



---

VirusScan for Windows 3.1x

## User's Guide

## COPYRIGHT

Copyright © 1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

## LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), WHICH SETS FORTH GENERAL LICENSE TERMS FOR NETWORK ASSOCIATES SOFTWARE. FOR THE SPECIFIC TERMS OF YOUR LICENSE, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees and subject to the terms and conditions of this Agreement, Network Associates 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 is bundled with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified individually for any of such Software products on the applicable product invoicing or packaging.
  - a. **Use.** The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section 1. The Software is "in use" on a computer when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make one copy of the Software solely for backup or archival purposes, provided that the copy you make contains all proprietary notices.
  - b. **Server Use.** To the extent that the applicable product invoicing or packaging sets forth, you may install and use the Software on a Client Device or as a server ("Server") within a multi-user or networked environment ("Server Use") for either (i) connecting, directly or indirectly, to not more than the maximum number of specified Client Devices or "seats"; or (ii) deploying not more than the maximum number of agents (pollers) specified for deployment. If the applicable product invoicing or packaging does not specify a maximum number of Client Devices or pollers, this license gives you a single product use license subject to the provisions of subsection (a) above. A separate license is required for each Client Device or seat that can connect to the Software at any time, regardless of whether such licensed Client Devices or seats are connected to the Software concurrently, or are actually using the Software at any particular time.

Your use of software or hardware that reduces the number of Client Devices or seats that connect to and use the Software simultaneously (e.g., using “multiplexing” or “pooling” hardware or software) does not reduce the number of licenses you must have in total. Specifically, you must have that number of licenses that would equal the number of distinct inputs to the multiplexing or pooling software or hardware “front end.” If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses that you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits set forth in the product invoicing or packaging. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the proprietary notices for the Documentation.

- c. **Volume Use.** If the Software is licensed with volume use terms specified in the applicable product invoicing or packaging, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume use terms specify. This license authorizes you to make or download one copy of the Documentation for each such copy of the Software you may make according to the volume use terms, provided that each such copy contains all of the proprietary notices for the Documentation. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software is installed does not exceed the number of licenses you have obtained.
2. **Term.** This license is effective for the period of time specified in the product invoicing or packaging, or in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of the Agreement set forth here conflict with the provisions of the product invoicing or packaging, the README.1ST document, the LICENSE.TXT document, the product invoice, package, or the other text document will constitute the terms of your license grant to use the Software. Either you or Network Associates may terminate your license earlier than the period specified in the appropriate document in accordance with the terms set forth therein. This Agreement and your license will terminate automatically if you fail to comply with any of the limitations or other requirements described. When this agreement terminates, you must destroy all copies of the Software and Documentation. You may terminate this Agreement at any point by destroying the Software and Documentation together with all copies of the Software and Documentation.
3. **Updates.** During the term of your license, you may download revisions, upgrades, or updates to the Software when Network Associates publishes them via its electronic bulletin board system, website or through other online services.
4. **Ownership Rights.** The Software and the Documentation are protected by United States copyright laws and international treaty provisions. Network Associates owns and retains all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. You acknowledge that your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and that you will not acquire any rights to the Software except as expressly set forth in this Agreement. You agree that any copies of the Software and Documentation will contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software, or permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement. You may not transfer any of the rights granted to you under this Agreement. You may not copy the Documentation accompanying the Software. You may not reverse engineer, decompile, or disassemble the Software, except to the extent that the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon the Software in whole or in part. You may not copy the Software except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by Network Associates. Network Associates reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

## 6. Warranty and Disclaimer

- a. **Limited Warranty.** Network Associates warrants that for thirty (30) days from the date of original purchase or distribution the media (for example, the diskettes) on which the Software is contained will be free from defects in materials and workmanship.
- b. **Customer Remedies.** Network Associates' and its suppliers' entire liability, and your exclusive remedy, shall be, at Network Associates' option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media on which the Software is contained with a copy on non-defective media. You must return the defective media to Network Associates at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent that Network Associates is subject to restrictions under United States export control laws and regulations.

**Warranty Disclaimer.** To the maximum extent permitted by applicable law, and except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, NETWORK ASSOCIATES MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES, OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY LAW, NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATIONS MIGHT NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

Your purchase of or payment for the Software may entitle you to additional warranty rights, which Network Associates will specify in the product invoicing or packaging you received with your purchase, or in the README.1ST , LICENSE.TXT or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the product invoice or packaging, the README.1ST, the LICENSE.TXT, or similar documents, the invoice, packaging, or text file will set forth the terms of your warranty rights for the Software.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL NETWORK ASSOCIATES OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL NETWORK ASSOCIATES BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE NETWORK ASSOCIATES CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF NETWORK ASSOCIATES SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.
8. **United States Government.** The Software and accompanying Documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.
9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department’s list of Specially Designated Nations or the United States Commerce Department’s Table of Denial Orders. By downloading or using the Software, you are agreeing to the foregoing provisions and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

IN ADDITION, YOU SHOULD BE AWARE THAT EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH

RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE. SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR ON THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY BUSINESS OR PERSONAL USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST, THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION OF ENCRYPTION TECHNOLOGY TO, OR IMPORTATION FROM: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE THAT IT IS YOUR RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS, AND THAT NETWORK ASSOCIATES HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

11. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, “High Risk Activities”). Network Associates expressly disclaims any express or implied warranty of fitness for High Risk Activities.
12. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. The Agreement set forth here is advisory in nature and does not supersede the provisions of any Agreement set forth in the README.1ST, LICENSE.TXT, or other text file that accompanies the Software and purports to set forth the terms of your license agreement. Where the provisions of this Agreement conflict with the provisions of the README.1ST or the LICENSE.TXT document, the text document will constitute the terms of your license grant to use the Software. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of Network Associates. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by Network Associates or a duly authorized representative of Network Associates. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.
13. **Network Associates Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact Network Associates for any other reason, please call (408) 988-3832, fax (408) 970-9727, write Network Associates, Inc. at 3965 Freedom Circle, Santa Clara, California 95054, or visit the Network Associates website at <http://www.nai.com>.

# Preface

## What Happened?

If you've ever lost important files stored on your hard disk, watched in dismay as your computer ground to a halt only to display a prankster's juvenile greeting on your monitor, or found yourself having to apologize for abusive e-mail messages you never sent, you know first-hand how computer viruses and other harmful programs can disrupt your productivity. If you haven't yet suffered from a virus "infection," count yourself lucky. But with more than 16,000 known viruses in circulation capable of attacking Windows- and DOS-based computer systems, it really is only a matter of time before you do.

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

## Why worry?

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

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

The threat from viruses and other malicious software is real, and it is growing worse. The International Computer Security Association has estimated the total worldwide cost in time and lost productivity simply of detecting and cleaning virus infections at \$1 billion per year, a figure that doesn't include the costs of data loss and recovery in the wake of attacks that destroyed data.

## Where Do Viruses Come From?

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

Why did this happen to me?

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

## Virus prehistory

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

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



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

## Viruses and the PC revolution

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

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

### Boot-sector viruses

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

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

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

Realistically, nearly every step in the boot process, from reading the MBR to loading the operating system, is vulnerable to viral sabotage. Some of the most tenacious and destructive viruses still include the ability to infect your computer's boot sector or MBR among their repertoire of tricks. Among other advantages, loading at boot time can give a virus a chance to do its work before your anti-virus software has a chance to run.

But boot sector and MBR viruses have a particular weakness: they must spread by means of floppy disks or other removable media, riding concealed in that first track of disk space. As fewer users exchange floppy disks and as software distribution has come to rely on other media, such as CD-ROMs, other virus types have recently eclipsed the boot sector threat. The popularity of large-capacity floppy disks like the Iomega Zip disk and similar disks from Syquest and others, however, could cause a resurgence.

### File infector viruses

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

Later viruses quickly overcame this limitation, sometimes with fairly clever programming. Virus writers might, for instance, have their virus add its code to the beginning of an executable file, so that when users start a program, the virus code executes immediately, then transfers control back to the legitimate software, which runs as though nothing unusual has happened. Once it activates, the virus “hooks” or “traps” requests that legitimate software makes to the operating system and substitutes its own responses. Particularly clever viruses can even subvert attempts to clear them from memory by trapping the `CTRL+ALT+DELETE` keyboard sequence for a warm reboot, then faking a restart. Sometimes the only outward indication that anything on your system is amiss—before any payload detonates, that is—might be a small change in the file size of infected legitimate software.

## Stealth, mutating, encrypted, and polymorphic viruses

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

Because viruses needed to avoid continuously reinfecting host systems—doing so would quickly balloon an infected file's size to easily detectable proportions or would consume enough system resources to point to an obvious culprit—their authors also needed to tell them to leave certain files alone. They addressed this problem by having the virus write a code "signature" that would flag infected files with the software equivalent of a "do not disturb" sign. Although that kept the virus from giving itself away immediately, it opened the way for anti-virus software to use the code signatures themselves to find the virus.

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

## Macro viruses

By 1995 or so, the virus war had come to something of a standstill. New viruses appeared continuously, prompted in part by the availability of ready-made virus "kits" that enabled even some non-programmers to whip up a new virus in no time. Most existing anti-virus software, however, could easily be updated to detect and dispose of the new virus variants, which consisted primarily of minor tweaks to well-known templates.

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

That distinction melted away when Microsoft began adding macro capabilities to Word and Excel, its flagship applications in its Office suite. Using the stripped-down version of its Visual BASIC language included with the suite, users could create document templates that would automatically format and add other features to documents created with Word and Excel. Virus writers seized the opportunity that this presented to conceal and spread viruses in documents that you, the user, created yourself.

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

## On the Frontier

Malicious software has even begun intruding into areas once thought completely out of bounds. Users of the mIRC Internet Relay Chat client, for example, have reported encountering viruses constructed from the mIRC scripting language. Script viruses get sent as plain text, which would ordinarily preclude them from getting infected, but older versions of the mIRC client software would interpret the instructions coded into the script to perform unwanted actions on the recipient's computer. The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it.

Some virus writers do it for the thrill of it, some to gain notoriety in their own peer group. Still others do it to exact revenge against employers or others they believe have treated them badly. Whatever their motives, they continue to develop new ways to cause you trouble.

## How to Protect Yourself

Network Associates anti-virus software already gives you an important bulwark against infection and damage to your data, but anti-virus software is only one part of the security measures you should take to protect yourself and your data. Most measures are common sense—checking disks you receive from unknown or questionable sources, either with anti-virus software or some kind of verification utility, is always a good idea. Malicious programmers have gone so far as to mimic the programs you trust to guard your computer, pasting a familiar face on software with a less-than-friendly purpose. Network Associates includes VALIDATE.EXE, a verification utility, with its distributions to prevent this type of manipulation, but neither it nor any anti-virus software can detect when someone substitutes a trojan or other malicious program for one of your favorite shareware or commercial utilities.

Web and Internet access poses its own risks. Having a top-notch firewall in place to protect your network and implementing other network security measures is a necessity when unscrupulous attackers can penetrate your network from nearly any point on the globe, whether to steal sensitive data or implant malicious code. You should also make sure that your network is not accessible to unauthorized users, and that you have an adequate training program in place to teach and enforce security standards.

To learn about the origin, behavior and other characteristics of particular viruses, consult the Virus Information Library maintained on the Network Associates web site. Some Network Associates products also come with a Virus List that also catalogs all of the viruses that the program can detect and summarizes information about their sizes, the types of infections they attempt, and whether the product can remove them from your files.

Network Associates can provide you with other software in the Total Virus Defense (TVD) suite, the most comprehensive anti-virus solution available, and Total Network Security (TNS), the industry's most advanced network security suite. Network Associates backs them both with outstanding support, training and a worldwide network of research and development teams. Contact your Network Associates representative, or visit the Network Associates web site at <http://www.nai.com>, to find out how to enlist the power of Total Virus Defense on your side.

## How To Contact Network Associates

### Customer service

To order products or obtain product information, contact the Network Associates Customer Care department at (408) 988-3832 or write to the following address:

Network Associates, Inc.  
3965 Freedom Circle  
Santa Clara, CA 95054  
U.S.A.

### Technical support

Network Associates is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web 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 Network Associates software, and for access to Network Associates news and virus information.

World Wide Web	<a href="http://support.nai.com">http://support.nai.com</a>
----------------	---

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

Automated Voice and Fax Response System	(408) 988-3034
Internet	<a href="mailto:support@nai.com">support@nai.com</a>
CompuServe	GO NAI
America Online	keyword NAI

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 278-6100
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, system LOGIN script, and NOTES.INI
- Specific steps to reproduce the problem.

## Network Associates training

For information about scheduling on-site training for any Network Associates product, call (800) 338-8754.

## International contact information

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

### **Network Associates Australia**

Level 1, 500 Pacific Highway  
St. Leonards, NSW 2065  
Australia

Phone: 61-2-9437-5866

Fax: 61-2-9439-5166

### **Network Associates Deutschland GmbH**

Industriestrasse 1  
D-82110 Germering  
Germany

Phone: 49 8989 43 5600

Fax: 49 8989 43 5699

### **Network Associates France S.A.**

50 rue de Londres  
75008 Paris  
France

Phone: 33 1 44 908 737

Fax: 33 1 45 227 554

### **Network Associates International Ltd.**

Minton Place, Victoria Street  
Windsor, Berkshire  
SL4 1EG  
United Kingdom

Phone: 44 (0)1753 827500

Fax: 44 (0)1753 827520

### **Network Associates Canada**

139 Main Street, Suite 201  
Unionville, Ontario  
Canada L3R 2G6

Phone: (905) 479-4189

Fax: (905) 479-4540

### **Network Associates Europe B.V.**

Gatwickstraat 25  
1043 GL Amsterdam  
The Netherlands

Phone: 31 20 586 6100

Fax: 31 20 586 6101

### **Network Associates Hong Kong**

19/F, Matheson Centre  
3 Matheson Street  
Causeway Bay  
Hong Kong

Phone: 852-2832-9525

Fax: 852-2832-9530

### **Network Associates Japan Co, Ltd.**

Toranomon 33 Mori Bldg.  
3-8-21 Toranomon  
Minato-Ku, Tokyo 105  
Japan

Phone: 81 3 5408 0700

Fax: 81 3 5408 0780

**Network Associates  
Korea**

135-090, 18th Floor, Kyoung Am Bldg.  
157-27 Samsung-Dong, Kangnam-Ku  
Seoul, Korea

Tel: 82-2-555-6818

Fax: 82-2-555-5779

**Network Associates  
South East Asia**

78 Shenton Way  
#29-02  
Singapore 079120

Tel: 65-222-7555

Fax: 65-220-7255

**Network Associates  
Latin America**

150 S. Pine Island Road, Suite 205  
Plantation, Florida 33324  
United States

Phone: (954) 452-1731

Fax: (954) 236-8031



# Table of Contents

<b>Preface</b> .....	<b>vii</b>
What Happened? .....	vii
Where Do Viruses Come From? .....	viii
On the Frontier .....	xii
How to Protect Yourself .....	xii
How To Contact Network Associates .....	xiii
 <b>Chapter 1. Introducing VirusScan</b> .....	<b>1</b>
Main Features .....	1
How Virus Detection Works .....	2
When Should I Scan for Viruses? .....	2
 <b>Chapter 2. Installing VirusScan</b> .....	<b>3</b>
Before You Start .....	3
System requirements .....	3
Installation Procedure .....	3
Testing your installation .....	5
 <b>Chapter 3. On-Access Scanning</b> .....	<b>7</b>
What is On-access Scanning? .....	7
Starting VShield .....	7
Using the VShield Status window .....	7
Configuring On-access Scanning .....	8
Configuring VShield detection .....	9
Configuring VShield actions .....	12
Configuring VShield alerts .....	14
Configuring VShield reports .....	15
Configuring VShield exclusions .....	17
Configuring VShield security .....	19

<b>Chapter 4. On-Demand Scanning .....</b>	<b>21</b>
What is On-demand Scanning? .....	21
Starting VirusScan .....	21
Configuring On-demand Scanning .....	22
Configuring VirusScan detection .....	22
Configuring VirusScan actions .....	24
Configuring VirusScan alerts .....	26
Configuring VirusScan reports .....	27
Configuring VirusScan exclusions .....	29
Saving Scan Settings .....	31
Viewing Virus Information .....	32
Displaying the Virus List .....	32
The Virus Information window .....	33
Using Password Protection .....	34
<b>Chapter 5. Scheduled Scanning .....</b>	<b>35</b>
Using the VirusScan Console .....	35
Creating a Scan Task .....	35
Selecting the program to be run .....	36
Setting the task schedule .....	37
Viewing the task properties .....	38
Copying, Pasting, or Deleting a Scan Task .....	39
Configuring a Scan Task .....	39
Using the Detection page .....	40
Using the Action page .....	42
Using the Alert page .....	43
Using the Report page .....	45
Using the Exclusion page .....	46
Using the Security page .....	48
<b>Chapter 6. Removing a Virus .....</b>	<b>51</b>
If You Suspect You Have a Virus .....	51
If viruses are removed .....	51
If viruses are not removed .....	52

---

If VirusScan Detects a Virus .....	52
Removing a virus found in a file .....	52
Removing a virus found in memory .....	52
Understanding false alarms .....	53
<b>Appendix A. Network Associates Support Services .....</b>	<b>55</b>
PrimeSupport Options for Corporate Customers .....	55
Support Services for Retail Customers .....	58
Network Associates Consulting and Training .....	59
<b>Appendix B. Preventing Virus Infection .....</b>	<b>61</b>
Keys to a Secure System Environment .....	61
Detecting New and Unknown Viruses .....	62
Updating your VirusScan data files .....	62
Validating the VirusScan Program Files .....	63
Creating an Emergency Disk .....	64
Creating a clean boot diskette .....	64
Write-Protecting a Diskette .....	66
<b>Appendix C. Shared Installations .....</b>	<b>67</b>
General Procedure .....	67
Changes to Files .....	67
Win.ini file .....	67
Autoexec.bat file .....	67
Avconsol.ini file .....	67
Limitations .....	68
<b>Appendix D. Reference .....</b>	<b>71</b>
VirusScan Command-line Options .....	71
VirusScan DOS Error Levels .....	78
VSH File Format .....	79
VSC File Format .....	84
<b>Glossary .....</b>	<b>91</b>
<b>Index .....</b>	<b>95</b>



McAfee VirusScan for Windows 3.1x is Network Associates' powerful desktop anti-virus solution. The VirusScan protection strategy has three components: on-access scanning, on-demand scanning, and scheduled scanning.

