 on page 127.



Parent Company Information

Parent Company Name: EvenBigger MegaConglomerate, Inc.

Parent Address: 9000 West, 9000 South

Parent City: Elsewhere

State/Province: Texas - TX

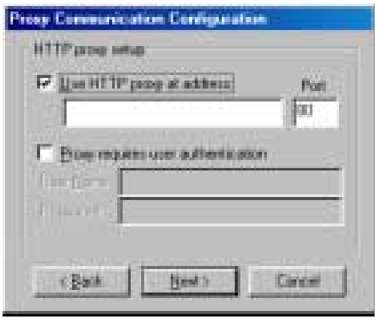
Parent Country: UNITED STATES - USA

Postal Code: 70700

Figure D-13. SecureCast Parent Company Information form

6. If your company is the subsidiary of another company, enter contact information for your parent company in the text boxes provided.

   When you have finished, click **Next>**. The **Proxy Communication Configuration** dialog box appears (Figure D-14).



Proxy Communication Configuration

HTTP proxy setup

☑ Use HTTP proxy at address

Port: 80

☐ Proxy requires user authentication

User Name:

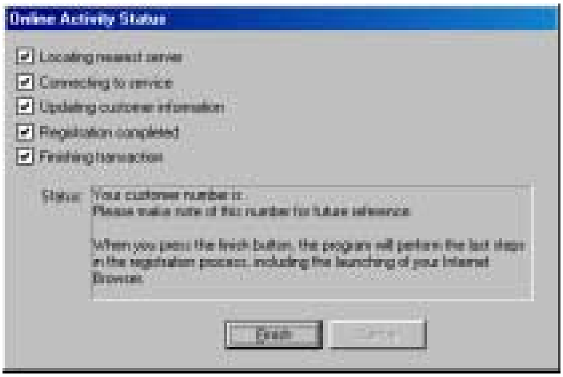
Password:

Figure D-14. SecureCast Proxy Communication Configuration

7. If your network requires you to connect to the Internet through a proxy server, select the Use HTTP proxy at address checkbox, then enter the server name or its Internet Protocol (IP) address in the text box provided. Next, verify that the correct port number appears in the Port text box, or enter the correct port number.

   If your proxy server requires you to sign on to use it, select the **Proxy requires users authentication** checkbox, then enter a user name and password with sufficient rights.

8. When you have finished, click **Next>**. The **Online Activity Status** panel appears displaying the progress of the registration process (Figure D-15 on page 128).



☑ Locating nearest server
☑ Connecting to service
☑ Updating customer information
☑ Registration completed
☑ Finishing transaction

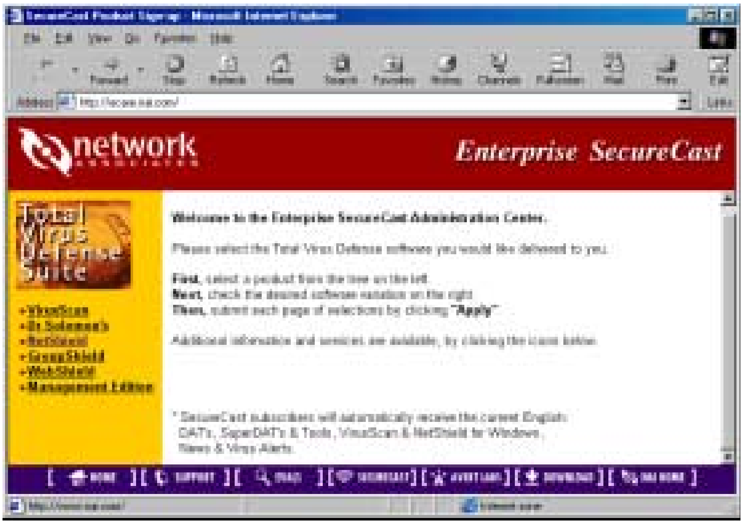
Status: Your customer number is:
Please make note of this number for future reference.

When you press the finish button, the program will perform the last steps in the registration process, including the launching of your Internet Browser.

Figure D-15. SecureCast Online Activity Status panel

9. Click **Finish** after a check mark appears in all the boxes.

   The setup process in complete. At that point, your web browser will connect to the Network Associates SecureCast service electronic customer care page. If you are a corporate user, the window resembles the one shown in Figure D-16:



Welcome to the Enterprise SecureCast Administration Center.

Please select the Total Virus Defense software you would like delivered to you.

First, select a product from the tree on the left.
Next, check the desired software variation on the right.
Then, submit each page of selections by clicking "**Apply**"

Additional information and services are available, by clicking the icons below.

* SecureCast subscribers will automatically receive the current English DATs, SuperDAT's & Tools, VirusScan & NetShield for Windows, News & Virus Alerts.

Figure D-16. SecureCast Electronic Corporate Customer Care

You can use this page to download product updates and upgrades, contact technical support, and get other information directly from Network Associates. The terms of your grant will determine what information you see here and what you can download.

