



NetShield NetWare

User's Guide

Version 3.1.8

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>.

Table of Contents

Preface	xi
What happened?	xi
Why worry?	xi
Where do viruses come from?xii
Virus prehistoryxii
Viruses and the PC revolution	xiii
On the frontier	xvi
How to protect yourself	xvi
How to contact Network Associates	xviii
Customer service	xviii
Technical support	xviii
Network Associates training	xix
Comments and feedbackxx
Reporting new items for anti-virus data file updatesxx
International contact information	xxi
Chapter 1. Introducing NetShield NetWare	23
Introduction23
What Is NetShield NetWare?23
NetShield Features24
Superior detection24
Automated protection24
Administrative ease24
Chapter 2. Installing NetShield NetWare	25
Before You Start25
Server requirements25
Client requirements26
Installation Steps26
Creating an NDS object with NSHINST.NLM32
Validating Your Files33
Testing Your Installation35

Chapter 3. Getting Started	37
Enabling NetShield components	37
Starting the NetShield server	37
Stopping the NetShield server	37
Starting the AntiVirus Console	38
Remote Administration	40
Using the AntiVirus Console	41
Creating a task with the Scan wizard	44
Adjusting server performance	51
Chapter 4. On-Access Scanning	55
Using NetShield's on-access scanner	55
Configuring the on-access task	55
Chapter 5. On-demand and Scheduled Scanning	67
Using NetShield's on-demand scanner	67
Creating an on-demand task	67
Running your scan task	80
Viewing scan results	81
Chapter 6. Virus Notification	83
Using NetShield's Alerting Features	83
Configuring Alert Manager	83
Using Centralized Alerting	101
Configuring Centralized Alerting	102
Customizing alert messages	103
Chapter 7. Updating NetShield	107
Overview	107
Updating Strategies	107
Rumor strategy	108
Configuring AutoUpdate	109
Scheduling AutoUpdate	111
Updating NetShield .DAT files	113
Troubleshooting AutoUpdate	113

Appendix A. Network Associates Support Services 115

- PrimeSupport Options for Corporate Customers115**
 - PrimeSupport Basic115**
 - PrimeSupport Extended116**
 - PrimeSupport Anytime116**
 - Ordering PrimeSupport118**
- Support Services for Retail Customers118**
- Network Associates Consulting and Training119**
 - Professional Consulting Services119**
 - Total Education Services120**

Index 121

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+DEL** keyboard sequence for a warm reboot, then faking a restart. Sometimes the only outward indication that anything on your system is amiss—before any payload detonates, that is—might be a small change in the file size of infected legitimate software.

Stealth, 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 and perform unwanted actions on the recipient's computer. The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it.

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 website. 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 website 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
McCandless Towers
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 <http://support.nai.com>

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

Automated Voice and Fax (408) 988-3034
Response System

Internet support@nai.com

CompuServe GO NAI

America Online keyword MCAFEE

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers Monday through Friday between 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
- For workstation problems, the contents of the workstation's AUTOEXEC.BAT, CONFIG.SYS and user LOGIN script
- Contents of the server's AUTOEXEC.NCF, STARTUP.NCF, and SYSSLOG.ERR files
- A current config report (generated by Novell's CONFIG.NLM utility) from the affected server, created while NetShield is loaded
- 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.

Comments and feedback

Network Associates appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please address your comments about Network Associates documentation to: Network Associates, Inc., 3965 Freedom Circle, Santa Clara, CA 95054. You can also send faxed comments to (408) 970-9727 or e-mail to tvd_documentation@nai.com.

Reporting new items for anti-virus data file updates

Network Associates anti-virus software offers you the best available detection and removal capabilities, including advanced heuristic scanning that can detect new and unnamed viruses as they emerge. Occasionally, however, an entirely new type of virus that is not a variation on an older type can appear on your system and escape detection. Because Network Associates researchers are committed to providing you with effective and up-to-date tools you can use to protect your system, please tell them about any new viruses that your software does not now detect. Note that Network Associates reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

virus_research@nai.com

Use this address to report new virus strains.

To report items to our European research office, use this e-mail address:

virus_research_europe@nai.com

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

avert-jp@nai.com

Use this address to report harmful items to our office in Japan.

avert_apac@nai.com

Use this address to report harmful items to our Asia-Pacific office.

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

NA Network Associates Oy

Kielotie 14B

01300 Vantaa

Finland

Phone: 358 9 836 2620

Fax: 358 9 836 26222

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 Canada

139 Main Street, Suite 201

Unionville, Ontario

Canada L3R 2G6

Phone: (905) 479-4189

Fax: (905) 479-4540

Network Associates International B.V.

Gatwickstraat 25

1043 GL Amsterdam

The Netherlands

Phone: 31 20 586 6100

Fax: 31 20 586 6101

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 Japan, Inc.

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

Network Associates Korea

135-090, 18th Floor, Kyoung Am Bldg.
157-27 Samsung-Dong, Kangnam-Ku
Seoul, Korea
Phone: 82-2-555-6818
Fax: 82-2-555-5779

Network Associates Portugal

Rua Gen. Ferreira Marines, 10-6 C
1495 ALGÉS
Portugal
Phone: 351 1 412 1077
Fax: 351 1 412 1488

Network Associates South East Asia

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

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
ITALY
Phone: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

Network Associates Latin America

150 S. Pine Island Road, Suite 205
Plantation, Florida 33324
United States
Phone: (954) 452-1731
Fax: (954) 236-8031

Network Associates South Africa

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

Network Associates Spain

Serrano 240, Plta. -1
28016 Madrid
Spain
Phone: 34 91 458 52 21
Fax: 34 91 457 45 17

Introducing NetShield NetWare

1

Introduction

Networked computing and the emergence of collaborative technologies have dramatically increased the speed at which viruses spread in the corporate workplace. Infected files in a network environment can rapidly escalate an individual user incident into a large-scale virus outbreak. The expense of cleaning a network-based infection can be staggering. These expenses include lost employee productivity, potential loss of data, internal help desk service costs, and additional network administrator and desktop service personnel support. These issues make server virus protection a must. During critical business cycles, insufficient protection could cost your company its competitive edge.

What Is NetShield NetWare?

NetShield is a superior client/server anti-virus solution that enables you to scan for and clean virus-infected files on Novell NetWare servers. NetShield combines award-winning Network Associates Hunter virus scanning technology with robust server management capabilities to minimize the virus threat within networks. Hunter scanning technology combines several virus analysis technologies to detect all virus types, including macro, file, multi-partite, stealth, polymorphic, and encrypted viruses. The Hunter engine also stops viruses that infect Visual Basic 5.0, Office 95, and Office 97 files, which keeps you safe from the newest threats to data security.

NetShield is an important element of a comprehensive security program that includes regular backups, meaningful password protection, training, and awareness. Network Associates urges you to set up and comply with such a security program to prevent future infection.

NetShield Features

Superior detection

- NetShield's Hunter scan technology identifies viruses with pinpoint accuracy.
- Continuous background scanning looks for viruses whenever you create, open, save, run, or copy files over your network.
- User-initiated scan operations identify all known file, macro, multi-partite, stealth, encrypted, and polymorphic viruses.
- NetShield scans and cleans compressed files.
- NetShield uses advanced heuristic scanning technology to detect previously unknown macro viruses.

Automated protection


- NetShield can automatically notify you when it finds a virus; clean, isolate, or delete the infected file; and record its actions in a log file.
- Network administrators can schedule NetShield scan operations for convenient times, or initiate immediate scan operations at any time.

Administrative ease

- NetShield can send virus alert messages to alphanumeric pagers, or via e-mail, Simple Network Management Protocol (SNMP) alerts, and network broadcasts. You can also tell NetShield to run a particular program to alert you when it finds a virus.
- Administrators can use NetShield to collect and distribute virus alert messages to other servers and workstations on the network in order to centralize anti-virus security measures.
- An intuitive Scan Wizard makes task creation quick and easy.
- Administrators can automatically update and distribute new data files to servers and workstations with the included AutoUpdate utility.

Before You Start

Network Associates distributes NetShield in two ways: as an archived file that you can download from the Network Associates website or from other electronic services; and on CD-ROM. Once you have downloaded the NetShield archive or placed the NetShield installation disc in your CD-ROM drive, the installation steps you follow after that are the same for each distribution type. Review the system requirements shown below to verify that NetShield will run on your system, then follow the steps on [page 26](#).

-
-  **IMPORTANT:** If you have on your NetWare server an active NetShield version that you plan to upgrade, you must first unload the NetShield NLM file before you proceed with your installation. For instructions, see [“Stopping the NetShield server” on page 37](#).
-

Server requirements

NetShield will install and run on a server equipped with

- A processor equivalent to an Intel Pentium or later. To run Novell NetWare 5.0, you must have a processor equivalent to an Intel Pentium/133 or faster. Network Associates recommends a Pentium II or compatible processor.
- A CD-ROM drive. If you downloaded your copy of NetShield, this is an optional item.
- At least 2MB of free disk space for program files and sufficient space for NetShield to use to decompress and check archived file for viruses.
- At least 3MB of free random-access memory (RAM) dedicated for NetShield's use.
- Novell NetWare versions 3.12, 4.10, 4.11, or 5.0.
- Current Novell NetWare software patches for the NetWare version you use. You can find a list of current patches at this website:

<http://support.novell.com/misc/patlist.htm>

Client requirements

The NetShield client will install and run on a workstation equipped with

- A processor equivalent to an Intel 80486 or later. Network Associates recommends at least a Pentium or compatible processor.
- At least 6MB of free disk space for program files.
- Windows 95, Windows 98 or Windows NT.
- SPX protocol support (Microsoft or Novell).
- Novell NetWare client software (either Microsoft Client for NetWare or Novell's Client 32).
- NetWare Directory Services (optional).

Installation Steps

Choose the type of NetShield distribution you have, then follow the corresponding steps to prepare your files for installation.

- **If you downloaded your copy of NetShield** from the Network Associates website or from another electronic service, make a new, temporary folder on your hard disk, then use WinZip, PKZIP, or a similar utility to extract the NetShield installation files to that temporary folder. You can download the necessary utilities from most online services.
- **If your copy of NetShield came on a CD-ROM disc**, insert that disc into your CD-ROM drive.

Next, follow these steps:

1. Choose **Run** from the **Start** menu.

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

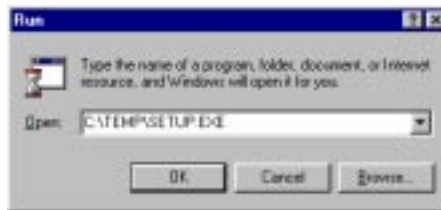


Figure 2-1. The Run dialog box

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

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

- NOTE:** If your NetShield copy came on a NetShield Security Suite or a Total Virus Defense CD-ROM, you must also specify which folder contains NetShield NetWare. See the CONTENTS.TXT file included on that CD-ROM for details.

The first Setup wizard panel will appear (Figure 2-2).



Figure 2-2. Welcome to Setup panel

3. Click **Next>** to continue.

The next wizard panel displays the NetShield end-user license agreement. Read this agreement carefully—if you install NetShield, you agree to abide by the terms of the license.

4. If you do not agree to the license terms, click **No**. Setup will quit immediately. Otherwise, click **Yes** to continue.

The Setup Type panel will appear (Figure 2-3).

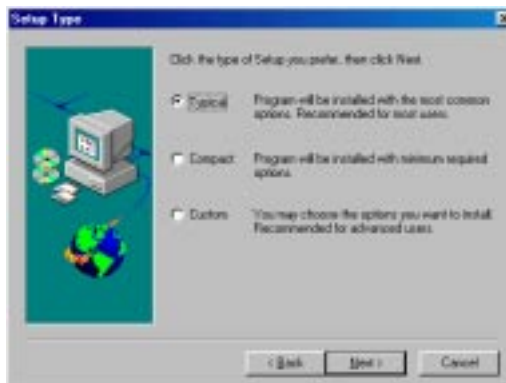


Figure 2-3. Setup Type panel

5. Select the NetShield component sets you want to install. You can choose from these options:
 - **Typical.** Select this option to install the NetShield client and server software, together with all utilities. Network Associates recommends this installation for most environments.
 - **Compact.** Select this option to install only the AntiVirus Console.
 - **Custom.** Select this option to choose the specific NetShield components you want to install. By default, the Custom option installs the same components as the Typical installation, but you can choose instead to install either the server software, the client software, or both.
6. When you have chosen the component set you want to install, click **Next>** to continue.

If you have an earlier NetShield version installed on either the server or the client computer, you'll see the Previous Installation Found panel (see [Figure 2-4 on page 29](#)). If you are installing NetShield for the first time, skip to [Step 9](#).



Figure 2-4. Previous Installation Found panel

7. Setup can install your new NetShield version over your existing NetShield installation or it can first uninstall the existing version before it installs the new version. Choose either of these options:
 - **Preserve.** This tells Setup to replace older program files with current files but retain the program settings from your earlier version, including the tasks you've created and any other configuration options you've chosen.
 - **Uninstall.** This tells Setup to remove the existing program version from your system, including all configuration files, before it continues with the installation. You will need to recreate any tasks you need and reconfigure other program settings.
8. When you have told Setup how to proceed, click **Next>** to continue.

The Choose Console Component Directory screen appears (Figure 2-5).



Figure 2-5. Choose Console Component Directory panel

- Click **Browse** to locate the folder you want to use for the installation. By default, Setup installs the AntiVirus Console files in this path:

C:\Program Files\Network Associates\NetShield

If you have a previous version of NetShield installed in this path:

C:\Program Files\McAfee\NetShield

Setup will install your upgrade to this same directory.

- When you have chosen your directory, click **Next>** to continue.

The Select Network Servers panel appears (see [Figure 2-6 on page 30](#)).



Figure 2-6. Select Network Server(s) panel

- Select a NetWare server from the list, if any appear there, or click **Browse** to locate a server on your network. Next, click **Add** to display the Server Information dialog box ([Figure 2-7](#)).



Figure 2-7. Server Information dialog box

- Enter a user name and a password in the text boxes provided, then click **Connect**. The workstation connects to the server.

NOTE: The user name you enter must have administrator or supervisor rights on the NetWare server you chose in [Step 11](#).

13. Specify an installation directory for the server in the **Directory** text box, or click **Browse** to locate a suitable directory. Next, specify a path in the text box below for Setup to use to create a NetWare Directory Services (NDS) object. Click **OK** to close the Server Information dialog box.

- NOTE:** For Setup to create the NetShield NDS object on servers running NetWare 4.x, you must have Novell Client32 installed on the computer you're using to install NetShield. If the server is running NetWare 4.x and the NDS Path field is unavailable, you must create the NDS object with NSHINST.NLM. If you do not want to create an NDS user, or if you are running a NetWare version earlier than 4.x, leave this text box blank. In this case, you might not have access to some NetShield alerting features. For more information, see [“Creating an NDS object with NSHINST.NLM” on page 32.](#)

14. Repeat [Steps 11 to 13](#) for each NetWare server that you want to host a copy of NetShield.
15. When you have finished choosing NetWare servers, click **Next>** to continue.

The Confirm Installation Settings panel appears ([Figure 2-8](#)).



Figure 2-8. Confirm Installation Settings panel

16. Review the installation settings. If the options shown are not correct, click **<Back** and make any necessary changes. If all installation options are correct, click **Next>**.

NetShield begins copying files to the servers you specified. Once Setup has copied the NetShield files, it asks you to view the WHATSNEW.TXT file. Click **Yes** to review additional information about NetShield.

Creating an NDS object with NSHINST.NLM

To run correctly on NetWare 4.x servers, NetShield must create an NetWare Directory Services (NDS) user as part of the installation process. If NetShield cannot create an NDS user, you might lose access to some of the program's alerting capabilities.

NetShield can create the NDS object in either of two ways:

- If you run Setup from a workstation that provides 32-bit NDS support—such as one running Novell's Client32—NetShield creates the NDS object automatically during installation. See [Step 13 on page 31](#) for details.
 - **NOTE:** Microsoft's NDS support (MSNDS) provides support only for 16-bit applications. If you use MSNDS you *must* run NSHINST.NLM from each server that will run NetShield.
- If you run Setup from a workstation that does not provide 32-bit support, or if NetShield could not create the NDS object during installation, then you must log on to the server from the NetWare console and run the NSHINST.NLM utility.

To run the NSHINST.NLM utility, follow these steps:

1. Log on to the NetWare server to which you just installed NetShield.
2. If NetShield is active, unload the NetShield NLM. For instructions, see [“Stopping the NetShield server” on page 37](#).
3. Type this command at the console:

```
LOAD <InstallPath>\NSHINST.NLM
```

Here, <InstallPath> is the server directory in which you just installed NetShield. By default, this would be SYS:MCAFFEE\NETSHLD.

4. Log on to NetShield with your administrator's account name and password, then press **ENTER** to continue.
5. On the line provided, specify the NDS context in which you want to create the NDS object, then press **ENTER**.

NetShield creates the NDS object in the context you specified.

- **NOTE:** When you create an NDS object, NetWare generates an internal password for it to use to interact with the NetWare directory. If this password gets out of sync with what NetShield expects to see, NetShield cannot log in to NDS. If this occurs, run NSHINST.NLM again and specify the same NDS context you used before to generate a new password for the object.
-

Validating Your Files

Downloading or copying files from any outside source places your computer at risk of virus infection—even if the risk is small. Downloading anti-virus software is no exception. Network Associates uses strict and extensive security measures to ensure that the products you purchase and download from its website and its other electronic services are safe, reliable, and free from virus infections. But anti-virus software tends to attract the attention of virus- and trojan-horse writers, some of whom find it amusing to post infected copies of commercial software, or use the same file names to camouflage their own work.

You can protect yourself from this possibility by ensuring that you

- Download your files only from the Network Associates website; and
- Validate the files you download.

Network Associates includes a copy of VALIDATE.EXE, its validation software, with each NetShield package.