VirusScan continuously monitors your system for virus activity using its on-access component, VShield. If a virus is detected, you can automatically take action to remove the virus, move infected files to another location, or delete the infected files.

VirusScan can also be user-initiated to scan a file, folder, disk, or volume. This is the on-demand scanning component of VirusScan's protection strategy.

Scheduled scanning lets you configure VirusScan to perform specific scans at pre-determined times or intervals. This way, you can scan particularly vulnerable areas of your system often, or perform a thorough scan of the entire system while it is not being used.

VirusScan is an important element of a comprehensive security program that includes a variety of safety measures, such as regular backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program as a preventive measure to protect against future infection. For tips on creating a secure environment, see [Appendix B, "Preventing Virus Infection."](#)

## Main Features

- NCSA-certified scanner assures detection of 100 percent of the viruses found "in the wild." See the National Computer Security Association web site at <http://www.NCSA.com> for certification status.
- VShield, VirusScan's on-access scanner, provides real-time identification of both known and unknown viruses upon file access, create, copy, rename, and run; and system start-up.
- On-demand scanning provides user-initiated detection of known boot, file, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.
- Code Trace™, Code Poly™, and Code Matrix™ Scanning employ Network Associates' proprietary technologies for pinpoint virus identification accuracy.

- VirusScan can be configured for an automated response on virus detection, including logging, deletion, isolation, or cleaning. VirusScan can also be configured to send alerts and reports to a centralized server location.
- VirusScan includes a scheduler to set up daily, weekly, or monthly scans.
- Monthly updates of virus signatures and product upgrades are included with the purchase of a Network Associates subscription license to assure the best detection and removal rates.

## How Virus Detection Works

VirusScan monitors your computer and searches for characteristics (sequences of code) unique to each known virus. If a virus is detected, VirusScan takes whatever action you have configured it to take. For viruses that are encrypted or mutated, VirusScan uses algorithms for detection that rely on statistical analysis, heuristics, and code disassembly.

## When Should I Scan for Viruses?

VirusScan's on-access scanner will perform automatic scans of your system every time you access, create, copy, rename, or run a file, or start up your system. It also protects your system against viruses when you upload and download from networks.

For maximum protection, you should also use VirusScan's on-demand scanning feature to scan for viruses whenever you add files to your system. If you copy files from a diskette or download files from an online service, you should run VirusScan to ensure that a virus has not been introduced.

### Scan when you insert an unknown diskette

Every time you insert an unknown diskette in your drive, scan it before executing, installing, or copying its files.

### Scan when you install or download new files

Every time you install new software on your hard drive or download executable files from an online service, run VirusScan to check the files before you use them.

### Scan on a regular basis

Perform on-demand scans of your system regularly, from as frequently as once a day to once a month, depending on how susceptible your system is to virus infection. Schedule scans of your most vulnerable system areas for maximum security.

## Before You Start

Follow the steps below before you install VirusScan for Windows 3.1x. This will minimize the risk of spreading viruses that may already be present on your system.

1. Review the system requirements for VirusScan.
2. Ensure that your system is virus-free. If you suspect that your system is already infected, see [“If You Suspect You Have a Virus” on page 51](#) before you start the installation procedure.

## System requirements

- IBM-compatible personal computer running Windows 3.1x; 386 or better
- 5MB hard drive space
- 4MB of available memory (8MB recommended).

## Installation Procedure

This section describes the basic installation procedure. See [Appendix C, “Shared Installations”](#) for information on shared installations.

---

**NOTE:** If you suspect your system is already infected by a virus, see [“If You Suspect You Have a Virus” on page 51](#) before installing VirusScan.

---

Follow these steps to install VirusScan on your system:

1. Start Windows.
2. Do one of the following:
  - If you are installing from diskette or compact disc, insert the VirusScan installation diskette or compact disc.
  - If you are installing from files downloaded from a BBS or the Network Associates website, decompress the zipped files into a directory on your local drive or the network.

3. Choose **Run** from the File menu.
  - If you are installing from diskette, enter:  
`x:\setup.exe`  
where *x* is the drive that contains the diskette. Click **OK**.
  - If you are installing from compact disc, enter:  
`x:\win\setup.exe`  
where *x* is the drive that contains the compact disc. Click **OK**.
  - If you are installing from downloaded files, enter:  
`x:\path\setup.exe`  
where *x:\path* is the location of the files. Click **OK**.
4. The license agreement for VirusScan appears. Read it carefully, then click **Yes** to continue.
5. When the Welcome screen appears, read the information in it, then click **Next** to continue.
6. Select the installation type:
  - **Typical** performs a complete installation of VirusScan with the most common options.
  - **Compact** installs VirusScan with the minimum required options.
  - **Custom** lets you select the VirusScan components that you want to install.
7. Select the directory where VirusScan will be installed.
  - Enter a directory name in the text box provided, then click **Next**.
  - Click **Browse** to navigate to a specific directory, then click **Next**.
8. When prompted, review your settings and click **Next** to continue. VirusScan files are copied to the hard drive.
9. You are prompted to insert a blank diskette into the A: drive. Follow the on-screen instructions to create an emergency disk that will help you recover in the event of a boot-sector infection.

---

**NOTE:** If don't want to create an emergency disk now, click **Cancel**. You can create an emergency disk later by double-clicking the emergency disk icon in the VirusScan program group.

---



10. Click **Yes** to review the What's New text file for information about VirusScan's new features.
11. Review the changes made to files on your system, then click **Next**.
12. Select **Yes** to restart your computer, then click **Finish**. The system restarts. All changes are enabled. VirusScan is now running.

---

**NOTE:** If you canceled the emergency disk creation in step 8, you should make an emergency disk immediately. See [“Creating an Emergency Disk” on page 64](#) for more information.

---

## Testing your installation

The Eicar Standard AntiVirus Test File is a combined effort by anti-virus vendors throughout the world to create a single standard by which customers can verify their anti-virus installations.

To test your installation, copy the following line into its own file and name it EICAR.COM.

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

---

**NOTE:** Make sure that this character string appears on a single line in the actual file.

---

When finished, you will have a 69- or 70-byte file. When VirusScan scans this file, it will report finding the EICAR-STANDARD-AV-TEST-FILE virus. Despite what VirusScan reports, however, it has not really found a virus. Instead, it has successfully found a file designed to test its virus-detection capability.

Delete the EICAR.COM file when installation testing is completed so that unsuspecting users are not unnecessarily alarmed.



## What is On-access Scanning?

On-access scanning is one of the three components of the protection strategy used by VirusScan for Windows 3.1x. (The others are on-demand scanning and scheduled scanning.)

On-access scanning is done by VShield, a memory-resident program that uses a series of VxD (dynamically loaded virtual device driver) modules to provide real-time protection for your system. On-access scanning helps prevent virus infection by automatically checking programs—such as files, directories, drives, and any media—as they are accessed.

In this chapter, you will find procedures for starting and configuring VShield, VirusScan's on-access scanning component.

## Starting VShield

VShield, VirusScan's on-access scanner, is a virtual device driver. By default, VShield is automatically enabled each time you start Windows, and is active in the background during each Windows session.

You can enable VShield in either of these ways:

- Double-click the VShield desktop icon. If the leftmost button in the resulting dialog box reads "Disable," VShield is enabled. If it reads "Enable," you must click the button to enable VShield.
- Run VSHWIN.EXE, which you can find in the installation directory.

If for some reason VShield is not active when you start Windows, you will need to reconfigure VShield to load at start-up. For information on how to do this, see ["Configuring On-access Scanning" on page 8](#).

## Using the VShield Status window

When VShield is enabled, you can use the VShield Status window ([Figure 3-1 on page 8](#)) to configure your scanning options or view the status of scanned files. To display this window, double-click the VShield icon on the desktop.

---

**NOTE:** If you don't see the VShield icon, run the VShield Configuration Manager (VSHCFG16.EXE) and select **Show Icon on the desktop**.

---



**Figure 3-1. VShield Status window**

The VShield Status window shows the name of the last file scanned, the number of files scanned, the number of infected files, and the number of files that have been cleaned, deleted, or moved.

In addition, the following options are available:

- **Disable/Enable** activates or deactivates on-access scanning during the current Windows session.
- **Properties** configures the detection, action, and reporting settings of on-access scanning. See [“Configuring On-access Scanning” on page 8](#) for more information.
- **Close** closes the VShield Status window.

## Configuring On-access Scanning

Use the VShield Configuration Manager to configure on-access scanning. You can start the Configuration Manager in either of these ways:

- Select **Properties** from the VShield Status window. See [“Using the VShield Status window”](#) for details on displaying this window.
- Run VSHCFG16.EXE, which is found in the installation directory (the default location is **C:\Neta\Viruscan**).

The VShield Configuration Manager appears, with the Detection page on top ([Figure 3-2 on page 9](#)).

## Configuring VShield detection

Use the Detection page (Figure 3-2) to tell VShield which items to scan and when scanning should take place.



**Figure 3-2. VShield Configuration Manager (Detection page)**

Follow these steps to configure the detection options:

1. Select the event(s) that will make VShield launch a scan.
  - **Run** scans whenever you run a file.
  - **Create** scans whenever you create a file.
  - **Copy** scans whenever you copy a file.
  - **Rename** scans whenever you rename a file.

---

**NOTE:** For maximum protection, Network Associates recommends selecting all of the items above.

---

2. Select the event(s) that will make VShield scan floppy diskettes.
  - **Access** scans when a diskette is accessed.
  - **Shutdown** scans the floppy drive each time you shut down your system.

---

**NOTE:** For maximum protection, Network Associates recommends selecting all of the items above.

---

3. Select the file types that VShield should scan.

- **All Files** scans all files, no matter the type.
- **Program Files Only** scans only files with certain extensions. To change the extensions included in this list, click **Extensions**.

---

**NOTE:** Default extensions are .EXE, .COM, .DO?, and .XL? (the question mark is a wildcard). This list makes a scan that checks Word and Excel document and template files (.DOC, .DOT, .XLS, and .XLT) as well as program files.

---

- **Compressed Files** scans files compressed with PKLITE or LZEXE.

4. Configure the general preferences.

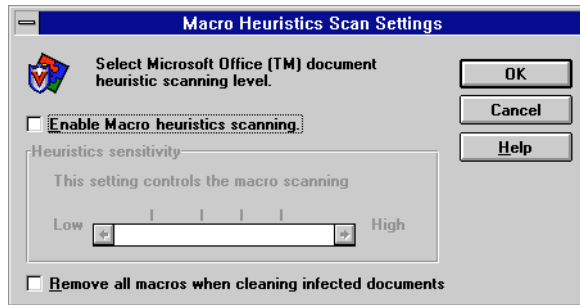
- **Load VShield at startup** activates on-access scanning when you start Windows.
- **VShield can be disabled** allows on-access scanning to be disabled.
- **Show icon on the desktop** lets you view the VShield Status window and select VShield properties using a desktop icon.

---

**NOTE:** Network Associates recommends selecting all items. However, system administrators may want to enable only **Load VShield at start-up** when configuring users' software. For information on VShield's administrator lockdown capabilities, see [“Configuring VShield security” on page 19](#).

---

5. If desired, click **Macro Heuristics** to set the scanning that VirusScan uses to clean virus-like macros from Microsoft Word and Excel documents. The Macro Heuristics Scan Settings dialog box ([Figure 3-3 on page 11](#)) appears.



**Figure 3-3. Macro Heuristics Scan Settings dialog box**

- a. Enable or disable macro heuristics scanning. It is enabled by default.
- b. Use the slider to set the sensitivity of the macro heuristics scanning.
- c. Decide whether you want VirusScan to remove macros when it is cleaning infected documents. By default, VirusScan removes macros.

---

**NOTE:** If you move the slider up to High *and* select Remove All Macros when Cleaning Infected Documents, VirusScan removes every macro from any Word or Excel document that is scanned—not just virus-like macros.

---

- d. Click **OK**.
6. Click one of the following:
  - **Apply** saves your changes without exiting the Vshield Configuration Manager.
  - **OK** saves your changes and returns to the Vshield Status window.
  - **Cancel** returns to the VShield Status window without saving your changes.

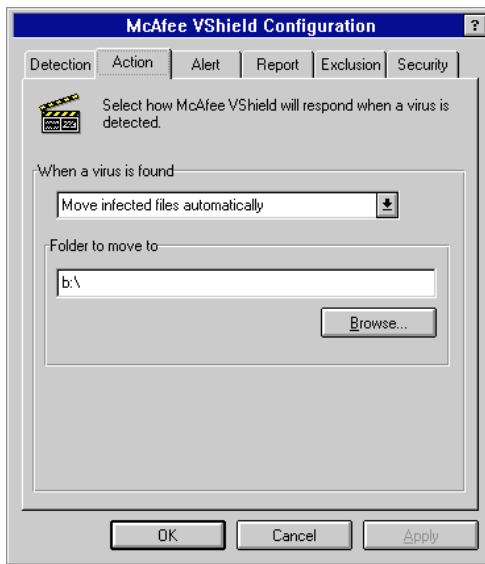
---

**NOTE:** To lock and password-protect any changes you made, see [“Configuring VShield security” on page 19](#).

---

## Configuring VShield actions

Use the Action page (Figure 3-4) to tell VShield what to do if it detects a virus.



**Figure 3-4. VShield Configuration Manager (Action page)**

Follow these steps to configure the action settings:

1. On the When a Virus is Found list, choose one of the following actions:
  - **Prompt user for action** makes VShield ask what to do each time it finds a virus. The possible options are:
    - **Clean file.**
    - **Delete file.**
    - **Exclude file.**
    - **Stop access.**
    - **Continue access.** This action is recommended for attended systems.
  - **Move infected files automatically** moves each infected file to a folder that you choose. Specify a path in the Folder To Move To text box or choose **Browse** to locate a folder.



The path to the folder can be relative. For example, if you type \Infected in the text box, VShield creates a folder called "Infected" on the drive where the infected file was found. Any infected file is moved to this folder.

---

**NOTE:** If an infected file cannot be cleaned or VShield lacks the proper file access permissions, file access will be denied.

---

- **Clean infected files automatically** makes VShield clean an infected file without asking for permission.
- **Delete infected files automatically** makes VShield delete an infected file without asking for permission. You must then restore a clean copy of the deleted file from backups.
- **Deny access to infected files and continue** prevents any programs on your system from accessing an infected file until you tell VShield what to do with that file. This action is recommended for systems left unattended during scans.

2. Click one of the following:

- **Apply** saves your changes without exiting the Vshield Configuration Manager.
- **OK** saves your changes and returns to the Vshield Status window.
- **Cancel** returns to the VShield Status window without saving your changes.

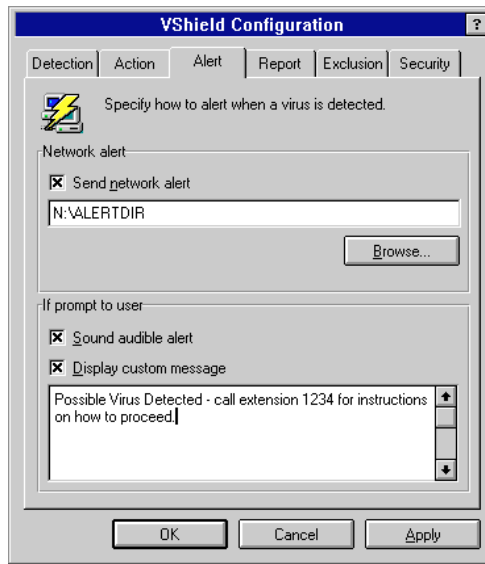
---

**NOTE:** To lock and password-protect any changes you made, see ["Configuring VShield security" on page 19](#).

---

## Configuring VShield alerts

Use the Alert page (Figure 3-5) to tell VShield which method to use when warning you or others when a virus is detected.



**Figure 3-5. VShield Configuration Manager (Alert page)**

Follow these steps to configure VShield alerting:

1. Select **Send network alert** to have VShield send alerts to a network path monitored by NetShield, Network Associates's server anti-virus solution. Click **Browse** to navigate to the directory.

---

**NOTE:** This directory should contain the Centralized Alerting file, CENTALERT.TXT. For more information on Centralized Alerting, see the NetShield documentation.

---

2. Select **Sound audible alert** and/or **Display custom message**. You can change the message by clicking in the text box and editing the text.
3. Click one of the following:
  - **Apply** saves your changes without exiting the Vshield Configuration Manager.
  - **OK** saves your changes and returns to the Vshield Status window.

- **Cancel** returns to the VShield Status window without saving your changes.

---

**NOTE:** To lock and password-protect any changes you made, see [“Configuring VShield security” on page 19.](#)

---

## Configuring VShield reports

Use the Report page (Figure 3-6) to tell VShield how to log virus activity and which information to include in the log entry.



**Figure 3-6. VShield Configuration Manager (Report page)**

---

**NOTE:** The log file is a text file that can be viewed using any text editor, such as Notepad.

---

Follow these steps to configure report settings.

1. Select **Log to file**, then do one of the following:
  - Enter a path and file in the text box
  - Choose a path by clicking **Browse**.
2. Limit the size of the log file by selecting **Limit size** and specifying a size between 10KB and 999KB.

---

**NOTE:** The default log file is **C:\Neta\Viruscan\VSHLOG.TXT**.  
The default maximum log file size is 100KB.

---

3. Choose the information that should be included in the log file. Options include:
  - Virus detection
  - Virus cleaning
  - Infected file deletion
  - Infected file move
  - Session settings
  - Session summary
  - Date and time
  - User name.
4. Click one of the following:
  - **Apply** saves your changes without exiting the Vshield Configuration Manager.
  - **OK** saves your changes and returns to the Vshield Status window.
  - **Cancel** returns to the VShield Status window without saving your changes.