Troubleshooting the Enterprise SecureCast service

Registration problems

If you try to register during a busy time of day on the web, you may encounter a delay while the server tries to process your registration request. If you receive the error message “1105 Error” or “Database Error: Unable to connect to the data source,” this means that there is a database problem on the server. Try submitting the form again, or try to register later. If you continue to have problems subscribing to the Enterprise SecureCast channel, contact Network Associates Download Support (Monday to Friday, 8 A.M. to 8 P.M. Central time) at (801) 492-2650.

Unsubscribing from the SecureCast service

You can stop the SecureCast service from delivering InfoPaks at any time you want to. To do so, right-click the BackWeb icon in your Windows system tray, then choose **Start SecureCast** from the shortcut menu that appears.

Next, follow these steps:

1. In the list box on the left side of the BackWeb client window (see Figure D-9 on page 124), 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/

Product Support E

Updates

You will receive one free year of updates on new virus signature files. Updating the virus signature files for McAfee VirusScan on a regular schedule is essential in ensuring that all new viruses are detected for a completely protected system.

To update your signature files, simply click on the UPDATE button in the McAfee VirusScan home page. Make sure that your PC is connected to the Internet as VirusScan will automatically update the files for you.

After one year from your purchase of this software, you can purchase another year of DAT signature files update for $4.95.

How to Contact McAfee

BEFORE YOU CONTACT McAfee Software for technical support, locate yourself near the computer with McAfee VirusScan installed and verify the information listed below:

- Have you sent in your product registration card?
- Version of McAfee VirusScan
- Customer number if registered
- Model name of hard disk (internal or external)
- Version of system software
- Amount of memory (RAM)
- Extra cards, boards or monitors
- Name and version of conflicting software
- EXACT error message as on screen
- What steps were performed prior to receiving error message?
- A complete description of problem

Customer service

To order products or obtain product information, contact the McAfee Customer Care department at (972) 308-9960 or write to the following address:

McAfee Software
3965 Freedom Circle
Santa Clara, CA 95054
U.S.A.

If you need further assistance or have specific questions about our products, send your questions via email to the appropriate address below:

- For general questions about ordering software: mcafeestore@beyond.com
- For help in downloading software: mcafeedownloadhelp@beyond.com
- For a status on an existing order: mcafeeorderstatus@beyond.com

To inquire about a promotion: mcafeepromotions@beyond.com

Technical support

Support via the web

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web (http://www.mcafeehelp.com) a valuable resource for answers to technical support issues.

We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

Take advantage of the McAfee Product KnowledgeCenter—your free online product support center - 24 hours a day, 7 days a week (http://www.mcafeehelp.com).

Telephone support numbers

30-Day Free Telephone Support	972-308-9960
Per Minute Telephone Support	1-900-225-5624
Per Incident Telephone Support ($35)	1-800-950-1165

Disclaimer: Time and telephone numbers are subject to change without prior notice.

Download Information (License ID #: VSF500R) F

As a valued McAfee customer, we are committed to keeping your system FREE from virus infection. To protect against the newest virus threats, keep your VirusScan installation up to date!

Per your McAfee Software License Agreement, you are eligible for one (1) FREE Upgrade within ninety (90) days of purchase. This document explains the different ways you can access your FREE VirusScan upgrade.

If you have difficulties downloading or applying the upgrade files through any of the methods listed below, you can call McAfee Technical Support at 972-855-7044.

SecureCast™ (For Windows 95/98 Retail Version):

SecureCast is the easiest way to Update & Upgrade your copy of VirusScan for Windows 95/98. With a click of a button, SecureCast will automatically deliver your software Updates and your FREE product Upgrade to your system. To update your copy of VirusScan, just click the Update button on the VirusScan Central interface.

Internet Access

You will need a World Wide Web (WWW) browser, such as Internet Explorer, Netscape or the AOL web browser to access the McAfee web site.

1. Enter the WWW address for the McAfee Home Page into the appropriate area of your Internet browser. Type: http://www.mcafee.com

2. When the McAfee Home page is loaded, click the "download" tab

3. When the download centers page is loaded (http://www.mcafee.com/centers/download/), look for the highlighted, underlined "Upgrades" and click on this link.

4. On the Upgrade information page, click on the Upgrade McAfee Antivirus link

5. On the McAfee Antivirus Upgrade page enter the Licensed ID#: identified at the top of this card in the appropriate location. Press submit.

6. On the McAfee Antivirus customer identification page enter your email address in location provided and press submit.

7. If previously registered, the thank you page is displayed. To begin download of product - click on the download button.
8. If not previously registered, the McAfee Product Registration page is displayed. You will be asked to enter your Last Name, First Name, Postal Code, Country, State and a password that you make up. Press submit. Once submitted a thank you page is displayed. An access URL will be emailed automatically to email address that you have entered.
9. When the email is opened you will be instructed to click on the url enclosed. A thank you is displayed with a download button. Click on the download button to begin downloading the upgrade.
10. After the file is downloaded and saved to your hard drive, extract or unzip the file (if necessary), and run the setup program.

The information provided in this article is provided "as is" without warranty of any kind. In no event shall McAfee be liable for any damages incurred by use or misuse of the information contained in this article. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Index