To validate your files, follow these steps:

1. Install NetShield as described in “[Installation Steps](#)” on [pages 26 to 31](#).
2. Click **Start** in the Windows taskbar, point to **Programs**, then choose **MS-DOS Prompt**.
3. In the window that appears, change your command-line prompt to point to the directory that contains the NetShield files you installed. If you chose the default installation options, you’ll find the files in this path:

C:\Program Files\Network Associates\NetShield

To get to this directory, type `cd progra~1\networ~1\netshi~1` at the command prompt, then press **ENTER**. If you installed NetShield in a different directory, type the correct path to that directory.

4. Run VALIDATE.EXE. To do so, type `validate *.*` at the command-line prompt.

VALIDATE.EXE scans all of the files stored in your NetShield program directory, then generates a file list that includes the file name, its size in bytes, its creation date and time, and two validation codes in separate columns. To use VALIDATE.EXE to examine individual files, simply follow `validate` with the name of the file you want to verify at the prompt, or use the DOS wildcards `?` and `*` to specify a range of files.

- **NOTE:** Network Associates recommends that you redirect the output from VALIDATE.EXE to your printer so that you can review it easily. If you have set your printer to capture output from MS-DOS programs, simply type `validate >lpt1` at the command-line prompt. To learn how to set your printer to print from MS-DOS programs, consult your Windows documentation.
-

To ensure that you have exactly the same files as did the engineers who packaged your copy of NetShield, you need to compare the validation codes you generated when you ran VALIDATE.EXE against the packing list supplied with NetShield. The packing list is a text file that contains the validation codes that Network Associates engineers generated from independent cyclical redundancy check (CRC) processes when they packaged NetShield for delivery. This method provides a high degree of security and prevents tampering.

5. To display the packing list, type `type packing.lst` at the command-line prompt, then press **ENTER**.
-

- **NOTE:** Network Associates again recommends that you redirect the output from PACKING.LST to your printer. To do so, type `type packing.lst>lpt1` at the command-line prompt.
-

6. Compare the output from VALIDATE.EXE to that from PACKING.LST. The sizes, creation dates and times, and validation codes for each file name should match exactly. If they do not, delete the file immediately—do *not* open the file or examine it with any other utility; doing so can risk virus infection.
-

- 🔥 **IMPORTANT:** Checking your NetShield installation with VALIDATE.EXE does not *guarantee* that your copy is free from defects, copying errors, virus infections or tampering, but the program's security features make it extremely unlikely that anyone has tampered with files that have correct validation codes. See the files LICENSE.TXT or README.1ST included with your copy of NetShield to learn the license terms that cover your use of the program.
-

Testing Your Installation

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


To test your installation, follow these steps:

1. Open a standard Windows text editor, such as NotePad, then type the following line:

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

-
- NOTE:** The line shown above should appear as *one line* in your text editor window. If you are reading this manual on your computer, you can copy the line directly from the Acrobat file to Notepad.
-

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

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

Enabling NetShield components


NetShield NetWare consists of an AntiVirus Console client application and the NetShield server application, which is a NetWare Loadable Module (NLM). You can use the AntiVirus Console to configure and control the NetShield server from any workstation on the network. The Console also allows you to see scanning statistics and receive virus alert messages.

Although you need the AntiVirus Console to administer the server software, you do not need to keep it running in order for the NetShield NLM to perform its background scanning operations or any scan tasks you schedule. You must, however, have the NLM running in order to perform all scan tasks.

Starting the NetShield server

To start the NetShield NLM, follow these steps:

1. Log on to the NetWare server that hosts the NetShield NLM you want to activate, either at the server itself, or from elsewhere on your network.

 **NOTE:** To log on, you'll need administrator or supervisor rights to the server.

2. Type `netshld` at the NetWare console prompt, then press **ENTER**.

NetShield locates its support files and initializes itself. It will continue running until you shut it down again. See [“Stopping the NetShield server”](#) for details.

Stopping the NetShield server

To unload the NetShield NLM, follow these steps:

1. Log on to the NetWare server that hosts the NetShield NLM you want to unload, either at the server itself, or from elsewhere on your network.
2. Type `unload netshld` at the NetWare console prompt, then press **ENTER**.

NetShield immediately begins its shutdown process.

Starting the AntiVirus Console

To start the AntiVirus Console

- In Windows NT 3.51, start Program Manager, open the NetShield program group, then double-click the AntiVirus Console icon.
- In Windows NT 4.0, Windows 95, and Windows 98, click **Start** in the taskbar, point to **NetShield** in the **Programs** submenu, then choose **AntiVirus Console**.

The AntiVirus Console window appears (Figure 3-1).

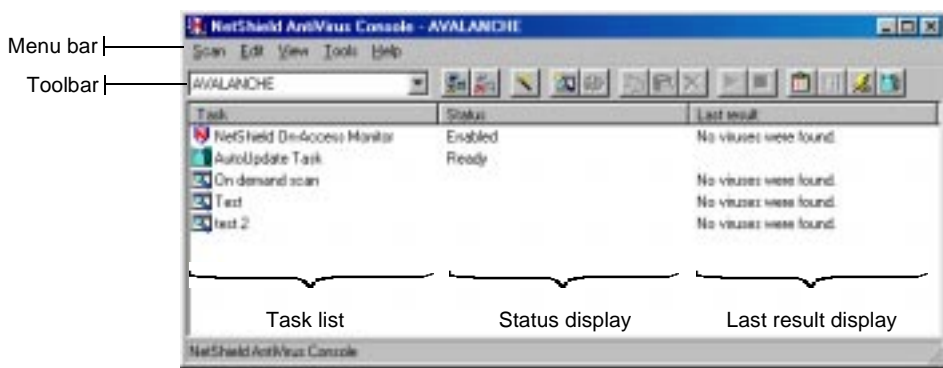


Figure 3-1. AntiVirus Console window

From here, you can connect to and administer any server running NetShield NetWare or NetShield NT. To do so, you must log onto each NetShield server that you want to configure. See [“Remote Administration” on page 40](#) for details. The Console window then changes to display the current set of settings for that server. The next sections describe the window elements you’ll see.

The task list

A task is a set of instructions to run a particular program or scan operation, in a particular configuration, at a certain time. The task list initially displays a default set of tasks that provide your server with a minimum level of protection. You can create additional tasks to suit your needs. NetShield can perform three types of tasks: on-access tasks; on-demand or scheduled tasks; and AutoUpdate tasks.

On-access tasks

NetShield’s on-access scanner looks for viruses in files opened, saved, or copied to and from the NetShield server. You can configure NetShield’s on-access task to specify which files the scanner examines and how it responds when it finds infected files. To learn how to change the settings that govern the on-access task, see [“Configuring the on-access task” on page 55](#).

On-demand and scheduled tasks

On-demand tasks let you initiate a scan operation immediately. You can specify which volumes on your network you want to scan, tell NetShield how to respond if it finds an infected file, and choose options for alerting and logging, then have NetShield go to work. Scheduled tasks run at specific times, or repeatedly at specific intervals, and can include all of the options permitted for an on-demand scan. To learn how to configure on-demand tasks and schedule them, see [Chapter 5, “On-demand and Scheduled Scanning.”](#)

AutoUpdate tasks

AutoUpdate automatically retrieves new data files from an FTP a server on your network that you designate as a distribution site. AutoUpdate can also post the downloaded files to another distribution server for other computers to download. To learn how to create and schedule AutoUpdate tasks, see [Chapter 7, “Updating NetShield.”](#)

Task statistics

Double-click a listed task—or select a task, then choose **Statistics** from the **Scan** menu—to see status information and results from the most recent scan operation (see [Figure 3-2 on page 39](#)).



Figure 3-2. Task Statistics window

The status bar

As you move the cursor around the Console window, the status bar displays information about each item your cursor touches.

The last results display

The last results display shows a summary of the latest results for a listed task.

Remote Administration

When you start the AntiVirus Console, the name of the server it is connected to appears in the Console title bar. If you use the Console to configure a NetShield NT server running on the same computer, you will not see the server name in the title bar.

To administer a remote computer running NetShield, follow these steps:

1. Click  or select **Remote Connection** from the **Tools** menu.

The Connect to Remote Computer dialog box appears ([Figure 3-1 on page 40](#)).

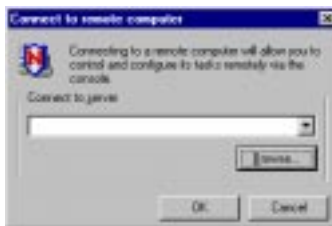


Figure 3-1. Connect to Remote Computer dialog box

2. Choose one of the listed servers, or enter the name of the server that you want to administer in the text box. You can also click **Browse** to locate the computer on the network. The target server must have the NetShield server software for Windows NT or Novell NetWare installed.

-
- NOTE:** Which configuration options you have available to you will vary according to which NetShield version the target server runs. If you cannot connect to a server, click **Advanced**, then select **Enable broadcast discovery** to have the Console search for your server.
-

3. Click **OK**.
4. NetShield asks you for the password for that server. Enter your password in the text box provided, then click **OK**.

-
- NOTE:** Your initial NetShield password will be `netshield`. Network Associates recommends that you change your password immediately after you log on to your server. See [page 43](#) for details.
-







The name of the new server appears in the Console title bar and any configured tasks appear in the Console task window. Tasks configured to run on other servers disappear.


Using the AntiVirus Console

The AntiVirus Console includes a set of commands that allow you to create, delete, configure, run, stop, import and export, and copy scan tasks to suit your most demanding security needs.


The toolbar at the top of the Scheduler window gives you quick access to the program's most common commands. Most of those same commands also appear in the menus at the top of the Scheduler window, and in shortcut menus that appear when you click a listed task with your right mouse button.

From the Console window, you can:







- **Connect to a NetShield server.** Choose **Remote Connection** from the **Tools** menu, or click  in the Console toolbar. The Connect to Remote Computer dialog box will appear. See [“Remote Administration” on page 40](#) to learn how to complete your connection.
- **Disconnect from a NetShield server.** Choose **Disconnect Computer** from the **Tools** menu, or click  in the Console toolbar. The task list clears as you disconnect.
- **Start the Scan Wizard.** Choose **Scan Wizard** from the **Scan** menu, or click  in the Console toolbar. The first Scan Wizard panel will appear. Follow the instructions shown on each panel to configure an on-demand or a scheduled scan task.
- **Create a new task.** Choose **New Task** from the **Scan** menu, or click  in the Console toolbar. A Task Properties dialog box will appear. See [“On-demand and Scheduled Scanning” on page 67](#) to learn how to configure your new task.
- **Configure a scan task.** Select one of the tasks listed in the Console window, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar. The Task Properties dialog box for that task will appear. See [“On-demand and Scheduled Scanning” on page 67](#) to learn how to change your task configuration.
- **Copy a task.** Use this feature to copy on-demand task settings that you want to use as templates for other, similar tasks. Select one of the on-demand tasks listed in the Console window, then choose **Copy** from the **Edit** menu, or click  in the Console toolbar. This copies the task to the Windows clipboard.

To copy the task back into the Console window, click in a blank area at the bottom of the task list, then choose **Paste** from the **Edit** menu, or click  in the Console toolbar. To copy the task to a different copy of NetShield running on another computer, use the Console to connect to the other computer before you paste the task to the Console window. See [“Remote Administration” on page 40](#) to learn how to connect to another computer.

When you paste the task back into the Console window, NetShield prompts you to name the task. Type a name, then press **ENTER**. NetShield then opens the Task Properties dialog box to give you an opportunity to modify the task before you save it. See [“Using NetShield’s on-demand scanner” on page 67](#) to learn how to change task settings. Click **OK** to close the Task Properties dialog box when you have changed the task settings to meet your needs.

- **Delete a task.** Select one of the tasks listed in the Console window, then choose **Delete** from the **Scan** menu, or click  in the Console toolbar. NetShield will ask you to confirm that you want to delete the selected task. Click **Yes** to delete the task, or click **No** to keep it.

NOTE: You can delete only tasks that you create—you may not delete the on-access or AutoUpdate tasks that come with the Console. You can, however, disable any task you don’t want to run.

- **Start a task.** Select one of the tasks listed in the Console window, then choose **Start** from the **Scan** menu, or click  in the Console toolbar. The task you selected will start immediately and run with the options you’ve chosen. To start the on-access task, select it in the list, then choose **Enable** from the **Scan** menu.
- **Stop a task.** Select one of the tasks listed in the Console window, then choose **Stop** from the **Scan** menu, or click  in the Console toolbar. To stop the on-access task from running, select it in the task list, then choose **Disable** from the **Scan** menu.
- **Connect to the Virus Information Library.** Choose **Online Virus Info Library** from the **Help** menu, or click  in the Console toolbar. NetShield will launch your default browser software and connect to the Network Associates website to display the library.
- **Open the Windows NT Event Viewer.** If you are connected to a Windows NT server, you can choose **Event Viewer** from the **Tools** menu, or click  in the Console toolbar to open the Windows NT Event Viewer. If you are connected to a NetWare server, this button and the corresponding menu item will be unavailable.
- **Configure Alert Manager.** Choose **Configure Alert Manager** from the **Tools** menu, or click  in the Console toolbar. The Alert Manager Properties dialog box will open. See [“Virus Notification” on page 83](#) to learn how to tell NetShield to alert you when it finds a virus.
- **Configure AutoUpdate.** Choose **AutoUpdate** from the **Tools** menu, or click  in the Console toolbar to open the AutoUpdate Properties dialog box. See [“Updating NetShield” on page 107](#) to learn how to use AutoUpdate to get current NetShield data files.

- **Rename a task.** Select a listed task, then choose **Rename** from the **Scan** menu. Type the new task name in the task list, then press **ENTER**.
- **View the NetShield Activity Log.** Choose **Activity Log** from the **Scan** menu to open the log file NetShield uses to record its actions during scan operations. See [“Logging on-demand scan activity” on page 74](#) to learn more about creating log files.
- **Import a task.** Choose **Import** from the **Edit** menu. Locate a file with the extension `.VSC` in the Select Import File dialog box that appears, then click **OK** to have it appear in the task list. NetShield prompts you to name the task. Type a name, then press **ENTER**.

NetShield then opens the Task Properties dialog box to give you an opportunity to modify the task before you save it. See [“Using NetShield’s on-demand scanner” on page 67](#) to learn how to change task settings. Click **OK** to close the Task Properties dialog box when you have changed the task settings to meet your needs.

- **Export a task.** Select a listed task that you created, then choose **Export** from the **Edit** menu. Name your file in the Select Export File dialog box that appears and choose a location to save it, then click **Save**. NetShield saves the task as a `.VSC` file that records all of the task options you chose. You can copy this file to another server, mail it, or otherwise distribute it for use with any other NetShield installation.
- **Change your Console view.** Choose **Toolbar** or **Statusbar** from the **View** menu to display or hide each of these Console window elements. Choose **Refresh** from the **View** menu to update the task list display immediately.


Choose **Options** from the **View** menu to set an interval for NetShield to automatically refresh the task list display. By default, the Console window refreshes every three seconds. Enter an interval in the **Refresh Time** text box, or click the arrows beside the text box to change the value shown. Click **OK** to save your settings and close the Options dialog box.

- **Enable virus alerts.** Choose **Alerts** from the **Tools** menu to open the Alert Properties dialog box. From here you can enable NetShield’s Centralized Alerting, activate the Alert Manager, and edit the priority and content of any alert messages NetShield sends. See [“Virus Notification” on page 83](#) to learn how to configure and send alert messages.
- **Change your password.** Choose **Change Password** from the **Tools** menu. In the dialog box that appears, enter the password you have used to log on to the NetShield server you are now controlling. Enter a new password in the text box provided, then confirm it. Click **OK** to close the dialog box.
- **Choose server options.** See [“Adjusting server performance” on page 51](#) to learn how to adjust the on-access scan cache and use other options.
- **Open the online help file.** Choose **Help Topics** from the **Help** menu to open the NetShield online help file.

Creating a task with the Scan wizard

NetShield comes with a preconfigured on-access task that enables it to begin scanning for viruses as soon as you install it. To ensure more than a minimal level of anti-virus security, however, you should tailor the application to your own particular needs by configuring the on-access task and creating a set of on-demand or scheduled tasks that closely examine your network traffic for viruses. You can use NetShield's Scan wizard to create a basic set of on-demand tasks right away, then modify them to work better in your environment as you become more familiar with NetShield and your network's susceptibility to viruses.

To use the Scan wizard to create a task, follow these steps:

1. Start the AntiVirus Console and log on to a NetWare server running NetShield. See [“Starting the AntiVirus Console” on page 38](#) and [“Remote Administration” on page 40](#) for details.
2. Choose **Scan Wizard** from the **Scan** menu, or click  in the Console toolbar.

The first Scan wizard panel appears ([Figure 3-2](#)).



Figure 3-2. Welcome to Scan Wizard panel

3. Click **Next>** to continue.

The Scan wizard displays a panel where you can specify which volumes you want NetShield to scan for viruses (see [Figure 3-3 on page 45](#)). By default, NetShield scans all local NetWare volumes on its host server and all of the subfolders they contain. A scan operation this inclusive could take a long time, so you might want to narrow this scan for regular use.



Figure 3-3. Specify scan targets panel

4. Choose your scan targets. You can
 - **Supplement existing scan targets.** Click **Add** to open the Add Scan Item dialog box (Figure 3-4).



Figure 3-4. Add Scan Item dialog box

Next, choose a scan target from the list. You can choose to scan all local NetWare volumes, or a particular volume or file. If you choose to scan a volume or file, enter the path to the volume—or the path and file name—in the **Description** text box. You can specify the path in Universal Naming Convention (UNC) notation, or you can click **Browse** to locate the correct file or volume on the server. When you have finished, click **OK** to close the dialog box.

-
- NOTE:** The NetShield NetWare server will ignore any volumes on your computer that are not formatted as Novell NetWare volumes.
-

- **Delete existing scan targets.** Select a listed target, then click **Remove**.