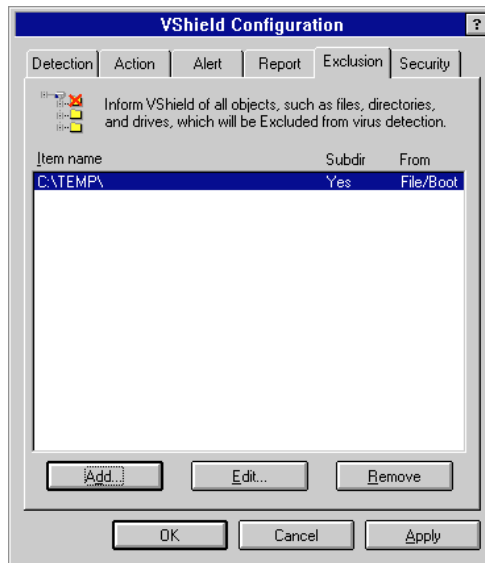
---

**NOTE:** To lock and password-protect any changes you made, see [“Configuring VShield security” on page 19](#).

---

## Configuring VShield exclusions

Use the Exclusion page (Figure 3-7) to exclude items from scans.



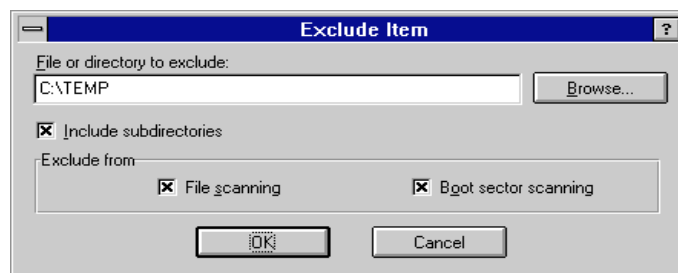
**Figure 3-7. VShield Configuration Manager (Exclusion page)**

**NOTE:** The folder C:\Neta\Viruscan\Infected is automatically excluded.

### Adding an item to the exclusion list

To add an item to the exclusion list, follow these steps:

1. Click **Add** on the Exclusion page. The Exclude Item dialog box (Figure 3-8) appears.



**Figure 3-8. Exclude Item dialog box**

2. Type the path to the file or folder you want to exclude from scanning, or click **Browse** to locate a folder.

---

**NOTE:** You can browse to folders only. To exclude a file, manually type its path and file name in the Exclude Item dialog box.

---

3. Select **Include subfolders** to exclude all subfolders within the selected folder.
4. If desired, exclude the folder from file scanning or boot sector scanning by selecting the appropriate box(es).
5. Click **OK**.
6. Do one of the following:
  - Click **Apply** to save your changes without exiting the Configuration Manager.
  - Click **OK** to save your changes and return to the VShield Status window.
  - Click **Cancel** to return to the VShield Status window without saving your changes.

---

**NOTE:** To lock and password-protect any changes you made, see [“Configuring VShield security” on page 19](#).

---

## Removing an item from the exclusion list

To remove an item from the list, follow these steps:

1. Select the item, then click **Remove**.
2. Do one of the following:
3. Click one of the following:
  - **Apply** saves your changes without exiting the Vshield Configuration Manager.
  - **OK** saves your changes and returns to the Vshield Status window.
  - **Cancel** returns to the VShield Status window without saving your changes.

---

**NOTE:** To lock and password-protect any changes you made, see [“Configuring VShield security” on page 19](#).

---

## Editing an item on the exclusion list

To edit an existing exclusion list item, follow these steps

1. Select the item, then click **Edit**.
2. The Exclude Item dialog box ([Figure 3-8 on page 17](#)) appears. Make your changes, then click **OK**.
3. Click one of the following:
  - **Apply** saves your changes without exiting the Vshield Configuration Manager.
  - **OK** saves your changes and returns to the Vshield Status window.
  - **Cancel** returns to the VShield Status window without saving your changes.

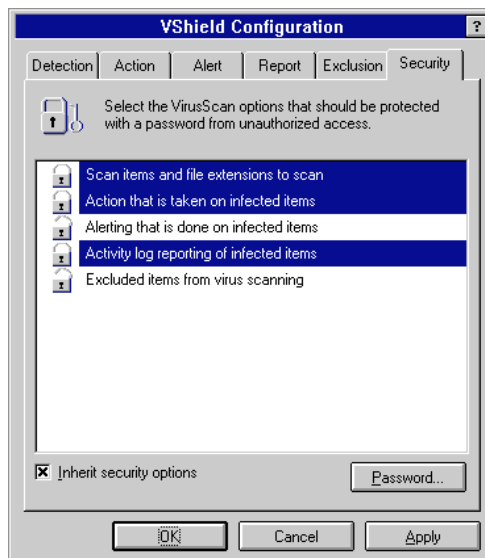
---

**NOTE:** To lock and password-protect any changes you made, see [“Configuring VShield security” on page 19](#).

---

## Configuring VShield security

Use the Security page ([Figure 3-9](#)) to lock and password-protect VShield settings. You might use this feature if you are a system administrator and want to keep users from compromising security by changing VShield settings.



**Figure 3-9. VShield Configuration Manager (Security page)**

Follow these steps to lock VShield settings:

1. Select which of the following VShield settings you want to password protect:

- **Scan items and file extensions to scan**
- **Action that is taken on infected items**
- **Alerting that is done on infected items**
- **Activity log reporting of infected items**
- **Excluded items from virus scanning.**

---

**NOTE:** Each setting that is password protected will be highlighted, and the lock to its left will be closed.

---

2. Click **Password** to create or change a password. You will be prompted to enter and confirm your password.
3. Click one of the following:
  - **Apply** saves your changes without exiting the Vshield Configuration Manager.
  - **OK** saves your changes and returns to the Vshield Status window.
  - **Cancel** returns to the VShield Status window without saving your changes.



## What is On-demand Scanning?

On-demand scanning is one of the three components of the protection strategy used by VirusScan for Windows 3.1x. (The others are on-access scanning and scheduled scanning.)

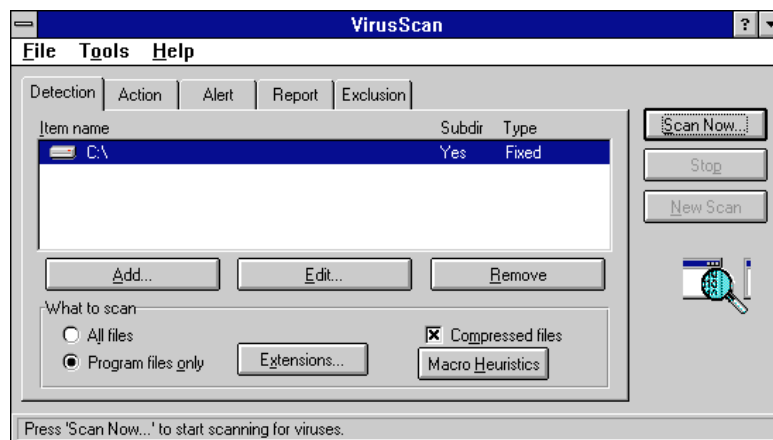
On-demand scanning lets you scan specific items as you are working, and scan new media or specific files to determine whether a computer virus is present. VirusScan immediately detects known boot, file, multi-partite, stealth, encrypted, and polymorphic viruses located within files, drives, and diskettes.

In this chapter, you'll find procedures for starting VirusScan's on-demand component, as well as steps you need to take to configure and customize scanning functions.

## Starting VirusScan

To start VirusScan, double-click on the VirusScan icon in the VirusScan program group. As it loads, VirusScan performs a self-check of its program files and your computer's memory to ensure that they are virus-free.

Once the self-check is complete, the VirusScan Main window ([Figure 4-1](#)) appears, with the Detection page on top.



**Figure 4-1. VirusScan Main window (Detection page)**

---

**NOTE:** If VirusScan fails the self-check or exits Windows while loading, turn off your computer and run the VirusScan command-line program from the emergency disk. See [“Creating an Emergency Disk” on page 64](#) for instructions on making an emergency disk.

---

From the Main window, you can establish scan settings, start an on-demand scan, view the activity log and virus list, print reports, and view scan results.

## Configuring On-demand Scanning

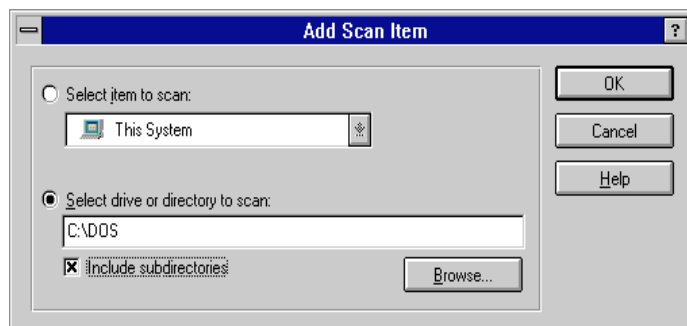
You access the configurable features of VirusScan through five tabbed pages. The following sections explain how to use these pages to configure VirusScan to suit your needs.

## Configuring VirusScan detection

Before scanning or cleaning your system with VirusScan, you must use the Detection page to specify the items to be included in the scan.

To select drives, directories, or files for scanning, follow these steps:

1. Start VirusScan. The VirusScan main window appears, with the Detection page on top ([Figure 4-1 on page 21](#)).
2. To add an item to the list, click **Add**. The Add Scan Item dialog box appears ([Figure 4-2](#)). (The C: drive is selected by default.)



**Figure 4-2. Add Scan Item dialog box**

3. To add groups of drives or media, select **Select item to scan**, then choose one of the following options:
  - **This System** scans all fixed, removable, and network volumes connected to your computer.

- **All Removable Media** scans all local removable media, such as floppy disks and compact discs.
- **All Fixed Disks** scans all local hard drives.
- **All Network Drives** scans all mapped network volumes.

---

**NOTE:** All directories and subdirectories on the location you select will be scanned.

---

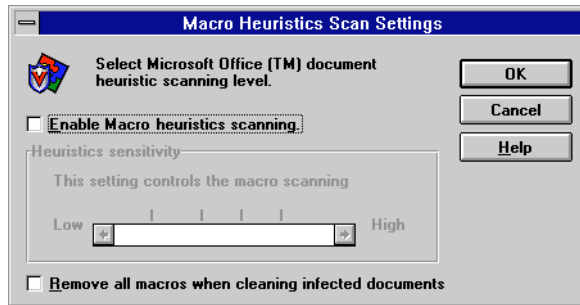
4. To add a specific drive, file, or folder, select **Select drive or directory to scan** and then do one of the following:
  - Click in the text box and enter the path to the item you want to scan.
  - Click **Browse** to navigate to the file, drive, or folder.
5. If desired, select Include subdirectories to scan the subdirectories in the drive or directory you chose in [Step 4](#).
6. Click **OK**. The items you selected appear in the Selections list.
7. To remove an item from the list to be scanned, select it from the list and click **Remove**. The item disappears.
8. Select the file types VirusScan should check for viruses.
  - Select **All files** to scan all files, no matter what type. This results in a more thorough—but slower—scan.
  - Select **Program files only** to scan only files with certain extensions. To edit the extensions on this list, click **Extensions**.

---

**NOTE:** Default extensions are .EXE, .COM, .DO?, and .XL? (the question mark is a wildcard). This list scans Word and Excel document and template files (.DOC, .DOT, .XLS, and .XLT) as well as program files.

---

- Select **Compressed files** to scan inside files compressed with PKLITE or LZEXE.
9. If desired, click **Macro Heuristics** to set the scanning that VirusScan uses to clean virus-like macros from Microsoft Word and Excel documents. The Macro Heuristics Scan Settings dialog box ([Figure 4-3 on page 24](#)) appears.



**Figure 4-3. Macro Heuristics Scan Settings dialog box**

- a. Enable or disable macro heuristics scanning. It is enabled by default.
- b. Use the slider to set the sensitivity of the scan.
- c. Decide whether you want VirusScan to remove macros when it is cleaning infected documents. By default, VirusScan removes macros.
- d. Click **OK**.

---

**NOTE:** If you move the slider up to High *and* select Remove All Macros when Cleaning Infected Documents, VirusScan removes every macro from any Word or Excel document that is scanned—not just virus-like macros.

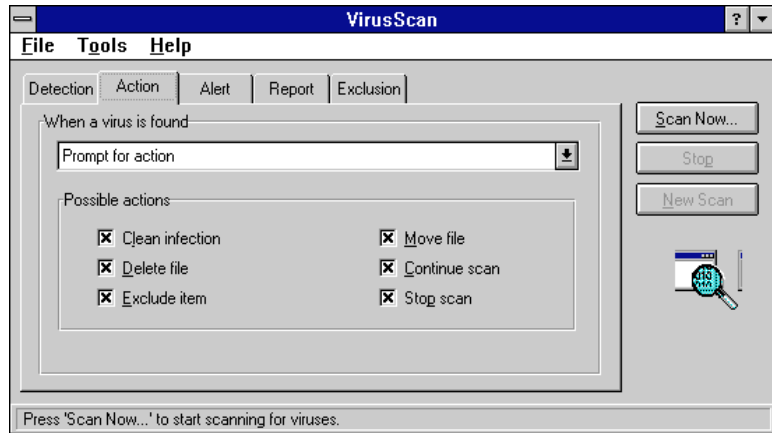
---

10. Do one of the following:
  - To save these selections in a settings file, see [“Saving Scan Settings” on page 31](#).
  - To further configure VirusScan, select another page.
  - To scan immediately using the current settings, click **Scan**.
  - To lock and password-protect these settings, see [“Using Password Protection” on page 34](#).

## Configuring VirusScan actions

Follow these steps to tell VirusScan what actions to take when it detects a virus:

1. Start VirusScan and select the Action page. The VirusScan main window appears, with the Action page on top ([Figure 4-4 on page 25](#)).



**Figure 4-4. VirusScan Main window (Action page)**

2. Select one of the following actions:

- **Prompt for action** makes VirusScan ask what to do each time it encounters a virus. Use this option if the computer will be attended while the scan is running.

---

**NOTE:** Choose the actions available to the user by selecting the appropriate checkboxes under Possible Actions.

---

- **Move infected files to a directory** tells VirusScan to automatically move all infected files to a quarantine directory.

---

**NOTE:** You must specify the directory where you want the files moved. The default directory is `\infected`. Unless you specify the entire path (e.g., `C:\mystuff\infected`), VirusScan creates the directory at the root of the drive on which the virus was found (e.g., `C:\infected`).

---

- **Clean infected file** tells VirusScan to automatically clean viruses from infected files.
- **Delete infected file** tells VirusScan to automatically delete infected files it finds.

---

**NOTE:** This option permanently removes the infected files from your system. You must restore deleted files from uninfected backups.

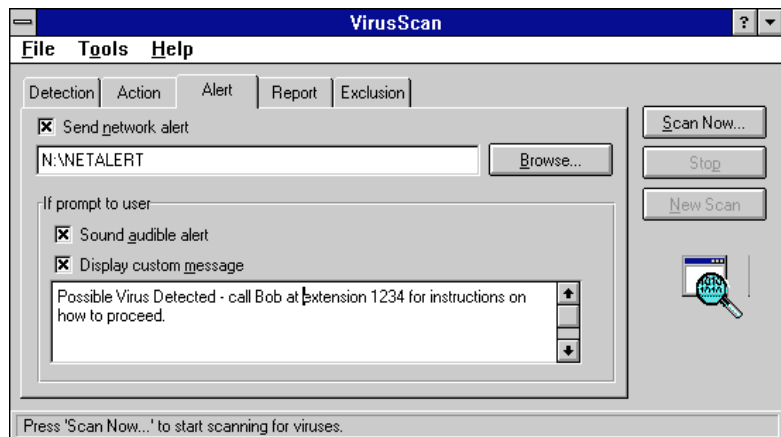
---

- **Continue scanning** tells VirusScan to ignore infected files and continue scanning. VirusScan does not take any action when it detects a virus.
3. Do one of the following:
    - To save these selections in a settings file, see [“Saving Scan Settings” on page 31](#).
    - To further configure VirusScan, select another page.
    - To scan immediately using the current settings, click **Scan**.
    - To lock and password-protect these settings, see [“Using Password Protection” on page 34](#).

## Configuring VirusScan alerts

VirusScan can be configured to send an alert when it detects a virus infection. Use the procedure below to configure VirusScan’s alerting features:

1. Start VirusScan and select the Alert page. The VirusScan main window (Figure 4-5) appears, with the Alert page on top.



**Figure 4-5. VirusScan Main window (Alert page)**

2. Click **Send network alert** if you want VShield to send alerts to a network path monitored by NetShield, Network Associates’s server anti-virus solution. Click **Browse** to navigate to the directory.

---

**NOTE:** This directory should contain the Centralized Alerting file, CENTALERT.TXT. For more information on Centralized Alerting, see the NetShield documentation.

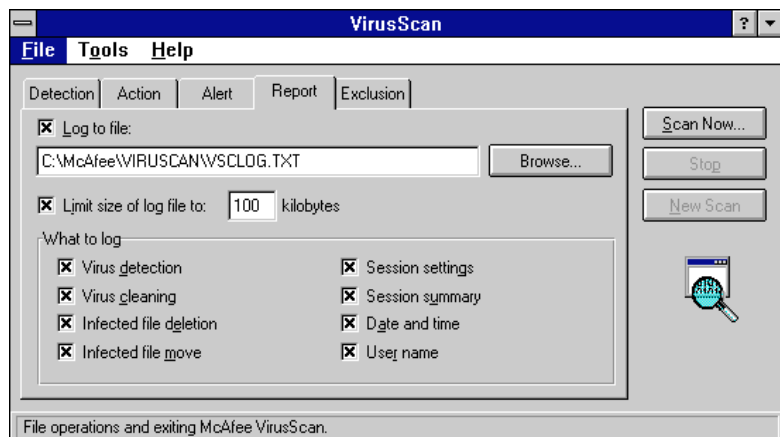
---

3. If you selected **Prompt for action** on the Action page, select **Sound audible alert** and/or **Display custom message**. You can change the message by clicking in the text box and editing the message text.
4. Do one of the following:
  - To save these selections in a settings file, see [“Saving Scan Settings” on page 31](#).
  - To further configure VirusScan, select another page.
  - To scan immediately using the current settings, click **Scan**.
  - To lock and password-protect these settings, see [“Using Password Protection” on page 34](#).