- **Modify or narrow existing scan targets.** Select a listed target, then click **Edit** to open the Edit Scan Item dialog box (Figure 3-5).



Figure 3-5. Edit Scan Item dialog box

Choose or specify a new scan target, then click **OK** to close the dialog box.

5. When you have chosen your scan targets, click **Next>** to continue.

The Scan wizard displays a panel where you can specify how you want NetShield to perform your scan operation (Figure 3-6).



Figure 3-6. Choose scan options panel

6. Choose your scan options. You can
 - **Scan volume subfolders.** By default, NetShield scans all subfolders in the volumes you target for scanning. To scan only the root level of your chosen volumes, clear the **Include subfolders** checkbox.
 - **Scan compressed files.** Also by default, NetShield scans all files in target volumes that are compressed in the LZH and PKZIP archiving formats. You can prevent NetShield from scanning these files, however, by clearing the **Scan inside compressed files** checkbox.

- **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations. To do so, select the **Scan program files only** checkbox. To see or designate the file name extensions NetShield will scan, click **File Types** to open the Program File Extensions dialog box (Figure 3-7).

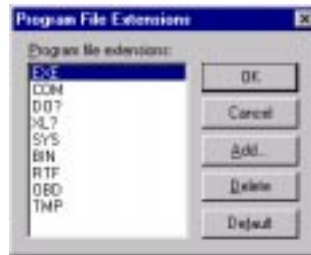


Figure 3-7. Program File Extensions dialog box

By default, NetShield scans files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .SYS, .OBD, .BIN, and .TTS. Files with .DO?, .XL?, .RTF and .OBD extensions are Microsoft Word, Microsoft Excel, and Microsoft Office binder files, all of which can harbor macro virus infections—the ? character is a wildcard that enables NetShield to scan document and template files.

- To add to the list, click **Add**, then type the extension you want NetShield to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Delete**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

To scan all volume, folders and files on your NetWare server, select the **Scan All files** checkbox. This will slow your scan operations down considerably, but will ensure that your system is virus free.

7. When you have finished choosing your scan options, click **Next>** to continue.

The Scan wizard displays a panel where you can choose alerting and logging options (see Figure 3-8 on page 48).



Figure 3-8. Choose alert and logging options panel

8. Activate the alert options you want and tell NetShield where to record its actions. You can

- **Send alerts via Alert Manager.** To have NetShield send a message for Alert Manager to deliver whenever it finds a virus, select the **Notify Alert Manager** checkbox. Alert Manager will send the alert message via all of the channels you've configured it to use. See [“Virus Notification” on page 83](#) to learn how to configure Alert Manager.
- **Log scan activity.** To have NetShield keep a record of its scan operations in a text file you can open and review, select the **Log to file** checkbox, then choose a text file NetShield can use to record its actions. By default, the program uses a file called ACTIVITY.TXT. To use a different text file, type the path and file name in the text box provided, or click **Browse** to locate the file on your hard disk.

To keep the log file from growing too large, select the **Limit size of log file to** checkbox, then enter a size, in kilobytes, beyond which the file should not grow. NetShield will clear the log and start again when it reaches the limit you specify.

9. When you have chosen your reporting and alert options, click **Next>** to continue.

The wizard displays a panel where you can choose how NetShield will respond when it detects a virus (see [Figure 3-9 on page 49](#)).



Figure 3-9. Specify virus response panel

10. Choose one of the listed responses. You can

- **Continue Scanning.** This tells NetShield to note when it detects a virus, then to continue scanning without taking any other action. If you have configured alert and logging options, NetShield will alert you that it has found a virus and will record the incident in its log.
- **Move infected file to a folder.** This tells NetShield to quarantine the infected file in a specific folder. By default, NetShield stores the file in a folder named Infected on the volume that hosts the NetShield server. You cannot specify a different folder from within the Scan wizard, but you can when you configure scan task options. See [“On-demand and Scheduled Scanning” on page 67](#) for details.
- **Clean infected file.** This tells NetShield to try to remove the virus from the infected file and restore it to its original, uninfected condition. The data files that come with NetShield include virus cleaners for most virus types, but in some cases, NetShield will not be able to remove a virus. In that case, it will note the incident in any alert message it sends and in its log file, if you’ve enabled it, then it will continue scanning.
- **Delete infected file.** This tells NetShield to delete the infected file as soon as it detects it. You will need to restore the file from backups if you need it again.

11. When you have finished choosing your response, click **Next>** to continue.

The Scan wizard displays its final panel, where you can have NetShield run your new task immediately, or save it to run or schedule for later (see [Figure 3-10 on page 50](#)).



Figure 3-10. Run or save task panel

12. Tell NetShield what you want it to do with the task you've just created. You can

- **Run task now without saving.** This tells NetShield to run the task once, then discard it.
- **Save task without running.** This tells NetShield to save the task for later. You can then choose to run it as an on-demand task by selecting it in the task list and choosing **Start** from the **Scan** menu, or you can schedule it to run later. See [“On-demand and Scheduled Scanning” on page 67](#) for more details.

Enter a name for your task in the text box provided to save it in the AntiVirus Console task list.




- **Save and run task now.** This tells NetShield to run your task immediately and also to save it for you to run it later. Enter a name for your task in the text box provided to save it in the AntiVirus Console task list.

13. When you have specified what you want to do, click **Finish** to close the wizard panel.

If you asked NetShield to run your task immediately, you'll see the New Scan Task dialog box appear as NetShield begins scanning the volumes you specified (see [Figure 3-11 on page 51](#)). You can minimize this window to have NetShield scan in the background.



Figure 3-11. New Scan task window

To stop the scan operation, click . To pause the scan operation, click . To restart the scan operation after pausing or stopping it, click .

Adjusting server performance

The speed with which NetShield performs scan operations and its ability to make efficient use of processor time and other server resources depends in part upon the hardware available to it on its host computer. When you first start the NetShield NLM, it takes an inventory of the resources it can use, then configures itself for optimal performance. It will, for example, automatically take advantage of multiple processors, if the server has them, will configure the size of its scanned file cache, and will spawn an optimal number of on-access scan threads for the available server RAM.

You can fine-tune the program so that it better suits your environment if the default settings cause difficulty. The following sections describe the options you have available to you.

Changing the number of scan threads

NetShield can spawn multiple, concurrent on-access scan threads to perform efficient scan operations when your NetWare server handles a large amount of file system traffic. As network users read files from and write files to your server, NetShield will hand off the scan task necessary to examine these files to the next available scan thread. Users also see faster server response time.

Unless you operate the server only as a single-user machine, NetShield will ordinarily have a number of scan threads active. Under most circumstances, you should *not* change the default number NetShield sets, as increasing the number of scan threads will reduce the amount of RAM available to other applications. Decreasing the available scan threads—to one, for example—can slow down all server operations that open or close files to a single-threaded process. This is because NetShield must scan every file that your users read from or write to the server in order to protect them from infection.

If you need to free additional memory, or if NetShield's multiple scan threads cause other difficulties in your server environment, however, you can reduce the number of scan threads.

Follow these steps:

1. Start the AntiVirus Console, then log on to the NetShield server you want to administer. See [“Using the AntiVirus Console” on page 41](#) and [“Remote Administration” on page 40](#) to learn how to start the Console and log on to a NetShield server.

The AntiVirus Console task window will appear (see [Figure 3-1 on page 38](#)).

2. Choose **Server Options** from the **Tools** menu to open the Server Options dialog box. Click the Advanced tab to display the correct property page ([Figure 3-12](#)).



Figure 3-12. Server Options dialog box

3. Click the arrows to the right of the **On Access Scan Threads** checkbox, or enter a number in the text box provided. You can enter up to 19 threads.
4. Click **OK** to save your settings and close the dialog box.

Setting the size of the file cache

You can streamline some NetShield operations by having it add files that it has already scanned to a cache, so that it does not waste time scanning the same files repeatedly if they have not changed. When you first load the NetShield NLM, it sets the initial value for this cache based on the amount of RAM available on the server. As it finishes scanning files, NetShield adds them to its cache until it reaches the limit you set. The program will then skip these files during subsequent scan operations. The files remain in the cache until the server opens, closes, or otherwise alters them.

To change the size of the scanning cache, follow these steps:

1. Start the AntiVirus Console, then log on to the NetShield server you want to administer. See [“Using the AntiVirus Console” on page 41](#) and [“Remote Administration” on page 40](#) to learn how to start the Console and log on to a NetShield server.

The AntiVirus Console task window will appear (see [Figure 3-1 on page 38](#)).

2. Choose **Server Options** from the **Tools** menu to open the Server Options dialog box. Click the Advanced tab to display the correct property page (see [Figure 3-12 on page 52](#)).
3. Enter the number of files you want to cache in the text box labeled **Size of cache (file scanning)**. Increasing the number will speed up NetShield scan operations, but will also use additional RAM.
4. Click **OK** to save your settings and close the dialog box.

Disabling multiprocessor use

By default, NetShield uses all of the processors available on your NetWare server to conduct scan operations. It relies on NetWare’s symmetric multiprocessing scheduler to determine which processors to use. You can disable this feature and force NetShield to use only processor 0.

Follow these steps:

1. Start the AntiVirus Console, then log on to the NetShield server you want to administer. See [“Using the AntiVirus Console” on page 41](#) and [“Remote Administration” on page 40](#) to learn how to start the Console and log on to a NetShield server.

The AntiVirus Console task window will appear (see [Figure 3-1 on page 38](#)).

2. Choose **Server Options** from the **Tools** menu to open the Server Options dialog box. Click the Advanced tab to display the correct property page (see [Figure 3-12 on page 52](#)).
3. Clear the **Enable SMP** checkbox.
4. Click **OK** to save your settings and close the dialog box.


Using NetShield's on-access scanner

NetShield uses its on-access scanning component to provide your NetWare server with continuous, real-time virus detection and response. The on-access scanner checks for infections each time a network user opens or copies a file from, saves a file to, or otherwise uses any file stored on your server. You can configure the on-access scanner by modifying the task that appears in the AntiVirus Console window to suit your security needs.

Configuring the on-access task

To configure the on-access task, follow these steps:

1. Start the AntiVirus Console, then log on to the NetShield server you want to administer. See [“Using the AntiVirus Console” on page 41](#) and [“Remote Administration” on page 40](#) to learn how to start the Console and log on to a NetShield server.

The on-access task  appears in the AntiVirus Console task window ([Figure 4-1](#)).

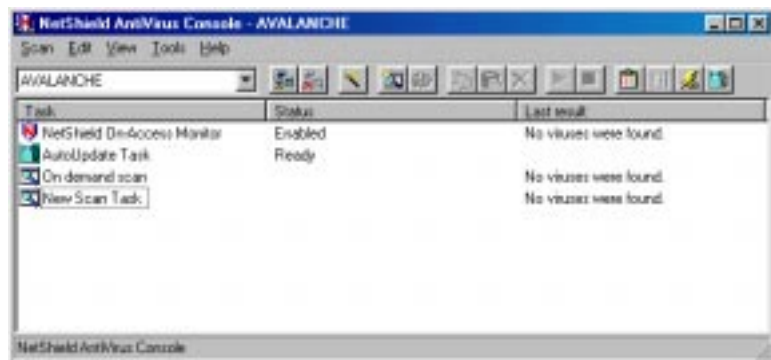


Figure 4-1. AntiVirus Console window



If enabled, the on-access scanner also displays the same icon  in the Windows system tray. Double-click the icon—either in the task list or in the system tray—to see status information and results from the most recent scan operation ([Figure 4-2 on page 56](#)). You can also click **Disable** to stop the on-access task from this window, or **Enable** to start it again.



Figure 4-2. NetShield Statistics window

2. Select the on-access task in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar. If you have opened the NetShield Statistics window (Figure 4-2), click **Properties**.

The NetShield Properties dialog box appears (Figure 4-3).

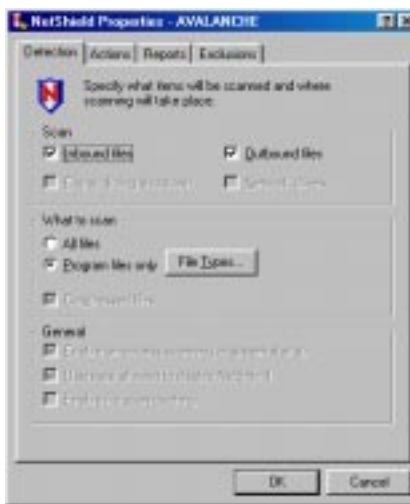



Figure 4-3. NetShield Properties dialog box - Detection page

The NetShield Properties dialog box includes four property pages, each of which governs an aspect of the on-access scanning operation. Click each tab in turn to display the corresponding property page and to specify how you want NetShield to perform the operation. When you have finished, click **OK** to save your changes and close the dialog box. Your scan task will begin running immediately with the options you chose.

The next sections describe the options you have available.

-
-  **IMPORTANT:** Because you can use the AntiVirus Console to administer servers that run both NetShield NetWare and NetShield NT, the options you see in the NetShield Properties dialog box will differ, depending on which platform you connect to. If you connect to a NetShield NT server, for example, you might have more options available to you in the Detection page. To learn more, see the NetShield NT *User's Guide*.
-

Choosing Detection options

Use the Detection page (see [Figure 4-3 on page 56](#)) to define the scope of the on-access scan operation—which file traffic NetShield should scan for viruses and which file name extensions it should treat as susceptible to infection.

Follow these steps:

1. In the **Scan** area, choose the file traffic you want NetShield to examine. Your choices are:
 - **Inbound Files.** Select the **Inbound Files** checkbox to scan all files written to or modified on the server.
 - **Outbound Files.** Select the **Outbound Files** checkbox to scan files read from the server.
2. Specify which of the files in each traffic stream you want NetShield to examine. Your choices are:
 - **All Files.** This tells NetShield to scan all files stored on your NetWare server. This option offers you the best protection against infection, but it can lengthen the time it takes to perform a scan operation.
 - **Program Files Only.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations. To do so, select the **Program files only** checkbox. To see or designate the file name extensions NetShield will scan, click **File Types** to open the Program File Extensions dialog box.

The Program File Extensions dialog box appears ([Figure 4-4](#)).

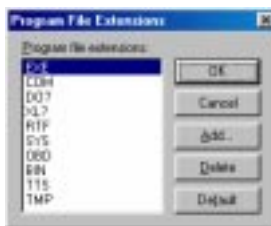


Figure 4-4. Program File Extensions dialog box

By default, NetShield scans files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .SYS, .OBD, .BIN, and .TTS. Files with .DO?, .XL?, .RTF and .OBD extensions are Microsoft Word, Microsoft Excel, and Microsoft Office binder files, all of which can harbor macro virus infections—the ? character is a wildcard that enables NetShield to scan document and template files.

- To add to the list, click **Add**, then type the extension you want NetShield to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Delete**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.


To scan all volumes, folders and files on your NetWare server, select the **All files** checkbox. This will slow your scan operations down considerably, but will ensure that your system is virus free.

3. Click the Actions tab to choose additional on-access task options. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Responding to infections

NetShield can prevent a virus infection from spreading by automatically cleaning, deleting, relocating or denying access to infected files. Use the Actions property page to choose the NetShield response that suits your working environment.

To tell NetShield how to respond to an infection, follow these steps:

1. To start from the AntiVirus Console, select the on-access task in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar. If you have opened the NetShield Statistics window (see [Figure 4-2 on page 56](#)), click **Properties**.

The NetShield Properties dialog box appears. Click the Actions tab to display the correct property page (see [Figure 4-5](#)).



Figure 4-5. NetShield Properties dialog box - Actions page

2. Choose the action NetShield will take when it finds a virus from the **When a virus is found** list. Your choices are:
 - **Deny access to infected files and continue.** This option tells NetShield to deny network users access to any infected files it finds on the server. NetShield will also rename infected files with the extension .VIR. Be sure to enable NetShield’s logging option so that you have a record of which files NetShield flagged as infected. See [“Logging on-access scan activity” on page 60](#) for details.

 - NOTE:** Because NetShield will actually stop a read or copy operation and change the file permissions on any file it identifies as infected—without waiting for your intervention—Network Associates recommends this option as your response if you plan to leave your server unattended for long periods. You can later verify the infection, then decide whether to clean, delete, or restore the file from backups.
 - **Move infected files to a folder.** This option tells NetShield to move infected files to a “quarantine” folder. By default, NetShield moves these files to a folder named Infected on the volume in which it resides. You can enter a different name in the **Folder to move to** text box, or click **Browse** to locate a suitable folder on the network.

 - NOTE:** If NetShield cannot move an infected file or cannot get access to it during a scan operation, it will rename the file with a .VIR extension and deny user access to it.

- **Clean infected files automatically.** This option tells NetShield to try to remove the virus from the infected file. NetShield uses this option as its default response.

 - NOTE:** If NetShield cannot remove a virus from an infected file, or if the virus has damaged the file beyond repair, NetShield will rename the file with a .VIR extension and deny user access to it. You should delete any such files and restore them from backups. Be sure to enable NetShield's logging option so that you have a record of which files NetShield flagged as infected. You can then restore damaged files from backup copies. See “[Logging on-access scan activity](#)” on page 60 for details.

- **Delete infected files automatically.** This option tells NetShield to delete infected files as soon as it detects them. Be sure to enable NetShield's logging option so that you have a record of which files NetShield flagged as infected.

3. To have NetShield warn users that the file they opened, copied or saved is infected, select the **Send Message to User** checkbox, then enter the message you want users to see.

-
- NOTE:** Users running Windows NT must have the Messenger service running to receive this message. Those running Windows 95 must be running the WinPopup utility to see this message. WinPopup comes with some Windows versions. Some WinPopup versions can truncate longer messages.
-


4. Select the **Disconnect remote users and deny access to network share** checkbox to have NetShield break the user's connection to the NetShield server and put the volume that contains infected files off-limits.
5. Click the Reports tab to choose additional on-access task options. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Logging on-access scan activity

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

The NetShield log file can serve as an important management tool for you to track virus activity on your network and to note which settings you used to detect and respond to the viruses NetShield found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your server.