## Configuring VirusScan reports

Follow these steps to configure where and how VirusScan logs its activity:

1. Start VirusScan and click the Report page. The VirusScan main window appears, with the Report page on top ([Figure 4-6](#)).



**Figure 4-6. VirusScan Main window (Report page)**

2. Select **Log to file**, then do one of the following:
  - Enter a path and file in the text box
  - Choose a path by clicking **Browse**.
3. Limit the size of the log file by selecting **Limit size** and specifying a maximum size.

---

**NOTE:** The default log file is **C:\Neta\Viruscan\VSHLOG.TXT**. This is a plain text file you can view with any text editor (such as Notepad) or by choosing **View activity log** from the File menu.

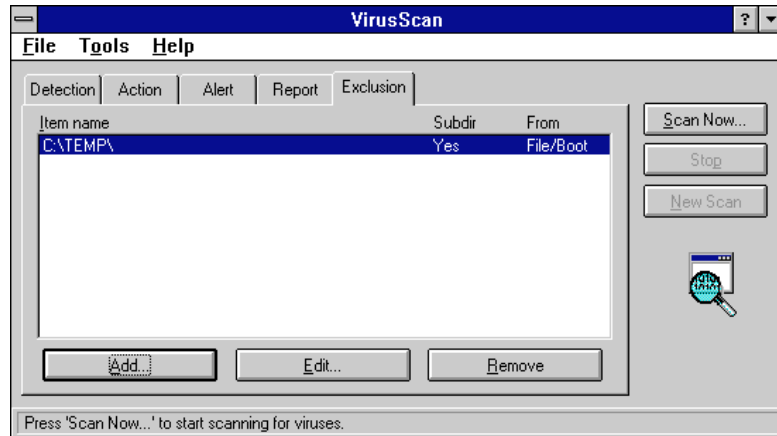
---

4. Choose the information that should be included in the log file. Options include:
  - Virus detection
  - Virus cleaning
  - Infected file deletion
  - Infected file move
  - Session settings
  - Session summary
  - Date and time
  - User name.
5. Do one of the following:
  - To save these selections in a settings file, see [“Saving Scan Settings” on page 31](#).
  - To further configure VirusScan, select another page.
  - To scan immediately using the current settings, click **Scan**.
  - To lock and password-protect these settings, see [“Using Password Protection” on page 34](#).



## Configuring VirusScan exclusions

The Exclusion page (Figure 4-7) lets you configure VirusScan to exclude files, folders, or volumes from its scan.



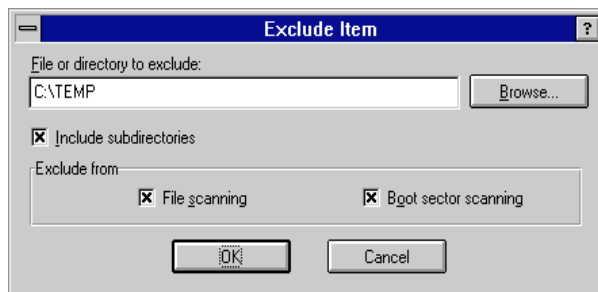
**Figure 4-7. VirusScan Main window (Exclusion page)**

**NOTE:** The folder C:\Neta\Viruscan\Infected is automatically excluded.

### Adding an item to the exclusion list

To add an item to the exclusion list, follow these steps:

1. On the Exclusion page, click **Add**. The Exclude Item dialog box (Figure 4-8) appears.



**Figure 4-8. Exclude Item dialog box**

2. Enter the path to the item you want to exclude or click **Browse** to navigate to the item. You may exclude a file, a folder, or an entire disk.
3. Select **Include subfolders** you do not want VirusScan to scan the subfolders in the folder you have excluded.
4. If desired, exclude the folder file scanning or boot sector scanning by checking the appropriate box(es).
5. Click **OK**.
6. Do one of the following:
  - To save these selections in a settings file, see [“Saving Scan Settings” on page 31](#).
  - To further configure VirusScan, select another page.
  - To scan immediately using the current settings, click **Scan**.
  - To lock and password-protect these settings, see [“Using Password Protection” on page 34](#).

### Removing an item from the exclusion list

To remove an item from the list, follow these steps:

1. On the Exclusion page, select the item you want to remove.
2. Click **Remove**.
3. Do one of the following:
  - To save these selections in a settings file, see [“Saving Scan Settings” on page 31](#).
  - To further configure VirusScan, select another page.
  - To scan immediately using the current settings, click **Scan**.
  - To lock and password-protect these settings, see [“Using Password Protection” on page 34](#).

### Editing an item on the exclusion list

To edit an existing item on the exclusion list, follow these steps

1. On the Exclusion page, select the item you want to edit.
2. Click **Edit**.
3. The Exclude Item dialog box ([Figure 4-8 on page 29](#)) appears. Make your changes, then click **OK**.

4. Do one of the following:
  - To save these selections in a settings file, see [“Saving Scan Settings” on page 31](#).
  - To further configure VirusScan, select another page.
  - To scan immediately using the current settings, click **Scan**.
  - To lock and password-protect these settings, see [“Using Password Protection” on page 34](#).

## Saving Scan Settings

The VirusScan File menu gives you two options for saving your settings:

- Save as default
- Save settings.

In each case, the settings are saved to a .VSC file—a configuration text file that outlines VirusScan’s settings. The name of each variable is followed by the equal sign (=) and a value that indicates which settings have been selected for VirusScan configuration.

The following subsections tell when you should use each save option.

### When to save as default

If you want VirusScan to use a changed configuration as its default settings, choose **Save as default**. Your changes are saved to the DEFAULT.VSC file.

### When to save settings

If you need more than one VirusScan configuration—perhaps you want to scan two local drives with different VirusScan settings—then you should choose **Save settings**. You will be asked to specify a name for a new .VSC file, and the current VirusScan settings are then saved there. Once the file is saved, you can use it by double-clicking on its name in the Windows File Manager.

---

**NOTE:** You may need to associate the .VSC file with VirusScan the first time you use it. See your Windows documentation for instructions.

---

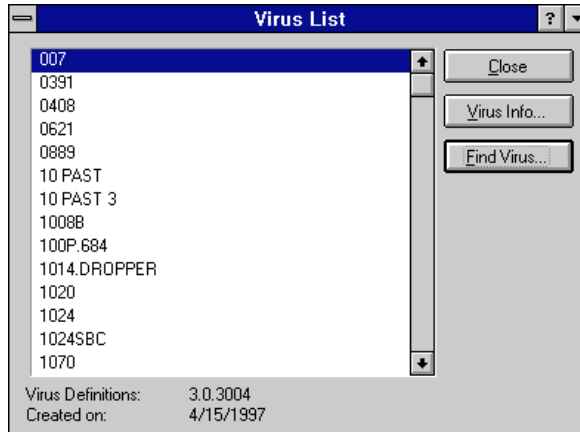
## Viewing Virus Information

The Virus List is a comprehensive list of viruses detected by VirusScan. The list provides a description of the viruses, including the infector type, virus characteristics, virus size, and cleaning status.

## Displaying the Virus List

To display and use the Virus List, follow these steps:

1. Start VirusScan. The VirusScan main window (Figure 4-1 on page 21) appears.
2. Choose **Virus List** from the Tools menu. The Virus List window (Figure 4-9) appears.

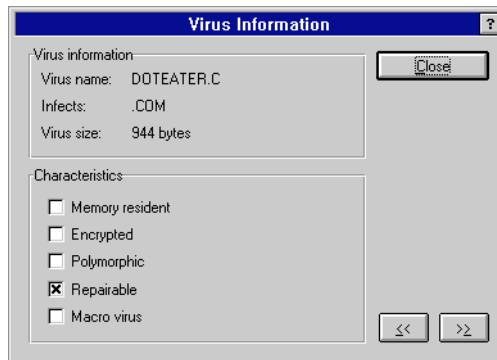


**Figure 4-9. Virus List window**

3. To view information about a virus, do one of the following:
  - Select it from the list and click **Virus Info**. The Virus Information window (Figure 4-10) appears.
  - Click **Find Virus** and type the name of the desired virus in the text box that appears. When you see the virus you want in the virus list, close the text box and click **Virus Info**. The Virus Information window (Figure 4-10) appears.

## The Virus Information window

The Virus Information window (Figure 4-10) gives detailed information about the virus you selected on the Virus List window.



**Figure 4-10. Virus Information window**

The Virus Information section of the window gives basic information about the virus:

- **Virus name** is the name of the virus.
- **Infects** tells what the virus infects, such as files of a particular type, the boot sector, or the master boot record.
- **Virus size** gives the size of the virus, in bytes.

The Characteristics section describes the behavior of the selected virus:

- **Memory Resident** means that the virus is a memory resident program that acts similar to a TSR or a device driver, and remains active in memory while the computer is running.
- **Encrypted** means that the virus tries to evade detection by self-encrypting.
- **Polymorphic** means that the virus tries to evade detection by changing its internal structure or its encryption techniques.
- **Repairable** means that a remover for the virus is available.
- **Virus Size** tells the amount, in bytes, by which the virus increases the size of a file it infects.

---

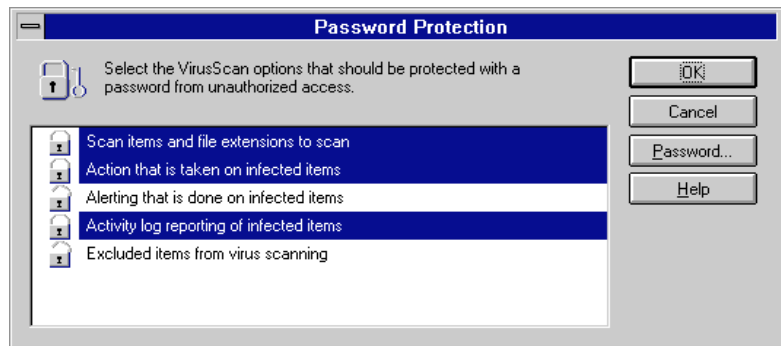
**NOTE:** The default size for an MBR or boot sector virus is 512 bytes.

---

## Using Password Protection

You can password-protect VirusScan settings to prevent unintentional changes from being made. Network administrators can use this option to prevent users causing a security breach by changing VirusScan settings. To use password protection, follow these steps:

1. Start VirusScan. The VirusScan main window appears (see [Figure 4-1 on page 21](#)).
2. Select Password Protect from the Tools menu. The Password Protection dialog box appears ([Figure 4-11](#)).



**Figure 4-11. Password Protection dialog box**

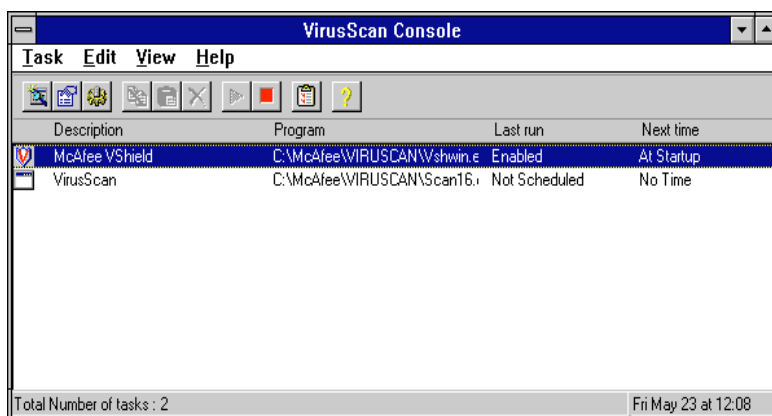
3. Select items from the list that you want to be password-protected.
4. Click **Password** to enter a password. You will be asked to confirm your password.
5. Do one of the following:
  - To save these settings and return to the Main window, click **OK**.
  - To cancel your changes and return to the Main window, click **Cancel**.

Scheduled scanning is one of the three components of the protection strategy used by VirusScan for Windows 3.1x. (The others are on-access scanning and on-demand scanning). Scheduled scanning lets you configure VirusScan to start a scan automatically at a predetermined time. Scans can be run once, daily, weekly, monthly, or even hourly.

In this chapter, you'll find procedures for using the VirusScan Console to configure and customize scheduled scanning.

## Using the VirusScan Console

Use the Virus Scan Console ([Figure 5-1](#)) to configure scheduled scanning. Start the VirusScan Console by double-clicking its icon in the VirusScan program group or by choosing **McAfee VirusScan Console** on the VirusScan Tools menu.



**Figure 5-1. VirusScan Console**

To view a task's properties, double-click on its name or right-click on the desired task and choose **Properties**. The Task Properties window ([Figure 5-2 on page 36](#)) appears, with the Program page on top.

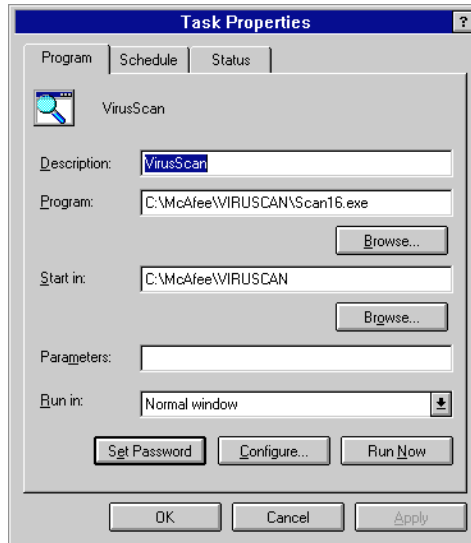
## Creating a Scan Task

The VirusScan Console uses scan tasks to perform and track scheduled scanning. You can configure and schedule each of these tasks separately, using tabbed pages on the Task Properties window.

## Selecting the program to be run

Follow these steps to select the program that a new scan task will run:

1. At the VirusScan Console, choose **New Task** on the Task menu or right-click on the task list and choose **New Task**. The Task Properties window (Figure 5-2) appears, with the Program page on top.



**Figure 5-2. Task Properties window (Program page)**

2. The default location of the VirusScan program file (C:\Neta\Viruscan\SCAN16.EXE) appears in the Program text box automatically. If desired, you can enter another location in the text box or browse for the location.
3. If you want to use the VirusScan Console to schedule another program, enter its path in the Program text box.

---

**NOTE:** You can use the Parameter text box to enter a program parameter. For example, if you are scheduling Notepad.exe, you could enter the name of a text file (e.g., WHATSNEW.TXT) to be opened when the program is run.

---

4. Enter the name of the task in the Description text box.
5. If desired, click **Set Password** to set a password for the task. The dialog box that appears will ask you to enter and confirm the password.
6. Configure the scanning options for the task. To do this, see [“Configuring a Scan Task” on page 39](#).

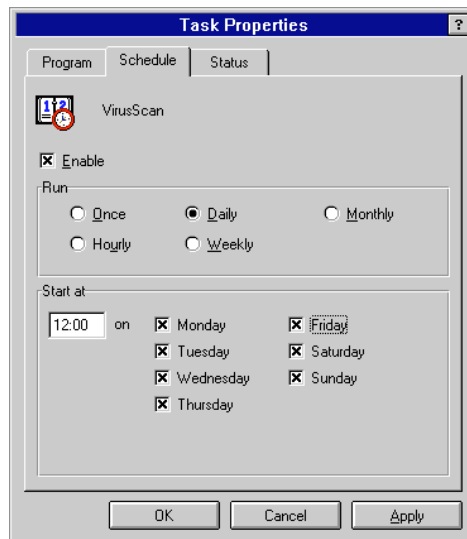


7. Click **Run Now** if you want the task to run immediately.
8. Click one of the following:
  - **OK** saves the changes and returns to the VirusScan Console.
  - **Cancel** abandons the changes and return to the VirusScan Console.
  - **Apply** applies the changes. You can then select another page.

## Setting the task schedule

Follow these steps to set the schedule for a scan task:

1. Select the Schedule page (Figure 5-3). (The appearance of the window varies slightly according to which option is selected.)



**Figure 5-3. Task Properties window (Schedule page)**

2. Select or deselect **Enable** to enable or disable the task.

---

**NOTE:** If the task is not enabled, it will not be run on schedule.

---

3. Specify the frequency of the scan:
  - If you select **Once**, also specify the time and date for the task.
  - If you select **Daily**, also select the day(s) of the week and time when the task should run.

- If you select **Monthly**, also select the day of the month and the time when the task should run.
- If you select **Hourly**, also select the number of minutes after the hour when task should run.
- If you select **Weekly**, also select the day(s) and time when the task should run.

---

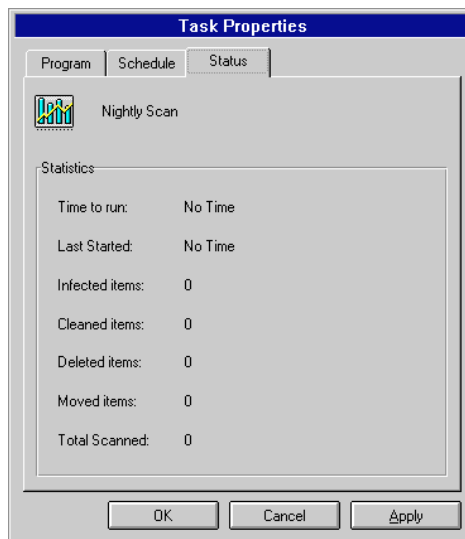
**NOTE:** The time must be entered in 24-hour format (i.e., 20:27, not 8:27 p.m.) for all options except **Hourly**.

---

4. Click one of the following:
  - **OK** saves the changes and returns to the VirusScan Console.
  - **Cancel** abandons the changes and return to the VirusScan Console.
  - **Apply** applies the changes. You can then select another page.

## Viewing the task properties

1. Select the Status page (Figure 5-4) to view statistics for the current task.



**Figure 5-4. Task Properties window (Status page)**

2. Click **OK** to exit the Task Properties window and return to the VirusScan Console.

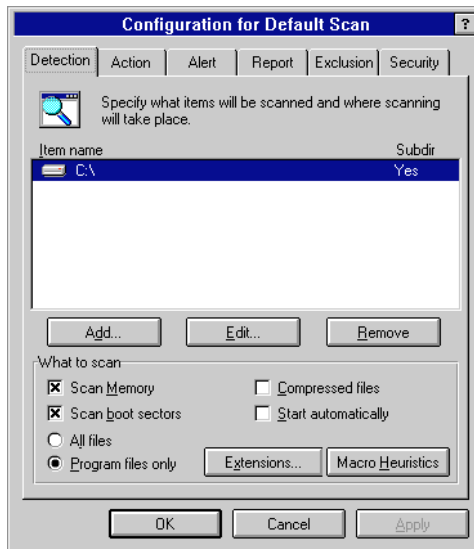
## Copying, Pasting, or Deleting a Scan Task

Tasks can be copied from or pasted to the VirusScan Console task list. This makes creating several tasks with similar configurations quick and easy.

- To copy a task, choose **Copy** from the Edit menu, or right-click on the desired task and choose **Copy**.
- To paste a task, select **Paste** from the Edit menu, or right-click on the task list and choose **Paste**.
- To delete a task, select the task and press **DELETE**.

## Configuring a Scan Task

To configure where and what you want VirusScan to scan, click **Configure** on the Program page of the Task Properties window. The Configuration window appears, with the Detection page on top ([Figure 5-5](#)).



**Figure 5-5. Configuration window (Detection page)**

The Configuration window has five tabbed pages. To move from one to another, click the desired page at the top of the window. The following sections describe each page in detail.

## Using the Detection page

Use the Detection page to specify which drives, files, and folders VirusScan should scan. Follow these steps to configure the detection options for a scan:

1. Add one or more items to the scan list. To add an item, select it from the Select Item to Scan list.
  - **My Computer** scans all fixed, removable, and network volumes connected to your computer.
  - **All Removable Media** scans all local removable media, such as floppy disks and CD-ROMs.
  - **All Fixed Disks** scans all local hard drives.
  - **All Network Drives** scans all mapped network volumes.

---

**NOTE:** All directories and subdirectories on the location you select will be scanned.

---

2. Add a specific drive, file, or folder. Click **Select drive or directory to scan** and specify the path to the item you want to scan.

---

**NOTE:** Click **Browse** to navigate to the file, drive, or folder.

---

3. Click **OK**. The items you selected appear in the Selections list.
4. To remove an item from the list to be scanned, select it from the list and click **Remove**.
5. Select the types of files you want VirusScan to check for viruses.
  - **All files** scans all files, no matter the type. This results in a more thorough, but slower, scan.
  - **Program files only** scans only those files with certain extensions. To edit the extensions included in this list, click **Extensions**.

---

**NOTE:** Default extensions are .EXE, .COM, .DO?, and .XL? (the question mark is a wildcard). This list scans Word and Excel document and template (.DOC, .DOT, .XLS, and .XLT) files as well as program files.

---

- **Compressed files** scans files compressed with PKLITE or LZEXE.

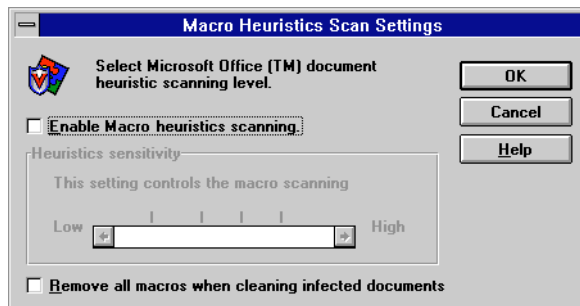
6. Select **Scan memory** if you want to scan your computer's memory for viruses.
7. Select **Start automatically** if you want the task to start automatically when the scheduled time comes.

---

**NOTE:** If you do not select **Start automatically**, VirusScan will launch when the scheduled time comes, but won't complete the task until you click **Scan Now**.

---

8. Select **Scan boot sectors** if you want to scan the boot sector(s) of the drive(s) specified in this task.
9. If desired, click **Macro Heuristics** to set the scanning that VirusScan uses to clean virus-like macros from Microsoft Word and Excel documents. The Macro Heuristics Scan Settings dialog box (Figure 5-6) appears.



**Figure 5-6. Macro Heuristic Scan Settings dialog box**

- a. Enable or disable macro heuristics scanning. It is enabled by default.
- b. Use the slider to set the sensitivity of the scan.
- c. Decide whether you want VirusScan to remove all macros when it is cleaning infected documents. By default, VirusScan removes all macros.

---

**NOTE:** If you move the slider up to High *and* select Remove All Macros when Cleaning Infected Documents, VirusScan removes every macro from any Word or Excel document that is scanned—not just virus-like macros.

---

- d. Click **OK**.

10. Do one of the following:

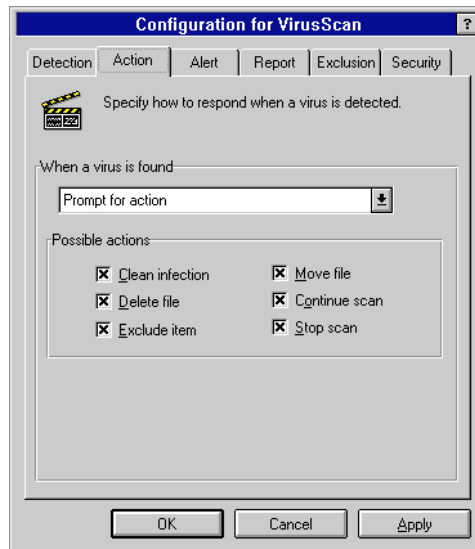
- Click **Apply** to save your changes.
- Click **OK** to save your changes and return to the VirusScan Console.
- Click **Cancel** to return to the VirusScan Console without saving your changes.
- See [“Using the Security page” on page 48](#) if you want to lock and password-protect your changes.

## Using the Action page

Use the Action page to tell VirusScan what to do when it encounters a virus.

Follow these steps to configure the action options for a scan:

1. Select the Action page. The Configuration window appears, with the Action page on top ([Figure 5-7](#)).



**Figure 5-7. Configuration window (Action page)**

2. Click the arrow to next to the list box, then select an action from the list:
  - **Prompt for action** makes VirusScan ask what to do with each virus it finds. Use this action if the computer will be attended while the scan is running.

Choose the actions available to VirusScan by selecting the appropriate checkboxes under Possible Actions.

- **Move infected files to a directory** automatically moves all infected files to a quarantine directory.

You must tell VirusScan where you want the files moved. The default is **\infected**. Unless you specify the entire path (e.g., **C:\mystuff\infected**), VirusScan creates the directory at the root of the drive where the virus was found (e.g., **C:\infected**).

- **Clean infected file** automatically clean viruses from infected files.
- **Delete infected file** automatically deletes infected files.

---

**NOTE:** The infected files are removed permanently from your system. You must restore the deleted files from backups.

---

- **Continue scanning** makes VirusScan continue scanning without taking any action regarding the infected files that it finds.

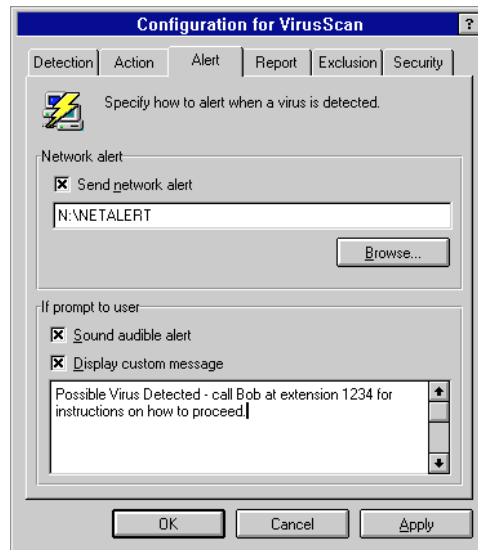
3. Do one of the following:

- Click **Apply** to save your changes.
- Click **OK** to save your changes and return to the VirusScan Console.
- Click **Cancel** to return to the VirusScan Console without saving your changes.
- See [“Using the Security page” on page 48](#) if you want to lock and password-protect your changes.

## Using the Alert page

Use the Alert page to tell VirusScan how to notify you and others when it finds a virus. Follow these steps to configure the alert options for a scan:

1. Select the Alert page. The Configuration window appears, with the Alert page on top ([Figure 5-8 on page 44](#)).



**Figure 5-8. Configuration window (Alert page)**

2. If you want VirusScan to send a Network alert to a server running NetShield, select **Send network alert** and enter the path to the alert file.

---

**NOTE:** This path should be to a folder containing the Centralized Alerting file, CENTALERT.TXT. For more information on Centralized Alerting, see the NetShield documentation.

---

3. If you selected **Prompt for action** on the Action page, select the appropriate boxes to have VirusScan sound an audible alert and/or display a custom message. You can edit the custom message by entering new text in the text box.
4. Do one of the following:
  - Click **Apply** to save your changes.
  - Click **OK** to save your changes and return to the VirusScan Console.
  - Click **Cancel** to return to the VirusScan Console without saving your changes.
  - See [“Using the Security page” on page 48](#) if you want to lock and password-protect your changes.



## Using the Report page

Use the Report page to specify whether VirusScan will log its actions, and which information it will include in the log. Follow these steps to configure the reporting options for a scan:

1. Select the Report page. The Configuration window appears, with the Report page on top (Figure 5-9).



**Figure 5-9. Configuration window (Report page)**

2. To enable logging of scan activity, select **Log to file** and enter the path to a text file.

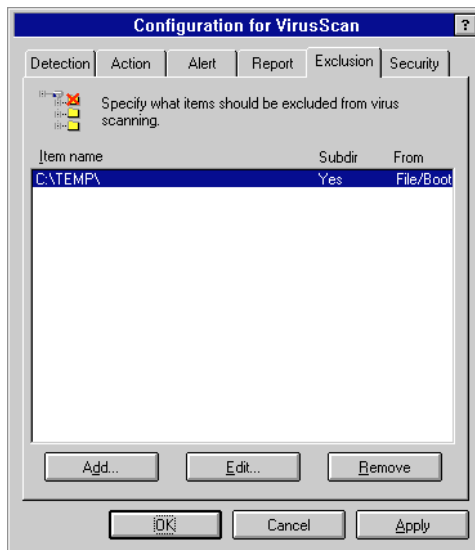
The default path is **C:\neta\virusscan\VSCLOG.TXT**. This is a plain text file and can be viewed with any text editor, such as Notepad, as well as by choosing **View Activity Log** from the File menu.

3. If you want to limit the size of the log file, select **Limit size of log file** and enter a maximum size.
4. Select from the checkboxes provided to specify what information should be included in the log file. The options available are:
  - Virus detection
  - Virus cleaning
  - Infected file deletion
  - Infected file move

- Session settings
  - Session summary
  - Date and time
  - User name.
5. Do one of the following:
- Click **Apply** to save your changes.
  - Click **OK** to save your changes and return to the VirusScan Console.
  - Click **Cancel** to return to the VirusScan Console without saving your changes.
  - See [“Using the Security page” on page 48](#) if you want to lock and password-protect your changes.

## Using the Exclusion page

Use the Exclusion page ([Figure 5-10](#)) to tell VirusScan which files, folders, or volumes to exclude from its scan.

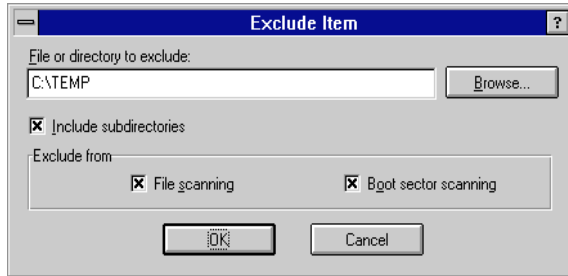


**Figure 5-10. Configuration window (Exclusion page)**

## Adding an item to the exclusion list

To add an item to the exclusion list, follow these steps:

1. On the Exclusion page, click **Add**. The Exclude Item dialog box (Figure 5-11) appears.



**Figure 5-11. Exclude Item dialog box**

2. Enter the path to the item you want to exclude, or click **Browse** to navigate to the item. You may exclude a file, a folder, or an entire disk.
3. Select **Include subfolders** to keep VirusScan from scanning inside subfolders of the folder you have excluded.
4. Indicate whether you want the folder excluded from file scanning or boot sector scanning by selecting the appropriate box(es).
5. Click **OK**.
6. Select what type(s) of scanning you want to exclude this item from:
  - To exclude the item from file scanning, select **File scanning**
  - To exclude the item from boot sector scanning, select **Boot sector scanning**.
7. Do one of the following:
  - Click **Apply** to save your changes.
  - Click **OK** to save your changes and return to the VirusScan Console.
  - Click **Cancel** to return to the VirusScan Console without saving your changes.
  - See “Using the Security page” on page 48 if you want to lock and password-protect your changes.

## Removing an item from the exclusion list

To remove an item from the list, follow these steps:

1. On the Exclusion page, select the item you want to remove, then click **Remove**.
2. Do one of the following:
  - Click **Apply** to save your changes.
  - Click **OK** to save your changes and return to the VirusScan Console.
  - Click **Cancel** to return to the VirusScan Console without saving your changes.
  - See [“Using the Security page” on page 48](#) if you want to lock and password-protect your changes.

## Editing an item on the exclusion list

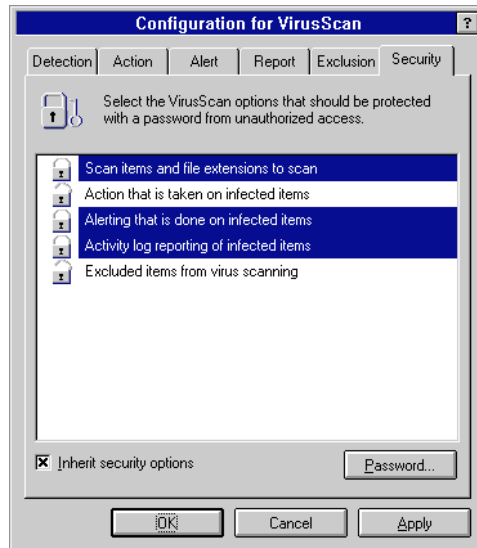
To edit an existing item on the exclusion list, follow these steps

1. On the Exclusion page, select the item you want to edit, then click **Edit**.
2. The Exclude Item dialog box ([Figure 5-11 on page 47](#)) appears. Make your changes, then click OK.
3. Do one of the following:
  - Click **Apply** to save your changes.
  - Click **OK** to save your changes and return to the VirusScan Console.
  - Click **Cancel** to return to the VirusScan Console without saving your changes.
  - See [“Using the Security page” on page 48](#) if you want to lock and password-protect your changes.

## Using the Security page

Use the Security page to password-protect VirusScan settings to prevent unintentional changes from being made. Follow these steps to configure the security options for a scan:

1. Select the Security page ([Figure 5-12 on page 49](#)).



**Figure 5-12. Configuration window (Security page)**

2. Select the VirusScan settings you want to password-protect:
  - **Scan items and file extensions to scan**
  - **Action that is taken on infected items**
  - **Alerting that is done on infected items**
  - **Activity log reporting of infected items**
  - **Excluded items from virus scanning.**

---

**NOTE:** Settings that are password-protected are highlighted in the list, and the lock to their left is closed.

---

3. Select **Inherit security options** if you want the options you have selected to be included by default on copies of this task.

---

**NOTE:** If you select **Inherit security options** on the main VirusScan task, the security options for that task will be inherited for **all** new tasks as well as for copies of the main VirusScan task.

---

4. If you have not already created a password, do so by clicking **Password**. You will be prompted to enter and confirm your password.

If you already have a password, you can change it now or at any time by clicking **Password**. You will be prompted to enter and confirm your new password.

5. Do one of the following:
  - Click **Apply** to save your changes.
  - Click **OK** to save your changes and return to the VirusScan Console.
  - Click **Cancel** to return to the VirusScan Console without saving your changes.

## If You Suspect You Have a Virus

If you have a virus on your system before you install VirusScan for Windows 3.1x—or suspect you have a virus—follow this procedure to create a virus-free environment.

1. Turn off your computer.

---

**NOTE:** Do not reboot using the reset button or CTRL+ALT+DELETE; if you do, some viruses might remain intact.

---

2. Make an emergency disk. See [“Creating an Emergency Disk”](#) on page 64 for details.
3. Insert the emergency disk in your computer’s A: drive and then turn on your computer.
4. Do one of the following:
  - If you were able to create the emergency disk with the automatic creation utility, simply follow the on-screen instructions.
  - If you are using a manually created, clean boot diskette, enter:

```
scan /ADL /ALL /CLEAN
```

at the command prompt. This starts the command-line version of VirusScan. It will display its progress on-screen.

---

**NOTE:** For detailed information on the VirusScan command-line options, see [Appendix D, “Reference.”](#)

---

## If viruses are removed

If VirusScan successfully removes all the viruses, shut down your computer and remove the diskette. Restart your computer and resume work. If you were installing VirusScan, begin the installation procedure described in [Chapter 2, “Installing VirusScan.”](#)

To find and eliminate the source of infection, scan all your diskettes immediately after installation.

### If viruses are not removed

If VirusScan cannot remove a virus, it sends one of the following messages:

- Virus could not be removed.
- There is no remover currently available for the virus.

If you receive either of these messages, refer to documents related to manually removing viruses on the Network Associates web site. For contact information, see [“How To Contact Network Associates” on page xiii](#).

### If VirusScan Detects a Virus

Viruses attack your computer system by infecting files—usually executable program or document files. Often, these files are damaged during the infection. VirusScan can safely remove many viruses from infected files. Some viruses, however, are designed to damage your files beyond repair. These irreparably damaged files, called “corrupted” files, can be moved by VirusScan to a quarantine directory or deleted to prevent another virus infection of your system.

### Removing a virus found in a file

If VirusScan detects a virus in a file, it will take the action you specified during configuration. See [“Configuring VShield actions” on page 12](#).

### Removing a virus found in memory

If VirusScan detects a virus on your system, clean your system immediately to prevent the virus from spreading throughout your PC or network. Remove viruses from files if you know or suspect that they are infected.

If a virus is resident in memory or has infected the Master Boot Record (MBR) or boot sector, shut down your computer and reboot from an emergency disk. Then remove the virus using the command-line version of VirusScan. For more information, see [“If You Suspect You Have a Virus” on page 51](#) and [Appendix C, “Shared Installations.”](#) Be sure you only use the command-line scanner to clean your system if a virus was detected in memory.