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

1. To start from the AntiVirus Console, select the on-access task in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar. If you have opened the NetShield Statistics window (see [Figure 4-2 on page 56](#)), click **Properties**.

The NetShield Properties dialog box appears. Click the Reports tab to display the correct property page. ([Figure 4-5](#)).



Figure 4-6. NetShield Properties dialog box - Reports page

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

By default, NetShield writes log information to the file `ACTIVITY.TXT` in the `\MCAFEES\NETSHLD` folder on the volume that stores your NetShield installation. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your server or on the network.

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

Enter a value between 10KB and 99,999KB (100 gigabytes). By default, NetShield limits the file size to 100KB. If the data in the log exceeds the file size you set, NetShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want NetShield to record in its log file. The log options you see will depend on which response you told NetShield to use when it finds a virus. See [“Responding to infections” on page 58](#) for details. You can choose to record this information:
 - **Virus detection.** Select this checkbox to tell NetShield to note the number of infected files it found during this scanning session.
 - **Virus cleaning.** Select this checkbox to tell NetShield to note the number of infected files from which it removed the infecting virus. You will not have this option if you do not choose **Clean infected files automatically** as NetShield’s response to virus infections.
 - **Infected file deletion.** Select this checkbox to tell NetShield to note the number of infected files it deleted from your system. You will not have this option if you do not choose **Delete infected files automatically** as NetShield’s response to virus infections.
 - **Infected file move.** Select this checkbox to tell NetShield to note the number of infected files it moved to your quarantine directory. You will not have this option if you do not choose **Move infected files to a folder** as NetShield’s response to virus infections.
 - **Session settings.** Select this checkbox to tell NetShield to list the options you choose in the NetShield Properties dialog box for each scanning session.
 - **Session summary.** Select this checkbox to tell NetShield to summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information. An on-access scanning session is the period of time NetShield remained loaded into memory on your NetWare server. It ends when you either unload NetShield or reboot your server.
 - **Date and time.** Select this checkbox to tell NetShield to append the date and time to each log entry it records.
 - **User name.** Select this checkbox to tell NetShield to append the name of the user connected to the server at the time it records each log entry.


- Click the Exclusions tab to choose additional on-access task options. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Excluding items from scan operations

Many of the files stored on your NetWare server are not vulnerable to virus infection, never change, or are inaccessible to outside traffic. On-access scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling NetShield to look only at susceptible file types (see [“Choosing Detection options” on page 57](#) for details), or you can tell NetShield to ignore entire files or folders that you know will not get infected.

As a first step, you might want to perform a comprehensive on-demand scan to ensure that your system has no infected files before you exclude any files or folders from the on-access scan operation.

To exclude files, folders, or volumes from on-access scan operations, follow these steps:

- To start from the AntiVirus Console, select the on-access task in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar. If you have opened the NetShield Statistics window (see [Figure 4-2 on page 56](#)), click **Properties**.

The NetShield Properties dialog box appears. Click the Exclusions tab to display the correct property page. ([Figure 4-7](#)).

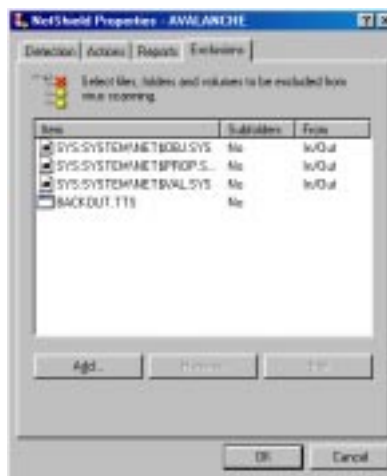


Figure 4-7. NetShield Properties dialog box - Exclusions page

The Exclusions page will initially list three system database files and the transaction file that NetWare uses to keep track of operating system processes. NetShield excludes these files from scan operations because they are not susceptible to virus infection and because NetWare keeps them open and in use almost constantly—scanning these files would interrupt the operating system without real benefit.

2. Specify the files or folders you want to exclude from on-access scan operations. You can
 - **Add files or folders.** Click **Add** to open the Add Exclusion Item dialog box (Figure 4-8).



Figure 4-8. Add Exclusion Item dialog box

- a. Type the volume, the path to the file, or the path to the folder you want to exclude from scanning, or click **Browse** to locate a file or folder on your server.

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

- b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.
- c. Specify whether NetShield should exclude the file or folder as network users save or copy it to the server, read it from the server, or both.
 - Select the **Inbound** checkbox to allow network users to save the file or folder to the server volume without NetShield scanning it.
 - Select the **Outbound** checkbox to allow network users to read the file or folder from the server without NetShield scanning it.
- d. Click **OK** to save your changes and close the dialog box.

Repeat steps a. through d. until you have specified all of the files and folders you want to exclude from on-access scanning.

- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclusion Item dialog box. Make the changes you need, then click **OK** to close the dialog box.
 - **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. NetShield will then scan this file or folder during its next on-access scanning operation.
3. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Using NetShield's on-demand scanner

NetShield's on-demand scanning component provides you with a method for scanning all or parts of your NetWare server for viruses at convenient times or at regular intervals. Use it to supplement the continuous protection you get with the NetShield on-access scanner, or to schedule regular scan operations when they won't interfere with your network users' work.

NetShield does not come with any default on-demand or scheduled scan tasks because the variety of NetWare server setups and network environments on which NetShield runs makes it impossible to anticipate your needs. You can, however, create an on-demand task quickly and easily with the Scan wizard (see [“Creating a task with the Scan wizard”](#) on page 44 to learn how), or import a task definition from other Network Associates anti-virus software to get started (see [“Using the AntiVirus Console”](#) on page 41 for more details).

Creating an on-demand task

To create an entirely new on-demand task, follow these steps:

1. Start the AntiVirus Console, then log on to the NetShield server you want to administer. See [“Using the AntiVirus Console”](#) on page 41 and [“Remote Administration”](#) on page 40 to learn how to start the Console and log on to a NetShield server.

The AntiVirus Console task window will appear ([Figure 5-1](#)).

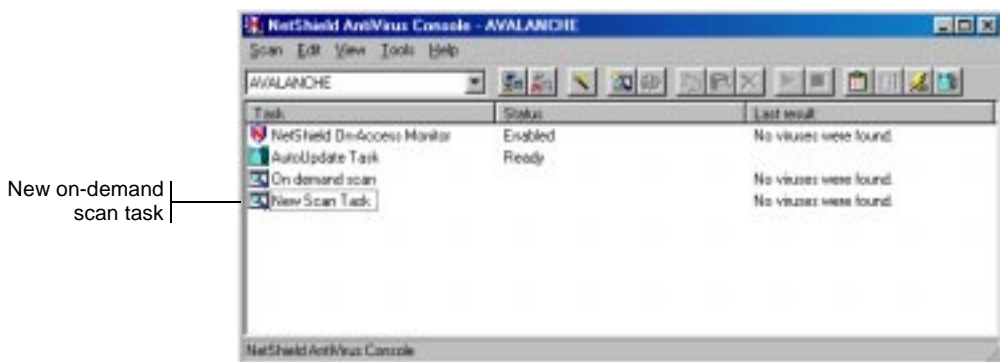



Figure 5-1. AntiVirus Console window

2. Choose **New Task** from the **Scan** menu, or click  in the Console toolbar.

A new on-demand task appears in the AntiVirus Console task window (see [Figure 5-1 on page 67](#)).

3. Type a new name for your task, then press **ENTER**.


NetShield opens the Task Properties dialog box ([Figure 5-2](#)).



Figure 5-2. Task Properties dialog box - Detection page

The Task Properties dialog box includes five property pages, each of which governs an aspect of the on-demand scanning operation. Click each tab in turn to display the corresponding property page and to specify how you want NetShield to perform the operation. When you have finished, click **OK** to save your changes and close the dialog box.

The next sections describe the options you have available.

 **IMPORTANT:** Because you can use the AntiVirus Console to administer servers that run both NetShield NetWare and NetShield NT, the options you see in the Task Settings dialog box will differ, depending on which platform you connect to. If you connect to a NetShield NT server, for example, you might have more options available to you in the Advanced Scanner Settings dialog box or other dialog boxes. To learn more, see the NetShield NT *User's Guide*.

Choosing detection options

Use the Detection page (see [Figure 5-2](#)) to define the scope of the on-access scan operation—which server volumes NetShield should scan for viruses and which file name extensions it should treat as susceptible to infection. By default, NetShield lists all of the NetWare volumes on its host server and all of the subfolders they contain. A scan operation this inclusive could take a very long time, so you might want to narrow this scan for regular use later.

1. Choose your scan targets. You can
 - **Supplement existing scan targets.** Click **Add** to open the Add Scan Item dialog box ([Figure 5-3](#)).

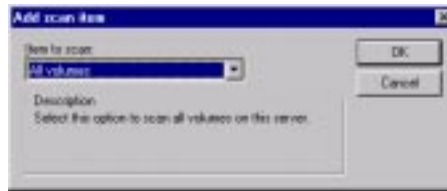


Figure 5-3. Add Scan Item dialog box

Next, choose a scan target from the list. You can choose to scan all local NetWare volumes, or a particular volume or file. If you choose to scan a volume or file, enter the path to the volume—or the path and file name—in the **Description** text box. You can specify the path in Universal Naming Convention (UNC) notation, or you can click **Browse** to locate the correct file or volume on the server. When you have finished, click **OK** to close the dialog box.

-
- NOTE:** The NetShield NetWare server will ignore any volumes on your computer that are not formatted as Novell NetWare volumes.
-

- **Delete existing scan targets.** Select a listed target, then click **Remove**.
- **Modify or narrow existing scan targets.** Select a listed target, then click **Edit** to open the Edit Scan Item dialog box (see [Figure 5-4 on page 70](#)).



Figure 5-4. Edit Scan Item dialog box

Choose or specify a new scan target, then click **OK** to close the dialog box.

2. Specify how you want NetShield to conduct the scan. You can
 - **Scan volume subfolders.** By default, NetShield scans all subfolders in the volumes you target for scanning. To scan only the root level of your chosen volumes, clear the **Include subfolders** checkbox.
 - **Scan compressed files.** Also by default, NetShield scans files in target volumes that are compressed in the LZH or PKZIP archiving formats. You can prevent NetShield from scanning these files, however, by clearing the **Compressed files** checkbox.
 - **Choose file types for scanning.** Viruses ordinarily cannot infect data files or files that contain no executable code. You can, therefore, safely narrow the scope of your scan operations to those files most susceptible to virus infection in order to speed up scan operations. To do so, select the **Program files only** checkbox. To see or designate the file name extensions NetShield will scan, click **File Types** to open the Program File Extensions dialog box (Figure 5-5).

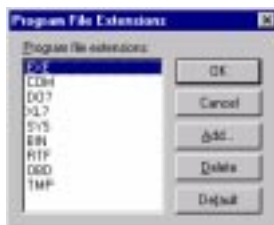


Figure 5-5. Program File Extensions dialog box

By default, NetShield scans files with the extensions .EXE, .COM, .DO?, .XL?, .RTF, .SYS, .OBD, .BIN, and .TTS. Files with .DO?, .XL?, .RTF and .OBD extensions are Microsoft Word, Microsoft Excel, and Microsoft Office binder files, all of which can harbor macro virus infections—the ? character is a wildcard that enables NetShield to scan document and template files.

- To add to the list, click **Add**, then type the extension you want NetShield to scan in the dialog box that appears.
- To remove an extension from the list, select it, then click **Delete**.
- Click **Default** to restore the list to its original form.

When you have finished, click **OK** to close the dialog box.

To scan all volumes, folders and files on your NetWare server, select the **All files** checkbox. This will slow your scan operations down considerably, but will ensure that your system is virus free.

3. To set a relative priority for your scan task over other server operations and to exclude certain sets of files from the scan operation, click **Advanced** to display the Advanced Scanner Settings dialog box (Figure 5-6).



Figure 5-6. Advanced Scanner Settings dialog box

You can

- **Set a priority for your scan task.** Drag the slider to the left to give the scan task a lower priority relative to other tasks your NetWare server must do. This ensures that other software on your server will not slow down during a scan operation, but the scan operation will take longer. Give the scan task low priority if you plan to run it when users need other services from the server.

Drag the slider to the right to give the scan task more priority relative to other server tasks. This takes processor time from other software and slows down other applications, but ensures that the scan operation completes faster. Give the scan task more priority if you plan to run it when few users need the server or other software.

By default, NetShield tries to balance scan task priority against the need for other services.

- **Exclude CD-ROM volumes from scanning.** Select the **Skip CD-ROM scanning** checkbox to tell NetShield to ignore CD-ROM discs mounted on your NetWare server. Although you cannot *infect* a CD-ROM disc from the server or your network, CD-ROM discs can still harbor viruses introduced during the writing or manufacturing process. Network Associates recommends that you scan CD-ROM discs.
- **Exclude file sets from scanning.** Select the **Skip files compressed by the OS** checkbox to exclude from your scan task any files that you have configured NetWare to keep compressed until it receives a request for them. Because scanning compressed files requires significant processor time, selecting this option can speed up scan time, but does entail some risk of virus infection.


Select the **Skip migrated files** checkbox to exclude files that NetWare has archived and stored on a secondary storage device. Because scanning files archived on a secondary storage device requires significant processor time, selecting this option can speed up scan time, but does entail some risk of virus infection.

When you have finished setting priorities and excluding file sets for this scan task, click **OK** to close the Advanced Scanner Settings dialog box.

4. Click the Actions tab to choose additional on-demand task options. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Responding to virus infections

NetShield can prevent a virus infection from spreading by automatically cleaning, deleting, relocating or denying access to infected files. Use the Actions property page to choose the NetShield response that suits your working environment.

1. To start from the AntiVirus Console, select the on-demand task you created in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar.

The Task Properties dialog box appears. Click the Actions tab to display the correct property page. (see [Figure 5-7 on page 73](#)).



Figure 5-7. Task Properties dialog box - Actions page

2. Choose the action NetShield will take when it finds a virus from the **When a virus is found** list. Your choices are:
 - **Continue Scanning.** This tells NetShield to note when it detects a virus, then to continue scanning without taking any other action. If you have enabled its alerting and logging options, NetShield will tell you that it has found a virus and will record the incident in its log. See [“Logging on-demand scan activity” on page 74](#) for details.
 - **Move infected file to a folder.** This option tells NetShield to move infected files to a “quarantine” folder. By default, NetShield moves these files to a folder named Infected on the volume in which it resides, and replicates the path to the infected file there. For example, if NetShield found an infected file in SYS:USERS\JOE and you specified SYS:INFECTED as the quarantine directory, NetShield would copy the file to SYS:INFECTED\USERS\JOE.

You can enter a different name in the text box provided, or click **Browse** to locate a suitable folder on the network.

-
- **NOTE:** If NetShield cannot move an infected file during a scan operation, it will alert you that it has found a virus—provided that you have enabled its alerting option—report its failure to move the infected file, and take no other action. If you have enabled its logging option, NetShield will record the incident in its log. See [“Virus Notification” on page 83](#) and [“Logging on-demand scan activity” on page 74](#) for more information.
-

- **Clean infected file.** This option tells NetShield to try to remove the virus from the infected file. NetShield uses this option as its default response.

NOTE: If NetShield cannot remove a virus from an infected file, or if the virus has damaged the file beyond repair, NetShield will alert you that it has found a virus—provided you have enabled its alerting option—report the cleaning failure, but will take no other action. If you have enabled its logging option, NetShield will record the incident in its log. See [“Virus Notification” on page 83](#) and [“Logging on-demand scan activity” on page 74](#) for more information.


- **Delete infected file.** This option tells NetShield to delete infected files as soon as it detects them. Be sure to enable NetShield’s logging option so that you have a record of which files NetShield flagged as infected.
3. To have NetShield warn you when it finds an infected file, select the **Notify Alert Manager** checkbox. Alert Manager can warn you about virus infections by sending a message through a variety of channels. See [“Virus Notification” on page 83](#) to learn how to configure Alert Manager.
 4. Click the Reports tab to choose additional on-demand task options. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Logging on-demand scan activity

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

The NetShield log file can serve as an important management tool for you to track virus activity on your network and to note which settings you used to detect and respond to the viruses NetShield found. You can also use the incident reports recorded in the file to determine which files you need to replace from backup copies, examine in quarantine, or delete from your server. Use the Reports property page (see [Figure 5-8 on page 75](#)) to determine which information NetShield will include in its log file.

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

1. To start from the AntiVirus Console, select the on-demand task you created in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar.

The NetShield Properties dialog box appears. Click the Reports tab to display the correct property page. (Figure 5-8).



Figure 5-8. NetShield Properties dialog box - Reports page

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

By default, NetShield writes log information to the file ACTIVITY.TXT in the \MCAFEE\NETSHLD folder on the volume that stores your NetShield installation. You can enter a different name in the text box provided, or click **Browse** to locate a suitable file elsewhere on your server or on the network.

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


Enter a value between 10KB and 99,999KB (100 gigabytes). By default, NetShield limits the file size to 100KB. If the data in the log exceeds the file size you set, NetShield erases the existing log and begins again from the point at which it left off.