## Understanding false alarms

A false alarm is a report of a virus in a file or in memory when no virus actually exists. False alarms can occur if you are using more than one brand of virus detection software, because some anti-virus programs store their virus signature strings unprotected in memory. As a result, VirusScan may “detect” them falsely as a virus. Your system’s BIOS, use of validation codes, and other factors may also produce false alarms.

Always assume that any virus found by VirusScan is real and dangerous, and take necessary steps to remove it from your system. If, however, you have reason to believe that VirusScan is generating a false alarm (for example, it has detected a virus in only one file that you have been using safely for years), refer to the list of potential sources below:

- VirusScan may report a false alarm if more than one anti-virus program is running. Set up your computer so that only one anti-virus program is running at a time. Remark out lines in the AUTOEXEC.BAT file that refer to other anti-virus programs. Turn off your computer, wait a few seconds, and turn it on again to make sure that all code from other anti-virus programs is cleared from memory.
- Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer’s reference manual for details.
- If you set up validation/recovery codes, subsequent scans can detect changes in validated files. This can trigger false alarms if the executable files are self-modifying or self-checking. When using validation codes, specify an exceptions list to exclude such files from checking.
- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. VirusScan may detect these modifications as a possible infection, even though no virus may be present. Check your computer’s reference manual to determine if your PC has self-modifying boot code. To solve this problem, save validation/recovery information to the executable files themselves; this method does not save information about the boot sector or Master Boot Record.
- VirusScan may report viruses in the boot sector or Master Boot Record of certain copy-protected diskettes.



# Network Associates Support Services



Choosing Network Associates anti-virus and security software helps to ensure that the critical information technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from three levels of extended support under the Network Associates PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Personal Support program.

## PrimeSupport Options for Corporate Customers

The Network Associates PrimeSupport program offers a choice of Basic, Extended, or Anytime options. Each option has a range of features that provide you with cost-effective and timely support geared to meet your needs.

### PrimeSupport Basic

PrimeSupport Basic gives you telephone access to essential product assistance from experienced Network Associates technical support staff members. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport Basic as part of the package for two years from your date of purchase. If you purchased your Network Associates product with a perpetual license, you can renew your PrimeSupport Basic plan for an annual fee.

PrimeSupport Basic includes these features:

- Telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website

## PrimeSupport Extended

PrimeSupport Extended gives you personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products. By calling in advance, your PrimeSupport Extended representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Extended gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Extended on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Extended includes these features:

- Access to an assigned technical support engineer.
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate.
- Committed response times: your support engineer will respond within one hour to pages, within four hours to voice mail, and within 12 hours to e-mail.
- Telephone access to technical support from Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website.
- Ability to designate up to five people in your organization as customer contacts.

## PrimeSupport Anytime

PrimeSupport Anytime offers round-the-clock, personalized, proactive support for Network Associates products deployed in the most business-critical information systems. PrimeSupport Anytime delivers the features of PrimeSupport Extended 24 hours a day, seven days a week, with shorter response time commitments. You may purchase PrimeSupport Anytime on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Anytime includes these features:

- Access to an assigned technical support engineer.
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate.
- Committed response times: your support engineer will respond within half an hour to pages, within one hour to voice mail, and within four hours to e-mail.
- Telephone access to technical support 24 hours a day, seven days a week.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website.
- Ability to designate up to 10 people in your organization as customer contacts.

**Table A-1. PrimeSupport At a Glance**

Feature	Basic	Extended	Anytime
Technical support via telephone	Monday–Friday 8:00 a.m.–8:00 p.m.	Monday–Friday 7:00 a.m.–7:00 p.m.	24 hours a day, 7 days a week
Technical support via website	Yes	Yes	Yes
Software updates	Yes	Yes	Yes
Assigned support engineer	—	Yes	Yes
Proactive support contact	—	Yes	Yes
Designated customer contacts	—	5	10
Committed response time	—	Pager: 1 hour Voicemail: 4 hours E-mail: 12 hours	Pager: 30 mins. Voicemail: 1 hour E-mail: 4 hours

## Ordering PrimeSupport

To order PrimeSupport Basic, PrimeSupport Extended or PrimeSupport Anytime for your Network Associates products:

- Contact your sales representative, or
- Call Network Associates Support Services at 1-800-988-5737 or 1-650-473-2000 from 6 a.m. to 5 p.m. Pacific Time, Monday through Friday.

The PrimeSupport program described in this guide is available in North America only. To learn about PrimeSupport options available outside North America, contact your regional sales office. Contact information appears near the front of this guide.

## Support Services for Retail Customers

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

- Free data (.DAT) file updates for the life of your product via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service. You can also update your data files by using your web browser to visit:

**<http://www.nai.com/download/updates/updates.asp>**

- Free program (executable file) upgrades for one year via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service. If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your web browser to visit:

**<http://www.nai.com/download/upgrades/upgrades.asp>**

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

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

- Automated voice and fax system: (408) 988-3034
- Network Associates website: **<http://support.nai.com>**
- CompuServe: GO NAI
- America Online: keyword NAI
- Ninety days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

After your complimentary support period expires, you can take advantage of a variety of personal support options geared toward your needs. Contact Network Associates Customer Care at (972) 278-6100 to learn more about the options available, or visit the Network Associates website at:

**<http://www.nai.com/services/support/support.asp>**

## **Network Associates Consulting and Training**

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

### **Professional Consulting Services**

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

### **Total Education Services**

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

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

To learn more about these programs, contact your sales representative or call Total Service Solutions at 1-800-395-3151.





## Keys to a Secure System Environment

VirusScan for Windows 3.1x is an effective tool for preventing, detecting, and recovering from virus infection. It is most effective, however, when it is part of a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

To create a secure system environment and minimize your chance of infection, Network Associates recommends that you take the following steps:

- Follow the installation procedures as outlined in [Chapter 2, “Installing VirusScan.”](#) If you suspect you have a virus, take steps to clean your system before installing VirusScan. For this procedure, see [“If You Suspect You Have a Virus” on page 51.](#)
- Configure your AUTOEXEC.BAT file to load VShield automatically at start-up.

---

**NOTE:** Your AUTOEXEC.BAT is automatically modified if you followed the recommended installation procedures.

---

- Create an emergency disk, which contains the command-line version of VirusScan, by following the procedure outlined in [“Creating an Emergency Disk” on page 64.](#) Make sure the diskette is write-protected so that it cannot become infected.
- Make frequent backups of important files. Even with VirusScan, some viruses (as well as fire, theft, or vandalism) can render a disk unrecoverable without a recent backup.

While outlining a full security program is beyond the scope of this manual, following the steps provided in this appendix will help you gain a clearer understanding of what viruses are, how they affect your system, and what you can do to prevent an infection.

## Detecting New and Unknown Viruses

There are two ways for you to deal with new and unknown viruses that may infect your system:

- Update your VirusScan data files
- Upgrade the VirusScan program files.

VirusScan uses data (.DAT) files to detect viruses. Updating these files regularly can protect you against the latest virus threats. Network Associates updates these files each month to provide protection against the latest virus threats. Less often, Network Associates changes the VirusScan program itself to increase protection and add features. When this happens, you should upgrade your installation to the latest version of VirusScan.

## Updating your VirusScan data files

To offer the best virus protection possible, Network Associates continually updates the files VirusScan uses to detect viruses. After a certain time period, you are notified that you need to update the virus definition database. Network Associates recommends that you update these files regularly for maximum protection.

## What is a data file?

The files CLEAN.DAT, NAMES.DAT, and SCAN.DAT all provide virus information to the VirusScan software. These are the data files we're referring to in this section.

## Why would I need a new data file?

New viruses are discovered at a rate of more than 200 a month. Often, these new viruses are not detected using older data files. The data files that came with your copy of VirusScan might not be able to help VirusScan detect a virus that was discovered months after you bought the product.

Network Associates' virus researchers are working constantly to update the data files with more and newer virus definitions.

---

**NOTE:** Network Associates offers online virus signature file updates for the life of your product. However, we cannot guarantee backward compatibility of the virus signature files with a previous version's software. By upgrading to the latest version of VirusScan, you can keep the best level of defense against virus threats.

---

## How to apply the data file

To update your data files, take the following steps.

1. Download the data file (for example, DAT-3004.ZIP) from one of Network Associates' electronic services. On most services, the data file is located in the anti-virus area.

---

**NOTE:** Your ability to access these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.

---

2. Copy the file to a new directory.
3. The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompression software. If you don't have the decompression software, you can download PKUNZIP (shareware) from Network Associates electronic sites.
4. Locate the directories on your hard drive where your VirusScan software is currently loaded (typically, in **C:\Neta\Viruscan**). This varies depending on the version of the software you have and on whether a different directory was specified during installation.
5. Copy the new files into these directory or directories, overwriting the old data files.

---

**NOTE:** There might be part of the software in more than one directory. If so, place the updated files in each directory.

---

6. You must reboot your computer for VirusScan to recognize and be able to use the updated files.

## Validating the VirusScan Program Files

When you download a file from any source other than the Network Associates bulletin board or other Network Associates service, you should verify that the file is authentic, unaltered, and uninfected. Network Associates anti-virus software includes a utility program called Validate that you can use to ensure that your version of VirusScan is authentic. When you receive a new version of VirusScan, run Validate on all of its program files. For details on the Validate program, see the README.1ST text file that accompanied your software.

## Creating an Emergency Disk

In case your system becomes infected, you should have an emergency disk. This section describes how to create one.

Your system must be virus-free to make an emergency disk. Any virus residing on your system could be transferred to your emergency disk and reinfect your system.

If you suspect your computer is infected, go to another computer and scan it. If this computer is virus-free, follow the steps below, which detail how to use the emergency disk creation utility included with VirusScan.

---

**NOTE:** If you suspect your computer is infected, and you cannot find another computer with VirusScan installed on it, go to [“Creating a clean boot diskette” on page 64](#) which tells how to manually create a clean boot diskette. This can serve as a substitute for an emergency disk until you install VirusScan and can create an emergency disk.

---

1. Insert a blank diskette in drive A:.
2. Run the emergency disk creation utility by double-clicking the icon in the VirusScan program group.
3. Follow the on-screen instructions. If there is a problem creating the emergency disk, make sure the disk you inserted is not write-protected.
4. When the emergency disk creation utility is finished, remove the diskette from the drive. Write-protect the diskette, label it, and store it in a safe place. For more information, see [“Write-Protecting a Diskette” on page 66](#).

## Creating a clean boot diskette

If you are working from a computer that does not have VirusScan installed, you can create a clean boot diskette. This diskette will serve as a substitute for an emergency disk until you can install VirusScan and use the included emergency disk creation utility.

To create a clean boot diskette, follow these steps from a DOS prompt (you must either exit to DOS or open a DOS window):

---

**NOTE:** This procedure must be carried out on a virus-free system.

---

1. Insert a blank diskette in the A: drive.

2. Format the diskette by typing the following command at the C:\> prompt:

```
format a: /s /u
```

3. This overwrites any information already on the diskette.

---

**NOTE:** If you are using DOS 5.0 or an earlier version of DOS, do not type the /u. If you are unsure of which version you are using, type **ver** at the C:\> prompt for version information.

---

4. When the system prompts you for a volume label, enter an appropriate name using no more than eleven characters.
5. Change to the VirusScan directory by typing the following command at the C:\> prompt:

```
cd \mcafee\viruscan
```

6. Copy the DOS version of VirusScan to the diskette by typing the following commands at the C:\mcafee\viruscan prompt:

```
copy scan.exe a:
copy scan.dat a:
copy clean.dat a:
copy names.dat a:
```

7. Change back to the root directory by typing the following command at the C:\mcafee\viruscan prompt:

```
cd\
```

8. Copy useful DOS programs to the diskette by typing the following command at the C:\ prompt:

```
copy c:\dos\chkdsk.* a:
```

9. Repeat the last step for any other useful programs you want to add to the diskette. Here are some programs you might want:

- debug.\*
- diskcopy.\*
- fdisk.\*
- format.\*
- label.\*
- mem.\*
- sys.\*

- unerase.\*
- xcopy.\*

---

**NOTE:** If you use a disk compression utility, be sure to copy the drivers required to access the compressed diskettes onto the emergency disk. See the documentation for your compression utility for more information about those drivers.

---

10. Label and write-protect this diskette, then store it in a secure place. See [“Write-Protecting a Diskette” on page 66](#) for more information.

## Write-Protecting a Diskette

Floppy diskettes are convenient, portable devices for storage and retrieval of computer data. Diskettes are used to save files (write) and recover files (read). They are also the most common vehicle viruses use to invade your computer’s system.

One way to help avoid infection via floppy diskette is to *write-protect* diskettes for read-only data. If your system does become infected with a virus, the write-protection feature keeps your clean diskettes from also becoming infected, preventing reinfection after your system is cleaned.

---

**NOTE:** Any diskettes that are not write-protected should be scanned and cleaned before you write-protect them.

---

## Write-protecting 3.5” floppy diskettes

1. Position the diskette face down with the metal slide facing you.

Examine the small rectangular hole on the upper left side. There should be a square, plastic tab that you can slide up and down across the hole.

2. To write-protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the hole is open.

## General Procedure

1. Log in to an administrative-level account on the Windows 3.1x shared workstation.
2. Perform the installation procedure that begins on [page 3](#). Where necessary, change to the appropriate directory for a shared installation.
3. When the installation is complete, restart the computer and log back in to the same administrative-level account.
4. Make the changes described in the following section.

## Changes to Files

### Win.ini file

Add the following entry to the [VirusScan] section of the WIN.INI file:

```
nainipath=x:\test\folder
```

This entry allows an alternate location of the AVCONSOL.INI file.

### Autoexec.bat file

If you want to place the DATs in a separate folder, you must add an entry like the following in the AUTOEXEC.BAT file.

```
set mcafee.scan=x:\test\DATS
```

This entry allows SCAN.EXE or SCANPM.EXE to continue to function as designed.

### Avconsol.ini file

#### New entries

There are two new entries in the [VirusScan Console] section of the AVCONSOL.INI file.

- `RefreshRate=3` gives the default setting, in seconds, for how often AVCONSOL.EXE checks the .INI file for changes. You can set the value between 1 second and 10 seconds.

---

**NOTE:** Network access is reduced significantly if you set a higher value.

---

- `NewTaskPath=x:\new=vsconfig` gives the default location where a new task created in AVCONSOL.EXE will be stored.

## VShield configuration files

You can change the location of the VShield configuration file by editing [Item-0] in AVCONSOL.INI. In [Item-0], you should find an entry called `SzVshFile`.

Add an entry similar to the following:

```
SzVshFile=x:\test\directory
```

This adds the ability to browse to the directory where you want the VShield configuration file to reside.

---

**NOTE:** If you do not find a `SzVshFile` entry, add it to [Item-0].

---

## Scan16 configuration files

If you want to place the Scan16 task configuration files in a separate directory, modify the `SzVscFile` entry under each item in AVCONSOL.INI that indicates a Scan16 task.

## Limitations

Particular types of shared installations impose limitations on status updates and logging.

## Status updates

If AVCONSOL.EXE is accessed by a user account that has read-only access to the directory where the configuration file resides, the status will not be updated by any function that the account tries to use. Even if the user account runs a scheduled task, there will be no indication that the task was run.

---

**NOTE:** This limitation does not apply to administrator-level accounts.

---



## Logging

If the executables are installed to a directory where user accounts only have read-only access, the log directories should allow read-write access so that logging can be done accurately.

If system results for all users are recorded to the same log file, the log file should be set to its maximum size.



## VirusScan Command-line Options

The following table lists all of the VirusScan options you can use when you're running the DOS command-line scanner, SCAN.EXE. To run VirusScan for Windows 3.1x from the command line, first use the `cd` command to change directories to the directory in which VirusScan was installed. Then, type `scan /?` to display a list of options and descriptions of how they can be used.

---

**NOTE:** When specifying 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 directory in which VirusScan is installed.

---

Command-line Option	Description
<code>/?</code> or <code>/HELP</code>	Does not scan. Instead, displays a list of VirusScan command-line options with a brief description of each. Use either of these options alone on the command line (with no other options).
<code>/ADL</code>	Scans all local drives (including compressed, CD-ROM, and PCMCIA drives, but not diskettes), in addition to those specified on the command line.  To scan both local and network drives, use <code>/ADL</code> and <code>/ADN</code> together in the same command line.
<code>/ADN</code>	Scans all network drives for viruses, in addition to those specified on the command line.  To scan both the local drives and network drives, use <code>/ADL</code> and <code>/ADN</code> together in the same command line.