4. Select the checkboxes that correspond to the information you want NetShield to record in its log file. The log options you see will depend on which response you told NetShield to use when it finds a virus. See [“Responding to virus infections” on page 72](#) for details. You can choose to record this information:
 - **Virus detection.** Select this checkbox to tell NetShield to note the number of infected files it found during this scanning session.
 - **Virus cleaning.** Select this checkbox to tell NetShield to note the number of infected files from which it removed the infecting virus. You will not have this option if you do not choose **Clean infected file** as NetShield’s response to virus infections.
 - **Infected file deletion.** Select this checkbox to tell NetShield to note the number of infected files it deleted from your system. You will not have this option if you do not choose **Delete infected file** as NetShield’s response to virus infections.
 - **Infected file move.** Select this checkbox to tell NetShield to note the number of infected files it moved to your quarantine directory. You will not have this option if you do not choose **Move infected file to a folder** as NetShield’s response to virus infections.
 - **Session settings.** Select this checkbox to tell NetShield to list the options you choose in the Task Properties dialog box for each scanning session.
 - **Session summary.** Select this checkbox to tell NetShield to summarize its actions during each scanning session. Summary information includes the number of files scanned, the number and type of viruses detected, the number of files moved or deleted, and other information.
 - **Date and time.** Select this checkbox to tell NetShield to append the date and time to each log entry it records.
 - **User name.** Select this checkbox to tell NetShield to append the name of the user connected to the server at the time it records each log entry.
5. Click the Schedule tab to choose additional on-demand task options. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Scheduling your on-demand task

NetShield provides you with tools to schedule scan operations at particular dates and times, or at particular intervals. You can schedule NetShield to run a scan operation in your absence, at convenient times or dates, or in other ways that suit your needs.

To schedule your on-demand task, follow these steps:

1. To start from the AntiVirus Console, select the on-demand task you created in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar.

The NetShield Properties dialog box appears. Click the Schedule tab to display the correct property page. (Figure 5-9).



Figure 5-9. The Task Properties dialog box - Schedule page

2. Select the **Enable scheduler** checkbox. The options in the **Run** and the **Start At** areas will become active.
3. Choose how often you want the task to run in the **Run** area, or select **At Startup** to run your task as soon as NetShield loads. Depending on which interval you select, the **Start At** area gives you a different set of choices for your task schedule. The choices are:
 - **Once.** This runs your task exactly once on the date and at the time you specify. Enter the time in the leftmost text box in the **Start At** area, then select a month and a date from the lists to the right.

- **Hourly.** This runs your task each hour as long as your server is active and NetShield is running. Specify in the text box provided how many minutes NetShield should wait after each hour to run your task.
 - **Daily.** This runs your task once at the time you specify on the days you indicate. Click **Which Days** to open a dialog box where you can select the days on which you want your task to run. After you've done so, click **OK** to close the dialog box, then enter in the **Start At** text box the time each day when the task will run.
 - **Weekly.** This runs your task once each week on the day and at the time you specify. Enter the time in the text box provided, then choose a day from the list to the right.
 - **Monthly.** This runs your task once each month on the day and at the time you specify. Enter the time in the leftmost text box, then enter the day of the month on which you want the task to run.
4. Click the Schedule tab to choose additional on-demand task options. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.


NOTE: For NetShield to run your task, your server must be active and NetShield must be running. If your server is down or if NetShield is not running at the time your task should start, the task will start at the next scheduled time.

Excluding items from scan operations

Many of the files stored on your NetWare server are not vulnerable to virus infection, never change, or are inaccessible to outside traffic. On-demand or scheduled scan operations that examine these files can take a long time and produce few results. You can speed up scan operations by telling NetShield to look only at susceptible file types (see “[Choosing detection options](#)” on page 69 for details), or you can tell NetShield to ignore entire files or folders that you know will not get infected.

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

To exclude files, folders, or volumes from on-access scan operations, follow these steps:

1. To start from the AntiVirus Console, select the on-demand task you created in the task list, then choose **Properties** from the **Scan** menu, or click  in the Console toolbar.

The NetShield Properties dialog box appears. Click the Exclusions tab to display the correct property page. (Figure 5-10).

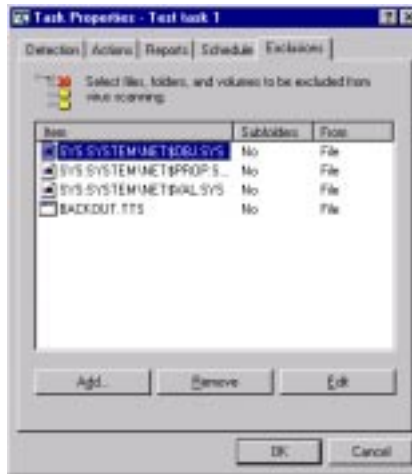


Figure 5-10. Task Properties dialog box - Exclusions page

The Exclusions page will initially list three system database files and the transaction file that NetWare uses to keep track of operating system processes. NetShield excludes these files from scan operations because they are not susceptible to virus infection and because NetWare keeps them open and in use almost constantly—scanning these files would interrupt the operating system without real benefit.

2. Specify the items you want to exclude. You can
 - **Add files, folders or volumes to the exclusion list.** Click **Add** to open the Add Exclusion Item dialog box (Figure 5-11).

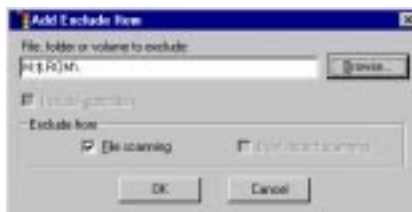


Figure 5-11. Add Exclude Item dialog box

- a. Type the volume, the path to the file, or the path to the folder that you want to exclude from scanning, or click **Browse** to locate a file or folder on your server.


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

- b. Select the **Include Subfolders** checkbox to exclude all subfolders within the folder you just specified.
 - c. Verify that NetShield should exclude the file or folder from file scanning. This is your only option if you use the AntiVirus Console to administer a NetWare server. If you use the Console to connect to an NT server, you can also have NetShield scan your server's master boot record and hard disk boot blocks.
 - d. Click **OK** to save your changes and close the dialog box.
 - e. Repeat steps a. through d. until you have listed all of the files and folders you do not want scanned.
- **Change the exclusion list.** To change the settings for an exclusion item, select it in the Exclusions list, then click **Edit** to open the Edit Exclusion Item dialog box. Make the changes you need, then click **OK** to close the dialog box.
 - **Remove an item from the list.** To delete an exclusion item, select it in the list, then click **Remove**. NetShield will then scan this file or folder during its next on-access scanning operation.
3. To save your changes and return to the AntiVirus Console, click **OK**. To return to the AntiVirus Console without saving your changes, click **Cancel**.

Running your scan task

Once you have configured your task with the scan options you want, you can disconnect from the NetShield server and allow the task to run unattended. If you scheduled your task to run at a certain time, NetShield will start your task when you specified, provided that the server is active and NetShield is running. If you have not scheduled your task but plan to run it immediately, you should probably remain connected to the server so that you can monitor the progress of the scan operation and respond to any alert messages you see.

To start an on-demand task immediately, follow these steps:

1. If you do not have it already running, start the AntiVirus Console, then connect to the NetWare server that will run your task. See [“Using the AntiVirus Console” on page 41](#) and [“Remote Administration” on page 40](#) to learn how to start the Console and log on to a NetShield server.
2. Select your on-demand task in the task list ([Figure 5-12](#)), then choose **Start** from the **Scan** menu, or click  in the Console toolbar.

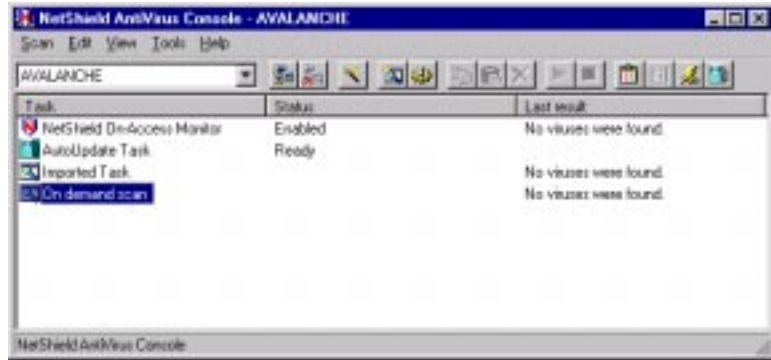


Figure 5-12. AntiVirus Console window

Your scan task will begin. The AntiVirus Console will report its progress in the **Status** column and will display a summary of the scan results in the **Last result** column.

Viewing scan results

After your scan operation finishes, or even as a task runs, you can see a more detailed statistical summary of the number of files that NetShield scanned, together with the number of viruses it found and the actions it took in response.

To see statistics and results for your task, follow these steps:

1. If you do not have it already running, start the AntiVirus Console, then connect to the NetWare server that will run your task. See [“Using the AntiVirus Console” on page 41](#) and [“Remote Administration” on page 40](#) to learn how to start the Console and log on to a NetShield server.
2. Double-click your on-demand task in the task list ([Figure 5-12](#)), or choose **Statistics** from the **Scan** menu, to open the Task Statistics dialog box (see [Figure 5-13 on page 82](#)).



Figure 5-13. Task Statistics dialog box

The Task Statistics dialog box shows each of the scan targets you have chosen for this task in an upper pane, along with a statistical summary at the bottom. If your scan task is still in progress, it shows the file NetShield is scanning now and the status of the scan operation.

You can also dynamically update your task configuration from this dialog box. Click **Properties** to open the Task Properties dialog box, then change the task options you want to modify. See [pages 67 to 80](#) to review how to configure an on-demand task. The task will run with your new settings immediately, but the Task Statistics dialog box will not refresh until you close it, then open it again.

When you have finished reviewing task statistics, click **Close** to return to the AntiVirus Console.

Using NetShield's Alerting Features

Once you configure it with the options you want, you can let NetShield look for and remove viruses from your server automatically, as it finds them, with almost no further intervention. With activity logging enabled, you can also see results of each NetShield scanning operation and track its progress at your leisure, or you can view scanning results and statistics from the AntiVirus Console whenever you choose to connect to your server.

If, however, you want NetShield to inform you immediately when it finds a virus so that you can take appropriate action, you can configure the included Alert Manager component to send an alert message to you or to any other administrator you designate, using any of a variety of channels. See [“Configuring Alert Manager”](#) below to learn how to configure the types of alert methods you want.

NetShield also includes a Centralized Alerting module that lets you collect alert messages from any workstation on your network that has a Network Associates anti-virus client product installed and properly configured. See [“Using Centralized Alerting” on page 101](#) to learn how to enable this feature.

NetShield also gives you complete control from the AntiVirus Console over the content of its alert messages and the relative priorities you assign to them. See [“Customizing alert messages” on page 103](#) to learn how to create or modify alert messages that suit your needs.

Configuring Alert Manager

NetShield uses the Network Associates Alert Manager utility to notify you or others when it detects a virus in files on your servers. Alert Manager gives you a wide variety of notification options that you can use individually or in combinations that suit your needs.

If you have Alert Manager installed on other computers on your network, you can also forward alert messages to those computers, which can in turn notify workstations that they host about infected files on your server.

-
- **NOTE:** In large organizations, you can use this forwarding feature to send alerts to centralized notification systems or to MIS departments in order to keep track of virus statistics and problem areas.
-

To enable and configure Alert Manager, follow these steps:

1. Start the AntiVirus Console, then choose **Alerts** from the **Tools** menu. To learn how to start the AntiVirus Console, see [“Starting the AntiVirus Console” on page 38](#).

The Alerts Properties page (see [Figure 6-1](#)) appears.

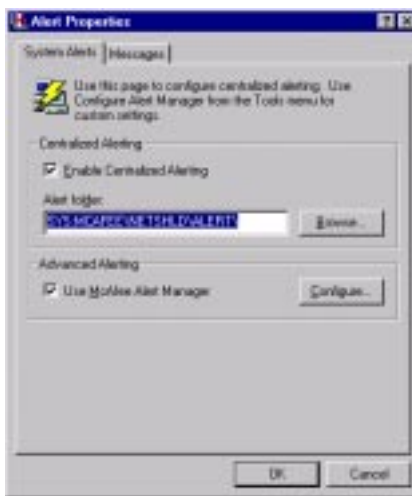



Figure 6-1. Alert Properties dialog box - System Alerts page

2. Select **Use McAfee Alert Manager**, then click **OK** to return to the AntiVirus Console.
3. Choose **Configure Alert Manager** from the **Tools** menu, or click  in the Console toolbar.

NetShield opens the Alert Manager dialog box (see [Figure 6-2 on page 85](#)).

The Alert Manager dialog box includes seven different alert methods, each with configuration options shown in individual property pages. Click the tab that corresponds to the alert method you want to configure to see the options available. When you have finished choosing your options, click **OK** to save your changes, close the Alert Manager dialog box, and return to the AntiVirus Console. Click **Cancel** to close the Alert Manager dialog box without saving your changes.

The following sections describe the options available for each method.

Viewing the Summary page



Figure 6-2. Alert Manager Properties dialog box (Summary Property page)

The Summary page lists all of the alert methods you've told NetShield to use to notify you when it finds a virus on your NetShield server. In the example shown in [Figure 6-2](#), Alert Manager has all seven of its alert options configured and ready to go. If you have not yet configured Alert Manager, the Summary Page will be blank.

Click next to each listed alert method to display the computers, printers, phone numbers, or e-mail addresses that will receive alert messages from NetShield. To remove an alert method, select it, then click **Remove**. To change the configuration options for a listed method, select it, then click **Properties**. Alert Manager will open the same property page you used to configure your options for that alert method.

See the following sections to learn how to choose options for each alert method.

Forwarding alert messages to other computers

Alert Manager can forward the alert messages that NetShield generates to other computers on your network. If you have installed Alert Manager on each of the destination computers, they can in turn forward alert messages to the recipients listed in their Alert Manager Summary pages. You might use this feature to pass alert messages across network domains or to construct a hierarchical arrangement for passing alert messages.

To configure Alert Manager's Forwarding options, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Forward tab.

The Forward page (Figure 6-3) appears with a list of all of the computers you have chosen to receive forwarded messages. If you have not yet chosen a destination computer, this list will be blank.



Figure 6-3. Alert Manager Properties dialog box - Forward page

3. To update this list, you can:
 - **Remove a listed computer.** Select one of the destination computers listed, then click **Remove**.
 - **Add a computer to the list.** Click **Add** to open the Forward Properties dialog box (Figure 6-4 on page 87), then enter the name of the computer that will receive forwarded messages in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click **Browse** to locate the computer on the network. To choose additional options, continue with [Step 4](#).
 - **Change configuration options.** Select one of the destination computers listed, then click **Properties**. Alert Manager opens the Forward Properties dialog box (see Figure 6-4 on page 87). Change any of the information you want to change in the **Computer** text box, then continue with [Step 4](#) to learn how to choose new or different configuration options.

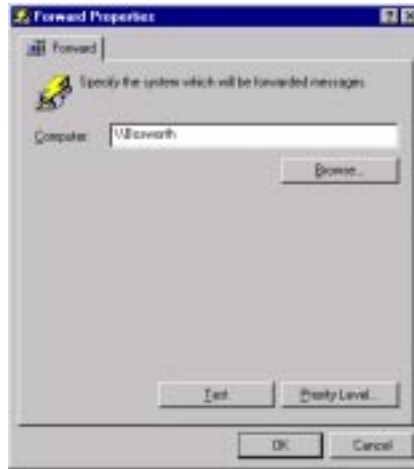


Figure 6-4. Forward Properties dialog box

4. Click **Priority Level** to specify which types of alert messages the destination computer will receive.

In the Priority Level dialog box that appears (Figure 6-5), drag the slider to the right to send the destination computer fewer, but higher priority, messages. Drag the slider to the left to send the destination computer more alert messages, including lower priority messages. Next, click **OK** to save your changes and return to the Forward Properties dialog box.



Figure 6-5. Priority Level dialog box

5. Click **Test** to send the destination computer a test message. The message will appear instantly in a dialog box on the destination computer's screen and the recipient will need to click **OK** to acknowledge it.
6. Click **OK** to return to the Alert Manager dialog box.
7. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click **OK**. To close the Alert Manager dialog box without saving changes, click **Cancel**.

Sending alerts as a network messages

Alert Manager can send the alert messages that NetShield generates to other computers or users on your network using a standard NetWare network broadcast message. The alert message appears on the destination computer's screen and requires the recipient to acknowledge it.

Destination computers running Windows NT must have the Messenger service running to receive alert messages. Those running Windows 95 or Windows 3.1x must also be running the WinPopup utility to receive network messages. WinPopup comes with some Windows versions. See your Windows documentation for details.

To configure Alert Manager to send alerts as network messages, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Network Message tab.

The Network Message page appears with a list of the computers or user names you have configured to receive network messages (Figure 6-6). If you have not yet chosen a destination computer or a user, this list will be blank.



Figure 6-6. Alert Manager Properties dialog box - Network Message page

3. To update this list, you can:
 - **Remove a listed computer or user.** Select one of the destination computers or recipient names listed, then click **Remove**.
 - **Add a computer or user to the list.** Click **Add** to open the Network Message Properties dialog box (Figure 6-7), then enter the name of the recipient or the destination computer in the text box provided. You can enter the computer name in Universal Naming Convention (UNC) notation, or you can click **Browse** to locate the computer on the network. To choose additional options, continue with [Step 4](#).

NOTE: If the recipient name you specify is both a valid user name and a computer, Alert Manager will send the message to the user name.

 - **Change configuration options.** Select one of the destination computers or recipient names listed, then click **Properties**. Alert Manager opens the Network Message Properties dialog box (Figure 6-7). Change any of the information you want to change in the Computer text box, then continue with [Step 4](#) to learn how to choose new or different configuration options.



Figure 6-7. Network Message Properties dialog box

4. Click **Priority Level** to specify which types of alert messages the destination computer or user will receive.

In the Priority Level dialog box (see [Figure 6-5 on page 87](#)), drag the slider to the right to send the destination computer or user fewer, but higher priority, messages. Drag the slider to the left to send the destination computer or user more network messages, including lower priority messages. Next, click **OK** to save your changes and return to the Network Message Properties dialog box.

5. Click **Test** to send the destination computer or user a test message.

The message will appear instantly in a dialog box on the destination computer's screen and the recipient will need to click **OK** to acknowledge it. If your recipient does not receive the message, check the NetShield activity log for an error message.

6. Click **OK** to return to the Alert Manager Properties dialog box.
7. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click **OK**. To close the Alert Manager dialog box without saving changes, click **Cancel**.

Sending alert messages to e-mail addresses

Alert Manager can send the alert messages that NetShield generates to a recipient's e-mail address either via standard Internet e-mail or via NetWare's Message Handling Service (MHS). Alert messages appear in the recipient's mail box. If your message is particularly urgent, you might want to supplement an e-mail message with other methods to ensure that your recipient sees the alert in time to take appropriate action.

To configure Alert Manager to send alerts as e-mail messages, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the E-Mail tab.

The E-Mail page appears with a list of the e-mail addresses you have chosen to receive alert messages (see [Figure 6-8 on page 91](#)). If you have not yet chosen an e-mail address, this list will be blank.



Figure 6-8. Alert Manager Properties dialog box - E-mail page

3. To update this list, you can:
 - **Remove a listed address.** Select one of the e-mail addresses listed, then click **Remove**.
 - **Add an e-mail address to the list.** Click **Add** to open the E-Mail Properties dialog box (see [Figure 6-9](#)). Enter the e-mail address for your alert recipient in the **Address** text box, enter a subject in the **Subject** text box, then enter your e-mail address in the **From** text box. Use the standard Internet address format `<username>@<domain>` (administrator_1@mail.com, for example). To choose additional options, continue with [Step 4](#).
 - **Change configuration options.** Select one of the e-mail addresses listed, then click **Properties**. Alert Manager opens the E-Mail Properties dialog box ([Figure 6-9](#)). Change any of the information you want to change in the text boxes shown, then continue with [Step 4](#) to learn how to choose new or different configuration options.

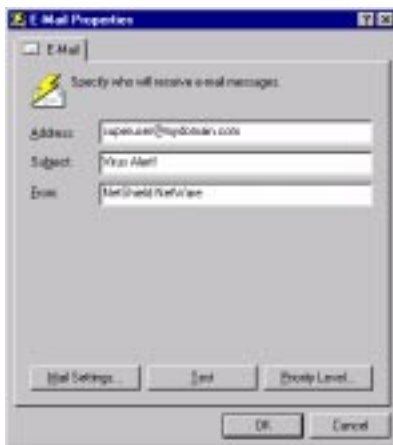


Figure 6-9. E-Mail Properties dialog box

4. Click **Priority Level** to specify which types of alert messages your recipient will receive.

In the Priority Level dialog box (see [Figure 6-5 on page 87](#)), drag the slider to the right to send the recipient fewer, but higher priority, messages. Drag the slider to the left to send the recipient more messages, including lower priority messages. Next, click **OK** to save your changes and return to the E-Mail Properties dialog box.

5. Click **Mail Settings** to specify the network server you use to send Internet mail via NetWare's MHS. In the dialog box that appears ([Figure 6-10](#)), enter the server name in the **Server** text box and, in the **Login** text box, a user name for an active mail account that NetShield can use to log on to the server.



Figure 6-10. MHS dialog box

You can enter the server name as an Internet Protocol (IP) address, as a name your local domain name server can recognize, or in Universal Naming Convention (UNC) notation. Click **OK** to save your changes and return to the E-Mail Properties dialog box.

6. Click **Test** to send a test message to the e-mail address you entered. The message will appear in your recipient's mailbox.
7. Click **OK** to return to the Alert Manager Properties dialog box.
8. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click **OK**. To close the Alert Manager dialog box without saving changes, click **Cancel**.

Sending alert messages to pagers

Alert Manager can send the alert messages that NetShield generates to a recipient's pager, provided that you have a modem and telephone line connected to your NetShield server. Alert Manager supports both alphanumeric pagers and pagers that receive only numeric messages. Depending on how your recipient's paging service operates, you might need to write a custom script to dial and select the correct menu options before NetShield can deliver its message.

To configure Alert Manager to send alert messages to a pager, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Pager tab.

The Pager page (see [Figure 6-11 on page 94](#)) appears with a list of the pager numbers you have chosen to receive alert messages. If you have not yet chosen a pager number, this list will be blank.



Figure 6-11. Alert Manager Properties dialog box - Pager page

3. To update this list, you can:

- **Remove a listed pager number.** Select one of the pager numbers listed, then click **Remove**.
- **Add a pager number to the list.** Click **Add** to open the Pager Properties dialog box (see [Figure 6-12 on page 95](#)). Choose the type of pager your recipient uses from the list at the top of the page, then enter the information for that pager type in the text boxes provided.
 - If your recipient uses an alphanumeric pager, enter the pager number and, if necessary, the recipient's ID and password in the text boxes provided. Next, select the **Use Alert Message** button to send NetShield's standard alert message, or select the **Use Custom Message** button, then enter your custom message in the text box below.
 - If your recipient uses a numeric pager, enter the pager number and the numeric message you want to send in the text boxes provided. Next, enter the number of seconds Alert Manager should wait before transmitting its message in the **Delay** box.

Give Alert Manager enough time to get past the initial greeting and any other preliminary messages the paging service plays before it accepts messages. If the service requires touch tones to activate menu options, you might need to write a login script for use with your modem.

To choose additional options, continue with [Step 4](#).

- **Change configuration options.** Select one of the pager numbers listed, then click **Properties**. Alert Manager opens the Pager Properties dialog box (Figure 6-12). Change any of the information you want to change in the text boxes shown, then continue with [Step 4](#) to learn how to choose new or different configuration options.



Figure 6-12. Pager Properties dialog box

4. Click **Priority Level** to specify which types of alert messages your recipient will receive.

In the Priority Level dialog box (see [Figure 6-5 on page 87](#)), drag the slider to the right to send the recipient fewer, but higher priority, messages. Drag the slider to the left to send the recipient more messages, including lower priority messages. Next, click **OK** to save your changes and return to the Pager Properties dialog box.

5. Click **Modem Settings** to configure your modem to send pager messages. In the dialog box that appears (see [Figure 6-13 on page 96](#)), choose the type of modem connected to your server from the **Modem** list, the COM port it uses from the **Port** list, and the rate at which it can transmit data from the **Baud** list. Next, enter in the text boxes provided any dialing prefixes or suffixes the modem must dial to reach outside lines, use particular long-distance carriers, enter personal identification numbers or perform similar tasks.

Choose the dialing method—**Tone** or **Pulse**—that you want the modem to use and select the **Speaker Off** checkbox to have the modem dial and connect silently. Click **OK** to save your settings and return to the Pager Properties dialog box.



Figure 6-13. Modem Properties dialog box

6. Click **Test** to send a test message to the pager number you entered. If your recipient uses an alphanumeric pager, he or she will receive a text message from Alert Manager. If your recipient uses a numeric pager, he or she will see the telephone number or other message you specified in the Pager Properties dialog box.
7. Click **OK** to return to the Alert Manager Properties dialog box.
8. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click **OK**. To close the Alert Manager dialog box without saving changes, click **Cancel**.

Sending alert messages to a NetWare print queue

Alert Manager can send the alert messages that NetShield generates as a print job for your NetWare print server to process. To use this option, you must first set up your printer with NetWare and choose the correct printer driver for your target printer. See your NetWare documentation for details.

To configure Alert Manager to send alert messages to a NetWare print queue, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the Printer tab.

The Printer page (Figure 6-14) appears with a list of all of the NetWare printer queues you have chosen to receive alert messages. If you have not yet chosen a printer queue, this list will be blank.



Figure 6-14. Alert Manager Properties dialog box - Printer page

3. To update this list, you can:
 - **Remove a listed print queue.** Select one of the print queues listed, then click **Remove**.
 - **Add a print queue to the list.** Click **Add** to open the Printer Properties dialog box (see [Figure 6-15 on page 98](#)), then enter in the text box provided the name of the print queue to which you want to send messages. You can enter the NDS or bindery print queue name, or you can click **Browse** to locate the print queue on the network. To choose additional options, continue with [Step 4](#).
 - **Change configuration options.** Select one of the print queues listed, then click **Properties**. Alert Manager opens the Printer Properties dialog box (see [Figure 6-15 on page 98](#)). Change any of the information you want to change in the **Printer** text box, then continue with [Step 4](#) to learn how to choose new or different configuration options.



Figure 6-15. Printer Properties dialog box

4. Click **Priority Level** to specify which types of alert messages the destination printer will receive.

In the Priority Level dialog box (see [Figure 6-5 on page 87](#)), drag the slider to the right to send the destination printer fewer, but higher priority, messages. Drag the slider to the left to send the destination printer more network messages, including lower priority messages. Next, click **OK** to save your changes and return to the Printer Properties dialog box.

5. Click **Test** to send the destination printer a test message. The message will print as a simple, unformatted line of text.
6. Click **OK** to return to the Alert Manager Properties dialog box.
7. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click **OK**. To close the Alert Manager dialog box without saving changes, click **Cancel**.

Sending alert messages via SNMP

Alert Manager can send the alert messages that NetShield generates to other computers via the Simple Network Management Protocol (SNMP). To see the alert messages that NetShield sends, you must have an SNMP management system configured with an SNMP viewer, such as Hewlett-Packard's OpenView. To learn how to set up and configure your SNMP management system, see the documentation for your SNMP viewer software.

To configure NetShield to send alert messages via SNMP, follow these steps:

1. Open the Alert Manager Properties dialog box.
2. Click the SNMP tab.

The SNMP page (Figure 6-16) appears.



Figure 6-16. Alert Manager Properties dialog box - SNMP page

3. Select the **Enable SNMP Traps** checkbox.
4. Click **Priority Level** to specify which types of alert messages your SNMP management computer will receive.

In the Priority Level dialog box (see [Figure 6-5 on page 87](#)), drag the slider to the right to send the SNMP computer fewer, but higher priority, messages. Drag the slider to the left to send the SNMP computer more alert messages, including lower priority messages. Next, click **OK** to save your changes and return to the SNMP dialog box.

5. Click **Test** to send the SNMP computer a test message. To use this option, you must also install and activate SNMP on your NetWare server. See your NetWare documentation for details.
6. Click **OK** to return to the Alert Manager Properties dialog box.
7. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click **OK**. To close the Alert Manager dialog box without saving changes, click **Cancel**.

Launching a program as an alert

Alert Manager can alert you when it finds a virus by starting any program or executing any batch file on your network. For example, if your company uses cc:Mail or a special mail package that NetShield does not support directly, you can write a batch file that will send alert messages to your mail package for delivery.

-
- NOTE:** Any program that Alert Manager starts will run in the background without a visible user interface.
-

To configure NetShield to execute a program when it finds a virus, follow these steps:


1. Open the Alert Manager Properties dialog box.
2. Click the Program tab.

The Program page (Figure 6-17) appears.



Figure 6-17. Alert Manager Properties dialog box - Program page

3. Enter the name and path of the program you want NetShield to run when it finds a virus, or click **Browse** to locate the program file on the network.
4. To have NetShield start the program only when it first finds a particular virus, select the **First Time** button. To start the program each time it finds a virus, select the **Every Time** button.

 **IMPORTANT:** If you select **First Time**, NetShield will start the program you designate the first time it encounters a particular virus. If it finds more than one occurrence of that virus as it scans through the same directory, it will not start the program again. If, however, it finds one occurrence of a virus, then goes on to find a different virus before finding another copy of the first virus, NetShield will start the same program three times in a row. Starting multiple instances of the same program could cause your server to run out of memory.

5. Click **Priority Level** to specify which types of alert events will trigger a program launch.
6. In the Priority Level dialog box (see [Figure 6-5 on page 87](#)), drag the slider to the right to tell NetShield to start the program in response to fewer, but higher priority, alert events. Drag the slider to the left to have NetShield start the program more often, in response to lower priority alert events. Next, click **OK** to save your changes and return to the Program Properties dialog box.
7. To test NetShield's ability to start the program, click **Test**.
8. To configure other notification options, click a different tab. To save your configuration options and close the Alert Manager dialog box, click **OK**. To close the dialog box without saving changes, click **Cancel**.

Using Centralized Alerting

Although NetShield works principally to protect your NetWare server from virus infection, you can also use its Centralized Alerting module to track virus activity elsewhere on your network. Centralized Alerting collects alert messages sent from other Network Associates client-based anti-virus software in an alert folder on your server. To use the feature, you must configure your client software to send alert messages to the alert folder and you must tell NetShield to monitor the folder for activity. Once activated, the Centralized Alerting feature enables NetShield to pick up any alert messages it finds in the alert folder and pass them to Alert Manager for delivery according to your instructions. See “[Configuring Alert Manager](#)” from [pages 83 to 100](#) to learn how to choose your delivery options.

Configuring Centralized Alerting

To activate Centralized Alerting in NetShield, follow these steps:

1. Start the AntiVirus Console, then choose **Alerts** from the **Tools** menu.

The Alert Properties window appears (Figure 6-1 on page 84).

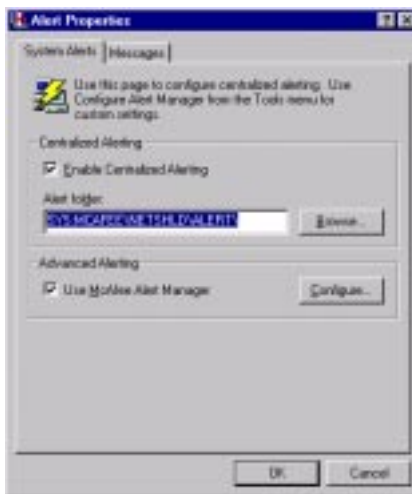


Figure 6-18. Alert Properties dialog box

2. Select **Enable Centralized Alerting**. By default, NetShield comes with this feature enabled.
3. Enter the location of the alert folder you want to use in the text box provided, or click **Browse** to locate a folder elsewhere on your server or on the network. By default, NetShield comes with an alert folder at `\MCAFEES\NETSHLD\ALERT`.

NOTE: To allow other workstations on your network to send messages to this folder, you must give create, write and delete permissions for this folder to all users. See your NetWare documentation for details.

4. Click **OK** to close the Alert Properties dialog box.
5. Configure each workstation that runs Network Associates anti-virus client software to send alert messages to the alert folder you designated. Usually, this requires only that you activate Centralized Alerting in the client software and designate the correct folder on your server. See the *User's Guide* for each client package you have running for details.

Customizing alert messages

NetShield comes with a wide range of alert messages suited to nearly all of the situations you'll encounter when the program finds a virus on your server or elsewhere on your network. The alert messages include a preset priority level and incorporate variables that identify the infected file and system, the infecting virus, and other information that you can use to get a quick but thorough overview of the situation.

You can, however, enable or disable individual alert messages, or change the contents and priority level for any message to suit your own circumstances. NetShield will still activate the alert message in response to specific trigger events, however, so you should try to retain the overall sense of any alert messages you choose to edit.

Enabling and disabling alert messages

Although NetShield can alert you whenever it finds a virus or whenever nearly any aspect of its normal operation changes significantly, you might not want to receive alert messages in each of these circumstances. By default, NetShield comes with all of its alert messages enabled. To prevent NetShield from sending specific alert messages, disable those you do not want to receive in the Alert Properties dialog box.

Follow these steps:

1. Start the AntiVirus Console, then choose **Alerts** from the **Tools** menu.

The Alert Properties window appears (see [Figure 6-18 on page 102](#)). Click the Messages tab to display the correct property page ([Figure 6-19](#)).



Figure 6-19. Alert Properties dialog box - Messages page

2. Review the list of messages shown. Clear the checkbox beside those you do not want NetShield to send to disable them. Select the checkbox beside those messages you do want NetShield to send.
3. Click **OK** to save your changes and close the Alert Properties dialog box. To close the dialog box without saving your changes, click **Cancel**.

Changing priorities for alert messages

Some of the situations NetShield will encounter as it scans your system will require more of your immediate attention than others. Under most circumstances, you would probably rather receive an alert message when NetShield encounters a virus on your server than when your log file reaches capacity. By default, NetShield assigns a priority level to each of its alert messages that reflects the urgency most system administrators would give to them. You can rearrange these priority levels to suit your own needs, and use them to filter the messages you receive from Alert Manager, so that you can concentrate on those most important first.

To change the priority level assigned to an alert message, follow these steps:

1. Start the AntiVirus Console, then choose **Alerts** from the **Tools** menu.

The Alert Properties window appears (see [Figure 6-18 on page 102](#)). Click the Messages tab to display the correct property page (see [Figure 6-19 on page 103](#)).




2. Select one of the alert messages listed, then click **Edit**.

The Configure System Message dialog box appears ([Figure 6-20](#)).



Figure 6-20. Configure System Message dialog box

3. Choose a priority level from the **Priority** list. You can assign each alert message a **High**, **Medium**, or **Low** priority.

The icons shown beside each message tell you the priority level now assigned to it:  indicates a high-priority message,  indicates a medium-priority message, and  indicates a low-priority message.

As you reassign the priority for a message, the icon beside it will change to show its new priority status.


4. Click **OK** to save your changes and close the Configure System Message dialog box.
5. To filter your messages, configure each alert method you have set up in Alert Manager to accept only messages of a certain priority for delivery.

For example, suppose you wanted to have Alert Manager page you whenever NetShield finds a virus on your server, but do not want it to send routine operational messages. To do this, you would assign a high priority to virus alerts, and a medium or low priority to the routine messages. Next, you would tell Alert Manager to send only high priority messages to your pager. You can still have Alert Manager send the other, routine messages via e-mail or other, less urgent means.

To learn how to set priority levels for message delivery in Alert Manager, locate the section earlier in this chapter that describes the alert method you want to change, then read the instructions for the Priority Level dialog box. To learn how to change the priority level for message forwarding, for example, see [Step 4 on page 87](#).

Customizing alert messages

To help you respond to a situation that requires your attention, NetShield includes enough information in its alert messages to identify the source of whatever problem it has found and some information about the circumstances in which it found the problem. You can add information or comments to the alert message that explain more about the problem, list people to contact for a resolution, or help the recipient to understand what to do.