Command-line Option	Description
<code>/AF filename</code>	<p>Stores validation/recovery codes in <i>filename</i>.</p> <p>Helps you detect new or unknown viruses. /AF logs validation and recovery data for executable files, the boot sector, and Master Boot Record on a hard disk or diskette in a file you specify. The log file is about 89 bytes per file validated.</p> <p>You must specify a <i>filename</i>, which can include the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. If <i>filename</i> exists, VirusScan updates it. /AF adds about 300% more time to scanning.</p> <p><b>NOTE:</b> /AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves.</p> <p>The /AF option does not store any information about the Master Boot Record or boot sector of the drive being scanned.</p>
<code>/ALERTPATH &lt;directory&gt;</code>	<p>Designates &lt;directory&gt; as a network path monitored by NetShield for Centralized Alerting.</p>
<code>/ALL</code>	<p>Overrides the default settings by scanning all files.</p> <p>This option substantially increases the scanning time required. Use it if you have found a virus or suspect one.</p> <p><b>NOTE:</b> The list of extensions for standard executables has changed from previous releases of VirusScan.</p>
<code>/APPEND</code>	<p>Used in conjunction with /REPORT, appends the report message text to the specified report file, if it exists. Otherwise, the /REPORT option overwrites the specified report file, if it exists.</p>
<code>/AV</code>	<p>To help you detect and recover from new or unknown viruses, /AV adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL), increasing the size of each file by 98 bytes. To update files on a shared network drive, you must have update access rights.</p> <p>To exclude self-modifying or self-checking files, and damaged files that might cause false alarms, use the /EXCLUDE option. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.</p> <p><b>NOTE:</b> The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned.</p>
<code>/BOOT</code>	<p>Scans only the boot sector and Master Boot Record on the specified drive.</p>

Command-line Option	Description
<code>/CF filename</code>	<p>Helps you detect new or unknown viruses. Checks validation data stored by the /AF option in <i>filename</i>. If a file or system area has changed, VirusScan reports that a viral infection may have occurred. The /CF option adds about 250% more time to scanning.</p> <p>Using any of the /AF, /CF, or /RF options together in a command line returns an error.</p> <p><b>NOTE:</b> Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF, VirusScan continuously reports that the boot sector has been modified even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.</p>
<code>/CLEAN</code>	Cleans infected files.
<code>/CLEANDOC</code>	Cleans viruses from infected Word document files.
<code>/CLEANDOCALL</code>	Cleans all macros from infected Word document files.
<code>/CONTACTFILE filename</code>	<p>Identifies a file containing a message string to display when a virus is found. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation.</p> <p>Any character is valid except a backslash (\). Messages that begin with a slash (/) or a hyphen (-) should be placed in quotation marks.</p>
<code>/CV</code>	<p>Helps you detect new or unknown viruses. Checks validation data added by the /AV option. If a file is modified, VirusScan reports that a viral infection may have occurred. The /CV option adds about 50% more time to scanning.</p> <p>Using any of the /AV, /CV, or /RV options together in the same command line returns an error.</p> <p><b>NOTE:</b> The /CV option does not check the boot sector for changes.</p>
<code>/DEL</code>	Deletes infected files.
<code>/EXCLUDE filename</code>	<p>Excludes any files listed in <i>filename</i> from the scan. This option allows you to exclude files from /AF and /AV validation and /CF and /CV checking. Self-modifying or self-checking files can cause a false alarm during a scan.</p>
<code>/FAST</code>	<p>Speeds up the scan.</p> <p>Reduces scanning time by about 15%. Using the /FAST option, VirusScan examines a smaller portion of each file for viruses.</p> <p>Using /FAST might miss some infections found in a more comprehensive (but slower) scan. Do not use this option if you have found a virus or suspect one.</p>

Command-line Option	Description
<code>/FORCE</code>	Cleans partition table viruses by writing a generic Master Boot Record over the disk's boot record.
<code>/FREQUENCY hours</code>	<p>The number of hours that must occur between subsequent successful scans (Example: <code>/FREQUENCY 1</code>).</p> <p>In environments where the risk of viral infection is very low, use this option to prevent unnecessary or too-frequent scans. The lower the number of <i>hours</i> specified, the greater the scan frequency and the greater your protection against infection.</p>
<code>/LOAD filename</code>	<p>Performs a scan using the information saved in <i>filename</i>.</p> <p>You can store all custom settings in a separate configuration file (an ASCII text file), then use <code>/LOAD</code> to load those settings from that file.</p>
<code>/LOCK</code>	<p>Halts the system to stop further infection if VirusScan finds a virus.</p> <p><code>/LOCK</code> is appropriate in highly vulnerable network environments, such as open-use computer labs. If you use <code>/LOCK</code>, we recommend you use it with <code>/CONTACTFILE</code> to tell users what to do or whom to contact if a virus is found and the system locks up.</p>
<code>/LOG</code>	Stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the root of the current drive.
<code>/MANY</code>	<p>Scans multiple diskettes consecutively in a single drive. VirusScan prompts you for each diskette. Once you have established a virus-free system, use this option to check multiple diskettes quickly.</p> <p>The VirusScan program should reside on a disk that will not be removed during the scan.</p> <p>For example, if you are scanning disks in the computer's A: drive, and you are running the program from a disk in the A: drive, the program will become unavailable as soon as you remove the diskette to put another in. The following command causes an error during execution:</p> <pre>a:\scan a: /many</pre>
<code>/MAXFILESIZE xxx.x</code>	Scans only files with size not more than xxx.x megabytes.
<code>/MEMEXCL</code>	<p>Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.)</p> <p>This command-line option has been added to prevent VirusScan from checking areas in upper memory which might contain memory-mapped hardware and might cause false alarms.</p>
<code>/MOVE directory</code>	Moves all infected files found during a scan to the specified directory. To preserve drive and directory structure, this option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files.

Command-line Option	Description
/NOBEEP	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	<p>Disables CTRL-C and CTRL-BREAK during scans.</p> <p>Users will not be able to halt scans in progress using CTRL-C or CTRL-BREAK. Use this option in conjunction with /LOG to create a meaningful audit trail of regularly scheduled scans.</p>
/NOCOMP	<p>Skips checking of compressed executables created with the LZEXE or PKLITE file-compression programs.</p> <p>Reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files that have been created using the LZEXE or PKLITE file-compression programs. VirusScan decompresses each file in memory and checks for virus signatures, which takes time but results in a more thorough scan. If you use /NOCOMP, VirusScan does not check inside compressed files for viruses, although it can check for modifications to those files if they have been validated using validation/recovery codes.</p>
/NODDA	<p>No direct disk access.</p> <p>Prevents VirusScan from accessing the boot record. This feature has been added to allow VirusScan to run under Windows NT.</p> <p>You might need to use this option on some device-driven drives.</p>
/NODOC	Does not scan Word document files.
/NOEMS	Prevents VirusScan from using expanded memory (LIM EMS 3.2), ensuring that EMS is available to other programs.
/NOEXPIRE	Disables the "expiration date" message if the VirusScan data files are out of date.
/NOMEM	<p>Reduces scan time by omitting all memory checks for viruses. Use /NOMEM only when you are absolutely certain that your computer is virus-free.</p> <p>VirusScan can check system memory for all critical known computer viruses that can inhabit memory. In addition to main memory from 0KB to 640KB, VirusScan checks system memory from 640KB to 1088KB that can be used by computer viruses on 286 and later systems. Memory above 1088KB is not addressed directly by the processor and is not presently susceptible to viruses.</p>

Command-line Option	Description
<code>/PAUSE</code>	<p>Enables screen pause.</p> <p>If you specify <code>/PAUSE</code>, the “Press any key to continue” prompt appears when VirusScan fills up a screen with messages (for example, when you’re using the <code>/SHOWLOG</code> or <code>/VIRLIST</code> options). Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with many drives or that have severe infections without requiring you to attend.</p> <p>We recommend that you omit <code>/PAUSE</code> when keeping a record of VirusScan’s messages using the report options (<code>/REPORT</code>, <code>/RPTCOR</code>, <code>/RPTMOD</code>, and <code>/RPTERR</code>).</p>
<code>/PLAD</code>	<p>Preserve last access dates (on proprietary drives only).</p> <p>Prevents changing the last access date attribute for files stored on a network drive in a proprietary network. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use <code>/PLAD</code> to ensure that the last access date does not change as the result of scanning.</p>
<code>/REPORT filename</code>	<p>Creates a report of infected files and system errors.</p> <p>Saves the output of VirusScan to <i>filename</i> in ASCII text file format. If <i>filename</i> exists, <code>/REPORT</code> erases and replaces it (or, if you use <code>/APPEND</code>, adds the report information to the end of the existing file).</p> <p>You can include the destination drive and directory (such as <code>D:\VSREPRTVALL.TXT</code>), but if the destination is a network drive, you must have rights to create and delete files on that drive. You can also use <code>/RPTALL</code>, <code>/RPTCOR</code>, <code>/RPTMOD</code>, and <code>/RPTERR</code> to add scanned files, corrupted files, modified files, and system errors to the report.</p>
<code>/RF filename</code>	<p>Removes recovery and validation data from <i>filename</i> created by the <code>/AF</code> option.</p> <p>If <i>filename</i> resides on a shared network drive, you must be able to delete files on that drive. Using any of the <code>/AF</code>, <code>/CF</code>, or <code>/RF</code> options together in the same command line returns an error.</p>
<code>/RPTALL</code>	Adds list of files scanned to the report file (used with <code>/REPORT</code> ).
<code>/RPTCOR</code>	<p>When used in conjunction with <code>/REPORT</code>, adds the names of corrupted files to the report file.</p> <p>A corrupted file may be a file that has been damaged by a virus. You can use <code>/RPTCOR</code> with <code>/RPTMOD</code> and <code>/RPTERR</code> on the same command line.</p> <p><b>NOTE:</b> There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).</p>



Command-line Option	Description
/RPTERR	<p>Adds a list of system errors to the report file. This option is used in conjunction with /REPORT.</p> <p>System errors include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.</p>
/RPTMOD	<p>Adds list of modified files to the report file. This option is used in conjunction with /REPORT.</p> <p>VirusScan identifies modified files when the validation/recovery codes do not match (using the /CF or /CV options). You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.</p>
/RV	<p>Removes validation and recovery data from files validated with the /AV option.</p> <p>To update files on a shared network drive, you must have access rights to update them. Using any of the /AV, /CV, or /RV options together in the same command line returns an error.</p>
/SHOWLOG	<p>Displays the contents of SCAN.LOG.</p> <p>SCAN.LOG stores the time and date VirusScan is being run by updating or creating a file called SCAN.LOG in the current directory and the date and time of previous scans that have been recorded in the SCAN.LOG file using the /LOG switch.</p> <p>The SCAN.LOG file contains text and some special formatting. To pause when the screen fills with messages, specify the /PAUSE option.</p>
/SUB	<p>Scans subdirectories inside a directory.</p> <p>By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. Use /SUB to scan all subdirectories inside any directories you have specified. Do not use /SUB if you are scanning an entire drive.</p>
/VIRLIST	<p>Displays the name and a brief description of each virus that VirusScan detects. To pause when the screen fills with messages, specify the /PAUSE option. Use /VIRLIST alone or with /PAUSE on the command line.</p> <p>You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, in DOS, enter:</p> <pre>scan /virlist &gt; filename.txt</pre> <p><b>NOTE:</b> Because VirusScan can detect many viruses, this file is more than 250 pages long.</p>

## VirusScan DOS Error Levels

When you run VirusScan in the DOS environment, a DOS error level is set. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan.

---

**NOTE:** See your DOS operating system documentation for more information.

---

VirusScan can return the following error levels:

ERRORLEVEL	Description
0	No errors occurred; no viruses were found.
1	Error occurred while accessing a file (reading or writing).
2	A VirusScan data file is corrupted.
3	An error occurred while accessing a disk (reading or writing).
4	An error occurred while accessing the file created with the /AF option; the file has been damaged.
5	Insufficient memory to load program or complete operation.
6	An internal program error has occurred (out of memory error).
7	An error occurred in accessing an international message file (MCA-FEE.MSG).
8	A file required to run VirusScan, such as SCAN.DAT, is missing.
9	Incompatible or unrecognized option(s) or option argument(s) specified in the command line.
10	A virus was found in memory.
11	An internal program error occurred.
12	An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or VirusScan was unable to remove the virus.
13	One or more viruses were found in the Master Boot Record, boot sector, or files.
14	The SCAN.DAT file is out of date; upgrade VirusScan data files.
15	VirusScan self-check failed; it may be infected or damaged.
16	An error occurred while accessing a specified drive or file.
17	No drive, directory, or file was specified; nothing to scan.
18	A validated file has been modified (/CF or /CV options).

ERRORLEVEL	Description
19-99	Reserved.
100+	Operating system error; VirusScan adds 100 to the original number.
102	CTRL+C or CTRL+BREAK was used to interrupt the Scan. (You can disable CTRL+C or CTRL+BREAK with the /NOBREAK command-line option.)

## VSH File Format

The VSH file is a configuration text file, formatted similarly to the Windows INI file, which outlines VShield's settings. Each variable in the file has a name followed by the equal sign (=) and a value. The values define which settings have been selected for VShield configuration. The variables are arranged in seven groups: General, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, SecurityOptions, and ExclusionOptions. To edit the VSH file, open it with a text editor, such as Notepad.

---

**NOTE:** In Boolean variables, possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.

---

## General

Variable	Description
bLoadAtStartup	Type: Boolean (1/0) Defines if VShield should be loaded at system startup Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Defines if VShield can be disabled Default value: 1
bShowTaskbarIcon	Type: Boolean (1/0) Defines whether VShield taskbar icon is displayed Default value: 1
bNoSplash	Type: Boolean (1/0) Instructs VShield to not show splash screen when program is launched Default value: 0

## DetectionOptions

Variable	Description
szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO? XL?
szDefaultProgramExtensions -	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO? XL?
bScanOnExecute	Type: Boolean (1/0) Instructs VShield to scan when files are run Default value: 1
bScanOnOpen	Type: Boolean (1/0) Instructs VShield to scan when files are opened Default value: 1
bScanOnCreate	Type: Boolean (1/0) Instructs VShield to when files are created Default value: 1
bScanOnRename	Type: Boolean (1/0) Instructs VShield to when files are renamed Default value: 1
bScanOnBootAccess	Type: Boolean (1/0) Instructs VShield to scan the boot record of a disk drive the first time it is accessed Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs program to scan inside all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs program to scan inside compressed files (PkLite, LZEXE) Default value: 1

## AlertOptions

Variable	Description
bNetworkAlert	Type: Boolean (1/0) Instructs VShield to send a network alert to a folder being monitored by NetShield for Centralized Alerting. Default Value: 0
szNetworkAlertPath	Type: String Specifies path being monitored by NetShield for Centralized Alerting. Default Value: None

## ActionOptions

Variable	Description
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: Possible Virus Detected
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
uVshieldAction	Type: Integer (1-5) Instructs VShield to take the action specified when a virus is detected Possible values: 1 - Prompt for action 2 - Move infected files to a folder 3 - Clean infected files automatically (Deny access if files can't be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files Default value: 1
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1

Variable	Description
bButtonDelete	Type: Boolean (1/0) Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected Default value: 1
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection Default value: 0

## ReportOptions

Variable	Description
szLogFileName	Type: String Defines log file name Default value: C:\McAfee\Viruscan\Vshlog.txt
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100

Variable	Description
bLogDetection	Type: Boolean (1/0) Defines if scanning results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1
bLogSettings	Type: Boolean (1/0) Defines if session settings should be logged on shutdown Default value: 1
bLogSummary	Type: Boolean (1/0) Defines if session summary should be logged on shutdown Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1

## SecurityOptions

Variable	Description
szPasswordProtect	Type: String This option is not user-configurable. Default Value: 0
szPasswordCRC	Type: String This option is not user-configurable. Default Value: 0

## ExclusionOptions

Variable	Description
szExclusionsFileName	Type: String This option is not user-configurable.
NumExcludedItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 0
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VShield to exclude the item from on-access scanning Default value: \Recycled . * 1 1 * * The string is separated into fields using the pipe ( ) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file-access scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file-access scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VShield to exclude subfolders of the excluded item 2 - Instructs VShield to not exclude subfolders

## VSC File Format

The VSC file is a configuration text file, similar in format to the Windows INI file, which outlines VirusScan's settings. Each variable in the file has a name followed by the equal sign (=) and a value. The values define which settings have been selected for VirusScan configuration. The variables are arranged in eight groups: ScanOptions, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, ScanItems, SecurityOptions, and ExcludedItems. To edit the VSC file, open it with a text editor, such as Notepad.

---

**NOTE:** In Boolean variables, possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.

---



## ScanOptions

Variable	Description
bAutoStart	Type: Boolean (0/1) Instructs VirusScan to automatically start scan when launched Default Value: 0
bAutoExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning Default Value: 0
bAlwaysExit	Type: Boolean (0/1) NEED DESCRIPTION HERE Default Value: 0
bSkipMemoryScan	Type: Boolean (0/1) Instructs VirusScan to skip memory scan Default Value: 0
bSkipBootScan	Type: Boolean (0/1) Instructs VirusScan to skip boot sector scanning Default Value: 0
bSkipSplash	Type: Boolean (0/1) Instructs VirusScan to skip display of the VirusScan splash screen on startup Default Value: 0

## DetectionOptions

Variable	Description
bScanAllFiles	Type: Boolean (0/1) Instructs VirusScan to scan all file types Default Value: 0
bScanCompressed	Type: Boolean (0/1) Instructs VirusScan to Scan in compressed files Default Value: 1

Variable	Description
szProgramExtensions	Type: String Specifies which file extensions VirusScan will scan Default Value: EXE COM DO? XL?
szDefaultProgramExtensions	Type: String Specifies default value for szProgramExtensions Default Value: EXE COM DO? XL?