-
-  **IMPORTANT:** Although you can edit the alert message text to say what you want, you should try to keep its essence intact, because NetShield will send each message only when it encounters certain conditions. NetShield will send the “task has started” alert message, for example, only when it actually starts a task.
-

To customize alert message text, follow these steps:

1. Start the AntiVirus Console, then choose **Alerts** from the **Tools** menu.

The Alert Properties window appears (see [Figure 6-18 on page 102](#)). Click the Messages tab to display the correct property page (see [Figure 6-19 on page 103](#)).

2. Select one of the alert messages listed, then click **Edit**.

The Configure System Message dialog box appears (see [Figure 6-20](#) on [page 104](#)).

3. Change or add to the text shown. Text enclosed in percentage signs —%COMPUTERNAME%, for example—represents a variable that NetShield fills with text at the time it generates the alert message.

NetShield uses these variables in alert messages:

- %FILENAME% - NetShield replaces this variable name with a file name. This could include the name of an infected file it found, or the name of a file it tried exclude from a scan operation.
- %TASKNAME% - NetShield replaces this variable name with the name of an active task. NetShield might use this to report the name of the task that found a virus, or the name of a task that reported an error during a scan operation.
- %VIRUSNAME% - NetShield replaces this variable name with the name of an infecting virus.
- %DATE% - NetShield replaces this variable name with the date on which it performed a program operation.
- %TIME% - NetShield replaces this variable name with the time at which it performed a program option.
- %COMPUTERNAME% - NetShield replaces this variable name with the name of a computer as it appears on the network. This could include an infected computer, a computer that reported a device driver error, or any other computer with which NetShield interacted.
- %SOFTWARENAME% - NetShield replaces this variable name with the name of an executable file. This could include the application that detected a virus, an application that reported an error, or any other application with which NetShield interacted.
- %SOFTWAREVERSION% - NetShield replaces this variable name with a version number taken from an active software package. This could include the application that detected a virus, an application that reported an error, or any other application with which NetShield interacted.
- %USERNAME% - NetShield replaces this variable name with the name of the user currently logged into the NetWare server. This can, for instance, tell you if somebody cancelled a scan operation.

4. Click **OK** to save your changes and return to the Alert Properties dialog box, then click **OK** again to return to the AntiVirus Console.

Overview

New viruses appear “in the wild” at a rate of more than 200 a month. If a virus is really new—that is, it doesn’t resemble other viruses or has a very different code signature, older software or data (.DAT) files cannot detect or remove it from your system. The .DAT files that came with your copy of NetShield may not, for example, detect a virus that appeared after you bought the product. Network Associates updates the data files for its anti-virus software each month to keep up with the pace of virus creation and deployment. Network Associates recommends that you update your .DAT files on a regular basis to prevent infection from new viruses.

To update your NetShield .DAT files, download new files from the Network Associates website, then copy them to the program directory for your NetShield installation. See [“Updating NetShield .DAT files” on page 113](#) to learn the procedure. Next, you’ll need to update the NetShield servers on your network. You can distribute your new .DAT files and update the servers on your network automatically with NetShield’s AutoUpdate utility. See [“Configuring AutoUpdate” on page 109](#) to learn how.

Updating Strategies

When you update your .DAT files, you should take into account how you have your networking environment set up. This typically means using the trusted source strategy, the rumor strategy, or a combination of both.

Trusted source strategy

Using the trusted source strategy, each server is configured to accept .DAT file updates only from a trusted server. Simply update the master server and each server checks in for the “official news” ([Figure 7-1](#)).

The command-and-control strategy provides a higher level of security and control over updating. However, this strategy provides less flexibility.

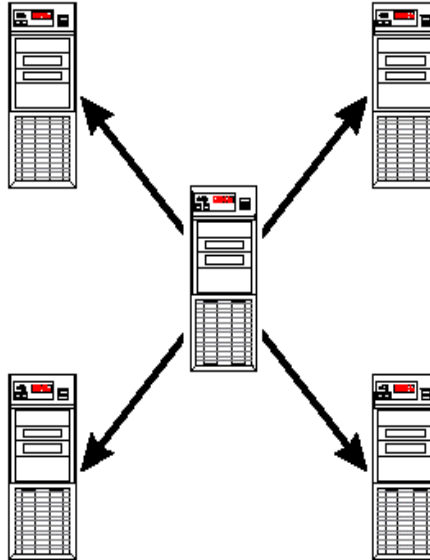


Figure 7-1. Command-and-Control Strategy

Rumor strategy

Using the rumor strategy, all NetWare servers are configured to provide and accept .DAT file updates. Whenever any NetWare server is updated, the updated .DAT files are passed around like a rumor, and all servers configured to accept updates eventually “get the news” (see [Figure 7-2 on page 109](#)).

The rumor strategy results in faster dissemination of updates and system redundancy. However, the rumor strategy offers less control than the trusted source strategy.

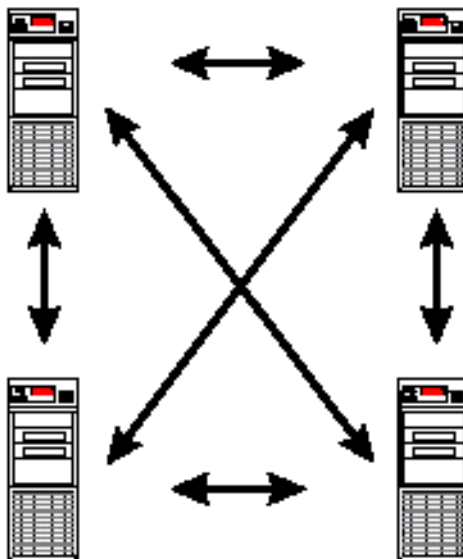


Figure 7-2. Rumor Strategy

Configuring AutoUpdate

To configure AutoUpdate to acquire and install the latest .DAT files on your NetShield servers, follow these steps:

1. Install current .DAT files on the trusted servers. See [“Updating NetShield .DAT files” on page 113](#) for details.
2. Open the NetShield Console, see [“Starting the AntiVirus Console” on page 38](#) for instructions.
3. Choose **AutoUpdate** from the **Tools** menu.

The AutoUpdate Properties dialog box appears (see [Figure 7-3 on page 110](#)).



Figure 7-3. AutoUpdate Properties dialog box

4. To configure this server to provide updates to other servers, select **Provide Updates to Other Servers**.
5. To accept updates from other servers, select **Accept Updates from Other Servers**.
6. To configure this server to only accept updates from a trusted server, select **Only Accept Updates from Trusted Server**. Enter the name of the trusted server or click **Browse** to locate a server.
7. Select **Automatically Load Update** to configure NetShield to automatically load the update when it is received.

OR

Select **Require Manual Confirmation of Reload** to reload the update only when permission is granted by a user.

8. If this server accepts updates, you must schedule when the server makes requests for updates. Click **Schedule** to schedule the server to request an update. See [“Scheduling AutoUpdate” on page 111](#).

OR

If this server only provides updates, click **OK**. AutoUpdate is configured.

Scheduling AutoUpdate

For a server to receive updates, you must schedule it to request them. Scheduling allows you to update .DAT files automatically at any time you choose. You can set AutoUpdate to run one time only, each time NetShield starts, or at hourly, daily, weekly, or monthly intervals.

Use the Schedule property page to enable or disable the scheduler and to specify when updates will occur. To schedule AutoUpdate, follow these steps:

1. Click **Schedule** in the AutoUpdate Properties window.

The Schedule dialog box appears (Figure 7-4).



Figure 7-4. Schedule dialog box

2. Select the **Enable Schedule** checkbox.

NOTE: If you do not enable the schedule, NetShield will not request or receive updates automatically.

3. Determine how often you want the server to request updates. You can choose one of these options:
 - **Once.** Select this option to schedule NetShield to request a one time update. Enter the time and date in the space provided.
 - **Hourly.** Select this option to schedule NetShield to request an update once each hour. Set the request to start x minutes after the hour where x is a number between 0 and 59. For example, to set the request to occur 30 minutes after every hour (8:30, 9:30, 10:30, etc.), select the Hourly option and enter 30 in the minutes field.

- **Weekly.** Select this option to schedule NetShield to request an update once each week. Enter the time and day of the week for the request to start.
- **Monthly.** Select this option to schedule NetShield to request an update once each month. Enter the time and day of the month for the request to start.
- **At Startup.** Select this option have NetShield request an update every time it starts.
- **Daily.** Select this option to schedule NetShield to request an update on specific days. Enter the time for the request to start. Then, click **Which Days** to specify the days you want to request an update.

The Days dialog box appears (Figure 7-5). Choose which days the update request will run.

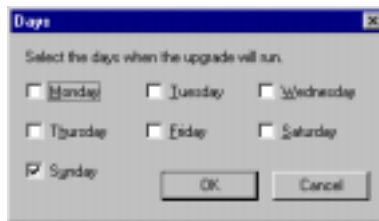


Figure 7-5. Days dialog box

4. Click **OK**.

AutoUpdate will now run on the days and at the times you scheduled.

Updating NetShield .DAT files

To update your NetShield .DAT files, follow these steps:


1. Download the .DAT file (for example, DAT-3107.ZIP) from one of Network Associates' electronic services, see [“How to contact Network Associates” on page xviii](#). On most services, you'll find the .DAT file in the anti-virus area.
2. Copy the file to a new directory.
3. The file is compressed in .ZIP format. Use any decompression utility that can extract files compressed with PKZIP—this can include PKUNZIP, WinZip, or others. You can download the necessary utilities from the Network Associates website or from most online services.
4. Locate the directory on the hard drive where NetShield is currently installed. Typically, the files are stored in \MCAFEE\NETSHLD.
5. Unload the NetShield NLM. See [“Stopping the NetShield server” on page 37](#) for details.
6. Back up the existing .DAT files to a different directory, then copy the new files into the NetShield program directory, overwriting the old .DAT files.

NOTE: Parts of the software might reside in different directories. If so, copy each updated file to the appropriate directory.

7. Reload the NetShield NLM to use the updated .DAT files. See [“Starting the NetShield server” on page 37](#) for more details.

Troubleshooting AutoUpdate

If you have trouble connecting to the server you use to distribute updated files to your network, you can enable NetShield's broadcast discovery feature to locate appropriate servers from which to download new files. By default, NetShield comes with this feature disabled because using it increases traffic on your network. If you cannot locate a server, however, enabling this feature tells NetShield to perform a very thorough search for the machine on the network.

 **IMPORTANT:** In general, you should keep this feature disabled unless you have a lot of difficulty connecting to NetShield servers. Connecting in this manner is slower and less efficient than other methods.

To enable broadcast discovery for AutoUpdate, follow these steps:

1. Start the AntiVirus Console, then log on to the NetShield server you want to administer. See “Using the AntiVirus Console” on page 41 and “Remote Administration” on page 40 to learn how to start the Console and log on to a NetShield server.

The AntiVirus Console task window will appear (see Figure 3-1 on page 38).

2. Choose **Server Options** from the **Tools** menu to open the Server Options dialog box (Figure 7-6).

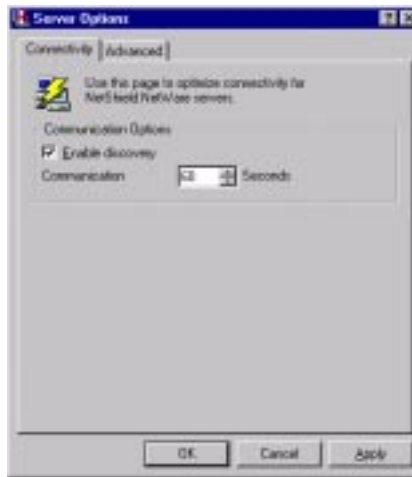


Figure 7-6. Server Options dialog box

3. Select the **Enable Discovery** checkbox.
4. In the **Seconds** text box, enter the time you want NetShield to continue looking for a server on the network before it gives up. By default, NetShield will continue searching for 60 seconds.
5. Click **OK** to save your settings and close the dialog box.

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 6:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday.

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

Support Services for Retail Customers

If you purchased 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 electronic bulletin board system or 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 MCAFEE
- 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.

Index

A

aborting tasks, 42

Actions page

on-access scanning properties, 59 to 60

on-demand scanning properties, 72 to 74

Activity Log

in **Scan** menu, 43

viewing, 43

Add Exclusion Item dialog box, 64, 79

advanced settings for on-demand scanning, 71

Alert Manager

configuring, 42, 83 to 101

E-mail notification, 90

enabling, 43

Forward page, 85 to 87

Network message page, 88 to 90

Pager notification, 93

Print notification, 96

sending alert messages via, 48

SNMP notification, 99

Summary page, 85

alert messages

changing priority of, 104

customizing, 103

editing content of, 43

enabling and disabling, 103

program launch as, 99 to 100

setting priority for, 43

values for variables in, 106

variables in, 106

Alerts

in **Tools** menu, 43

America Online, technical support
via, xviii, 119

AntiVirus Console

changing views of, 43

Event Viewer, opening, 42

last results display, 39

menus, 41

opening the NetShield help file, 43

overview, 41 to 43

shortcut menus in, 41

starting, 38

status bar, 39

toolbar, 41

anti-virus software

reporting new viruses not detected by to
Network Associates, xx

anti-virus software, use of code signatures for
virus detection, xv

archived files, as NetShield distribution
method, 25

assistance, opening the NetShield help
file, 43

authenticating Network Associates files, use
of VALIDATE.EXE for, 33 to 34

AutoUpdate

configuring, 42

in **Tools** menu, 42

task, definition of, 39

B

Basic, as macro virus programming
language, xvi

boot-sector viruses, definition and behavior
of, xiii to xiv

"Brain" virus, xiii

broadcasting network messages, 88 to 90

C

cache, scanning, setting size of, 53

CD-ROM volumes, excluding from on-demand scans, 72

CD-ROM, as NetShield distribution method, 25

Centralized Alerting, activating, 43

Change Password

in **Tools** menu, 43

checking files with VALIDATE.EXE, 33 to 34

cleaning infected files, 49, 60, 74

Client32, required to create NDS object during setup, 32

code signatures, use of by viruses, xv

COMMAND.COM files, virus infections in, xiv

compact installation, components installed, 28

compressed files, disabling scanning for, 46, 70

CompuServe, technical support via, xviii, 119

Concept virus, introduction of, xv to xvi

configuration, scan tasks, 41

Configure Alert Manager in **Tools** menu, 42

configuring

on-access scanning, 55 to 65

on-demand scanning, 67 to 80

connecting to remote NetShield servers, 40 to 41

console

AntiVirus

changing views of, 43

connecting to remote NetShield servers via, 40 to 41

disconnecting from remote NetShield servers, 41

last results display in, 39

menus in, 41

opening the NetShield help file from, 43

opening the Windows NT Event Viewer from, 42

overview of, 41 to 43

shortcut menus in, 41

starting, 38

status bar in, 39

task list in, 38

toolbar in, 41

NetWare

creating an NDS object from, 32

starting the NetShield server from, 37

stopping the NetShield server from, 37

consulting services, 119

contents of log file, 62, 76

context menus in AntiVirus Console, 41

Copy

in **Edit** menu, 41

copying tasks, 41 to 42

costs from virus damage, xi to xii

creating an on-demand task, 67 to 80

CTRL+ALT+DEL, ineffective use of to clear viruses, xiv

custom installation, components installed, 28

Customer Care

contacting, xviii

D

damage from viruses, xi

payloads, xiii

.DAT file updates, reporting new items for, xx

date and time, recorded in log file, 62, 76

default NetShield server password, 40

- default scan targets, [47, 58, 70](#)
 - definition of virus, [xi](#)
 - Delete
 - in **Scan** menu, [42](#)
 - deleting
 - infected files, [49, 60, 74](#)
 - tasks, [42](#)
 - denying access to infected files, [59](#)
 - detection of viruses, use of code signatures for, [xv](#)
 - Detection page
 - advanced settings, [71](#)
 - on-access scanning properties, [57 to 58](#)
 - on-demand scanning properties, [69](#)
 - Disable
 - in **Scan** menu, [42](#)
 - Disconnect Computer
 - in **Tools** menu, [41](#)
 - disconnecting
 - network users from infected volume, [60](#)
 - remote NetShield servers, [41](#)
 - disguising virus infections, [xv](#)
 - disks, floppy, as medium for virus transmission, [xiii to xiv](#)
 - document files, as agents for virus transmission, [xv to xvi](#)
- ## E
- Edit menu
 - Copy**, [41](#)
 - Export**, [43](#)
 - Import**, [43](#)
 - Paste**, [41](#)
 - educational services, description of, [120](#)
 - EICAR "virus," use of to test installation, [35](#)
 - electronic services, contacting for technical support, [119](#)
 - e-mail, addresses for reporting new viruses to Network Associates, [xx](#)
 - e-mail, as agent for virus transmission, [xvi](#)
 - Enable
 - in **Scan** menu, [42](#)
 - encrypted viruses, [xv](#)
 - Event Viewer
 - in **Tools** menu, [42](#)
 - opening from the AntiVirus Console, [42](#)
 - Excel files, as agents for virus transmission, [xvi](#)
 - excluding items
 - from on-access task, [63 to 64](#)
 - from on-demand task, [72, 78 to 80](#)
 - Exclusions page
 - on-access scanning properties, [63 to 65](#)
 - on-demand scanning properties, [79 to 80](#)
 - executable files, as agents for virus transmission, [xiv](#)
 - Export
 - in **Edit** menu, [43](#)
 - exporting tasks, [43](#)
 - extensions, use of to identify scan targets, [47, 58, 70](#)
- ## F
- file cache, setting size of, [53](#)
 - file name extensions, use of to identify vulnerable files, [47, 58, 70](#)
 - file validation, use of VALIDATE.EXE for, [33 to 34](#)
 - file-infector viruses, definition and behavior of, [xiv](#)
 - floppy disks, role in spreading viruses, [xiii to xiv](#)
- ## H
- hardware requirements, NetShield, [25](#)
 - hardware, making best use of, [51](#)

help file, opening from AntiVirus Console, [43](#)

Help menu

Help Topics, [43](#)

Online Virus Info Library, [42](#)

Help Topics

in **Help** menu, [43](#)

hiding

AntiVirus toolbar and status bar, [43](#)

virus infections, [xv](#)

history of viruses, [xi to xvi](#)

I

Import

in **Edit** menu, [43](#)

importing tasks, [43](#)

Inbound Files checkbox, in on-access scan properties, [57, 64](#)

infected files

choosing responses to, [58, 72](#)

cleaning, [49, 60, 74](#)

deleting, [49, 60, 74](#)

recorded in log file, [62, 76](#)

denying access to, [59](#)

detecting

with on-access scanning, [57](#)

with on-demand scanning, [69](#)

disabling user access to, [60](#)

moving, [49, 59, 73](#)

recorded in log file, [62, 76](#)

response recommended when server left unattended, [59](#)

use of .VIR extension to designate, [59 to 60](#)

use of quarantine folder to isolate, [49, 59, 73](#)

initial NetShield server password, [40](#)

installation

connecting to a NetWare server during, [30](#)

creating an NDS object after, [32](#)

steps, [26 to 31](#)

testing effectiveness of, [35](#)

installing NetShield, [25 to 33](#)

Internet

spread of viruses via, [xvi](#)

Internet Relay Chat

as agent for virus transmission, [xvi](#)

L

last results, display in AntiVirus Console, [39](#)

launching tasks, [42](#)

library of virus information, connecting to, [42](#)

limiting log file size, [62, 75](#)

list of tasks in AntiVirus Console, [38](#)

log file

information recorded in, [62, 76](#)

limiting size of, [62, 75](#)

recording NetShield actions in, [61 to 63, 75 to 76](#)

viewing NetShield activity with, [43](#)

LZH files, disabling scanning for, [46, 70](#)

M

macro viruses

Concept virus, [xv to xvi](#)

definition and behavior of, [xv to xvi](#)

malicious software

payload, [xiii](#)

script viruses, [xvi](#)

types

trojan horses, [xiii](#)

worms, [xii](#)

master boot record (MBR), susceptibility to virus infection, [xiv](#)

memory, virus infections in, [xiii](#) to [xiv](#)

menus, in AntiVirus Console, [41](#)

Microsoft NDS client, inability to create NDS object during setup, [32](#)

Microsoft Visual Basic, as macro virus programming language, [xvi](#)

Microsoft Word and Excel files, as agents for virus transmission, [xvi](#)

migrated files, excluding from on-demand scans, [72](#)

minimizing log file size, [62](#), [75](#)

mIRC script virus, [xvi](#)

moving infected files, [49](#), [59](#), [73](#)

multiprocessing, disabling NetShield use of, [53](#) to [54](#)

mutating viruses, definition of, [xv](#)

N

NDS object, creating with NSHINST.NLM, [31](#) to [32](#)

NetShield

- activity log, viewing, [43](#)
- administering remote servers with, [40](#) to [41](#)
- AntiVirus Console
 - starting, [38](#)
 - using, [41](#) to [43](#)
- connecting to remote servers, [40](#) to [41](#)
- disconnecting from remote servers, [41](#)
- distribution
 - via archived files, [25](#)
 - via CD-ROM, [25](#)
- getting started with, [37](#) to [43](#)
- hardware requirements for, [25](#)
- icon in Windows system tray, [55](#)
- installation, [25](#) to [33](#)
 - steps, [26](#) to [31](#)

- introduction to, [23](#)
- multiprocessing, use of, disabling, [53](#) to [54](#)
- on-access scanning, [55](#) to [65](#)
 - Actions page, [59](#) to [60](#)
 - Detection page, [57](#) to [58](#)
 - Exclusions page, [63](#) to [65](#)
 - Properties dialog box, [56](#)
 - Reports page, [61](#) to [63](#)
- on-demand scanning, [67](#) to [80](#)
 - Actions page, [72](#) to [74](#)
 - advanced settings, [71](#)
 - Detection page, [69](#)
 - Exclusions page, [79](#) to [80](#)
 - Reports page, [74](#) to [76](#)
 - Schedule page, [77](#) to [78](#)
 - Task Properties dialog box, [68](#)
- overview of, [37](#) to [43](#)
- Scan wizard
 - starting, [41](#)
 - use of to create tasks, [44](#) to [50](#)
- server
 - changing password for access to, [43](#)
 - default password for, [40](#)
 - performance, adjusting, [51](#) to [54](#)
 - starting, [37](#)
 - administrator or supervisor rights required, [37](#)
 - stopping, [37](#)
- Setup, [25](#) to [33](#)
- system requirements for, [25](#)
- validating with VALIDATE.EXE, [33](#)

NetWare

- console
 - administrator or supervisor rights required for connection to, [37](#)
 - creating an NDS object from, [32](#)
 - starting the NetShield server from, [37](#)

- stopping the NetShield server from, [37](#)
 - server, connecting to during installation, [30](#)
 - version 4.x servers, requirement to use NSHINST.NLM to create NDS object, [32](#)
 - volumes, as sole scan targets, [45, 69](#)
 - Network Associates
 - consulting services from, [119](#)
 - contacting
 - Customer Care, [xviii](#)
 - outside the United States, [xxi](#)
 - via America Online, [xviii](#)
 - via CompuServe, [xviii](#)
 - within the United States, [xix](#)
 - educational services, [120](#)
 - support services, [115](#)
 - training, [xix, 119](#)
 - website address for software updates and upgrades, [118](#)
 - New Task
 - creating, [41](#)
 - in **Scan** menu, [41, 68](#)
 - new viruses, reporting to Network Associates, [xx](#)
 - notification, when virus detected, [48](#)
 - NSHINST.NLM, creating NDS object with, [31](#)
- O**
- Office, Microsoft, files as agents for virus transmission, [xvi](#)
 - on-access scanning
 - excluding files and folders, [63 to 64](#)
 - Inbound Files and Outbound files checkboxes, [57, 64](#)
 - Properties dialog box, [56](#)
 - Actions page, [59 to 60](#)
 - Detection page, [57 to 58](#)
 - Exclusions page, [63 to 65](#)
 - Reports page, [61 to 63](#)
 - on-access task
 - definition of, [38](#)
 - logging activity, [60](#)
 - statistics and scan results, [55 to 56](#)
 - on-demand scanning
 - choosing scan targets, [69](#)
 - disabling compressed file scanning in, [46, 70](#)
 - excluding
 - CD-ROM volumes from, [72](#)
 - files and folders from, [78 to 80](#)
 - migrated files from, [72](#)
 - scheduling scan tasks, [77 to 78](#)
 - setting priority for, [71](#)
 - starting when NetShield starts, [77](#)
 - Task Properties dialog box, [68](#)
 - Actions page, [72 to 74](#)
 - advanced settings, [71](#)
 - Detection page, [69](#)
 - Exclusions page, [79 to 80](#)
 - Reports page, [74 to 76](#)
 - Schedule page, [77 to 78](#)
 - on-demand task
 - creation with Scan wizard, [44 to 50](#)
 - definition of, [39](#)
 - statistics and scan results, [81 to 82](#)
 - online help, opening from the AntiVirus Console, [43](#)
 - Online Virus Info Library
 - connecting to, [42](#)
 - in **Help** menu, [42](#)

Options

in **View** menu, 43

origin of viruses, xi to xvi

Outbound Files checkbox, in on-access scan properties, 57, 64

overview, AntiVirus Console, 41 to 43

P

password

changing for NetShield servers, 43

default for NetShield server, 40

Paste

in **Edit** menu, 41

pausing a scan operation, 51

payload, definition of, xiii

PC viruses, origins of, xiii

performance, adjusting for NetShield server, 51 to 54

PKZIP, disabling scanning for, 46, 70

plain text, use of to transmit viruses, xvi

polymorphic viruses, definition of, xv

pranks, as virus payloads, xiii

PrimeSupport

Anytime, options, 116

at a glance, 117

availability, 118

Basic, options, 115

Extended, options, 116

ordering, 118

priority for scan tasks, setting, 71

Professional Consulting Services

description of, 119

program extensions, designating as scan targets, 47, 58, 70

program launch, as alert message, 99 to 100

Properties

in **Scan**

menu, 41, 56, 58, 61, 63, 72, 75, 77, 79

Properties dialog box

Actions page, 59 to 60

Detection page, 57 to 58

Exclusions page, 63 to 65

Reports page, 61 to 63

Q

quarantine folder, use of to isolate infected files, 49, 59, 73

quitting tasks, 42

R

RAM, virus infections in, xiii to xiv

recording NetShield actions, 61 to 63, 75 to 76

Refresh

in **View** menu, 43

Remote, 40

remote administration, 40 to 41

Remote Connection

in **Tools** menu, 40 to 41

removing tasks, 42

Rename

in **Scan** menu, 43

renaming tasks, 43

reporting viruses not detected to Network Associates, xx

Reports page

on-access scanning properties, 61 to 63

on-demand scanning properties, 74 to 76

restarting with CTRL+ALT+DEL, ineffective use of to clear viruses, xiv

results

on-access task statistics, 55 to 56

on-demand task statistics, 81 to 82

scan operations, 39

retail customers, support features included with purchase, 118

- running tasks, 42
 - at scheduled times, 77 to 78
 - from the Scan wizard, 50
 - immediately, 80 to 81
 - when NetShield starts, 77

S

scan

- operations
 - server required to perform, 37
- results, 39
- targets
 - changing or modifying, 69
 - choosing for on-demand scan, 69
 - deleting, 69

tasks

- configuring, 41
- copying, 41 to 42
- creating, 41
- deleting, 42
- importing, 43
- renaming, 43
- setting priority for, 71
- starting, 42
- stopping, 42

Scan menu

- Activity Log**, 43
- Delete**, 42
- Disable**, 42
- Enable**, 42
- New Task**, 41, 68
- Properties**, 41, 56, 58, 61, 63, 72, 75, 77, 79
- Rename**, 43
- Scan Wizard**, 41, 44
- Start**, 42
- Stop**, 42

Scan Wizard

- in **Scan** menu, 41, 44
- running scan tasks, 50
- starting, 41
- use of to create on-demand task, 44 to 50

scanning

- cache, setting size of, 53
- choosing times and intervals for, 77 to 78
- configuring the on-access scanner for, 55 to 65
- configuring the on-demand scanner for, 67 to 80
- excluding
 - CD-ROM volumes from, 72
 - migrated files from, 72
 - other items from, 63 to 64, 78 to 80
- immediately, 80 to 81
- pausing, 51
- scheduling on-demand scan tasks, 77 to 78
- speeding up scan times, 63 to 64, 72, 78 to 80
- threads, changing numbers of, 51 to 52
- when NetShield loads, 77

Schedule page, 77 to 78

scheduling

- choosing intervals, 77 to 78
- on-demand scanning, 77 to 78

script viruses, xvi

server

- administrator or supervisor rights required for access to, 37
- changing password for access to NetShield, 43
- connecting to NetWare server during installation, 30
- hardware, maximizing use of available resources, 51

- NetShield
 - default password for, 40
 - starting, 37
 - stopping, 37
 - performance, adjusting, 51 to 54
 - response recommended when left unattended, 59
 - Server Options
 - in **Tools** menu, 51 to 54
 - session settings
 - recorded in log file, 62, 76
 - session summary
 - recorded in log file, 62, 76
 - Setup, for NetShield, 25 to 33
 - shortcut menus, in AntiVirus Console, 41
 - shutting down the NetShield server, 37
 - signatures, use of for virus detection, xv
 - skipping
 - CD-ROM volumes in scan tasks, 72
 - migrated files in scan operations, 72
 - scan items, 63 to 64, 78 to 80
 - SNMP, 99
 - software updates and upgrades, website
 - address for obtaining, 118
 - speeding up scan times, 63 to 64, 72, 78 to 80
 - spreadsheet files, virus infections
 - in, xv to xvi
 - Start
 - in **Scan** menu, 42
 - starting
 - AntiVirus Console, 38
 - NetShield server, 37
 - administrator or supervisor rights required for access to, 37
 - tasks, 42
 - statistics, 39
 - on-access task results, 55 to 56
 - on-demand task results, 81 to 82
 - status bar, 39
 - showing and hiding in AntiVirus Console, 43
 - Statusbar
 - in **View** menu, 43
 - stealth viruses, definition of, xv
 - steps, to install NetShield, 26 to 31
 - Stop
 - in **Scan** menu, 42
 - stopping
 - NetShield server, 37
 - scan operations, 51
 - tasks, 42
 - support
 - for retail customers, options, 118
 - hours of availability, 119
 - PrimeSupport
 - Anytime, 116
 - at a glance, 117
 - availability, 118
 - Basic, 115
 - Extended, 116
 - ordering, 118
 - via electronic services, 119
 - symmetric multiprocessing, disabling
 - NetShield use of, 53 to 54
 - system files, as agents for virus transmission, xiv
 - system requirements, NetShield, 25
 - system tray, in Windows taskbar, NetShield icon in, 55
- ## T
- task
 - statistics, 39
 - task list
 - in AntiVirus Console, 38
 - refreshing, 43

- Task Properties dialog box
 - Actions page, 72 to 74
 - advanced settings, 71
 - Detection page, 69
 - Exclusions page, 79 to 80
 - Reports page, 74 to 76
 - Schedule page, 77 to 78
- task, creating with Scan wizard, 44 to 50
- taskbar, location of NetShield icon in system tray, 55
- tasks
 - aborting, 42
 - AutoUpdate, definition of, 39
 - configuring, 41
 - on-access task, 55 to 65
 - on-demand tasks, 67 to 80
 - copying, 41 to 42
 - creating, 41
 - definition of, 38
 - deleting, 42
 - exporting, 43
 - importing, 43
 - making templates for, 41 to 42
 - on-access, definition of, 38
 - on-demand, definition of, 39
 - removing, 42
 - renaming, 43
 - running
 - from the Scan wizard, 50
 - immediately, 80 to 81
 - when NetShield starts, 77
 - scheduled, definition of, 39
 - scheduling, 77 to 78
 - server required to perform, 37
 - starting, 42
 - stopping, 42
 - types available in NetShield, 38
- technical support
 - e-mail address for, xviii
 - hours of availability, 119
 - information needed from user, xix
 - online, xviii
 - PrimeSupport
 - Anytime, 116
 - at a glance, 117
 - availability, 118
 - Basic, 115
 - Extended, 116
 - ordering, 118
 - via electronic services, 119
- technical support, features included with retail purchase, 118
- templates, making from existing tasks, 41 to 42
- testing your installation, 35
- text messages, use of to transmit viruses, xvi
- threads used in scan operations, changing number of, 51 to 52
- Toolbar
 - in **View** menu, 43
- toolbar
 - showing and hiding in AntiVirus Console, 43
- Tools menu
 - Alerts**, 43
 - AutoUpdate**, 42
 - Change Password**, 73
 - Configure Alert Manager**, 42
 - Disconnect Computer**, 41
 - Event Viewer**, 42
 - Remote Connection**, 40 to 41
 - Server Options**, 51 to 54
- Total Education Services
 - description of, 119

Total Service Solutions

contacting, [119](#)

tracking NetShield actions, use of log file for, [61 to 63](#), [75 to 76](#)

training for Network Associates products, [xix](#), [119](#)

scheduling, [xix](#)

trojan horse, definition of, [xiii](#)

typical installation, components installed, [28](#)

U

Universal Naming Convention (UNC), use of for specifying scan targets, [45](#), [69](#)

updates and upgrades, website address for obtaining, [118](#)

user name, recorded in log file, [62](#), [76](#)

V

VALIDATE.EXE, use of to verify Network Associates software, [xvi](#), [33 to 34](#)

View menu

Options, [43](#)

Refresh, [43](#)

Statusbar, [43](#)

Toolbar, [43](#)

.VIR extension

use of with infected files, [59 to 60](#)

Virus Information Library

connecting to, [42](#)

viruses

"Brain" virus, [xiii](#)

alert messages

enabling, [43](#)

when virus detected, [48](#)

boot-sector infectors, [xiii to xiv](#)

cleaning, recorded in log file, [62](#), [76](#)

Concept, [xv to xvi](#)

costs of, [xi to xii](#)

current numbers of, [xi](#)

definition of, [xi](#)

detecting

with on-access scanning, [57](#)

with on-demand scanning, [69](#)

detecting, recorded in log file, [62](#), [76](#)

effects of, [xi](#)

encrypted, definition of, [xv](#)

file infectors, [xiv](#)

history of, [xi to xvi](#)

macro, [xv to xvi](#)

mutating, definition of, [xv](#)

origins of, [xi to xvi](#)

payload, [xiii](#)

polymorphic, definition of, [xv](#)

programs similar to

trojan horses, [xiii](#)

worms, [xii](#)

reporting new strains to Network Associates, [xx](#)

responding to, [58](#), [72](#)

role of PCs in spread of, [xiii](#)

script language, [xvi](#)

spread of via e-mail and Internet, [xvi](#)

stealth, definition of, [xv](#)

use of code signatures by, [xv](#)

why worry?, [xi to xii](#)

viruses, disguising infections of, [xv](#)

Visual Basic, as macro virus programming language, [xvi](#)

.VSC files

locating, [43](#)

saving tasks as, [43](#)

W

warm boot, ineffective use of to clear viruses, [xiv](#)

website, Network Associates technical support via, [119](#)

why worry about viruses?, [xi](#) to [xii](#)

Windows 95 and 98, starting the AntiVirus Console from, [38](#)

Windows NT 3.51 and 4.0, starting the AntiVirus Console from, [38](#)

Windows NT Event Viewer, opening from the AntiVirus Console, [42](#)

Windows, system tray, NetShield icon in, [55](#)

wizard, Scan

 creation of task with, [44](#) to [50](#)

 starting, [41](#)

Word files, as agents for virus transmission, [xvi](#)

worms, definition of, [xii](#)

Z

.ZIP files

 as NetShield distribution method, [25](#)