## AlertOptions

Variable	Description
bNetworkAlert	Type: Boolean (0/1) Instructs VirusScan to send an alert (.ALR) file to a network path being monitored by NetShield for Centralized Alerting when a virus is found Default Value: 0
bSoundAlert	Type: Boolean (0/1) Instructs VirusScan to sound an audible alert when a virus is detected Default Value: 1
szNetworkAlertPath	Type: String Specifies the network alert path being monitored by NetShield for Centralized Alerting. The folder this path points to should contain the Centralized Alerting file, CENTALERT.TXT Default Value: None

## ActionOptions

Variable	Description
bDisplayMessage	Type: Boolean (0/1) Instructs VirusScan to display a message upon detection of a virus Default Value: 0
ScanAction	Type: Integer (0-5) Instructs VirusScan to take the action specified when a virus is detected Possible values: 0 - Prompt for action 1 - Move automatically 2 - Clean automatically 3 - Delete automatically 4 - Continue Default Value: 0
bButtonClean	Type: Boolean (0/1) Instructs VirusScan to display the Clean button if ScanAction=0 Default Value: 1
bButtonDelete	Type: Boolean (0/1) Instructs VirusScan to display the Delete button if ScanAction=0 Default Value: 1
bButtonExclude	Type: Boolean (0/1) Instructs VirusScan to display the Exclude button if ScanAction=0 Default Value: 1
bButtonMove	Type: Boolean (0/1) Instructs VirusScan to display the Move button if ScanAction=0 Default Value: 1
bButtonContinue	Type: Boolean (0/1) Instructs VirusScan to display the Continue button if ScanAction=0 Default Value: 1
bButtonStop	Type: Boolean (0/1) Instructs VirusScan to display the Stop button if ScanAction=0 Default Value: 1

Variable	Description
szMoveToFolder	Type: String Indicates where infected files should be moved Default Value: \Infected
szCustomMessage	Type: String Indicates text of message to be displayed on virus detection Default Value: Possible Virus Detected

## ReportOptions

Variable	Description
bLogToFile	Type: Boolean (0/1) Instructs VirusScan to log scan activity to a file Default Value: 1
bLimitSize	Type: Boolean (0/1) Instructs VirusScan to limit the size of the log file Default Value: 1
uMaxKilobytes	Type: Integer (10-999) Specifies maximum size of log file in kilobytes Default Value: 10
bLogDetection	Type: Boolean (0/1) Instructs VirusScan to log virus detection Default Value: 1
bLogClean	Type: Boolean (0/1) Instructs VirusScan to log virus cleaning Default Value: 1
bLogDelete	Type: Boolean (0/1) Instructs VirusScan to log file deletions Default Value: 1
bLogMove	Type: Boolean (0/1) Instructs VirusScan to log file moves Default Value: 1
bLogSettings	Type: Boolean (0/1) Instructs VirusScan to log session settings Default Value: 1

Variable	Description
bLogSummary	Type: Boolean (0/1) Instructs VirusScan to log session summaries Default Value: 1
bLogDateTime	Type: Boolean (0/1) Instructs VirusScan to log date and time of scan activity Default Value: 1
bLogUserName	Type: Boolean (0/1) Instructs VirusScan to log user name Default Value: 1
szLogFileName	Type: String Specifies path to log file Default Value: C:\McAfee\Viruscan\VSCLOG.TXT

## ScanItems

Variable	Description
ScanItem_x, where x is a zero-based index	Type: String Instructs VirusScan to scan the item Default value: C:\ 1 * * The string is separated into fields using the pipe ( ) character: Field 1 - Path of item to scan. Field 2 - Boolean (1/0) Possible values: 1 - Instructs VirusScan to scan subfolders of the item 2 - Instructs VirusScan not to scan subfolders of the item

## SecurityOptions

Variable	Description
szPasswordProtect	Type: String This variable is not user-configurable Default Value: 0

Variable	Description
szPasswordCRC	Type: String This variable is not user-configurable Default Value: 0
szSerialNumber	Type: String This variable is not user-configurable Default Value: 0

## ExcludedItems

Variable	Description
NumExcludeItems	Type: Integer (0-n) Defines the number of items excluded from scanning Default value: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VirusScan to exclude the item from scanning Default value: \Recycled *.* 1 1 * * The string is separated into fields using the pipe ( ) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a filename. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VirusScan to exclude subfolders of the excluded item 2 - Instructs VirusScan to not exclude subfolders

# Glossary

BIOS	A read-only memory chip that contains the coded instructions for using hardware such as a keyboard or monitor. Always present in portable computers, a BIOS (boot ROM) is not susceptible to infection (unlike the boot sector on a disk). Some BIOS chips contain anti-virus features that can generate a false alarm, installation failure, and other problems.
boot	To start a computer. The computer loads start-up instructions from a disk's boot ROM (BIOS) or boot sector. See also " <a href="#">cold boot</a> " and " <a href="#">warm boot.</a> "
boot sector	A portion of a disk that contains the coded instructions for the operating system to start the computer.
boot sector infection	Contamination of the boot sector by a virus. A boot sector infection is particularly dangerous because information in the boot sector is loaded into memory first, <i>before</i> virus protection code can be executed. The only certain way to eliminate a boot sector infection is to start your computer from a clean start-up diskette, then remove the infection using VirusScan.
boot disk	A write-protected diskette that contains the computer's system and start-up files. You can use this diskette to start up your computer. It is important to use a virus-free boot disk to guarantee that a virus is not introduced into the computer.
cold boot	To turn on a computer, or to restart a computer by turning it off, waiting a few seconds, and turning it on again. Other methods of restarting (such as pressing a reset button or pressing CTRL+ALT+DEL) may not remove all traces of a virus infection from memory. See also " <a href="#">boot</a> " and " <a href="#">warm boot.</a> "
compressed executable	A file that has been compressed using a file compression utility such as LZEXE or PKLITE. See also " <a href="#">compressed file.</a> "
compressed file	A file that has been compressed using a file compression utility such as PKZIP. See also " <a href="#">compressed executable.</a> "
conventional memory	Up to 640KB (1MB) of main memory in which DOS executes programs.
corrupted file	A file that has been irreparably damaged, by a virus for example.
detection	Scanning memory and disks for clues that a virus may be present. Some detection methods include searching for common viral patterns or strings, comparing suspicious file activity with known virus activity, and monitoring files for unauthorized changes.

disinfect	To eradicate a virus so that it can no longer spread or cause damage to a system.
exception list	List of files to which validation codes should not be added because they have built-in virus detection, contain self-modifying code, or are unlikely to be infected by a virus. Such files are usually skipped in validation checking because they may trigger a false alarm.
executable (file)	A file containing coded instructions to be executed by the computer. Executable files include programs and overlays (auxiliary program code which cannot be executed directly by the user).
expanded memory	Computer memory above the DOS 1MB limit of conventional memory that is accessed by memory paging. You need special software, conforming to an expanded memory specification, to take advantage of expanded memory.
extended memory	Linear memory above the DOS 1MB limit of conventional memory. Often used for RAM disks and print spoolers.
false alarm	Reporting a viral infection when none is present.
fast	A scanning option that is faster than normal but less comprehensive (because it checks a smaller portion of each file).
infected file	A file contaminated by a virus.
macro virus	A virus that infects macros, such as those used by applications like Microsoft Word and Excel. Though the text of a document created in one of these applications contains no executable code, and therefore is not infectable, a document can carry infectable macros with it. Macro viruses are the fastest-growing segment of the worldwide virus threat—the number of known macro viruses doubles every three months.
Master Boot Record (MBR)	A portion of a hard disk that contains a partition table that divides the drive into “chunks,” some of which may be assigned to operating systems other than DOS. The MBR accesses the boot sector.
memory	A storage medium where data or program code is kept temporarily while being used by the computer. DOS supports up to 640KB of conventional memory. Beyond that limit may be accessed as expanded memory, extended memory, or an upper memory block (UMB).
memory infection	Contamination of memory by a virus. The only certain way to eliminate memory infection is to <i>shut down your computer</i> , restart from a clean start-up diskette, and clean the source of the infection using VirusScan.



modified file	A file that has changed after validation codes have been added, possibly by a virus.
overlay infection	Virus contamination of a file containing auxiliary program code that is loaded by the main program.
polymorphic virus	A virus that attempts to evade detection by changing its internal structure or its encryption techniques.
read operation	Any operation in which information is read from a disk, including a hard drive, floppy diskette, CD-ROM, or network drive. DOS commands that perform read operations include DIR (directory listing), TYPE (display contents of a file), and COPY (copy files). See also <a href="#">"write operation."</a>
recovery codes	Information that VirusScan records about an executable file in order to recover (repair) it if it is damaged by a virus. See also <a href="#">"validation codes."</a>
self-modifying program	Software that changes its own program files, often to protect against viruses or illegal copying. These programs should be included in an exception list to prevent these modifications from being reported as a false alarm by VirusScan.
system errors	Errors that can prevent VirusScan from completing its job successfully. System error conditions include disk format errors, media errors, file system errors, network errors, device access errors, and report failures.
unknown virus	A virus not yet identified and listed in SCAN.DAT. VirusScan can detect unknown viruses by observing changes in files that could result from infection.
upper memory block (UMB)	Memory in the range 640kB to 1024kB, just above the DOS 640kB limit of conventional memory.
validate	To check that a file is authentic and has not been altered. Most validation methods rely on computing a statistic based on all the data in the file, which is unlikely to remain constant if the file itself is changed.
validation codes	Information that VirusScan records about an executable file in order to detect subsequent infection by a virus. See also <a href="#">"recovery codes."</a>
virus	A software program that attaches itself to another program on a disk or lurks in a computer's memory, and spreads from one program to another. Viruses can damage data, cause computers to crash, display messages, and so on.
warm boot	To restart (reset) a computer by pressing CTRL+ALT+DEL. See also <a href="#">"boot"</a> and <a href="#">"cold boot."</a>

write operation	Any operation in which information is recorded to a disk. Commands that perform write operations include those that save, move, or copy files. See also <a href="#">“read operation.”</a>
write-protection	A mechanism to protect files or disks from being changed. A file is write-protected by changing its system attributes. A diskette is write-protected by sliding its movable corner tab so that the square hole is open (3.5" diskettes) or by covering its corner notch with a write-protect tab (5.25" diskettes).

# Index

## A

- Alerting
  - centralized, [2](#), [14](#), [27](#), [44](#), [72](#), [81](#), [86](#)
- Alerts
  - configuring, [26](#)
- America Online
  - technical support via, [58](#)

## B

- Boot diskette
  - making a, [64](#)
- Boot record
  - preventing VirusScan from accessing, [75](#)
- Boot sector
  - limiting scan to, [72](#)

## C

- Centralized alerting, [2](#), [14](#), [27](#), [44](#), [72](#), [81](#), [86](#)
- Cleaning viruses
  - from files, [52](#)
  - from memory, [52](#)
- Compressed files
  - skipping during virus scans, [75](#)
- CompuServe
  - technical support via, [58](#)
- Configuration lockdown, [19](#), [34](#)
- Consulting services from Network Associates, [59](#)
- Control Break
  - disabling during scans, [75](#)
- Control C
  - disabling during scans, [75](#)
- Customer Care
  - contacting, [xiii](#)

## D

- Data files
  - updating, [62](#)
- Dates
  - preventing VirusScan from changing, [76](#)
- Default settings
  - creating multiple configuration files, [74](#)
- DEFAULT.CFG
  - using a different configuration file, [74](#)
- Direct drive access
  - disabling with VirusScan, [75](#)
- Directories
  - scanning, [77](#)
- Diskettes
  - scanning multiple, [74](#)
  - write-protecting, [66](#)
- Displaying list of detected viruses
  - with VirusScan, [77](#)
- DOS error levels
  - VirusScan, [78](#)
- Drives
  - scanning local, [71](#)
  - scanning network, [71](#)

## E

- EMS
  - preventing VirusScan from using, [75](#)
- Excluding files
  - during virus scans, [73](#)
- Exclusion list
  - adding an item, [17](#), [29](#), [47](#)
  - editing an item, [19](#), [30](#), [48](#)
  - removing an item, [18](#), [30](#), [48](#)
- Expanded memory
  - preventing VirusScan from using, [75](#)
- Expiration date message
  - disabling, [75](#)

**F**

- File types
  - determining which are scanned, [72](#)
- Files
  - moving infected files, [74](#)
  - preventing VirusScan from changing last access dates, [76](#)
- Floppy diskettes
  - scanning multiple, [74](#)
- Frequency
  - determining for VirusScan, [74](#)

**H**

- Help
  - displaying, [71](#)

**I**

- Infected files
  - moving, [74](#)
- Installation
  - procedure, [3](#)
  - testing, [5](#)

**L**

- Last access date
  - preventing VirusScan from changing, [76](#)
- Local drives
  - scanning, [71](#)
- Lockdown
  - configuration, [19, 34](#)
- Locking the system
  - if a virus is found, [74](#)
- Log file
  - creating with VirusScan, [74](#)
  - displaying, [77](#)
- LZEXE
  - and VirusScan, [75](#)

**M**

- Macro heuristic scanning, [10, 23, 41](#)
- Memory
  - excluding area from scans, [74](#)
  - omitting from scans, [75](#)
  - preventing VirusScan from using expanded, [75](#)
- Messages
  - displaying when a virus is found, [73](#)
  - pausing when displaying, [76](#)
- Moving
  - infected files, [74](#)

**N**

- Network Associates
  - consulting services, [59](#)
  - contacting
    - Customer Care department, [xiii](#)
    - outside the United States, [xv](#)
    - via America Online, [xiv](#)
    - via CompuServe, [xiv](#)
    - within the United States, [xiv](#)
  - customer service, [xiii](#)
  - education services, [59](#)
  - electronic services, [58](#)
  - PrimeSupport
    - Anytime, [56](#)
    - at a glance, [57](#)
    - Basic, [55](#)
    - Extended, [56](#)
  - PrimeSupport options, [55](#)
  - Professional Consulting Services, [59](#)
  - support services, [55](#)
  - technical support, [xiii, 55, 58](#)
  - training, [xv, 59](#)
  - web site, [xiv, 58](#)
- Network drives
  - scanning, [71](#)

**O**

- On-access scanning, [7](#)
  - configuring, [8](#)
- On-demand scanning, [21](#)

## P

- Password protection, [19, 34](#)
- Pausing
  - when displaying VirusScan messages, [76](#)
- PKLITE
  - and VirusScan, [75](#)
- Preventing infection, [61](#)
- PrimeSupport
  - Anytime, [56](#)
  - at a glance, [57](#)
  - availability, [58](#)
  - Basic, [55](#)
  - Extended, [56](#)
  - options, [55](#)
  - ordering, [57](#)
- Professional Consulting Services, [59](#)

## R

- Recovery codes
  - using with VirusScan, [72](#)
- Recovery data
  - adding to executable files, [72](#)
  - removing, [76 to 77](#)
- Reference, [71](#)
- Removing a virus
  - from a file, [52](#)
  - from memory, [52](#)
- Reports, [27](#)
  - adding names of corrupted files to, [76](#)
  - adding names of modified files to, [77](#)
  - adding names of scanned files to, [76](#)
  - adding system errors to, [77](#)
  - centralized, [2, 14, 27, 44, 72, 81, 86](#)
  - generating with VirusScan, [72, 76](#)

## S

- Scan
  - virus detection method, [2](#)
- Scan settings
  - saving, [31](#)
  - saving as default, [31](#)

## Scan task

- configuring, [39](#)
  - Action page, [42](#)
  - Alert page, [43](#)
  - Detection page, [40](#)
  - Exclusion page, [46](#)
  - Report page, [45](#)
  - Security page, [48](#)
- copying, [39](#)
- creating, [35](#)
- deleting, [39](#)
- pasting, [39](#)
- running a program, [36](#)
- setting the schedule, [37](#)
- viewing properties, [38](#)

## SCAN.LOG

- creating a log, [74](#)
- displaying, [77](#)

## Scanning

- configuring a scan task, [39](#)
- creating a scan task, [35](#)
- excluding files, [73](#)
- excluding the memory area, [74](#)
- file types scanned, [72](#)
- including subdirectories, [77](#)
- Macro heuristic, [10, 23, 41](#)
- moving infected files, [74](#)
- multiple diskettes, [74](#)
- network drives, [71](#)
- on access, [7](#)
- on demand, [21](#)
- preventing users from halting, [75](#)
- saving settings, [31](#)
- scheduled, [35](#)
- skipping compressed files, [75](#)
- speeding up, [73](#)
- system memory, [75](#)
- when to scan, [2](#)

## Start-up diskette

- making a, [64](#)

## Subdirectories

- scanning, [77](#)

## System requirements, [3](#)

**T**

Task properties, 38

Technical support, xiii

    e-mail address, xiv

    for retail customers, 58

    hours of availability, 58

    information needed from user, xiv

    online, xiii

    PrimeSupport

        availability, 58

        general discussion, 55

        ordering, 57

    via electronic services, 58

    via World Wide Web, xiv

    web site, 58

Total Education Services, 59

Training, 59

Training for Network Associates products, xv

**U**

Updates and upgrades

    obtaining via World Wide Web, 58

**V**

Validate, 63

Validating VirusScan, 63

Validation codes

    using with VirusScan, 72

Validation data

    adding to executable files, 72

    checking, 73

    checking during virus scans, 73

    removing, 76 to 77

Virus

    defined, 93

    new and unknown, 62

    preventing infection, 61

    updating data files, 62

Virus List

    Contents, 33

    displaying, 32

Viruses

    displaying list of detected, 77

    locking the system if found, 74

    removing, 51

    removing from a file, 52

    removing from memory, 52

VirusScan

    alerts, 26

    and expanded memory, 75

    command-line examples, 78

    command-line options, 71

    configuration lockdown, 34

    configuring exclusions, 29

    configuring reports, 27

    Console, 35

    disabling expiration date message, 75

    displaying a message when a virus is found, 73

    displaying list of detected viruses, 77

    DOS error levels, 78

    excluding files, 73

    excluding memory area from scans, 74

    generating a report file, 72, 76 to 77

    installation, 3

    introducing, 1

    locking the system, 74

    main features, 1

    multiple diskettes, 74

    password protection, 34

    preventing users from halting, 75

    scanning only the boot sector, 72

    setting the scan frequency, 74

    speeding the scan, 73

    validation, 76

## VirusScan command-line options

- [/? or /HELP, 71](#)
- [/ADL, 71](#)
- [/ADN, 71](#)
- [/AF, 72](#)
- [/ALL, 72](#)
- [/APPEND, 72](#)
- [/AV, 72](#)
- [/BOOT, 72](#)
- [/CF, 73](#)
- [/CONTACTFILE, 73](#)
- [/EXCLUDE, 73](#)
- [/FAST, 73](#)
- [/FREQUENCY, 74](#)
- [/LOAD, 74](#)
- [/LOCK, 74](#)
- [/LOG, 74](#)
- [/MANY, 74](#)
- [/MEMEXCL, 74](#)
- [/MOVE, 74](#)
- [/NOBEEP, 75](#)
- [/NOBREAK, 75](#)
- [/NOCOMP, 75](#)
- [/NODDA, 75](#)
- [/NOEMS, 75](#)
- [/NOEXPIRE, 75](#)
- [/NOMEM, 75](#)
- [/PAUSE, 76](#)
- [/PLAD, 76](#)
- [/REPORT, 76](#)
- [/RPTALL, 76](#)
- [/RPTCOR, 76](#)
- [/RPTERR, 77](#)
- [/RPTMOD, 77](#)
- [/RRF, 76](#)
- [/RV, 77](#)
- [/SHOWLOG, 77](#)
- [/SUB, 77](#)
- [/VCV, 73](#)
- [/VIRLIST, 77](#)

VSH file format, [79](#)

## VShield

- [Action page, 12](#)
- [Alert page, 14](#)
- [configuration lockdown, 19](#)
- [configuring, 8](#)
- [Detection page, 9](#)
- [Exclusion page, 17](#)
- [password protection, 19](#)
- [Report page, 15](#)
- [Security page, 19](#)
- [starting, 7](#)
- [Status window, 7](#)

**W**

Write-protecting diskettes, [66](#)